Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра административного и финансового права

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.2 Информационная безопасность в органах внутренних дел»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность

40.05.02 Правоохранительная деятельность
(код и наименование специальности)

Административная деятельность полиции
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Юрист

Форма обучения
Заочная

Год набора 2024

Рабочая программа дисциплины *«Б1.Д.В.2 Информационная безопасность в органах внутренних дел»* рассмотрена и утверждена на заседании кафедры

Кафедра административного и финансового права
наименование кафедры

протокол № 5 от "29" 02 2024 г.

Заведующий кафедрой
Кафедра административного и финансового права — Т.В. Летута
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:

доцент — Е.И. Максименко
должность *подпись* *расшифровка подписи*

преподаватель — А.Г. Голощапова
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
40.05.02 Правоохранительная деятельность — О.В. Журкина
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
С.А. Бектимирова — Н.Н. Бигалиева
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
Л.И. Носенко
личная подпись *расшифровка подписи*

№ регистрации _____

© Максименко Е.И.,
Голощапова А.Г., 2024
© ОГУ, 2024

1 Цели и задачи освоения дисциплины

Целью освоения дисциплины является ознакомление с основами правового регулирования отношений в информационной сфере, конституционными гарантиями прав граждан на получение информации и механизм их реализации, изучение понятия и видов защищаемой информации по законодательству РФ, системы защиты государственной тайны, основ правового регулирования отношений в области интеллектуальной собственности и способов ее защиты, понятия и видов компьютерных преступлений, а также формирование некоторых практических навыков работы.

Задачи:

- изучение основных вопросов правового регулирования информационной безопасности;
- приобретение теоретических и практических навыков по основам использования современных методов правовой защиты государственной, коммерческой, служебной, профессиональной и личной тайны, персональных данных в компьютерных системах; лицензирования и сертификации в области защиты информации;
- освоение навыков подготовки и анализа локальных нормативных актов в сфере регулирования информационной безопасности;
- формирование практических навыков и способностей осуществления мероприятий по обеспечению правовой защиты информации.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательным дисциплинам (модулям) вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.21 Информатика, Б1.Д.Б.22 Информационные технологии в юридической деятельности*

Постреквизиты дисциплины: *Б1.Д.В.Э.3.1 Административно-правовое обеспечение экономической и национальной безопасности*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4-В-2 Ведет деловую коммуникацию в письменной и электронной форме, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках	**Знать:** требования нормативных правовых актов в области защиты государственной тайны и конфиденциальной информации; **Уметь:** разрабатывать и оформлять результаты профессиональной деятельности в процессуальной и служебной документации;

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		Владеть: навыками разработки и оформления результатов профессиональной деятельности в процессуальной и служебной документации
ПК*-4 Способен использовать информационные и цифровые технологии в правоохранительной деятельности	ПК*-4-В-1 Владеет базовым программным обеспечением для работы с текстами и табличными данными в правоохранительной деятельности ПК*-4-В-2 Способен решать простые технические проблемы с цифровыми устройствами при осуществлении правоохранительной деятельности ПК*-4-В-3 Способен искать, анализировать, создавать и управлять информацией в цифровой среде	**Знать:** требования по обеспечению соблюдения режима секретности и конфиденциальности при обработке с помощью информационных и цифровых технологий. **Уметь:** обеспечивать соблюдение режима секретности и конфиденциальности. обеспечивать защиту информации при работе с цифровыми устройствами при осуществлении правоохранительной деятельности **Владеть:** навыками применения требований нормативных правовых актов в области защиты государственной тайны и информационной безопасности и обеспечения режима секретности; навыками безопасной работы с базовым программным обеспечением для работы с текстами и табличными данными в правоохранительной деятельности

4 Структура и содержание дисциплины

Применяемые методики, педагогические технологии, в том числе использование ресурсов электронной информационно-образовательной среды, формы реализации образовательного процесса по дисциплине определяются законодательством РФ в сфере образования, локальными нормативными актами и преподавателем, реализующим дисциплину.

4.1 Структура дисциплины

Соотношение суммарного объема работ, реализуемых с использованием ресурсов электронной информационно-образовательной среды, и общей трудоемкости дисциплины не должно превышать 80%.

Общая трудоемкость дисциплины составляет 6 зачетных единиц (216 академических часов).

Вид работы	Трудоемкость, академических часов		
	8 семестр	9 семестр	всего
Общая трудоёмкость	**108**	**108**	**216**
Контактная работа:	**7,25**	**8,25**	**15,5**
Лекции (Л)	2	4	6
Практические занятия (ПЗ)	4	4	8
Консультации	1		1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25	0,5
Самостоятельная работа: **Самостоятельная работа:**	**100,75**	**99,75**	**200,5**
- практико-ориентированные задания; - написание эссе (Э); - самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий; - изучение разделов курса в системе электронного обучения; - подготовка к практическим занятиям.	**экзамен**	**зачет**	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Правовые основы защиты информации в Российской Федерации. Основные понятия в области защиты информации.	40	-	-	-	40
2	Обеспечение информационной безопасности в органах внутренних дел	46	2	2	-	42
3	Защита информации от утечки на объектах информатизации органов внутренних дел	22	-	2	-	20
	Итого:	108	2	4	-	102

Разделы дисциплины, изучаемые в 9 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
4	Правовые основы регулирования защиты отдельных видов информации ограниченного доступа	46	2	2	-	42
5	Защита информационных процессов в компьютерных и телекоммуникационных	46	2	2	-	42

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
	системах					
6	Основные понятия и методы информационного противоборства	16	-	-	-	16
	Итого:	108	4	4	-	100
	Всего:	216	6	8	-	202

4.2 Содержание разделов дисциплины

Раздел 1 Правовые основы защиты информации в Российской Федерации. Основные понятия в области защиты информации

Понятие информации, информационного правоотношения. Информация как объект защиты. Информационная безопасность и защита информации. Понятие информационной безопасности органов внутренних дел и его структура. Обеспечение национальной безопасности Российской Федерации. Концепция национальной безопасности Российской Федерации. Проблемы информационной безопасности.

Общая характеристика информационно-правовых норм. Органы законодательства, регламентирующие деятельность по информационной безопасности. Общая характеристика организационных методов защиты информации. Требования к построению систем безопасности объектов информатизации ОВД. Правовые основы организационной защиты информации в ОВД.

Концепция и модели информационной безопасности. Основные направления организационной защиты информации в ОВД. Создание системы организационного обеспечения информационной безопасности объекта ОВД.

Раздел 2 Обеспечение информационной безопасности в органах внутренних дел

Система обеспечения информационной безопасности органов внутренних дел. Защита информации в обеспечении информационной безопасности ОВД. Организационно-правовые основы защиты информации в ОДВ. Юридическая ответственность за правонарушения в сфере защиты информации.

Задачи службы безопасности организации. Формирование структуры службы безопасности, организация ее деятельности. Организация внутриобъектового режима на объекте. Организация инженерно-технической защиты объекта. Организация безопасного функционирования информационных систем на объекте. Проверка наличия конфиденциальных документов, дел и носителей информации. Организация служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа. Проведение аналитико-разведывательной работы службой безопасности организации. Основные требования к организации охраны объектов. Организация охраны объекта.

Раздел 3 Защита информации от утечки на объектах информатизации органов внутренних дел

Угрозы информационной безопасности. Понятие и виды источников и каналов утечки информации на объектах информатизации. Технические каналы утечки информации. Организационная и техническая защита информации органов внутренних дел от утечки. Силы, средства и условия организационной защиты информации в ОВД. Организация и проведение специальных проверок объектов информатизации ОВД.

Раздел 4 Правовые основы регулирования защиты отдельных видов информации ограниченного доступа

Степени секретности сведений и грифы секретности носителей этих сведений. Органы защиты государственной тайны. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне. Межведомственная комиссия по защите государственной тайны. Полномочия. Обеспечение деятельности. Социальные гарантии гражданам,

допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны. Порядок проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.

Регуляторы в области защиты ПДн. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Ответственность за нарушение обработки ПДн. Ответственность за нарушение режима защиты персональных данных.

Служебная тайна. Профессиональная тайна. Тайна следствия и судопроизводства. Отличие служебной тайны от профессиональной. Требования к защите служебной и профессиональной тайны. Ответственность за нарушение режима защиты служебной тайны. Ответственность за нарушение режима защиты профессиональной тайны. Ответственность за нарушение тайны следствия и судопроизводства.

Коммерческая тайна. Ответственность за нарушение коммерческой тайны. Разрешительная система доступа к сведениям, составляющим коммерческую тайну. Мероприятия по реализации разрешительной системы доступа к сведениям, составляющим коммерческую тайну организации.

Классификация информационных ресурсов. Организация работ по засекречиванию и рассекречиванию информации в организации. Сотрудники организации как источники информации и каналы ее разглашения. Особенности отбора кадров на должности, связанные с допуском к информации ограниченного доступа. Проверка соискателей на должности, связанные с допуском к информации ограниченного доступа. Заключение контрактов и соглашений о секретности. Задачи и структура текущей работы с сотрудниками, допущенными к информации ограниченного доступа.

Раздел 5 Защита информационных процессов в компьютерных и телекоммуникационных системах

Основные угрозы безопасности информации в компьютерных системах. Понятие, виды и общая характеристика преступлений в сфере компьютерной информации. особенности расследования и способы совершения компьютерных преступлений. Средства и способы защиты компьютерной информации от несанкционированного доступа. Антивирусная защита компьютерных систем.

Организационно-правовые основы лицензирования деятельности по защите информации. Лицензирование деятельности технической и криптографической защите информации. Особенности сертификации средств защиты информации от утечки по техническим каналам. Особенности сертификации средств защиты информации от НСД.

Идентификация и аутентификация пользователей в Windows. Хранение и шифрование парольной информации. Разграничение доступа средствами ОС. Средства криптографической защиты информации в ОС Windows. Классификация вредоносного ПО. Способы заражения. Методы борьбы, возможные последствия. Особенности шпионского программного обеспечения, возможности, характер работы. Руткиты, классификация, методы обнаружения. Антивирусная защита. Методы работы антивирусных средств.

Информационно-телекоммуникационные системы как объект защиты. особенности защиты информации в информационно-телекоммуникационных системах. Защита информации при проведении совещаний и переговоров. Защита информации при приеме в организации посетителей, командированных лиц и иностранных представителей. Защита информации при осуществлении научно-публицистической и рекламной деятельности. Защита информации в кадровой службе. Общие правила по защите информации при работе с документами.

Раздел 6 Основные понятия и методы информационного противоборства

Основные термины и определения информационного противоборства. Информационное противоборство. Компоненты информационного пространства, информационная обстановка в ведении информационного противоборства. Межгосударственное противоборство в информационном пространстве в целях нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам. Общая классификация информационных операций при воздействии в информационном противоборстве (воздействии). Общие понятия об информационном оружии. Классификация, характеристика информационного оружия, основанного на различных технологиях.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	2	Обеспечение информационной безопасности в органах внутренних дел	2
2	3	Защита информации от утечки на объектах информатизации органов внутренних дел	2
3	4	Правовые основы регулирования защиты отдельных видов информации ограниченного доступа	2
4	5	Защита информационных процессов в компьютерных и телекоммуникационных системах	2
		Итого:	8

5 Учебно-методическое обеспечение дисциплины

В учебно-методическое обеспечение дисциплины входят нормативно-правовые акты, основная литература, дополнительная литература, периодические издания, интернет-ресурсы, программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий, а также компоненты электронной информационно-образовательной среды в соответствии с Положением об электронной информационной образовательной среде ОГУ.

5.1 Нормативно-правовые акты

1 Конституция Российской Федерации: офиц. текст: принята Всенародным голосованием 12 декабря 1993 г. (с изм. и доп.);

2 Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 г. № 149-ФЗ (с изм. и доп.);

3 О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: указ Президента Российской Федерации от 01.05.2022 г. № 250;

4 Об утверждении перечня сведений конфиденциального характера: указ Президента РФ от 06 марта 1997 г. № 188 (с изм. и доп.);

5 О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 02.07.2021 г. № 400;

6 Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 г. № 646;

7 Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации: приказ МВД России от 06.07.2012 г. № 678 (с изм. и доп.).

5.2 Основная литература

1 Мансуров, Г. З. Право цифровой безопасности : учебник : [16+] / Г. З. Мансуров. – Москва : Директ-Медиа, 2022. – 148 с. – Режим доступа: по подписке. –

URL: https://biblioclub.ru/index.php?page=book&id=687364 (дата обращения: 20.03.2024). – Библиогр. в кн. – ISBN 978-5-4499-3061-3. – DOI 10.23681/687364. – Текст : электронный.

2 Преступления в сфере высоких технологий и информационной безопасности : учебное пособие : [16+] / В. Ф. Васюков, А. Г. Волеводз, М. М. Долгиева, В. Н. Чаплыгина ; под науч. ред. А. Г. Волеводза ; Московский государственный институт международных отношений (Университет) Министерства иностранных дел Российской Федерации. – Москва : Прометей, 2023. – 1086 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=701090 (дата обращения: 20.03.2024). – Библиогр. в кн. – ISBN 978-5-00172-447-6. – Текст : электронный.

5.3 Дополнительная литература

1 Литвиненко, О. В. Правовые аспекты информационной безопасности : учебное пособие : [16+] / О. В. Литвиненко. – Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2021. – 63 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=694774 (дата обращения: 20.03.2024). – Библиогр.: с. 60-61. – Текст : электронный.

2 Овчинникова, Е. А. Основы информационного права Российской Федерации : учебное пособие : [16+] / Е. А. Овчинникова, С. С. Новиков. – Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2021. – 138 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=695007 (дата обращения: 20.03.2024). – Библиогр. в кн. – Текст : электронный.

3 Ищейнов, В. Я. Информационная безопасность и защита информации : теория и практика : учебное пособие : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 20.03.2024). – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.

5.4 Периодические издания

Законы России: опыт, анализ, практика: журнал. – Москва: Агентство «Роспечать», 2024.
Уголовный процесс: журнал. – Москва: Агентство «Роспечать», 2024.

5.5 Интернет-ресурсы

http://www.supcourt.ru/ – официальный сайт Верховного Суда Российской Федерации
http://sudact.ru/ – Судебные и нормативные акты Российской Федерации
http://elibrary.ru/defaultx.asp – Научная электронная библиотека
http://www.szrf.ru/ – Собрание законодательства Российской Федерации

5.6 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.
2. Пакет офисных приложений LibreOffice.
3. Программная система для организации видео-конференц-связи MTS Link.
4. Яндекс.Браузер - браузер, созданный компанией «Яндекс» на основе движка (бесплатная версия) Режим доступа: https://browser.yandex.ru.
5. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2024]. – Режим доступа в сети ОГУ http://garant.net.osu.ru.
6. КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2024].
7. http://edu.garant.ru/garant/study/ - Интернет-версия ГАРАНТ-Образование, Система ГАРАНТ для студентов, аспирантов и преподавателей.
8. Автоматизированная интерактивная система сетевого тестирования - АИССТ (зарегистрирована в РОСПАТЕНТ, Свидетельство о государственной регистрации программы для ЭВМ

№2011610456, правообладатель – Оренбургский государственный университет), режим доступа - http://aist.osu.ru.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.