Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Артеменков Михаил Николаевич
Должность: Ректор
Дата подписания: 10.11.2026 11:47:19
Уникальный программный ключ:
a63b74166e8f4fc17bd1e0462725f79e393bfdf9

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Смоленский государственный университет»

Кафедра государственно-правовых дисциплин

«Утверждаю»

Проректор по учебно-
методической работе
_____Устименко Ю.А.
«9» сентября 2022 г.

Рабочая программа дисциплины
Б1.О.12 Государственно-правовые основы информационной безопасности в России

Направление подготовки: 40.04.01 Юриспруденция
Направленность (профиль): Правовое обеспечение государственной и муниципальной службы
Форма обучения – заочная
Курс – 3
Семестр – 5
Всего зачетных единиц – 3; часов – 108 час.

Форма отчетности: зачет – 5 семестр.

Программу разработал:
кандидат педагогических наук, доцент кафедры государственно-правовых дисциплин
СмолГУ, Даниленкова Т.О.

Одобрена на заседании кафедры права
«9» июня 2022 г., протокол № 6

Смоленск
2022

1. Место дисциплины в структуре ОП

Дисциплина Б1.О.12 «Государственно-правовые основы информационной безопасности в России» относится к обязательной части ОП по направлению подготовки 40.04.01 Юриспруденция, направленность (профиль) Правовое обеспечение государственной и муниципальной службы. В рамках данной учебной дисциплины формируется особый понятийный аппарат со своей терминологией и проблемными вопросами, категориями, общими и особенными чертами, характерными для государственно-правовых основ информационной безопасности.

Изучение дисциплины «Государственно-правовые основы информационной безопасности в России» целесообразно после получения студентами знаний по общим правовым дисциплинам. Освоение учебной дисциплины «Государственно-правовые основы информационной безопасности в России» предполагает наличие у студента базовых знаний по таким дисциплинам, как актуальные проблемы права, организация предоставления государственных услуг, и является необходимым условием для адекватного понимания и практического применения остальных дисциплин программ магистратуры, предметом которых являются отдельные отрасли, институты или иные специальные сферы регулирования государственно-правовой специализации.

Знание дисциплины «Государственно-правовые основы информационной безопасности в России» является необходимым условием профессиональной подготовки.

2. Планируемые результаты обучения по дисциплине

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-7. Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	Знает: методы и средства поиска, систематизации и обработки правовой информации; цели, задачи, основные направления осуществления государственной информационной политики в области обеспечения информационной безопасности. Умеет: применять современные информационные технологии для поиска и обработки правовой информации; выявлять основные угрозы информационной безопасности личности, общества и государства. Владеет: навыками работы в правовых информационных системах; навыками сбора и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности
ПК-1. Способен квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности	Знает: концептуальные положения отраслевых и специальных наук, сущность и содержание основных понятий, категорий, институтов, правовых статусов субъектов правоотношений в различных отраслях материального и процессуального права; основные принципы разграничения компетенции органов государственной власти и местного самоуправления в сфере правоприменительной деятельности; историю появления и тенденции развития основных юридических категорий и понятий, их место в различных правовых системах современности; нормативные правовые основы и принципы государственной политики в сфере предоставления государственных услуг; Умеет: квалифицированно определять правовые нормы, подлежащие применению в конкретной сфере юридической деятельности; оперировать юридическими понятиями и

	категориями, раскрывающими природу, структуру и содержание организации предоставления государственных услуг; профессионально уяснять смысл и содержание нормы материального и процессуального права. Владеет: навыками квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности; навыками анализа юридических фактов, правовых отношений, являющихся объектами профессиональной деятельности

3. Содержание дисциплины

Тема 1. Основы информационной политики. Государственная политика в сфере информационной безопасности. Национальные интересы РФ в информационной сфере и их обеспечение. Тенденции развития информационного общества в России и в мире. Определение, сущность и содержание; объекты и субъекты государственной информационной политики. Обеспечение доступа граждан к информации о деятельности федеральных органов исполнительной власти.

Тема 2. Информационная безопасность: понятие, сущность, виды, субъекты. Источники угроз информационной безопасности. Понятие информационной безопасности, основные задачи и методы ее обеспечения. Понятие субъекта информационной безопасности. Виды субъектов информационной безопасности. Угрозы информационной безопасности. Понятие «источник угрозы информационной безопасности» и его виды. Правовое регулирование средств массовой информации.

Тема 3. Нормативно-правовые основы информационной безопасности в РФ. Правовые основы информационной безопасности общества. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Права граждан в информационной сфере. Ответственность за нарушения в сфере информационной безопасности. Особенности предупреждения преступлений в информационной сфере и обеспечения информационной безопасности.

Тема 4. Состояние информационной безопасности Российской Федерации. Комплекс мер, реализованный в Российской Федерации, по совершенствованию обеспечения ее информационной безопасности. Влияние современных условий политического и социально-экономического развития страны на обеспечение информационной безопасности. Основные задачи по обеспечению информационной безопасности. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности.

4. Тематический план

№ п/п	Наименование темы	Всего часов	Количество часов		
			лекции	практические занятия	самостоятельная работа
1	Основы информационной политики	26	1	2	23
2	Информационная безопасность:	26	1	2	23

	понятие, сущность, виды, субъекты. Источники угроз информационной безопасности				
3	Нормативно-правовые основы информационной безопасности в РФ	26	1	2	23
4	Состояние информационной безопасности Российской Федерации	26	1	2	23
5	Подготовка к зачету	4			4
	Всего	**108**	**4**	**8**	**96**

5. Виды образовательной деятельности

Лекции

Тема 1. Основы информационной политики

Государственная политика в сфере информационной безопасности.

Национальные интересы РФ в информационной сфере и их обеспечение.

Тенденции развития информационного общества в России и в мире.

Определение, сущность и содержание; объекты и субъекты государственной информационной политики.

Обеспечение доступа граждан к информации о деятельности федеральных органов исполнительной власти.

Тема 2. Информационная безопасность: понятие, сущность, виды, субъекты. Источники угроз информационной безопасности

Понятие информационной безопасности, основные задачи и методы ее обеспечения.

Понятие субъекта информационной безопасности. Виды субъектов информационной безопасности.

Угрозы информационной безопасности. Понятие «источник угрозы информационной безопасности» и его виды.

Правовое регулирование средств массовой информации.

Тема 3. Нормативно-правовые основы информационной безопасности в РФ

Правовые основы информационной безопасности общества.

Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации.

Права граждан в информационной сфере.

Ответственность за нарушения в сфере информационной безопасности.

Особенности предупреждения преступлений в информационной сфере и обеспечения информационной безопасности.

Тема 4. Состояние информационной безопасности Российской Федерации

Комплекс мер, реализованный в Российской Федерации, по совершенствованию обеспечения ее информационной безопасности.

Влияние современных условий политического и социально-экономического развития страны на обеспечение информационной безопасности.

Основные задачи по обеспечению информационной безопасности.

Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности.

Практические занятия

Тема 1. ***Основы информационной политики***

План изучения темы

1. Информационная политика как часть государственного управления.
2. Система и механизмы реализации информационного обеспечения государственной политики.
3. Конституция РФ о правах и свободах в сфере информации.

Самостоятельная работа:

1. Информационная безопасность и ее место в системе национальной безопасности Российской Федерации.
2. Политика и модели безопасности.

Самостоятельная работа выполняется в форме эссе.

Тема 2. ***Информационная безопасность: понятие, сущность, виды, субъекты. Источники угроз информационной безопасности***

План изучения темы

1. Информационная безопасность.
2. Информация как объект защиты.
3. Виды субъектов информационной безопасности Российская Федерация как субъект информационной безопасности. Субъекты РФ и муниципальные образования. Граждане и другие физические лица как субъекты информационной безопасности. Правовой статус общественных объединений и коммерческих организаций как субъектов информационной безопасности.
4. Угрозы информационной безопасности. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз.

Самостоятельная работа

1. Выявить угрозы информационной безопасности в предлагаемой ситуации (общение в социальной сети, передача логина пароля специалисту обслуживающей организации).
2. Оценить действия сотрудника предприятия, приведшие к инциденту, СВЯЗАННОМУ С УГРОЗОЙ информационной безопасности (в предлагаемой ситуации).
3. Проектирование модели угроз путем сопоставления угроз и методов их парирования (в предлагаемой ситуации).

Тема 3. ***Нормативно-правовые основы информационной безопасности в РФ***

План изучения темы

1. Основополагающие документы по информационной безопасности.
2. Понятие государственной тайны.
3. Средства защиты государственной тайны.
4. Основные задачи информационной безопасности.
5. Особенности предупреждения преступлений в информационной сфере и обеспечения информационной безопасности.
6. Преступность в информационной сфере.

Самостоятельная работа

1. Выделить нормативно-правовые акты, регулирующие циркулирование информации в организации (из списка организаций).
2. Выявить категории персональных данных и порядок обращения с ними в ситуации обращения за услугой в организацию (из списка ситуаций).
3. Выделить нормативно-правовые акты, закрепляющие недопустимость сокрытия или ограничения доступа к информации (из списка организаций).

Тема 4. ***Состояние информационной безопасности Российской Федерации***

План изучения темы

1. Анализ и характеристика наиболее перспективных направлений развития в области информационной безопасности.
2. Основные направления международного сотрудничества в области обеспечения информационной безопасности.
3. Проблемы взаимодействия Российской Федерации иными с государствами в области обеспечения информационной безопасности.

Самостоятельная работа

1. Составить краткий конспект по вопросу: Основные направления международного сотрудничества в области обеспечения информационной безопасности.
2. Составить краткий конспект по вопросу: Информационные войны и информационное противоборство.

6. Критерии оценивания результатов освоения дисциплины

6.1. Оценочные средства и критерии оценивания для текущей аттестации

Критерии оценки работы на практическом занятии

«отлично» – ответ на вопрос практического задания дан правильный. Объяснение хода его решения подробное, последовательное, грамотное, с теоретическими обоснованиями;

«хорошо» – ответ на вопрос практического задания дан правильный. Объяснение хода его решения подробное, но недостаточно логичное, с единичными ошибками в деталях, некоторыми затруднениями в теоретическом обосновании;

«удовлетворительно» – ответ на вопрос практического задания дан правильный. Объяснение хода его решения недостаточно полное, непоследовательное, с ошибками, слабым теоретическим обоснованием;

«неудовлетворительно» – ответ на вопрос практического задания дан неправильный. Объяснение хода его решения дано неполное, непоследовательное, с грубыми ошибками, без теоретического обоснования.

Требования к эссе

1. Текст должен отражать позицию автора по какому-либо актуальному вопросу (проблеме). Автор должен высказать свою точку зрения и сформировать непротиворечивую систему аргументов, обосновывающих предпочтительность выбранной позиции.
2. В тексте должно быть продемонстрировано владение предметом исследования, его понятийным аппаратом, терминологией, знание общепринятых научных концепций в

заданной предметной области, понимание современных тенденций и проблем в исследовании предмета.

3. Текст должен быть завершенным и четко структурированным, посвященным строго заданной выбранной темой проблематике.

4. Стилевое решение, структурная организация текста, лексика должны соответствовать заданной тематике и поставленной автором задаче.

5. Структура эссе: введение (в нем даётся краткая характеристика проблемной области по выбранной теме), основная (в ней раскрывается тема), заключение (в нем отражаются выводы по теме исследования, предложения о дальнейших работах в данной области и т.п.), список использованных ссылок и литературы (не менее 3).

6. Объем – не более 12000 знаков, шрифт Times New Roman прямого начертания, кегль (размер) шрифта 14, междустрочный интервал – полуторный.

Критерии оценивания эссе

Критерии	Максимальный балл
1. Уровень владения языком написания эссе (четкость и лаконичность изложения мыслей)	5
2. Владение предметом исследования, его понятийным аппаратом, терминологией, знание общепринятых научных концепций в заданной предметной области, понимание современных тенденций и проблем в исследовании предмета.	5
3. Представление собственной точки зрения (позиции, отношения) при раскрытии проблемы (творческий подход при осмыслении темы)	5
4. Раскрытие проблемы на теоретическом уровне или на бытовом уровне, с корректным использованием или без использования научных понятий в контексте раскрытия темы эссе.	5
5. Аргументация своей позиции с опорой на научные концепции, факты социально-экономической действительности или собственный опыт.	5
6. Соответствие работы формальным требованиям (структура эссе и его оформление)	5

Оценивание эссе

Эссе оценивается по балльной шкале, балы переводятся в оценки успеваемости следующим образом:

25 и более баллов – «отлично»;

19 – 24 баллов – «хорошо»;

15 – 18 баллов – «удовлетворительно;

менее 15 баллов – «неудовлетворительно».

Баллы учитываются в процессе текущей оценки знаний программного материала.

Примеры тестовых заданий:

1. Базовый закон, регулирующий информационные отношения:
1. ФЗ «Об информации, информационных технологиях и защите информации»; +
2. ФЗ «О коммерческой тайне»;
3. Закон РФ «Об авторском праве и смежных правах»;
4. ФЗ «Об архивном деле».

2. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов называются _____.

Ответ: информационные технологии

3. Виды ответственности, устанавливаемые за разглашение сведений, составляющих коммерческую тайну:

1. Административная; +
2. Дисциплинарная; +
3. Гражданско-правовая; +
4. Материальная.

4. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя называется _____ информации.

Ответ: конфиденциальность

Критерии выставления оценки за тест

Процент правильно выполненных тестовых заданий	Оценка
86% – 100%	отлично
69% - 85%	хорошо
50% - 68%	удовлетворительно
Менее 50%	неудовлетворительно

Баллы, полученные за тест, учитываются в процессе текущей и промежуточной оценки знаний программного материала.

6.2. Оценочные средства и критерии оценивания для промежуточной аттестации
Форма промежуточной аттестации – зачет.

Вопросы для подготовки к зачету

1. Информационная безопасность: понятие, основные задачи и методы ее обеспечения.
2. Угрозы информационной безопасности.
3. Государственная политика в сфере информационной безопасности.
4. Источник угрозы информационной безопасности и его виды.
5. Субъект информационной безопасности: понятие, виды.
6. Государственное управление в информационной сфере.
7. Влияние современных условий политического и социально-экономического развития страны на обеспечение информационной безопасности.
8. Основные задачи по обеспечению информационной безопасности.
9. Права граждан в информационной сфере.
10. Государственная тайна.
11. Основные этапы развития преступности в информационной сфере.
12. Понятие и виды преступлений в информационной сфере.
13. Уголовная ответственность за преступления, совершенные в информационной сфере.
14. Условия, формирующие и способствующие совершению преступлений в информационной сфере.
15. Меры предупреждения преступности в информационной сфере в современной России;
16. Основные направления международного сотрудничества в области обеспечения информационной безопасности.

17. Проблемы взаимодействия Российской Федерации с иными государствами в области обеспечения информационной безопасности.

18. Перспективные направления развития в области информационной безопасности.

19. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.

20. Основные разделы права и нормативно-правовые документы, регулирующие отношения в информационной сфере.

21. Категории информации по видам доступа к ней. Ограничение доступа к информации.

22. Порядок организации допуска и доступа к информации, составляющей различные виды тайн.

23. Особенности правовой защиты информации на предприятии. Основные нормативно-правовые и распорядительные документы, регулирующие отношения на предприятии по защите информации.

24. Особенности правовой защиты информации в информационных и телекоммуникационных сетях, а также в сети Интернет. Ответственность за правонарушения и преступления, связанные с этими сетями.

Критерии оценки ответа на зачете

«зачтено» – обучающийся справился с заданием, раскрыто основное содержание вопросов, не имеется грубых ошибок в освещении вопроса, в выполнении практической части задания, а также задание подготовлено и выполнено самостоятельно;

«не зачтено» – обучающийся не справился с заданием, не раскрыто основное содержание вопросов, имеются грубые ошибки в освещении вопроса, в выполнении практической части задания, а также задание подготовлено и выполнено несамостоятельно.

7. Перечень основной и дополнительной литературы

Нормативные правовые акты

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Система ГАРАНТ: https://base.garant.ru/12148555/

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Система ГАРАНТ: https://base.garant.ru/12148567/

3. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне». Система ГАРАНТ: https://base.garant.ru/12136454/

4. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Система ГАРАНТ: https://base.garant.ru/186117/

5. Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления». Система ГАРАНТ: https://base.garant.ru/194874/

6. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры». Система ГАРАНТ: https://base.garant.ru/71730198/

7. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности». Система ГАРАНТ: https://base.garant.ru/12181538/

8. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Система ГАРАНТ: https://base.garant.ru/71556224/

9. Указ Президента Российской Федерации от 22 мая 2015 г. №260 «О некоторых вопросах информационной безопасности Российской Федерации». Система ГАРАНТ: https://base.garant.ru/71035416/

7.1 Основная литература:

1. 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. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/498844
2. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. – Москва: Издательство Юрайт, 2022. – 253 с. – (Высшее образование). – ISBN 978-5-534-13960-0. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/496741

7.2 Дополнительная литература:

1. 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. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/496492
2. Рассолов, И. М. Информационное право: учебник и практикум для вузов / И. М. Рассолов. – 6-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2022. – 415 с. – (Высшее образование). – ISBN 978-5-534-14327-0. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/488767

7.3 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Компьютерная справочная система «КонсультантПлюс»: http://www.consultant.ru
2. Справочно-правовая система «Кодекс»: https://kodeks.ru/
3. Сетевой издание «Официальный интернет-портал правовой информации»: http://pravo.gov.ru/
4. Справочно-правовая система «Гарант»: https://www.garant.ru/
5. Образовательная платформа «Юрайт»: https://urait.ru
6. Электронная библиотека СмолГУ: http://www.smolgu.ru/biblioteka
7. Федеральный портал нормативных правовых актов: https://regulation.gov.ru/

8. Материально-техническое обеспечение

Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации: 214000, г. Смоленск, ул. Пржевальского, д.4, уч. корпус №2, ауд. 510.

Стандартная учебная мебель (60 учебных посадочных места), стол и стул для преподавателя – по 1 шт.

Кафедра для лектора – 1 шт.

Доска настенная трехэлементная – 1 шт.

Проекционный экран LUMA – 1 шт.

Мультимедиапроектор Acer – 1 шт.

Ноутбук HP 530 – 1шт.

Колонки Genius – 1 шт.

Помещение для самостоятельной работы: 214000, г. Смоленск, ул. Пржевальского, д.4, уч. корпус №2, ауд. 520 (компьютерная лаборатория с выходом в Интернет)

Компьютерный студенческий стол – 15 шт.
Компьютерный стол для преподавателя – 1 шт.
Интерактивная доска IQBoard
Мультимедиа проектор Optoma PX 329 DLP
16 персональных компьютеров с выходом в Интернет
Стандартная учебная мебель (16 учебных посадочных мест).

9. Программное обеспечение

1. Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), Лицензия 66920993 от 24.05.2016, (бессрочно)
2. Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), Лицензия 66975477 от 03.06.2016, (бессрочно)
3. KasperskyEndpointSecurity для бизнеса – Стандартный, Лицензия 1FB6181220135520512073, ежегодное обновление