

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

Кафедра № 33

УТВЕРЖДАЮ

Руководитель направления

проф., д.т.н., доц.

(должность, уч. степень, звание)

С.В. Беззатеев

(инициалы, фамилия)



(подпись)

«25» мая 2023 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Технологии защиты электронных платежей»  
(Наименование дисциплины)

Код направления подготовки/ специальности	10.05.05
Наименование направления подготовки/ специальности	Безопасность информационных технологий в правоохранительной сфере
Наименование направленности	Организация и технологии защиты информации (в информационных системах)
Форма обучения	очная

Санкт-Петербург– 2023



## Аннотация

Дисциплина «Технологии защиты электронных платежей» входит в образовательную программу высшего образования – программу специалитета по направлению подготовки/ специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» направленности «Организация и технологии защиты информации (в информационных системах)». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-1 «Способен принимать участие в создании системы защиты информации на объекте информатизации»

ПК-4 «Способен организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации»

ПК-5 «Способен осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации»

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. Дисциплина входит в состав части, формируемой участниками образовательных отношений, образовательной программы высшего образования (далее – ОП ВО).

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

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Профессиональные компетенции	ПК-1 Способен принимать участие в создании системы защиты информации на объекте информатизации	ПК-1.3.1 знать средства разработки систем защиты информации объектов информатизации; требования нормативных документов и стандартов в области информационной безопасности ПК-1.У.1 уметь проектировать, разрабатывать, внедрять и эксплуатировать системы защиты информации ПК-1.В.1 владеть навыками поддержания требуемого уровня информационной безопасности объекта информатизации
Профессиональные компетенции	ПК-4 Способен организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации	ПК-4.3.1 знать понятие и содержание политики информационной безопасности, показатели качества и эффективности системы безопасности предприятия ПК-4.У.1 уметь выделять объекты защиты и строить концепцию информационной безопасности, регулировать меры по обеспечению информационной безопасности ПК-4.В.1 владеть навыками разработки положений, регламентов и процессов взаимодействия структурных элементов объекта информатизации
Профессиональные компетенции	ПК-5 Способен осуществлять администрирование подсистем	ПК-5.3.1 знать методы и инструментальные средства администрирования и контроля подсистем обеспечения информационной безопасности объекта информатизации

	обеспечения информационной безопасности объекта информатизации	ПК-5.У.1 уметь осуществлять мониторинг и периодический контроль функционирования средств и подсистем обеспечения информационной безопасности объекта информатизации ПК-5.В.1 владеть навыками использования инструментальных средств мониторинга и анализа состояния системы информационной безопасности
--	--	---

## 2. Место дисциплины в структуре ОП

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

- Экономика
- Производственная (эксплуатационная) практика
- Учебная (ознакомительная) практика
- Учебная практика
- 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 и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№8
1	2	3
<b>Общая трудоемкость дисциплины, ЗЕ/ (час)</b>	4/ 144	4/ 144
<b>Из них часов практической подготовки</b>	17	17
<b>Аудиторные занятия, всего час.</b>	34	34
в том числе:		
лекции (Л), (час)	17	17
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	36	36
<b>Самостоятельная работа, всего (час)</b>	74	74
<b>Вид промежуточной аттестации:</b> зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Экз.	Экз.

Примечание: \*\* кандидатский экзамен

#### 4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий. Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 8					
Раздел 1. Электронные платежные системы. Виды электронных систем взаиморасчетов и организация платежей	2		2		10
Раздел 2. Основные модели электронной коммерции	2		2		10
Раздел 3. Угрозы безопасности электронной коммерции и электронных платежей. Безопасность банковских структур. Безопасность в банковской 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 защите информации	3		3		10
Раздел 7. Безопасные протоколы взаимодействия с веб-сервисами	4		4		14
Итого в семестре:	17		17		74
Итого	17	0	17	0	74

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

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

	<p>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.</p>
4	<p>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.</p>
5	<p>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.</p>
6	<p>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</p>
7	<p>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.</p>

#### 4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено					
Всего					

#### 4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – 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	2	5
7.	Защита электронных платежей с помощью EMV и P2PE	2	2	5
8.	Основные положения корпоративных стандартов обеспечения информационной безопасности	2	2	6
9.	Основные положения стандарт Центрального банка России по защите информации	2	2	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	17	

4.5. Курсовое проектирование/ выполнение курсовой работы Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся  
Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 8, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	50	50
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		



Подготовка к текущему контролю успеваемости (ТКУ)	14	14
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	10	10
Всего:	74	74

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

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 7-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.05B75	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 P 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 P 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 высших учебных заведений). - Библиогр.: с. 218 - 221 (36 назв.). - Предм. указ.: с. 222 - 226.	10
<a href="http://e.lanbook.com/books/element.php?pl1_id=3032">http://e.lanbook.com/books/element.php?pl1_id=3032</a>	Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ДМК Пресс, 2012. — 592 с	

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
<a href="http://e.lanbook.com/books/element.php?pl1_id=4959">http://e.lanbook.com/books/element.php?pl1_id=4959</a>	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 электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
<a href="http://www.cyberplat.ru">http://www.cyberplat.ru</a>	платежная система CyberPlat, предназначена для авторизации покупателей в Интернет и проверке их платежеспособности
<a href="http://www.assist.ru">http://www.assist.ru</a>	система карточных платежей в Интернет ASSIST (карты VISA, EuroCard/MasterCard, JCB, Diners Club, American Express) без регистрации их владельцев в системе
<a href="http://www.rbc.ru">http://www.rbc.ru</a>	РосБизнесКонсалтинг. Весь спектр деловой информации. Биржи “on-line”, экономические игры “on-line”
<a href="http://www.diasoft.ru">http://www.diasoft.ru</a>	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
<a href="http://www.infobez.ru">http://www.infobez.ru</a>	безопасность информационных систем Портал по безопасности информационных систем
<a href="http://www.cyberpol.ru">http://www.cyberpol.ru</a>	специализированный научно-информационный сайт "Компьютерная преступность и борьба с нею"

#### 8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
-------	--------------

	Не предусмотрено
--	------------------

8.2. Перечень информационно-справочных систем, используемых при осуществлении образовательного процесса по дисциплине  
Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

## 9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, 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. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Экзамен	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
«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.

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
«хорошо» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы;</li> <li>– не допускает существенных неточностей;</li> <li>– увязывает усвоенные знания с практической деятельностью направления;</li> <li>– аргументирует научные положения;</li> <li>– делает выводы и обобщения;</li> <li>– владеет системой специализированных понятий.</li> </ul>
«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;</li> <li>– допускает несущественные ошибки и неточности;</li> <li>– испытывает затруднения в практическом применении знаний направления;</li> <li>– слабо аргументирует научные положения;</li> <li>– затрудняется в формулировании выводов и обобщений;</li> <li>– частично владеет системой специализированных понятий.</li> </ul>
«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> <li>– обучающийся не усвоил значительной части программного материала;</li> <li>– допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;</li> <li>– испытывает трудности в практическом применении знаний;</li> <li>– не может аргументировать научные положения;</li> <li>– не формулирует выводов и обобщений.</li> </ul>

### 10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
1	<p>Электронные платежные системы. Виды электронных систем взаиморасчетов и организация платежей</p> <p>Основные понятия и термины электронной коммерции</p> <p>Структура основных бизнес-моделей электронной коммерции</p> <p>Платежные системы. Назначение и функции</p> <p>Виды электронной коммерции. Описание и характеристика</p> <p>Потенциальные угрозы электронного бизнеса</p> <p>Оценка уязвимости и рисков электронного бизнеса</p> <p>Направления обеспечения банковской безопасности.</p> <p>Законодательство в области информационной безопасности</p> <p>Основные задачи обеспечения безопасности информации фирмы</p> <p>Классификация преступлений в электронном бизнесе</p>	ПК-1.3.1
2	<p>Оценка последствий компьютерных преступлений (примеры)</p> <p>Политика информационной безопасности. Основные положения</p> <p>Программные методы защиты информации. Перечень и</p>	ПК-1.У.1

	характеристика Технические методы защиты информации	
3	Безопасность электронной коммерции в Internet Антивирусная защита Алгоритм работы антивирусной программы. ( сканеры, резидентные и др.)	ПК-1.В.1
4	Виды вирусов и их работы. Аппаратный и программный брандмауэр. Назначение и алгоритм работы Методы и средства защиты информации при работе с электронной почтой. Безопасность в банковской сфере, кредитные карточки Электронная цифровая подпись. Назначение и использование. Электронная цифровая подпись – принципы создания ЭЦП. Шифрование как средство защиты информации	ПК-4.3.1
5	Технологии оценки затрат на средства и методы защиты информации. Цели и концепция организации продаж через Интернет товаров или услуг существующего неэлектронного бизнеса Классификация бизнес-моделей. Основные бизнес-модели взаимодействия с административными и государственными структурами Назначение и структура В2С. Назначение и структура В2В. Назначение и структура С2С. Назначение и структура С2В. Основные принципы системы государственного регулирования интернет-экономики	ПК-4.У.1
6	Основные вопросы государственного регулирования в сфере интернет - экономики . Задачи электронного правительства Основные приоритеты деятельности государственных служб, связанных с закупками и платежами . Примеры Интернет- магазинов и их характеристики Электронные банковские системы для крупных, средних и небольших банков	ПК-4.В.1
7	Понятие хеш-функции и свойства Пластиковые карты и цифровая наличность Безопасность платежей в сети Интернет с использованием пластиковых кар Организационно-правовые вопросы защиты информации Основные угрозы информационной безопасности и технические методы защиты.	ПК-5.3.1
8	Удалённые платежи при помощи банковских карт. 38. Концепция безопасности банковских структур Объекты защиты в банковских структурах. 40. Основные составляющие банковской структуры Аудит систем информационной безопасности. Этапы и нормативные документы Защита электронной цифровой интеллектуальной собственности.	ПК-5.У.1
9	Утечка по побочным каналам. Защита информации в электронных платёжных системах. Электронная цифровая подпись. Назначение и	ПК-5.В.1

	использование Шифрование как средство защиты информации. Технологии оценки затрат на средства и методы защиты информации.	
--	---	--

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
	Учебным планом не предусмотрено	

Перечень тем для курсового проектирования/выполнения курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для курсового проектирования/выполнения курсовой работы

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

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
1.	Анализ электронных систем взаиморасчетов	ПК-1.3.1
2.	Анализ и организация платежей	ПК-1.У.1
3.	Построение модели электронной коммерции	ПК-1.В.1
4.	Анализ безопасности оформления кредитных карточек	ПК-4.3.1
5.	Построение система безопасности электронного перевода	ПК-4.У.1
6.	Защита электронных платежей с помощью токенизации	ПК-4.В.1
7.	Защита электронных платежей с помощью EMV и P2PE	ПК-5.3.1
8.	Основные положения корпоративных стандартов обеспечения информационной безопасности	ПК-5.У.1
9.	Основные положения стандарт Центрального банка России по защите информации	ПК-5.В.1
10.	Применение безопасные протоколы взаимодействия с веб-сайтами	ПК-4.У.1
11.	Применение безопасные протоколы взаимодействия с веб-сервисами	ПК-4.В.1

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

## **1. 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.

#### Планируемые 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;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходиться 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