

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

Кафедра № 84

УТВЕРЖДАЮ

Руководитель образовательной программы

доц., к.п.н.
(должность, уч. степень, звание)

П.М. Алексеева
(инициалы, фамилия)

(подпись)
«20» февраля 2025 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Правовые основы обеспечения информационной безопасности»
(Наименование дисциплины)

Код направления подготовки/ специальности	40.04.01
Наименование направления подготовки/ специальности	Юриспруденция
Наименование направленности	Юрист в области защиты прав и свобод человека
Форма обучения	очная
Год приема	2025

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц., к.ю.н.
(должность, уч. степень, звание) 20.02.2025
(подпись, дата) Е.В. Баданова
(инициалы, фамилия)

Программа одобрена на заседании кафедры № 84

«20» февраля 2025 г, протокол № 8

Заведующий кафедрой № 84

д.ю.н., доц.
(уч. степень, звание) 20.02.2025
(подпись, дата) Е.В. Болотина
(инициалы, фамилия)

Заместитель директора института №8 по методической работе

доц., к.э.н., доц.
(должность, уч. степень, звание) 20.02.2025
(подпись, дата) Л.В. Рудакова
(инициалы, фамилия)

Аннотация

Дисциплина «Правовые основы обеспечения информационной безопасности» входит в образовательную программу высшего образования – программу магистратуры по направлению подготовки/ специальности 40.04.01 «Юриспруденция» направленности «Юрист в области защиты прав и свобод человека». Дисциплина реализуется кафедрой «№84».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-2 «Способность квалифицировано толковать и применять нормативно-правовые акты, давать квалифицированные юридические заключения и консультации в конкретных сферах юридической деятельности»

Содержание дисциплины охватывает круг вопросов, связанных с организационным и правовым обеспечением информационной безопасности при решении задач профессиональной деятельности.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, семинары, самостоятельная работа.

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

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью изучения дисциплины является формирование у обучающихся способности использовать организационное и правовое обеспечение информационной безопасности при решении задач профессиональной деятельности

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-2 Способность квалифицировано толковать и применять нормативно-правовые акты, давать квалифицированные юридические заключения и консультации в конкретных сферах юридической деятельности	ПК-2.3.1 знать актуальные достижения и тенденции современной науки, тенденции и проблемы реализуемой государством правовой политики и действующего законодательства, проблемы применения и толкования норм законодательства с учетом сложившейся судебной практики ПК-2.У.1 уметь применять методику квалифицированного толкования нормативно-правовых актов и реализовывать их в профессиональной деятельности, квалифицированно определять нормативно-правовые акты, подлежащие применению в конкретной юридической деятельности, давать квалифицированные юридические заключения и консультации с учетом правовых позиций, выработанных правоприменительными органами

2. Место дисциплины в структуре ОП

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

- «Правовое регулирование ограничения прав и свобод человека»,
- «Правоохранительные органы в защите прав человека»,
- «Международно-правовые механизмы защиты прав человека»

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

- «Производственная правоприменительная практика»,
- «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
		№2
1	2	3
Общая трудоемкость дисциплины, 3Е/ (час)	3/ 108	3/ 108
Из них часов практической подготовки	17	17
Аудиторные занятия, всего час.	34	34

в том числе:		
лекции (Л), (час)	17	17
практические/семинарские занятия (ПЗ), (час)	17	17
экзамен, (час)	54	54
Самостоятельная работа , всего (час)	20	20
Вид промежуточной аттестации: 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 2					
Раздел 1. Организационное обеспечение защиты информации	8	8			10
Раздел 2. Правовое обеспечение защиты информации	9	9			10
Итого в семестре:	17	17			20
Итого	17	17	0	0	20

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 Организационное обеспечение защиты информации	Лекция 1. Введение. История возникновения органов по защите информации Лекция 2. Основные принципы, условия, подходы и требования к организации системы защиты информации Лекция 3. Отнесение сведений к различным видам конфиденциальной информации. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну Лекция 4. Засекречивание сведений и их носителей. Основания и порядок рассекречивания сведений и их носителей.
2 Правовое обеспечение защиты информации	Лекция 5. Правовая защита конфиденциальной информации Лекция 6. Основы защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу Лекция 7. Допуск предприятий к проведению работ с конфиденциальной информацией Лекция 8. Конфликты в информационной сфере. Информационные правонарушения: понятие, виды, характеристика. Преступления в информационной сфере: понятие, виды, характеристика. Компьютерные преступления. Киберпреступления и методы борьбы с ними. «Информационные войны»: понятие, характеристика, основные методы ведения. Юридический механизм профилактики информационно-правовых конфликтов.

	Лекция 9. Правовая защита интересов личности, общества и государства от недоброкачественной информации. Административно-правовая защита информации с ограниченным доступом
--	--

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
Семестр 2					
1	1. Государственная защита информации	1. Обсуждение вопросов семинара. 2. Комментированный письменный анализ нормативных актов	1	2	1
2	2. Защита персональных данных	1. Обсуждение вопросов 2. Комментированный письменный анализ нормативных актов 3. Решение ситуационных задач.	2	2	1
3	3. Электронная цифровая подпись. Защита прав и законных интересов субъектов информационной сферы	1. Обсуждение вопросов семинара. 2. Комментированный письменный анализ нормативных актов 3. Решение ситуационных задач.	2	2	1
4	4. Основы теории правового обеспечения информационной безопасности	1. Обсуждение вопросов семинара. 2. Комментированный письменный анализ нормативных актов	2	2	1
5	5. Отнесение сведений к конфиденциальной информации. Засекречивание и рассекречивание сведений	1. Обсуждение вопросов семинара. 2. Комментированный письменный анализ нормативных актов 3. Решение ситуационных задач.	2	2	2
6	6. Организация допуска и доступа персонала к конфиденциальной информации	1. Обсуждение вопросов семинара. 2. Комментированный письменный анализ нормативных актов. 3. Решение ситуационных задач.	2	2	2
7	7. Основы защиты информации при осуществлении международного	1. Обсуждение вопросов семинара. 2. Комментированный письменный анализ	2	2	2

	сотрудничества и выезде персонала предприятия за границу	нормативных актов. 3.Решение ситуационных задач.			
8	8.Конфликты в информационной сфере. Юридический механизм профилактики информационно-правовых конфликтов Информационные правонарушения: понятие, виды, характеристика. Преступления в информационной сфере: понятие, виды, характеристика. Компьютерные преступления. Киберпреступления и методы борьбы с ними. «Информационные войны»: понятие, характеристика, основные методы ведения.	1.Обсуждение вопросов семинара. 2.Комментированный письменный анализ нормативных актов. 3.Решение ситуационных задач.	2	2	2
9	9. Правовая защита интересов личности, общества и государства от недоброкачественной информации. Правовая основа защиты объектов информационных отношений от угроз в информационной сфере.	1.Обсуждение вопросов семинара. 2.Комментированный письменный анализ нормативных актов. 3.Решение ситуационных задач.	2	2	2
Всего			17	17	

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
Учебным планом не предусмотрено				
Всего				

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 2, час
----------------------------	------------	----------------

1	2	3
Изучение теоретического материала дисциплины (ТО)	8	8
Подготовка к текущему контролю успеваемости (ТКУ)	4	4
Домашнее задание (ДЗ)	4	4
Подготовка к промежуточной аттестации (ПА)	4	4
Всего:	20	20

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)
https://urait.ru/bcode/498844	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8.	
https://urait.ru/bcode/489946	Информационное право: учебник для вузов / М. А. Федотов [и др.] ; под редакцией М. А. Федотова. — Москва: Издательство Юрайт, 2022. — 497 с. — (Высшее образование). — ISBN 978-5-534-10593-3.	
https://urait.ru/bcode/488594	Бачило, И. Л. Информационное право: учебник для вузов / И. Л. Бачило. — 5-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 419 с. — (Высшее образование). — ISBN 978-5-534-00608-7.	

https://urait.ru/bcode/496338	Информационное право. Практикум: учебное пособие для вузов / Н. Н. Ковалева, Н. А. Жирнова, Ю. М. Тугушева, Е. В. Холодная ; под редакцией Н. Н. Ковалевой. — Москва : Издательство Юрайт, 2022. — 159 с. — (Высшее образование). — ISBN 978-5-534-12442-2.	
---	--	--

<https://urait.ru/bcode/488769>

Информационные технологии в юридической деятельности: учебник для вузов / П. У. Кузнецов [и др.] ; под общей редакцией П. У. Кузнецова. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-02598-9.

<https://urait.ru/bcode/496492>

Корабельников, С. М. Преступления в сфере информационной безопасности: учебное пособие для вузов / С. М. Корабельников. — Москва: Издательство Юрайт, 2022. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0.

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
http://pravo.gov.ru	Государственная система правовой информации. Официальный интернет-портал правовой информации
http://mon.gov.ru/	Сайт Министерства науки и высшего образования РФ
https://digital.gov.ru/ministry	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры)
www.edu.ru	Российский образовательный портал
http://www.garant.ru/	Информационно-правовая система «Гарант»
http://www.consultant.ru/	Информационно-правовая система «Консультант Плюс»
http://www.rg.ru/	Сайт Российской газеты
http://docs.cntd.ru/	Электронный фонд правовой и нормативно-технической документации
http://academic.ru/	Словари и энциклопедии
http://cyberleninka.ru/	Научная электронная библиотека "КиберЛенинка"
http://e.lanbook.com/	ЭБС издательства ЛАНЬ ЭБС "Лань" электронно-библиотечная система издательства "Лань".

http://www.urait.ru	ЭБС – электронная библиотека для ВУЗов, СПО (ссузов, колледжей), библиотек. Учебники, учебная методическая литература по различным дисциплинам. От издательства «Юрайт»
http://znanium.com/	ЭБС ZNANIUM ЭБС "Znaniium" электронно-библиотечная система издательства "ИНФРА-М"
www.scopus.com	Реферативная база данных Scopus на платформе SciVerse® компании Elsevier
http://www.scrf.gov.ru/security/information/	Совет Безопасности Российской Федерации
https://digital.gov.ru/ru/activity/directions/874/	«Информационная безопасность»: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
https://rkn.gov.ru/	Роскомнадзор

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	Учебная аудитория для проведения занятий лекционного типа - укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей)	32-11, 32-13, 33-07
2	Учебная аудитория для проведения занятий семинарского типа -	32-01

		укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации	
3		Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечено доступом в электронную информационно-образовательную среду организации	Читальный зал библиотеки; 21-17-кабинет курсового и дипломного проектирования
4		Аудитория для проведения промежуточной аттестации – укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации	32-15

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»	<ul style="list-style-type: none"> – 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"> – 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.
«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> – 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.
«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> – 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.

10.3. 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.	Понятие и признаки информации. Юридические особенности и свойства информации.	ПК-2.3.1
2.	Особенности формирования информационного общества в РФ.	ПК-2.У.1
3.	Правовая информированность и правовая культура.	ПК-2.3.1
4.	Информационное общество: понятие, стадии становления.	ПК-2.3.1
5.	Государственная информационно-правовая политика.	ПК-2.У.1
6.	Основные права и обязанности участников информационных правоотношений.	ПК-2.3.1
7.	Теории информационного общества.	ПК-2.3.1
8.	Информационная сфера: понятие, признаки, структура.	ПК-2.3.1
9.	Прогресс информационных технологий и необходимость обеспечения информационной безопасности.	ПК-2.3.1
10.	Основные понятия информационной безопасности	ПК-2.3.1
11.	Структура понятия информационная безопасность	ПК-2.3.1
12.	Система защиты информации и ее структура	ПК-2.3.1
13.	Информационные угрозы, их виды и причины возникновения	ПК-2.3.1
14.	Информационные угрозы для государства	ПК-2.3.1
15.	Информационные угрозы для компании	ПК-2.3.1
16.	Информационные угрозы для личности (физического лица)	ПК-2.3.1
17.	Действия и события, нарушающие информационную безопасность.	ПК-2.3.1
18.	Способы воздействия информационных угроз на объекты	ПК-2.У.1
19.	Внешние и внутренние субъекты информационных угроз	ПК-2.3.1
20.	Общая характеристика информационно-правовых норм	ПК-2.3.1
21.	Информационное законодательство	ПК-2.3.1

22.	Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.	ПК-2.3.1
23.	Деятельность международных организаций в сфере информационной безопасности	ПК-2.3.1
24.	Доктрина информационной безопасности РФ.	ПК-2.3.1
25.	Законодательство об информационной безопасности.	ПК-2.3.1
26.	Информационно-правовые конфликты. Понятие, причины возникновения и стадии развития.	ПК-2.3.1
27.	Основные виды информационно-правовых конфликтов.	ПК-2.У.1
28.	Юридический механизм профилактики информационно-правовых конфликтов.	ПК-2.У.1
29.	Информационные правонарушения: понятие, виды, характеристика.	ПК-2.3.1
30.	«Информационные войны»: понятие, характеристика, основные методы ведения.	ПК-2.У.1
31.	Информационно-психологические угрозы. Основные методики манипуляции сознанием.	ПК-2.У.1
32.	Защита детей от информации, причиняющей вред их здоровью и развитию.	ПК-2.У.1
33.	Особенности информационных отношений в сети Интернет.	ПК-2.У.1
34.	Понятие и виды средств массовой информации.	ПК-2.3.1
35.	Правовой статус журналиста. Журналистская этика.	ПК-2.3.1
36.	Правовые основы регулирования рекламной деятельности.	ПК-2.У.1
37.	Особенности правоотношений, возникающих при производстве, передаче и потреблении библиотечной и архивной информации.	ПК-2.У.1
38.	Правовой режим архивов. Хранение, комплектование и учет архивных фондов.	ПК-2.3.1
39.	Организация и взаимодействие библиотек.	ПК-2.3.1
40.	Право на тайну.	ПК-2.3.1
41.	Сведения, составляющие государственную тайну. Засекречивание и рассекречивание информации.	ПК-2.3.1
42.	Особенности правоотношений, возникающих при производстве, передаче и потреблении информации, составляющей государственную тайну.	ПК-2.3.1
43.	Субъекты и объекты информационных правоотношений, составляющих государственную тайну.	ПК-2.3.1
44.	Понятие и правовой режим коммерческой тайны.	ПК-2.3.1
45.	Сведения, составляющие коммерческую тайну.	ПК-2.3.1
46.	Особенности правоотношений, возникающих при производстве, передаче и потреблении информации, составляющей коммерческую тайну.	ПК-2.3.1
47.	Субъекты и объекты информационных правоотношений, составляющих коммерческую тайну.	ПК-2.3.1
48.	Защита прав на коммерческую тайну.	ПК-2.У.1
49.	Служебная тайна. Правовой режим ее охраны.	ПК-2.У.1
50.	Виды профессиональных тайн.	ПК-2.3.1
51.	Персональные данные: понятие и виды.	ПК-2.3.1
52.	Особенности охраны персональных данных.	ПК-2.У.1
53.	Особенности правового регулирования информационных правоотношений при производстве и распространении произведений науки, литературы и искусства.	ПК-2.У.1
54.	Контрафактная продукция и методы борьбы с ее распространением.	ПК-2.У.1
55.	Защита авторских прав.	ПК-2.У.1
56.	Правовое регулирование информационных правоотношений при создании объектов промышленной собственности (изобретение, промышленный образец, полезная модель).	ПК-2.У.1

57.	Компьютерные преступления и их классификация	ПК-2.3.1
58.	Субъекты и причины совершения компьютерных преступлений	ПК-2.3.1
59.	Вредоносные программы, их виды	ПК-2.У.1
60.	Защита от компьютерных вирусов. Популярные антивирусные программы и их классификация	ПК-2.У.1
61.	Электронная почта и ее защита	ПК-2.У.1
62.	Уголовно-правовой контроль над компьютерной преступностью в России	ПК-2.3.1
63.	Методы и средства защиты информации	ПК-2.3.1
64.	Организационно-правовой статус службы безопасности	ПК-2.3.1
65.	«Больные» мобильники и их «лечение».	ПК-2.У.1
66.	Криптографические методы защиты информации	ПК-2.3.1
67.	Аудит ИБ автоматизированных банковских систем	ПК-2.3.1
68.	Информационная безопасность предпринимательской деятельности	ПК-2.3.1
69.	Электронная коммерция и ее защита	ПК-2.3.1
70.	Обеспечение информационной безопасности должностных лиц и представителей деловых кругов	ПК-2.3.1

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.	<p>Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора</p> <p><i>Инструкция: Прочитайте текст и выберите один правильный ответ.</i></p> <p>Предмет информационного права на современном этапе развития законодательства – это ...</p> <p>а) информационные отношения, возникающие в процессе производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления информации</p> <p>б) совокупность результатов труда, воплощенных в информации, информационных ресурсах, информационных технологий, средств</p>	ПК-2.3.1

	<p>итехнологий коммуникации информации по сетям связи</p> <p>в) продукты, производные от информации и деятельность, связанная с ними</p> <p>г) общественные отношения в информационной сфере</p>	
2.	<p>Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора</p> <p><i>Инструкция: Прочитайте текст и выберите один правильный ответ.</i></p> <p>Ответственность за создание вредоносной программы наступает в</p> <p>а) любом случае</p> <p>б) совокупности с ответственностью за ее использование</p> <p>в) случаях, установленных законодательством</p> <p>г) случае наступления вредных последствий</p>	ПК-2.3.1
3.	<p>Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора</p> <p><i>Инструкция: Прочитайте текст, выберите правильные варианты ответа и запишите аргументы, обосновывающие выбор ответов</i></p> <p>Лица, занимающиеся предпринимательской деятельностью, не могут устанавливать режим коммерческой тайны в отношении сведений...</p> <p>а) о размере и составе имущества коммерческих организаций</p> <p>б) об оплате труда работников коммерческих организаций</p> <p>в) об использовании безвозмездного труда граждан в деятельности коммерческой организации</p> <p>г) об использовании новых технологий, позволяющих получить коммерческую выгоду</p>	ПК-2.У.1
4.	<p>Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора</p> <p><i>Инструкция: Прочитайте текст, выберите правильные варианты ответа и запишите аргументы, обосновывающие выбор ответов</i></p> <p>Основные объекты обеспечения информационной безопасности России</p> <p>а) помещения, предназначенные для ведения закрытых переговоров</p> <p>б) информационные ресурсы, содержащие сведения, которые относятся к государственной тайне и конфиденциальной информации</p> <p>в) информационные продукты</p> <p>г) квалифицированные кадры в области информационных технологий</p>	ПК-2.У.1
5.	<p>Задания на установление правильной последовательности.</p> <p><i>Инструкция: Прочитайте текст и установите последовательность</i></p> <p>1. Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 года N 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную</p>	ПК-2.У.1

	<p>опасность для жизни и здоровья людей и для окружающей природной среды»</p> <p>2. Федеральный закон РФ «Об информации, информационных технологиях и защите информации»</p> <p>3. Конституция РФ</p> <p>4. Доктрина информационной безопасности</p> <p>5. Указ Президента РФ от 16.08.2004 N 1085 (ред. от 08.11.2023) "Вопросы Федеральной службы по техническому и экспортному контролю"</p>							
6.	<p>Задания на установление правильной последовательности.</p> <p><i>Инструкция: Прочитайте текст и установите последовательность</i></p> <p>Основные этапы развития информационных систем:</p> <p>1. Эпоха ручной обработки информации</p> <p>2. Эпоха облачных технологий</p> <p>3. Электромеханические компьютеры</p> <p>4. Появление Мини-Компьютеров</p> <p>5. Эпоха персональных компьютеров</p> <p>6. Эпоха сетей и интернета</p> <p>7. Эпоха мейнфреймов</p> <p>8. Искусственный интеллект и большие данные</p>	ПК-2.3.1						
7.	<p>Задание на установление соответствия</p> <p><i>Инструкция: Прочитайте текст и установите соответствие</i></p> <p><i>Из предложенных характеристик выберите те, которые по смыслу соответствуют:</i></p> <p><i>К каждой позиции в левом столбце подберите соответствующую позицию в правом столбце:</i></p> <table><tr><td>1.Основными источниками угроз информационной безопасности являются</td><td>А. Перехват данных, хищение данных, изменение архитектуры системы</td></tr><tr><td>2.Основные объекты информационной безопасности</td><td>Б. Компьютерные сети, базы данных</td></tr><tr><td>3. Основными рисками информационной безопасности являются</td><td>В. Потеря, искажение, утечка информации</td></tr></table>	1.Основными источниками угроз информационной безопасности являются	А. Перехват данных, хищение данных, изменение архитектуры системы	2.Основные объекты информационной безопасности	Б. Компьютерные сети, базы данных	3. Основными рисками информационной безопасности являются	В. Потеря, искажение, утечка информации	ПК-2-У.1
1.Основными источниками угроз информационной безопасности являются	А. Перехват данных, хищение данных, изменение архитектуры системы							
2.Основные объекты информационной безопасности	Б. Компьютерные сети, базы данных							
3. Основными рисками информационной безопасности являются	В. Потеря, искажение, утечка информации							
8.	<p>Задание на установление соответствия</p> <p><i>Инструкция: Прочитайте текст и установите соответствие</i></p> <p><i>Из предложенных характеристик выберите те, которые по смыслу соответствуют:</i></p> <p>К каждой позиции в левом столбце подберите соответствующую позицию в правом столбце:</p> <table><tr><td>1. Принципом информационной безопасности является принцип недопущения:</td><td>А. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)</td></tr><tr><td>2. Принципом политики информационной безопасности является принцип:</td><td>Б. Усиления защищенности самого незащищенного звена сети (системы)</td></tr><tr><td>3. Принципом политики информационной</td><td>В. Невозможности миновать защитные средства сети</td></tr></table>	1. Принципом информационной безопасности является принцип недопущения:	А. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)	2. Принципом политики информационной безопасности является принцип:	Б. Усиления защищенности самого незащищенного звена сети (системы)	3. Принципом политики информационной	В. Невозможности миновать защитные средства сети	ПК-2.3.1
1. Принципом информационной безопасности является принцип недопущения:	А. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)							
2. Принципом политики информационной безопасности является принцип:	Б. Усиления защищенности самого незащищенного звена сети (системы)							
3. Принципом политики информационной	В. Невозможности миновать защитные средства сети							

	<div> <div>безопасности является принцип:</div> <div>4. Принципом политики информационной безопасности является принцип:</div> </div>	(системы) Г. Неоправданных ограничений при работе в сети (системе)	
9.	<p>Задание открытого типа с развернутым ответом</p> <p><i>Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ</i></p> <p>Кто несет ответственность за защищенность данных в компьютерной сети: владелец сети, администратор сети или пользователь сети?»?</p>	ПК-2.У.1	
10.	<p>Задание открытого типа с развернутым ответом</p> <p><i>Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ</i></p> <p>Назовите и раскройте виды информационной безопасности</p>	ПК-2.3.1	
11.	<p>Задание повышенной сложности с развернутым ответом</p> <p>Задача</p> <p><i>Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ</i></p> <p>С 21 января по 19 апреля 2023 года профессиональный программист Ершов А. незаконным путем добыл логины и пароли для доступа в сеть Интернет нескольких пользователей, провайдером которых является АО «ЦентрТелеком». Информация о логинах и паролях законных пользователей Интернет является коммерческой тайной АО «ЦентрТелеком». Получить пароли Ершову А. удалось с помощью системного администратора АО «ЦентрТелеком» Петрова Д., пользуясь его доверием. Ершов часто помогал профессиональными советами Петрову Д. и несколько раз оставался один за компьютером Петрова. Ершов А. с помощью добытого кода по ночам заходил в сеть Интернет, а на счета потерпевших списывались денежные суммы за пользование сетью Интернет в указанное время. За указанный период законные пользователи понесли убытки в сумме более 14 000 рублей. Чьи права в данном случае нарушены? Какие права нарушены? Какая ответственность и за какие нарушения возникают?</p>	ПК-2.У.1	
12.	<p>Задание повышенной сложности с развернутым ответом</p> <p>Задача</p> <p><i>Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ</i></p> <p>Программист Комаров М. по собственной инициативе разработал вирусную программу, но не использовал и не распространял данную программу.</p> <p>Правомерны ли действия программиста Комарова М.?</p> <p>Какая ответственность установлена за данное деяние?</p>	ПК-2.3.1	

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.

11. Методические указания для обучающихся по освоению дисциплины

11.1. 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 обучающимися 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, 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:

- Введение. Изложение актуальности, основной идеи, связи данной лекции с предыдущими занятиями, ее основные вопросы;
- В основной части лекции реализуется научное содержание темы, все главные узловые вопросы, проводится вся система доказательств с использованием наиболее целесообразных методических приемов. Каждый учебный вопрос заканчивается краткими выводами, логически подводящими студентов к следующему вопросу лекции;
- Заключительная часть имеет целью обобщать в кратких формулировках основные идеи лекции, логически завершая ее.

11.2. Методические указания для обучающихся по участию в семинарах.

Основной целью для обучающегося является систематизация и обобщение знаний по изучаемой теме, разделу, формирование умения работать с дополнительными источниками информации, сопоставлять и сравнивать точки зрения, конспектировать прочитанное, высказывать свою точку зрения и т.п. В соответствии с ведущей дидактической целью содержанием семинарских занятий являются узловые, наиболее трудные для понимания и

усвоения темы, разделы дисциплины. Спецификой данной формы занятий является совместная работа преподавателя и обучающегося над решением поставленной проблемы, а поиск верного ответа строится на основе чередования индивидуальной и коллективной деятельности.

При подготовке к семинарскому занятию по теме прослушанной лекции необходимо ознакомиться с планом его проведения, с литературой и научными публикациями по теме семинара.

Требования к проведению семинаров

Развернутая беседа - наиболее распространенная форма семинарских занятий. Она предполагает подготовку всех студентов по каждому вопросу плана занятия с единым для всех перечнем рекомендуемой обязательной и дополнительной литературы; выступления студентов (по их желанию или по вызову преподавателя) и их обсуждение; вступление и заключение преподавателя. Развернутая беседа позволяет вовлечь в обсуждение предложенной проблематики наибольшее число студентов, разумеется, при использовании всех средств их активизации: постановки хорошо продуманных, четко сформулированных дополнительных вопросов к выступающему и всей группе, умелой концентрации внимания студентов на сильных и слабых сторонах выступлений студентов, своевременном акцентировании внимания и интереса студентов на новых моментах, вскрывающихся в процессе работы и т.д. Для данного вида работы от студента требуется знания основных положений отраслевых наук, умение оперировать юридическими понятиями и категориями, навык ясного и логического изложения собственных мыслей.

11.3. Методические указания для обучающихся по прохождению практических занятий.

Практическое занятие является одной из основных форм организации учебного процесса, заключающаяся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения умений и навыков, опыта творческой деятельности.

Целью практического занятия для обучающегося является привитие обучающимся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающимся практических занятий:

- закрепление, углубление, расширение и детализация знаний при решении конкретных задач;
- развитие познавательных способностей, самостоятельности мышления, творческой активности;
- овладение новыми методами и методиками изучения конкретной учебной дисциплины;
- выработка способности логического осмысления полученных знаний для выполнения заданий;
- обеспечение рационального сочетания коллективной и индивидуальной форм обучения.

Требования к проведению практических занятий

Решение практических задач по темам раздела призвано закрепить, углубить, расширить и детализировать знания при решении конкретных жизненных ситуаций, выработать способности логического осмысления полученных знаний для выполнения профессиональных задач, обеспечить рациональное сочетание коллективной и индивидуальной форм обучения. Условия задач в письменной форме предоставляются преподавателем. Вопросы к условию задачи могут меняться. От студента при выполнении данного вида работ требуется знание основных положений отраслевого законодательства, текст нормативного источника, умение анализировать, толковать и правильно применять правовые нормы.

11.4. Методические указания для обучающихся по выполнению лабораторных работ *(не предусмотрено учебным планом по данной дисциплине)*.

11.5. Методические указания для обучающихся по прохождению курсового проектирования/выполнения курсовой работы *(не предусмотрено учебным планом по данной дисциплине)*.

11.6. 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.

Существенную часть самостоятельной работы студента представляет собой подготовка докладов к семинарам, которая предполагает проработку материала, его обобщение и изложение. При подготовке доклада необходимо ясно выражать свои мысли, формулировать четкие фразы. Выводы должны быть краткими, но обоснованными.

Доклад может сопровождаться презентациями, которые выполняются с помощью специальных компьютерных программ, например, Microsoft office PowerPoint. Выступление докладчика начинается объявлением темы доклада (сообщения) и завершается собственными выводами по заявленной проблематике.

Темы для самостоятельной работы:

1. Основные виды и функции информации.
2. Основные научные подходы к пониманию сущности и значения информации.
3. Особенности формирования информационного общества в РФ.
4. Теории информационного общества.
5. Понятие информационной сферы и законы ее развития.
6. Международные правовые источники регулирования информационных правоотношений.
7. Структура информационного законодательства.
8. Основные виды информационных правоотношений.
9. Ответственность участников информационных правоотношений.
10. Государственная информационно-правовая политика.
11. Правовая информированность и правовая культура.
12. Основные информационные права и свободы: характеристика.
13. Право на тайну.
14. Понятие и основные причины возникновения информационно-правовых конфликтов.
15. Характеристика и стадии развития информационно-правовых конфликтов.
16. Основные виды информационно-правовых конфликтов.
17. Информационные правонарушения: понятие, виды, характеристика.
18. Преступления в информационной сфере: понятие, виды, характеристика.
19. Уголовно-правовая характеристика шпионажа.
20. Уголовно-правовая характеристика государственной измены.
21. Информационные войны: понятие, характеристика, основные методы ведения.
22. Информационное оружие.
23. Статус журналиста.
24. Общие положения теории информационного управления.
25. Основные методики манипуляции сознанием.
26. Информационная безопасность РФ.
27. Основные угрозы информационной безопасности личности, общества и государства.
28. Доктрина информационной безопасности РФ.

29. Основные методы обеспечения информационной безопасности в РФ.
30. Юридический механизм профилактики информационно-правовых конфликтов.
31. Информационно-психологические угрозы.
32. Особенности правового регулирования распространения массовой информации.
33. Особенности правового регулирования отношений по доступу к государственной тайне.
34. Особенности правового регулирования отношений по защите коммерческой тайны.
35. Особенности правового регулирования отношений по защите личной тайны.
36. Особенности правового регулирования отношений по защите служебной тайны.
37. Особенности правового регулирования отношений по защите врачебной тайны.
38. Особенности правового регулирования отношений по защите банковской тайны.
39. Международно-правовая охрана интеллектуальной собственности.
40. Защита прав патентообладателей.
41. Защита авторских прав.
42. Доменное имя, как средство индивидуализации, участников правоотношений и защита прав на него.

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

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.

11.7. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Текущий контроль успеваемости осуществляется в виде:

- устный опрос на занятиях;
- систематическая проверка выполнения индивидуальных заданий;
- проведение контрольных работ;
- тестирование;
- контроль самостоятельных работ (в письменной или устной формах);
- контроль выполнения индивидуального задания на практику;
- иные виды, определяемые научно-педагогическим работником (далее – НПР).

В случае принятия решения о подведении итогов ТКУ, они могут проводиться:

1) один раз в семестр:

- на 9 (девятой) неделе в осеннем семестре;
- на 32 (тридцать второй) неделе в весеннем семестре.

2) два раза в семестр:

- на 8 (восьмой) и 14 (четырнадцатой) неделях в осеннем семестре;
- на 31 (тридцать первой) и 36 (тридцать шестой) неделях в весеннем семестре.

Ведомости для подведения итогов ТКУ выдаются работниками структурного подразделения старостам учебных групп очной и очно - заочной форм обучения. Старосты обязаны вернуть полностью заполненную ведомость в течение 14 (четырнадцати) дней с момента получения.

При подведении итогов ТКУ в ведомость обучающимся выставляются аттестационные оценки: «аттестован», «не аттестован». Система и возможные критерии оценки знаний, умений, навыков и/или опыта деятельности, характеризующих этапы формирования компетенций.

Критерии оценки уровня успеваемости обучающихся:

«АТТЕСТОВАН»

- обучающийся выполняет все требования НПР при выполнении и сдачи всех видов работ, указанных в РПД;
- обучающийся всесторонне усвоил материал, предусмотренный РПД на момент подведения итогов ТКУ;
- уверенно, логично, последовательно и грамотно излагает материал, предусмотренный РПД на момент подведения итогов ТКУ;
- опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные знания с деятельностью по направлению подготовки (специальности);
- грамотно обосновывает и аргументирует выдвигаемые выводы и идеи по материалу, предусмотренному РПД на момент подведения итогов ТКУ;
- свободно владеет системой специализированных понятий и терминологией, связанных с направлением подготовки (специальностью).

«НЕ АТТЕСТОВАН»

- обучающийся пропустил большую часть занятий и/или не выполняет требования НПР при выполнении и сдаче всех видов работ, указанных в РПД на момент подведения итогов ТКУ;
- обучающийся не усвоил значительной части материала, предусмотренного РПД на момент подведения итогов ТКУ;
- испытывает трудности в практическом применении знаний;
- не может аргументировать научные положения;
- не формулирует и не обосновывает выдвигаемые выводы и обобщения по материалу, предусмотренному РПД, на момент подведения итогов ТКУ;
- не владеет системой специализированных понятий и терминологией, связанных с направлением подготовки (специальностью).

ТКУ обучающихся заочной формы обучения включает в себя, в том числе, выполнение предусмотренных контрольных работ по каждой изучаемой дисциплине (модулю) в семестре.

Контрольные работы выполняются в течение семестра и, до начала экзаменационной сессии, загружаются в ЭИОС ГУАП. Загруженные и оцененные НПР контрольные работы являются необходимым условием для допуска к прохождению промежуточной аттестации по дисциплине (модулю).

1.8. 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».

В соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программы высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП» оценки текущего контроля успеваемости влияют на итоги промежуточной аттестации.

Ответы на тестовые задания

№ п/п	Примерный перечень вопросов для тестов
1.	<p>Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора</p> <p><i>Инструкция: Прочитайте текст и выберите один правильный ответ.</i></p> <p>Предмет информационного права на современном этапе развития законодательства – это ...</p> <p>а) информационные отношения, возникающие в процессе производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления информации</p> <p>б) совокупность результатов труда, воплощенных в информации, информационных ресурсов, информационных технологий, средств и технологий коммуникации информации по сетям связи</p> <p>в) продукты, производные от информации и деятельность, связанная с ними</p> <p>г) общественные отношения в информационной сфере</p> <p>А)</p>
2.	<p>Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора</p> <p><i>Инструкция: Прочитайте текст и выберите один правильный ответ.</i></p> <p>Ответственность за создание вредоносной программы наступает в</p> <p>а) любом случае</p> <p>б) совокупности с ответственностью за ее использование</p> <p>в) случаях, установленных законодательством</p> <p>г) случае наступления вредных последствий</p> <p>А)</p>
3.	<p>Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора</p> <p><i>Инструкция: Прочитайте текст, выберите правильные варианты ответа и запишите аргументы, обосновывающие выбор ответов</i></p> <p>Лица, занимающиеся предпринимательской деятельностью, не могут устанавливать режим коммерческой тайны в отношении сведений...</p> <p>а) о размере и составе имущества коммерческих организаций</p> <p>б) об оплате труда работников коммерческих организаций</p> <p>в) об использовании безвозмездного труда граждан в деятельности коммерческой организации</p> <p>г) об использовании новых технологий, позволяющих получить коммерческую выгоду</p> <p>А), Б), В)</p>
4.	<p>Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора</p> <p><i>Инструкция: Прочитайте текст, выберите правильные варианты ответа и запишите аргументы, обосновывающие выбор ответов</i></p> <p>Основные объекты обеспечения информационной безопасности России</p> <p>а) помещения, предназначенные для ведения закрытых переговоров</p> <p>б) информационные ресурсы, содержащие сведения, которые относятся к государственной тайне и конфиденциальной информации</p> <p>в) информационные продукты</p>

	г) квалифицированные кадры в области информационных технологий Б), В)								
5.	<p>Задания на установление правильной последовательности. <i>Инструкция: Прочитайте текст и установите последовательность</i></p> <ol style="list-style-type: none"> 1. Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 года N 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» 2. Федеральный закон РФ «Об информации, информационных технологиях и защите информации» 3. Конституция РФ 4. Доктрина информационной безопасности 5. Указ Президента РФ от 16.08.2004 N 1085 (ред. от 08.11.2023) "Вопросы Федеральной службы по техническому и экспортному контролю" <p>3, 2, 4, 5, 1</p>								
6.	<p>Задания на установление правильной последовательности. <i>Инструкция: Прочитайте текст и установите последовательность</i></p> <p>Основные этапы развития информационных систем:</p> <ol style="list-style-type: none"> 1. Эпоха ручной обработки информации (до 1940-х годов) 2. Электромеханические компьютеры (1940-е — начало 1950-х годов) 3. Эпоха мейнфреймов (1950-е — 1960-е годы) 4. Появление Мини-Компьютеров (1960-е — 1970-е годы) 5. Эпоха персональных компьютеров (1980-е — 1990-е годы) 6. Эпоха сетей и интернета (1990-е — начало 2000-х годов) 7. Эпоха облачных технологий (2010-е — настоящее время) 8. Искусственный интеллект и большие данные (настоящее время) 								
7.	<p>Задание на установление соответствия <i>Инструкция: Прочитайте текст и установите соответствие</i> Из предложенных характеристик выберите те, которые по смыслу соответствуют:</p> <p>К каждой позиции в левом столбце подберите соответствующую позицию в правом столбце:</p> <table border="1"> <tr> <td>1. Основными источниками угроз информационной безопасности являются</td><td>А. Перехват данных, хищение данных, изменение архитектуры системы</td></tr> <tr> <td>2. Основные объекты информационной безопасности</td><td>Б. Компьютерные сети, базы данных</td></tr> <tr> <td>3. Основными рисками информационной безопасности являются</td><td>В. Потеря, искажение, утечка информации</td></tr> <tr> <td colspan="2">1-А, 2-Б, 3-В</td></tr> </table>	1. Основными источниками угроз информационной безопасности являются	А. Перехват данных, хищение данных, изменение архитектуры системы	2. Основные объекты информационной безопасности	Б. Компьютерные сети, базы данных	3. Основными рисками информационной безопасности являются	В. Потеря, искажение, утечка информации	1-А, 2-Б, 3-В	
1. Основными источниками угроз информационной безопасности являются	А. Перехват данных, хищение данных, изменение архитектуры системы								
2. Основные объекты информационной безопасности	Б. Компьютерные сети, базы данных								
3. Основными рисками информационной безопасности являются	В. Потеря, искажение, утечка информации								
1-А, 2-Б, 3-В									
8.	<p>Задание на установление соответствия <i>Инструкция: Прочитайте текст и установите соответствие</i> Из предложенных характеристик выберите те, которые по смыслу соответствуют:</p>								

	<p>К каждой позиции в левом столбце подберите соответствующую позицию в правом столбце:</p> <table border="1"> <tr> <td>1. Принципом информационной безопасности является принцип недопущения:</td><td>А. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)</td></tr> <tr> <td>2. Принципом политики информационной безопасности является принцип:</td><td>Б. Усиления защищенности самого незащищенного звена сети (системы)</td></tr> <tr> <td>3. Принципом политики информационной безопасности является принцип:</td><td>В. Невозможности миновать защитные средства сети (системы)</td></tr> <tr> <td>4. Принципом политики информационной безопасности является принцип:</td><td>Г. Неоправданных ограничений при работе в сети (системе)</td></tr> </table> <p>1-Г, 2-В, 3-Б, 1-А</p>	1. Принципом информационной безопасности является принцип недопущения:	А. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)	2. Принципом политики информационной безопасности является принцип:	Б. Усиления защищенности самого незащищенного звена сети (системы)	3. Принципом политики информационной безопасности является принцип:	В. Невозможности миновать защитные средства сети (системы)	4. Принципом политики информационной безопасности является принцип:	Г. Неоправданных ограничений при работе в сети (системе)
1. Принципом информационной безопасности является принцип недопущения:	А. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)								
2. Принципом политики информационной безопасности является принцип:	Б. Усиления защищенности самого незащищенного звена сети (системы)								
3. Принципом политики информационной безопасности является принцип:	В. Невозможности миновать защитные средства сети (системы)								
4. Принципом политики информационной безопасности является принцип:	Г. Неоправданных ограничений при работе в сети (системе)								
9.	<p>Задание открытого типа с развернутым ответом</p> <p><i>Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ</i></p> <p>Кто несет ответственность за защищенность данных в компьютерной сети: владелец сети, администратор сети или пользователь сети)?</p> <p>Ответственность за защищенность данных в компьютерной сети несет владелец сети.</p> <p>Согласно ст. 15 ФЗ №149-Ф, «на территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области связи, настоящего Федерального закона и иных нормативных правовых актов Российской Федерации. Регулирование использования информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, осуществляется в Российской Федерации с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области. Порядок использования иных информационно-телекоммуникационных сетей определяется владельцами таких сетей с учетом требований, установленных настоящим Федеральным законом.».</p>								
10.	<p>Задание открытого типа с развернутым ответом</p> <p><i>Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ</i></p> <p>Назовите и раскройте виды информационной безопасности</p> <p>Согласно Указа Президента РФ от 02.07.2021 N 400 "О Стратегии национальной безопасности Российской Федерации", можно выделить информационную безопасность личности (физического лица), общества (корпоративную) и ИБ государства. «Быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз</p>								

	безопасности граждан, общества и государства».
11.	<p>Задание повышенной сложности с развернутым ответом</p> <p>Задача</p> <p><i>Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ</i></p> <p>С 21 января по 19 апреля 2023 года профессиональный программист Ершов А. незаконным путем добыл логины и пароли для доступа в сеть Интернет нескольких пользователей, провайдером которых является АО «ЦентрТелеком». Информация о логинах и паролях законных пользователей Интернет является коммерческой тайной АО «ЦентрТелеком». Получить пароли Ершову А. удалось с помощью системного администратора АО «ЦентрТелеком» Петрова Д., пользуясь его доверием. Ершов часто помогал профессиональными советами Петрову Д. и несколько раз оставался один за компьютером Петрова. Ершов А. с помощью добытого кода по ночам заходил в сеть Интернет, а на счета потерпевших списывались денежные суммы за пользование сетью Интернет в указанное время. За указанный период законные пользователи понесли убытки в сумме более 14 000 рублей. Чьи права в данном случае нарушены? Какие права нарушены? Какая ответственность и за какие нарушения возникают?</p>
12.	<p>Задание повышенной сложности с развернутым ответом</p> <p>Задача</p> <p><i>Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ</i></p> <p>Программист Комаров М. по собственной инициативе разработал вирусную программу, но не использовал и не распространял данную программу. Правомерны ли действия программиста Комарова М.? Какая ответственность установлена за данное деяние?</p>

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