

Минобрнауки России
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»
Кафедра административного и финансового права

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ
«С.1.В.ДВ.3.2 Правовое обеспечение компьютерной безопасности»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность

40.05.02 Правоохранительная деятельность
(код и наименование специальности)

Административная деятельность
(наименование направленности (профиля) образовательной программы)

Квалификация

Юрист

Форма обучения

Очная

Год набора 2018

Рабочая программа рассмотрена и утверждена на заседании кафедры

административного и финансового права

наименование кафедры

протокол № 6 от "20" февраля 2018 г.

Заведующий кафедрой
административного и финансового права

наименование кафедры

подпись

Е.В. Мищенко

расшифровка подписи

Исполнители:

профессор

должность

подпись

Е.В. Мищенко

расшифровка подписи

преподаватель

должность

подпись

Р.Я. Гайсин

расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по специальности

40.05.02 Правоохранительная деятельность

код наименование

личная подпись

Е.В. Мищенко

расшифровка подписи

Заведующий отделом комплектования научной библиотеки

личная подпись

Н.Н. Грицай

расшифровка подписи

Уполномоченный по качеству факультета

личная подпись

Л.И. Носенко

расшифровка подписи

№ регистрации 66267

© Мищенко Е.В., 2018

© Гайсин Р.Я., 2018

© ОГУ, 2018

1 Цели и задачи освоения дисциплины

Цель освоения дисциплины: является ознакомление с основами правового регулирования в отношении компьютерной безопасности, нормативно-правовыми актами регулирующие деятельность электронного документооборота в системе МВД России, формирование некоторых практических навыков работы по защите информации.

Задачи:

- изучение основных вопросов правового регулирования компьютерной 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 компьютерной безопасности;
- формирование практических навыков и способностей осуществления мероприятий по обеспечению компьютерной безопасности.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам по выбору вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: С.1.Б.23 Информационное и документационное обеспечение административной деятельности правоохранительных органов.

Постреквизиты дисциплины: Отсутствуют.

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: требования нормативных правовых актов в области защиты государственной тайны информационной безопасности. Уметь: обеспечивать соблюдение требований нормативно-правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности. Владеть: приемами соблюдения в профессиональной деятельности требований нормативных правовых актов в области защиты государственной тайны информационной безопасности, обеспечения соблюдения режима секретности.	ПК-22 способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 академических часа).

Вид работы	Трудоемкость, академических часов	
	9 семестр	всего
Общая трудоёмкость	144	144
Контактная работа:	53,25	53,25
Лекции (Л)	18	18
Практические занятия (ПЗ)	34	34

Вид работы	Трудоемкость, академических часов	
	9 семестр	всего
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: - практико-ориентированные задания (П-ОЗ); - самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий); - подготовка к практическим занятиям; - подготовка к коллоквиумам; - подготовка к промежуточной аттестации).	90,75	90,75
Вид итогового контроля	экзамен	

Разделы дисциплины, изучаемые в 9 семестре

№ раздела	Наименование разделов	Количество часов			
		всего	аудиторная работа		внеауд. работа
			Л	ПЗ	
1	Законодательные и правовые основы защиты компьютерной информации и информационных технологий	16	2	4	10
2	Проблемы защиты информации в АСОИУ	16	2	4	10
3	Теоретические основы компьютерной безопасности	16	2	4	10
4	Современные криптосистемы для защиты компьютерной информации	16	2	4	10
5	Методы идентификации и проверки подлинности пользователей компьютерных систем	16	2	4	10
6	Защита компьютерных сетей от удаленных атак	16	2	4	10
7	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	16	2	4	10
8	Комплексная защита процесса обработки информации в компьютерных системах	32	4	6	22
	Итого:	144	18	34	92
	Всего:	144	18	34	92

4.2 Содержание разделов дисциплины

Раздел 1 Законодательные и правовые основы защиты компьютерной информации и информационных технологий

Информация как объект юридической и физической защиты. Государственные информационные ресурсы. Защита государственной тайны как особого вида защищаемой информации. Защита конфиденциальной информации, в том числе интеллектуальной собственности и коммерческой тайны. Нормативно-правовая база защиты компьютерных сетей от несанкционированного доступа. Компьютерные преступления и особенности их расследования.

Раздел 2 Проблемы защиты информации в АСОИУ

Меры противодействия угрозам безопасности. Меры по обеспечению сохранности информации в АСОИУ. Основные задачи обеспечения безопасности информации в АСОИУ. Защита локальных сетей и операционных систем. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения АСОИУ. Рекомендации по защите информации в Internet.

Раздел 3 Теоретические основы компьютерной безопасности

Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы. Структура теории компьютерной безопасности. Основные уровни защиты информации. Защита машинных носителей информации и средств взаимодействия. Защита представления информации. Защита содержания информации. Основные виды атак на автоматизированные системы обработки информации. Классификация основных атак и вредоносных программ. Построение парольных систем; особенности применения криптографических методов. Способы реализации криптографической подсистемы. Особенности реализации систем с симметричными и несимметричными ключами. Концепция защищенного ядра; методы верификации. Защищенные домены. Применение иерархического метода для построения защищенной операционной системы. Исследование корректности систем защиты. Методология обследования и проектирования защиты. Модель политики контроля целостности.

Раздел 4 Современные криптосистемы для защиты компьютерной информации

Основные понятия и определения. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Дисковые шифраторы. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома. Поточные шифры, блочные шифры. Аддитивные поточные шифры. Методы генерации криптографически качественных псевдослучайных последовательностей.

Американский стандарт шифрования DES: Алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. Отечественный стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования. Понятия однонаправленной функции. Понятие однонаправленной функции с лазейкой.

Раздел 5 Методы идентификации и проверки подлинности пользователей компьютерных систем

Основные понятия и концепции. Идентификация и механизмы подлинности пользователя. Взаимная проверка подлинности пользователя. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний. Однонаправленные хэш-функции. Алгоритм безопасного хэширования SHA. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль-Гамала (EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи.

Раздел 6 Защита компьютерных сетей от удаленных атак

Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты.

Программно-аппаратные средства защиты ПЭВМ и сетей. Методы средства ограничения доступа к компонентам Методы и средства привязки программного обеспечения к аппаратному окружению к физическим носителям. Методы и средства хранения ключевой информации. Защита программ от изучения; защита от разрушающих программных воздействий; защита от изменений и контроль целостности.

Раздел 7 Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)

Классификация способов защиты. Защита от закладок и дизассемблирования. Способы встраивания защитных механизмов в программное обеспечение. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные ви-

русы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий. Понятие изолированной программной среды.

Раздел 8 Комплексная защита процесса обработки информации в компьютерных системах

Постановка проблемы комплексного обеспечения информационной безопасности автоматизированных систем. Состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ). Функциональные и обеспечивающие подсистемы, технология, управление. Методология формирования задач защиты: интеграция средств компьютерной безопасности.

Этапы проектирования КСИБ и требования к ним: предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение эксплуатации, сопровождение; Особенности проектирования на современном уровне и синтез КСИБ; типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД). Мониторинг и контроль окружающей среды; ведение специальной информационной базы данных КСИБ.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Законодательство Российской Федерации в области информационной безопасности	2
2	1	Компьютерные преступления и особенности их расследования	2
3	2	Основные непреднамеренные и преднамеренные угрозы информационной безопасности АСОИУ	2
4	2	Защита локальных сетей и операционных систем. Интеграция систем защиты	2
5	3	Основные понятия теории компьютерной безопасности	2
6	3	Защита машинных носителей информации и средств взаимодействия	2
7	4	Основные понятия и определения криптосистемы для защиты компьютерной информации	2
8	4	Отечественные и зарубежные стандарты защиты компьютерной информации	2
9	5	Идентификация: основные понятия и концепция	2
10	5	Аутентификация	2
11	6	Режим функционирования межсетевых экранов и их основные компоненты	2
12	6	Программно-аппаратные средства защиты ПЭВМ и сетей	2
13,14	7	Методы защиты программ от излучения и разрушающих программных воздействий	4
15	8	Комплексное обеспечение информационной безопасности автоматизированных систем	2
16	8	Внедрение и эксплуатация КСИБ	2
17	8	Инструментально-моделирующий комплекс для оценки качества функционирования защищенных информационных систем	2
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Нормативно-правовые акты

Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ).

Гражданский кодекс Российской Федерации (части 1-4): федер. закон от 30.11.1994 г. № 51-ФЗ (посл. ред.).

Уголовный кодекс Российской Федерации: федер. закон от 13.06.1996 г. № 63-ФЗ (посл. ред.).

Кодекс об административных правонарушениях Российской Федерации: федер. закон от 30 декабря 2001 г. № 195-ФЗ (посл. ред.) (с изм. и доп.).

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

О средствах массовой информации: закон РФ от 27.12.1991 № 2124-1 (посл. ред.) (с изм. и доп.).

О безопасности: федер. закон от 28.12.2010 г. № 390-ФЗ (посл. ред.).

О государственной тайне: закон РФ от 21.07.1993 № 5485-1 (посл. ред.).

Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ (посл. ред.).

О федеральной службе безопасности: федер. закон от 03.04.1995 № 40-ФЗ (посл. ред.).

Об электронной подписи: федер. закон от 06.04.2011 № 63-ФЗ (посл. ред.) (с изм. и доп.).

О коммерческой тайне: федер. закон от 29.07.2004 № 98-ФЗ (посл. ред.).

Об основах государственной политики в сфере информатизации: указ Президента РФ от 20.01.1994 № 170 (посл. ред.).

О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации: указ Президента РФ от 03.04.1995 № 334 (ред. от 25.07.2000).

Об утверждении Перечня сведений, отнесенных к государственной тайне: указ Президента РФ от 30.11.1995 № 1203 (посл. ред.).

О некоторых вопросах Межведомственной комиссии по защите государственной тайны: указ Президента РФ от 03.08.2018 № 471.

Об утверждении Перечня сведений конфиденциального характера: указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015).

О Стратегии национальной безопасности Российской Федерации до 2020 года: указ Президента РФ от 12.05.2009 № 537 (ред. от 01.07.2014).

О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны: постановление Правительства РФ от 15.04.1995 № 333 (посл. ред.).

5.2 Основная литература

Лапина, М.А. Информационное право: учебное пособие / М.А. Лапина, А.Г. Ревин, В.И. Лапин; ред. И.Ш. Килясханов. – М.: Юнити-Дана, 2015. – 336 с. – (Высшее профессиональное образование: Юриспруденция). – ISBN 5-238-00798-1; То же [Электронный ресурс]. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=118624>

Кочеткова, М.Н. Информационное право: учебное пособие / М.Н. Кочеткова, А.В. Терехов; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2014. – 80 с. – ISBN 978-5-8265-1315-6; То же [Электронный ресурс]. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=277808>.

5.3 Дополнительная литература

Гаврилов, Д.А. Правовая защита от недобросовестной конкуренции в сфере исключит. прав на средства индивидуализации и иные объекты пром. собствен.: Монография / Д.А. Гаврилов. – М.: Норма: НИЦ ИНФРА-М, 2014. – 192 с. – ISBN 978-5-91768-490-1. – Режим доступа: <http://znanium.com/catalog/product/459354>

Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом: учебное пособие / Н.Б. Ельчанинова; Министерство науки и высшего образования РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный уни-

верситет», Инженерно-технологическая академия. – Ростов-на-Дону; Таганрог: Изд-во Южного федерального университета, 2017. – 77 с. – ISBN 978-5-9275-2501-0; То же [Электронный ресурс]. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=499598>

Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. – М.; Берлин: Директ-Медиа, 2015. – 253 с. – ISBN 978-5-4475-3946-7; То же [Электронный ресурс]. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=276557>.

Килясханов, И.Ш. Информационное право в терминах и понятиях: учебное пособие / И.Ш. Килясханов, Ю.М. Саранчук. – М.: Юнити-Дана, 2015. – 135 с. – ISBN 978-5-238-01369-5; То же [Электронный ресурс]. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=115167>.

Ковалев, Д.В. Информационная безопасность: учебное пособие / Д.В. Ковалев, Е.А. Богданова; Министерство образования и науки РФ, Южный федеральный университет. – Ростов-на-Дону: Изд-во Южного федерального университета, 2016. – 74 с. – ISBN 978-5-9275-2364-1; То же [Электронный ресурс]. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=493175>.

Куняев, Н.Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере [Электронный ресурс] / Н.Н. Куняев. – М.: Логос, 2010. – 348 с. – ISBN 978-5-98704-513-8. – Режим доступа: <http://znanium.com/catalog/product/469026>

Лапина, М.А. Информационное право: учебное пособие / М.А. Лапина, А.Г. Ревин, В.И. Лапин; ред. И.Ш. Килясханов. – М.: Юнити-Дана, 2015. – 336 с. – (Высшее профессиональное образование: Юриспруденция). – ISBN 5-238-00798-1; То же [Электронный ресурс]. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=118624>.

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.

Фабричных, А.Г. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / А.Г. Фабричных, А.С. Дёмушкин, Т.В. Кондрашова, Н.Н. Куняев. – М.: Логос, 2011. – 452 с. – (Новая университетская библиотека). – ISBN 978-5-98704-541-1; То же [Электронный ресурс]. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=84996>.

5.4 Периодические издания

Государство и право: журнал. – М.: Академиздатцентр «Наука» РАН, 2018.

Право и государство: теория и практика: журнал. – М.: Агентство «Пресса России», 2018.

Российская юстиция: журнал. – М.: Агентство «Роспечать», 2018.

5.5 Интернет-ресурсы

<http://www.iqlib.ru/> – Электронная библиотека IQlib

<http://nbmgu.ru/> – Научная библиотека МГУ имени М.В. Ломоносова

<http://elibrary.rsl.ru/> – Электронная библиотека Российской государственной библиотеки (РГБ)

<http://elibrary.ru/defaultx.asp> – Научная электронная библиотека

<http://www.nlr.ru/> – Российская национальная библиотека

<http://www.szrf.ru/> – Собрание законодательства Российской Федерации

5.6 Программное обеспечение, профессиональные базы данных и информационные справочные системы

Операционная система Microsoft Windows

Пакет настольных приложений Microsoft Office (Word, Excel, PowerPoint, OneNote, Outlook, Publisher, Access)

ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990—2018]. – Режим доступа в сети ОГУ для установки системы: \\fileserver1\GarantClient\garant.exe

КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная

правовая система. / Разработчик ЗАО «Консультант Плюс», [1992—2018]. – Режим доступа к системе в сети ОГУ для установки системы: \\fileserver1\!\CONSULT\cons.exe

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.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключённой к сети «Интернет» и обеспечены доступом в электронную информационно-образовательную среду ОГУ.