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
Очная

Год набора 2022

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

Кафедра административного и финансового права
наименование кафедры

протокол № 7 от "25" февраля 2022г.

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

Исполнители:
Доцент _____ Ю.Д. Фот
должность *подпись* *расшифровка подписи*

_____
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
40.05.02 Правоохранительная деятельность _____ Е.В. Мищенко
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
_____ Н.Н. Бигалиева
личная подпись *расшифровка подписи*

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

№ регистрации _____

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.25 Правовая статистика*

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

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов		
	5 семестр	6 семестр	всего
Общая трудоёмкость	**108**	**108**	**216**
Контактная работа:	**34,25**	**47,25**	**81,5**
Лекции (Л)	18	16	34
Практические занятия (ПЗ)	16	30	46
Консультации		1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25	0,5
Самостоятельная работа: - *написание реферата (Р);* - *самоподготовка - проработка и повторение лекционного материала и материала учебников и учебных пособий;* - *подготовка к практическим занятиям;* - *подготовка к промежуточной аттестации.*	**73,75**	**60,75**	**134,5**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	**экзамен**	

Разделы дисциплины, изучаемые в 5 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Роль и место информационной безопасности в системе национальной безопасности Российской Федерации	12	2	2		8
2	Организационно-правовые основы защиты информации в органах внутренних дел	12	2	2		8
3	Концептуальные положения организационного обеспечения информационной безопасности объекта ОВД	12	2	2		8
4	Угрозы, источники угроз и каналы утечки информации. Силы, средства и условия организационной защиты информации в ОВД	12	2	2		8
5	Режим защиты государственной тайны	12	2	2		8
6	Защита персональных данных	12	2	2		8
7	Служебная и профессиональная тайны. Тайна следствия и судопроизводства.	12	2	2		8
8	Организация защиты коммерческой тайны	12	2	2		8
9	Порядок засекречивания и рассекречивания сведений ограниченного доступа. Подбор сотрудников на должности, связанные с допуском к информации ограниченного доступа.	12	2			10
	Итого:	108	18	16		74

Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
10	Организация деятельности службы	14	2	2		10

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
	безопасности					
11	Основы организации охраны объекта. Требования, предъявляемые к объектам, на которых ведутся работы с документами ограниченного доступа	14	2	2		10
12	Организация защиты информации при проведении совещаний по конфиденциальным вопросам, приеме посетителей, осуществлении научно-публицистической деятельности	14	2	2		10
13	Аттестация объектов информатизации. Лицензирование и сертификация в области защиты информации.	14	2	2		10
14	Программно-аппаратные средства защиты информации.	56	8	22		22
	Итого:	108	16	30		62
	Всего:	216	34	46		136

4.2 Содержание разделов дисциплины

№1 Роль и место информационной безопасности в системе национальной безопасности Российской Федерации

Понятие, структура информационного правоотношения. Обеспечение национальной безопасности Российской Федерации. Концепция национальной безопасности Российской Федерации. Проблемы информационной безопасности.

№2 Организационно-правовые основы защиты информации в органах внутренних дел

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.

№3 Концептуальные положения организационного обеспечения информационной безопасности объекта ОВД

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

№4 Угрозы, источники угроз и каналы утечки информации. Силы, средства и условия организационной защиты информации в ОВД

Угрозы информационной безопасности. Источники и каналы утечки информации. Силы, средства и условия организационной защиты информации в ОВД.

№5 Режим защиты государственной тайны

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.

№6 Защита персональных данных

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.

№7 Служебная и профессиональная тайны. Тайна следствия и судопроизводства.

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.

№8 Организация защиты коммерческой тайны

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.

№9. Порядок засекречивания и рассекречивания сведений ограниченного доступа. Подбор сотрудников на должности, связанные с допуском к информации ограниченного доступа.

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.

№10 Организация деятельности службы безопасности

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.

№11 Основы организации охраны объекта. Требования, предъявляемые к объектам, на которых ведутся работы с документами ограниченного доступа

Основные требования к организации охраны объектов. Организация охраны объекта. Основные методы охраны объекта. Ограждения периметра, отдельных участков территории объекта. Контрольно-пропускной пункт объекта. Техническая укрепленность строительных конструкций зданий и помещений, предназначенных для работы с документами ограниченного доступа. Защита периметра территории, зданий и открытых площадок с помощью технических средств охраны. Защита помещений объекта с помощью технических средств охраны. Оборудование объекта техническими средствами тревожной сигнализации. Применение систем контроля и управления доступом, охранного телевидения. Оборудование объекта системой оповещения и охранным освещением.

№12 Организация защиты информации при проведении совещаний по конфиденциальным вопросам, приеме посетителей, осуществлении научно-публицистической деятельности

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.

№13 Аттестация объектов информатизации. Лицензирование и сертификация в области защиты информации.

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.

№14 Программно-аппаратные средства защиты информации.

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.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Роль и место информационной безопасности в системе национальной безопасности Российской Федерации	2
2	2	Организационно-правовые основы защиты информации в органах внутренних дел	2
3	3	Концептуальные положения организационного обеспечения информационной безопасности объекта ОВД	2
4	4	Угрозы, источники угроз и каналы утечки информации. Силы, средства и условия организационной защиты информации в ОВД	2
5	5	Режим защиты государственной тайны	2
6	6	Защита персональных данных	2
7	7	Служебная и профессиональная тайны. Тайна следствия и судопроизводства.	2
8	8	Организация защиты коммерческой тайны	2
9	10	Организация деятельности службы безопасности	2
10	11	Основы организации охраны объекта. Требования, предъявляемые к объектам, на которых ведутся работы с документами ограниченного доступа	2
11	12	Организация защиты информации при проведении совещаний по конфиденциальным вопросам, приеме посетителей, осуществлении научно-публицистической деятельности	2
12	13	Аттестация объектов информатизации. Лицензирование и сертификация в области защиты информации.	2
13	14	Защита документов MICROSOFT OFFICE	2
14	14	Настройка параметров политики аудита для локальных папок и файлов	2
15,16	14	Создание скрытой информации. Установка паролей	4
17	14	Настройка параметров безопасности Интернет	2
18,19	14	Настройка параметров политики аудита для категории события	4
20,21	14	Настройка параметров политики аудита для локальных папок и файлов	4
22,23	14	Планирование, создание и изменение учетных записей пользователей.	4
		Итого:	46

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Организационно-правовое обеспечение информационной безопасности: учебное пособие. А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова и др. / Под ред. А.А. Стрельцова. – М.: Издательский центр «Академия», 2008. – 256 с.

Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227 (дата обращения: 20.03.2022). — Режим доступа: для авториз. пользователей.

5.2 Дополнительная литература

1. Информационная безопасность : учебное пособие. — Пермь : ПГГПУ, 2018. — 87 с. — ISBN 978-5-85219-007-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/129509 (дата обращения: 20.03.2022). — Режим доступа: для авториз. пользователей.

2. Информационная безопасность : учебное пособие / В. Н. Ясенев, А. В. Дорожкин, А. Л. Сочков, О. В. Ясенев ; под редакцией В. Н. Ясенева. — Нижний Новгород : ННГУ им. Н. И. Лобачевского, 2017. — 198 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/153011 (дата обращения: 29.03.2022). — Режим доступа: для авториз. пользователей.

3. Крыжановский, А. В. Информационная безопасность : методические указания / А. В. Крыжановский, И. С. Поздняк. — Самара : ПГУТИ, 2018. — 38 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182282 (дата обращения: 20.03.2022). — Режим доступа: для авториз. пользователей.

4. Терещенко, Л.К. Модернизация информационных отношений и информационного законодательства = Modernization of informational relationships and informational legislation [Текст]: монография / Л.К. Терещенко; Ин-т законодательства и сравн. правоведения при Правительстве Рос. Федерации. – М.: ИНФРА-М, 2014. – 227 с. – Парал. тит. л. англ. – ISBN 978-5-16-006123-8. – ISBN 978-5-16-100556-9.

5.3 Периодические издания

Журналы:

- «Информационная безопасность»;
- «Вестник информационной безопасности»;
- «Проблемы информационной безопасности. Компьютерные системы».

5.4 Интернет-ресурсы

1. http://www.fsb.ru – сайт ФСБ РФ
2. http://www.fstec.ru – сервер ФСТЭК РФ
3. http://www.gov.ru – сервер органов государственной власти РФ
4. http://www.minsvyaz.ru – сайт министерства информационных технологий и связи РФ
5. http://www.scrf.gov.ru – сайт Совета Безопасности РФ
6. www.consultant.ru – Консультант плюс
7. https://gost.ru – Росстандарт
8. http://docs.cntd.ru – Электронный фонд правовой и нормативно-технической документации
9. http://www.securrity.ru – Сайт Информационная безопасность
10. https://www.securitylab.ru – Информационный портал по информационной безопасности
11. https://securelist.ru/ - Сетевая штаб-квартира экспертов «Лаборатории Касперского»
12. https://moodle.osu.ru - Электронные курсы ОГУ в системе обучения moodle
13. https://openedu.ru/course/hse/DATPRO/ - «Открытое образование». Курсы, МООК: Защита информации.
14. https://ru.coursera.org/learn/metody-i-sredstva-zashity-informacii - «Coursera». Курсы, МООК: Методы и средства защиты информации

15. https://ru.coursera.org/learn/management-informacionnoi-bezopasnosti - «Coursera». Курсы, МООК: Менеджмент информационной безопасности

16. https://www.intuit.ru/studies/courses/3648/890/info – «Интуит. Национальный открытый университет» Курсы, МООК: Аттестация объектов информатизации по требованиям безопасности информации.

17. https://www.intuit.ru/studies/courses/3601/843/info - «Интуит. Национальный открытый университет» Курсы, МООК: Информационное право: Информация.

18. https://openedu.ru/course/ITMOUniversity/INTPRO/- «Открытое образование» Курсы, МООК: Правовые основы защиты интеллектуальной собственности.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

а) программно- аппаратное обеспечение:

1. Операционная система Microsoft Windows

2. Open Office/LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.

б) базы данных, информационно-справочные и поисковые системы:

– Консультант Плюс [Электронный ресурс] : справочно-правовая система / Компания Консультант Плюс. – Электрон. дан. – Москва, [1992–2016]. – Режим доступа : в локальной сети ОГУ \\fileserver1\!CONSULT\cons.exe

– Гарант [Электронный ресурс] : справочно-правовая система / НПП Гарант-Сервис. – Электрон. дан. - Москва, [1990–2016]. – Режим доступа \\fileserver1\GarantClient\garant.exe. В локальной сети ОГУ.

– Законодательство России [Электронный ресурс] : информационно-правовая система. – Режим доступа : http://pravo.fso.gov.ru/ips/, в локальной сети ОГУ.

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.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.