МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра №34

«УТВЕРЖДАЮ»
Руководитель направления
проф.,д.т.н.,доц.
(должность, уч. степень, звание)
С.В. Беззатеев
(подпись)
«24» июня 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Технологии защиты электронных платежей»
(Название дисциплины)

Код направления	10.05.03
Наименование направления/ специальности	Информационная безопасность автоматизированных систем
Наименование направленности	Обеспечение информационной безопасности распределенных информационных систем
Форма обучения	очная

Санкт-Петербург– 2019 г.

Лист согласования рабочей программы дисциплины

Программу составил(а)

доц.,к.э.н.,доц.	24.06.21	Т.Н. Елина
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Программа одобрена на заседании кафедры № 34
«24» июня 2021 г., протокол № 11

Заведующий кафедрой № 34

проф.,д.т.н.,доц.	«24» июня 2021 г	С.В. Беззатеев
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Ответственный за ОП 10.05.03(07)

доц.,к.т.н.,доц.	24.06.21	В.А. Мыльников
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Заместитель директора института (декана факультета) № 3 по методической работе

доц.,к.э.н.,доц.	24.06.21	Г.С. Армашова-Тельник
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Аннотация

Дисциплина «Технологии защиты электронных платежей» входит в вариативную часть образовательной программы подготовки обучающихся по специальности «10.05.03 «Информационная безопасность автоматизированных систем» направленность «Обеспечение информационной безопасности распределенных информационных систем». Дисциплина реализуется кафедрой №54.

Дисциплина нацелена на формирование у выпускника

общекультурных компетенций:

ОК-2 «способность использовать основы экономических знаний в различных сферах деятельности»;

профессиональных компетенций:

ПК-4 «способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы»,

ПК-13 «способность участвовать в проектировании средств защиты информации автоматизированной системы»,

ПК-19 «способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы»,

ПК-25 «способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении не штатных ситуаций».

Содержание дисциплины охватывает круг вопросов, связанных с применением на практике предлагаемые в настоящее время методы защиты конфиденциальной информации (правовые, организационные, программные и аппаратные) при организации и поддержке электронного бизнеса.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа.

Язык обучения по дисциплине «русский».

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью изучения учебной дисциплины является обеспечение освоения 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.

При изучении дисциплины решается задача получения обучаемыми теоретических знаний и практических навыков в области применения защитных механизмов при организации и ведении электронного бизнеса.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:
ОК-2 «способность использовать основы экономических знаний в различных сферах деятельности»:

знать – необходимые требования информационной безопасности;
уметь – эффективно применять информационно-технологические ресурсы;
владеть навыками – автоматизировать информационно-технологические ресурсы;
иметь опыт деятельности – эффективно применять методы информационной безопасности в автоматизированных системах;

ПК-4 «способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы»:

знать – риски информационной безопасности;
уметь – проводить анализ возможных рисков информационной безопасности;
владеть навыками – обеспечивать безопасность в распределенных ИС;
иметь опыт деятельности – в предотвращении и обеспечении информационной безопасности в ИС;

ПК-13 «способность участвовать в проектировании средств защиты информации автоматизированной системы»:

знать – разработки политики безопасности распределенных ИС;
уметь – разрабатывать политику безопасности распределенных ИС (РИС);
владеть навыками – руководить разработкой политики безопасности распределенных информационных систем (РИС);
иметь опыт деятельности – принимать меры и обеспечивать полную безопасность РИС;

ПК-19 «способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы»:

знать – меры необходимые для защищенности информационно-технологических ресурсов ИС;
уметь – проводить аудит защищенности информационно-технологических ресурсов ИС;
владеть навыками – защиты всех видов информационно-технологических ресурсов ИС;
иметь опыт деятельности – в своевременном аудите информационно-технологических ресурсов ИС;

ПК-25 «способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении не штатных ситуаций»:
знать – криптографические протоколы для передачи и хранения данных в РИС;
уметь – применять криптографические протоколы для передачи и хранения данных в РИС;
владеть навыками – владеть навыками применения криптографическими протоколами в РИС
иметь опыт деятельности – в использовании и применении криптографическими протоколами в РИС.

2. Место дисциплины в структуре ОП

Дисциплина базируется на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Экономика
- Международный бизнес
- Мировая экономика
- Производственная (эксплуатационная) практика
- Технологии защиты от скрытой передачи данных
- Защита от вредоносных программ
- Производственная (конструкторская) практика
- Учебная (ознакомительная) практика
- Учебная практика
- Распределенные сети хранения данных
- Распределенные информационные системы
- Защита информации в распределенных информационных системах
- Устройства и системы беспроводной связи
- Технологии обработки аудио- и видеоданных
- Мультимедиа технологии

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при изучении других дисциплин:

- Научно-исследовательская работа
- Производственная преддипломная практика

3. Объем дисциплины в ЗЕ/академ. час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№9
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	4/ 144	4/ 144

Из них часов практической подготовки	13	13
Аудиторные занятия, всего час., ***В том числе***	34	34
лекции (Л), (час)	17	17
Практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)	54	54
Самостоятельная работа, всего	56	56
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Экз.	Экз.

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 9					
Раздел 1. Электронные платежные системы. Виды электронных систем взаиморасчетов и организация платежей	2		2		8
Раздел 2. Основные модели электронной коммерции	2		2		8
Раздел 3. Угрозы безопасности электронной коммерции и электронных платежей. Безопасность банковских структур. Безопасность в банковская сфере, кредитные карточки.	2		2		10
Раздел 4. Политика информационной безопасности. Построение систем безопасности электронного бизнеса.	2		2		10
Раздел 5. Методы и средства обеспечения информационной безопасности электронного бизнеса	2		2		10
Раздел 6. Корпоративные стандарты обеспечения информационной безопасности систем. Стандарт Центрального банка России по	3		3		10

защите информации					
Раздел 7. Безопасные протоколы взаимодействия с веб-сервисами	4		4		
Итого в семестре:	17		17		56
Итого:	17	0	17	0	56

4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Электронные платежные системы. Виды электронных систем взаиморасчетов и организация платежей
2	Основные понятия и термины электронной коммерции и бизнеса. Понятие электронной коммерции. Краткий обзор основных понятий. Типология электронной коммерции. Структура основных бизнес-моделей электронной коммерции. Основные отличия и особенности моделей.
3	Потенциальные угрозы электронного бизнеса. Основные задачи обеспечения безопасности информации хозяйствующего субъекта при ведении электронного бизнеса. Оценка уязвимости систем электронной коммерции. Анализ и механизмы оценки рисков электронного бизнеса. Построение модели злоумышленника. Классификация преступлений в электронном бизнесе. Классификация и общая характеристика компьютерных преступлений. Анализ и оценка последствий компьютерных преступлений на основе современной статистики.
4	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. Стандарт Центрального банка России по защите информации (СТО БР ИББС-3.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (с изменениями 2014 г.). Основы построения и менеджмента систем безопасности электронного бизнеса. Аудит систем информационной безопасности электронного бизнеса.
5	Основы построения и использования банковских информационных систем. Основные задачи и функции. Обзор банковских информационных систем. Виртуальные банки. Интернет-банкинг. Обеспечение безопасности в банковской сфере. Особенности электронных методов платежа. Цифровая наличность. Электронные платежные системы. Основные принципы внедрения платежных систем в электронную коммерцию.
6	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. Система организационно-распорядительных документов

	организации по вопросам обеспечения безопасности информационных технологий. Регламентация действий всех категорий сотрудников, допущенных к работе с информационными системами
7	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. Способы устранения уязвимостей и противодействия вторжениям нарушителей.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	№ раздела дисциплины
Учебным планом не предусмотрено				

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
	Семестр 9			
1.	Анализ электронных систем взаиморасчетов	1	1	1
2.	Анализ и организация платежей	1	1	1
3.	Построение модели электронной коммерции	1	1	2
4.	Анализ безопасности оформления кредитных карточек	1	1	3
5.	Построение система безопасности электронного перевода	1	1	4
6.	Защита электронных платежей с помощью токенизации	2	1	5
7.	Защита электронных платежей с помощью EMV и P2PE	2	1	5
8.	Основные положения корпоративных стандартов обеспечения информационной безопасности	2	1	6
9.	Основные положения стандарт Центрального банка России по защите информации	2	1	6
10.	Применение безопасные протоколы взаимодействия с веб-сайтами	2	2	7
11.	Применение безопасные протоколы взаимодействия с веб-сервисами	2	2	7
	Всего:	17	13	

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа студентов

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 9, час
1	2	3
Самостоятельная работа, всего	56	56
изучение теоретического материала дисциплины (ТО)	40	40
Отчеты по лаб. работам		
Подготовка к текущему контролю (ТК)	16	16

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы студентов указаны в п.п. 8-10.

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.05В75	Воронов, А. В. Основы защиты информации: учебное пособие/ А. В. Воронов, Н. В. Волошина. - СПб.: ГОУ ВПО "СПбГУАП", 2009. - 78 с.	74
004 Ш 22.	Шаньгин, В. Ф Информационная безопасность [Текст]: научно-популярная литература / В. Ф. Шаньгин. - М.: ДМК Пресс, 2014. - 702 с.: рис. - (Администрирование и защита). - Загл. обл.: Информационная безопасность и защита информации. - Библиогр.: с. 679 - 685 (100 назв.). - Предм. указ.: с. 686 - 701	8
004 Р 69	Романьков, В. А. Введение в криптографию [Текст] : курс лекций / В. А. Романьков. - 2-е изд., испр. и доп. - М. : ФОРУМ, 2015. - 240 с. - Библиогр.: с. 233 - 234 (28 назв.). - Предм. указ.: с. 235 - 239. - ISBN 978-5-91134-573-0 : 431.00 р.	8
004 Р 98	Рябко, Б. Я. Криптографические методы защиты информации [Текст] : учебное пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стер. - М. : Горячая линия - Телеком, 2014. - 229 с. : рис. - (Специальность для	10

	высших учебных заведений). - Библиогр.: с. 218 - 221 (36 назв.). - Предм. указ.: с. 222 - 226.	
http://e.lanbook.com/books/element.php?pl1_id=3032	Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ДМК Пресс, 2012. — 592 с	

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.49(075)Е 60	Емельянова, Н. З. Защита информации в персональном компьютере: учебное пособие / Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. - М.: ФОРУМ, 2009. - 368 с.2.	10
Х Я 47	Яковец, Е. Н. Правовые основы обеспечения информационной безопасности Российской Федерации [Текст] : учебное пособие / Е. Н. Яковец. - М. : Юрлитинформ, 2010. - 336 с.	9
004 М 48	Мельников, В. П. Защита информации [Текст] : учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; ред. В. П. Мельников. - М. : Академия, 2014. - 304с.	5
http://e.lanbook.com/books/element.php?pl1_id=4959	Титов, А.А. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2010. — 195 с.	

7. Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

URL адрес	Наименование
http://www.cyberplat.ru	платежная система CyberPlat, предназначена для авторизации покупателей в Интернет и проверке их платежеспособности
http://www.assist.ru	система карточных платежей в Интернет ASSIST (карты VISA, EuroCard/MasterCard, JCB, Diners Club, American Express) без регистрации их владельцев в системе
http://www.rbc.ru	РосБизнесКонсалтинг. Весь спектр деловой информации. Биржи “on-line”, экономические игры “on-line”
http://www.diasoft.ru	коммерческие банки, сберегательные банки, международные финансовые организации, инвестиционные компании, депозитарии и регистраторы, фонды доверительного

	управления, страховые компании, производственные, бюджетные и торговые предприятия, заказные проекты, анализ финансового состояния банков, консалтинг
http://www.infobez.ru	безопасность информационных систем Портал по безопасности информационных систем
http://www.cyberpol.ru	специализированный научно-информационный сайт "Компьютерная преступность и борьба с нею"

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
1	Windows 7 и выше
2	MS Office 2010 и выше
3	MS Visual Studio 2012 и выше

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
1.	ЗАКОН РФ от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
2.	Закон РФ от 19 февраля 1993г. N 4524-1 "О федеральных органах правительственной связи и информации (с изменениями от 24 декабря 1993 года, по состоянию на 1 апреля 1994 года)"
3.	Закон РФ от 10 июня 1993 года N 5151-1 "О сертификации продуктов и услуг";
4.	Закон РФ от 10 июня 1993 года N 5154-1 "О стандартизации
5.	Закон РФ от 01 июля 1993 г. N 5306-1 "О внесении изменений и дополнений в Закон Российской Федерации "О федеральных органах государственной безопасности"
6.	Закон РФ от 21 июля 1993 года N 5485-1 "О Государственной тайне"; 7. Закон РФ от 20 января 1995 года N 15-ФЗ "О связи";
7.	Закон РФ от 03 апреля 1995г. N 40-ФЗ "Об органах Федеральной службы безопасности в Российской Федерации
8.	Закон РФ от 10 января 2002 года N 1-ФЗ " Об электронной цифровой подписи
9.	Автоматизированные системы. Термины и определения
10.	ГОСТ 34.003.90.
11.	Закон РФ «О государственной тайне» № 182 от 21.09.93. 12. Уголовный кодекс РФ № 63-ФЗ от 13.06.96

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Состав материально-технической базы представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Компьютерный класс	

10. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Экзамен	Список вопросов к экзамену; Задачи.

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ОК-2 «способность использовать основы экономических знаний в различных сферах деятельности»	
1	Экономика
6	Международный бизнес
6	Мировая экономика
9	Защита банковской информации
9	Прикладная экономика
9	Технологии защиты электронных платежей
9	Основы управленческой деятельности
9	Экономика проектов в информационных технологиях
ПК-4 «способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы»	
6	Производственная (эксплуатационная) практика
7	Технологии защиты от скрытой передачи данных
8	Производственная (конструкторская) практика
8	Защита от вредоносных программ
9	Технологии защиты электронных платежей
9	Защита банковской информации
9	Научно-исследовательская работа
9	Научно-исследовательская работа
10	Научно-исследовательская работа
10	Научно-исследовательская работа
10	Производственная преддипломная практика
ПК-13 «способность участвовать в проектировании средств защиты информации автоматизированной системы»	
2	Учебная (ознакомительная) практика
4	Учебная практика
7	Распределенные сети хранения данных
7	Распределенные информационные системы

8	Защита от вредоносных программ
8	Производственная (конструкторская) практика
8	Защита информации в распределенных информационных системах
9	Защита информации в сенсорных сетях
9	Технологии защиты электронных платежей
9	Защита банковской информации
9	Разработка мобильных приложений
10	Производственная преддипломная практика
ПК-19 «способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы»	
2	Учебная (ознакомительная) практика
4	Учебная практика
5	Устройства и системы беспроводной связи
5	Технологии обработки аудио- и видеоданных
5	Мультимедиа технологии
6	Производственная (эксплуатационная) практика
8	Производственная (конструкторская) практика
9	Научно-исследовательская работа
9	Научно-исследовательская работа
9	Технологии защиты электронных платежей
9	Защита банковской информации
10	Научно-исследовательская работа
10	Научно-исследовательская работа
10	Производственная преддипломная практика
ПК-25 «способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении не штатных ситуаций»	
6	Производственная (эксплуатационная) практика
7	Распределенные сети хранения данных
7	Распределенные информационные системы
9	Защита банковской информации
9	Технологии защиты электронных платежей
10	Производственная преддипломная практика

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4-балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	

$85 \le К \le 100$	«отлично» «зачтено»	- обучающийся глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
$70 \le К \le 84$	«хорошо» «зачтено»	- обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
$55 \le К \le 69$	«удовлетво-рительно» «зачтено»	- обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
$К \le 54$	«неудовлетво рительно» «не зачтено»	- обучающийся не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

10.4. Типовые контрольные задания или иные материалы:

1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
2.	Электронные платежные системы. Виды электронных систем взаиморасчетов и организация платежей
3.	Основные понятия и термины электронной коммерции
4.	Структура основных бизнес-моделей электронной коммерции
5.	Платежные системы. Назначение и функции
6.	Виды электронной коммерции. Описание и характеристика
7.	Потенциальные угрозы электронного бизнеса
8.	Оценка уязвимости и рисков электронного бизнеса
9.	Направления обеспечения банковской безопасности. Законодательство в области информационной безопасности
10.	Основные задачи обеспечения безопасности информации фирмы
11.	Классификация преступлений в электронном бизнесе
12.	Оценка последствий компьютерных преступлений (примеры)
13.	Политика информационной безопасности. Основные положения
14.	Программные методы зашиты информации. Перечень и характеристика
15.	Технические методы защиты информации

16.	Безопасность электронной коммерции в Internet
17.	Антивирусная защита
18.	Алгоритм работы антивирусной программы. (сканеры, резиденты и др.)
19.	Виды вирусов и их работы. Аппаратный и программный брандмауэр. Назначение и алгоритм работы
20.	Методы и средства защиты информации при работе с электронной почтой. Безопасность в банковская сфере, кредитные карточки
21.	Электронная цифровая подпись. Назначение и использование. Электронная цифровая подпись – принципы создания ЭЦП. Шифрование как средство защиты информации
22.	Технологии оценки затрат на средства и методы защиты информации. Цели и концепция организации продаж через Интернет товаров или услуг существующего неэлектронного бизнеса
23.	Классификация бизнес-моделей. Основные бизнес-модели взаимодействия с административными и государственными структурами
24.	Назначение и структура B2C. Назначение и структура B2B. Назначение и структура C2C. Назначение и структура C2B. Основные принципы системы государственного регулирования интернет-экономики
25.	Основные вопросы государственного регулирования в сфере интернет - экономики . Задачи электронного правительства
26.	Основные приоритеты деятельности государственных служб, связанных с закупками и платежами . Примеры Интернет- магазинов и их характеристики
27.	Электронные банковские системы для крупных, средних и небольших банков
28.	Удалѐнные платежи при помощи банковских карт. 38. Концепция безопасности банковских структур
29.	Объекты защиты в банковских структурах. 40. Основные составляющие банковской структуры
30.	Аудит систем ингформационной безопасности. Этапы и нормативные документы
31.	Защита электронной цифровой интеллектуальной собственности.
32.	Понятие хеш-функции и свойства
33.	Пластиковые карты и цифровая наличность
34.	Безопасность платежей в сети Интернет с использованием пластиковых кар
35.	Организационно-правовые вопросы защиты информации
36.	Основные угрозы информационной безопасности и технические методы защиты.
37.	Утечка по побочным каналам. Защита информации в электронных платѐжных системах.
38.	Электронная цифровая подпись. Назначение и использование
39.	Шифрование как средство защиты информации. Технологии оценки затрат на средства и методы защиты информации.

40. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Учебным планом не предусмотрено

41. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

№ п/п	Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации при тестировании (таблица 19)

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов

Контрольные и практические задачи / задания по дисциплине (таблица 20)

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
1.	Анализ электронных систем взаиморасчетов
2.	Анализ и организация платежей
3.	Построение модели электронной коммерции
4.	Анализ безопасности оформления кредитных карточек
5.	Построение система безопасности электронного перевода
6.	Защита электронных платежей с помощью токенизации
7.	Защита электронных платежей с помощью EMV и P2PE
8.	Основные положения корпоративных стандартов обеспечения информационной безопасности
9.	Основные положения стандарт Центрального банка России по защите информации
10.	Применение безопасные протоколы взаимодействия с веб-сайтами
11.	Применение безопасные протоколы взаимодействия с веб-сервисами

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

11. Методические указания для обучающихся по освоению дисциплины

Целью дисциплины является – получение студентами необходимых знаний, умений и навыков в области связанной с применением на практике и предлагаемые в настоящее время методы защиты конфиденциальной информации (правовые, организационные, программные и аппаратные) при организации и поддержке электронного бизнеса.

Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемы результаты при освоении обучающимся лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научится методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

- Изложение лекционного материала;
- Представление теоретического материала преподавателем в виде слайдов;
- Освоение теоретического материала по практическим вопросам;
- Список вопросов по теме для самостоятельной работы студента (Табл.21).

Методические указания для обучающихся по прохождению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

– получение новой информации по изучаемой дисциплине;

– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ (ЛР)

- В задании должно быть четко сформулирована задача, выполняемая в ЛР;
- Описаны входные и выходные данные для проведения ЛР;
- ЛР должна выполняться на основе полученных теоретических знаниях;
- Выполнение ЛР должно осуществляться на основе методических указаний, предоставляемых преподавателем;
- ЛР должна выполняться в специализированном компьютерном классе и может быть доработана студентом в домашних условиях, если позволяет ПО;
- Итогом выполненной ЛР является отчет.

Структура и форма отчета о лабораторной работе

- Постановка задачи;
- Входные и выходные данные;
- Содержание этапов выполнения;
- Обоснование полученного результата (вывод);
- Список используемой литературы.

Требования к оформлению отчета о лабораторной работе

- Лабораторная работа (ЛР) предоставляется в печатном/или электронном виде;
- ЛР должна соответствовать структуре и форме отчета представленной выше;
- ЛР должна иметь титульный лист (ГОСТ 7.32-2001 издания 2008 года) с названием и подписью студента(ов), который(ые) ее сделал(и) и оформил(и);
- Студент должен защитить ЛР. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя.

Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- список литературы, предоставленный преподавателем.

Примерный перечень тем для самостоятельного освоения представлен в таблице 21.

Таблица 21 –Примерный перечень тем для самостоятельного изучения

№ п/п	Тема
1.	Субъекты информационных отношений, их интересы и безопасность, пути нанесения им ущерба. Основные термины и определения.
2.	Основные источники и пути реализации угроз. Модели нарушителей.
3.	Состав и организационная структура системы обеспечения информационной безопасности
4.	Основные защитные механизмы.
5.	Российские, зарубежные (британский BS7799 - ISO 17799 и германский BSI) и международные стандарты и критерии защищенности систем (ISO15408-99)
6.	Средства выявления уязвимостей узлов сетей и средства обнаружения атак на узлы, протоколы и сетевые службы.

Методические указания для обучающихся по прохождению промежуточной аттестации

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

- экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой