

# АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

## Б1.В.ДВ.03.02 ПРАВОВАЯ ИНФОРМАТИКА

**Автор:** к.т.н., доцент Михнев И.П.

**Код и наименование направления подготовки, профиля:**

38.05.01 Экономическая безопасность, Экономико-правовое обеспечение экономической безопасности

**Квалификация (степень) выпускника:** Экономист

**Форма обучения:** очная, заочная

### **Цель освоения дисциплины:**

*Сформировать компетенцию в области правовой информатики.*

Компетенция направлена на формирование глубоких знаний в области правовой информатики, необходимых для самостоятельной работы на персональных компьютерах с использованием современных программных средств, навыков использования мощного инструмента поиска и творческой работы с информационными ресурсами международной сети Internet, возможностей использования имеющихся в России мощных компьютерных банков правовой информации; ознакомление с информационным обеспечением экономических и финансовых расчетов, теорией и практикой создания и управления базами данных.

### **План курса:**

**Тема 1. Информационное общество и право. Предмет и методы правовой информатики. Понятие информации, защиты информации и информационной безопасности.** Понятие информации, защиты информации и информационной безопасности. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства, на уровне региона и на локальном уровне. Основные положения теории информационной безопасности информационных систем. Основные составляющие обеспечения информационной безопасности хозяйственной деятельности.

**Тема 2. Государственная информационная политика. Законодательный уровень информационной безопасности. Компьютерные преступления. Ответственность за совершение компьютерных преступлений.**

Важность законодательного уровня информационной безопасности. Обзор российского законодательства в области обеспечения информационной безопасности. Доктрина информационной безопасности РФ, законы «О государственной тайне», «Об информации, информационных технологиях и о защите информации». Другие законы и законодательные акты. Концепция информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны и конфиденциальной информации, нормативно-справочные документы. Нормативные акты администрации Волгограда в области информационной безопасности.

Компьютерные преступления. Ответственность за совершение компьютерных преступлений. Уголовная и административная ответственность.

**Тема 3. Технология работы в справочно-правовых системах. Классификация атак. Понятие угрозы. Модель угроз. Рекомендации по обеспечению ИБ.**

Понятие атаки на информационную систему. Классификация атак. Виды противников или “нарушителей”, их классификация. Каналы утечки информации: визуально-оптический, акустический, электромагнитный и материально-вещественный. Понятие угрозы. Источники угроз и их классификация. Построение модели угроз организации. Примеры. Руководящие документы Гостехкомиссии России (Федеральная служба по техническому и экспортному контролю) по защите от несанкционированного доступа к информации. Специальные требования и рекомендации. Инструкция СТР-К. Рекомендации по защите конфиденциальной информации. Классы защищенности средств вычислительной техники и автоматизированных систем по руководящим документам Гостехкомиссии России. Показатели

защищенности. Система защиты информации от несанкционированного доступа. Рекомендуемые меры по обеспечению защиты информации в процессе эксплуатации информационной системы. Разрешительная система допуска. Рекомендации по плану доработки объектов информатизации на соответствие требованиям руководящих документов Гостехкомиссии России.

#### **Тема 4. Информационная безопасность. Основные понятия криптографии. Два современных направления в криптографии. Классические криптосистемы.**

Историческая справка. Возможные направления решения задачи обеспечения передачи секретной информации. Стеганография и криптография. Важность криптографии при решении задач обеспечения информационной безопасности хозяйственной деятельности и сохранения конфиденциальной информации. Основные понятия криптографии. Понятие криптосистемы, ключа. Возможные атаки на криптосистемы, понятие криптоанализа. Надежность криптосистемы. Два основных направления в современной криптографии. Классические криптосистемы. Одноалфавитные и многоалфавитные криптосистемы. Системы Цезаря и Виженера. Возможности криптоанализа многоалфавитных систем. Раскрытие системы Виженера. Надежность многоалфавитных систем. Электромеханические шифровальные машины. Абсолютно надежная криптосистема: «Одноразовый блокнот». Возможность использования таких систем на практике. Стандарты шифрования данных. Криптосистема DES. Российский стандарт шифрования ГОСТ 28147-89. Проблема выбора надежной криптосистемы для защиты своих данных. Перспективы развития криптоанализа. Проблема полного перебора всех ключей.

#### **Тема 5. Электронный документооборот и электронная подпись. Криптография с открытым ключом. Системы шифрования. Электронная подпись.**

Системы шифрования, не требующие передачи ключа. Проблемы использования таких систем. Протокол использования системы «Одноразовый блокнот», не требующий первоначального обмена секретными ключами. Криптография с открытым ключом. Понятие открытого и секретного ключа. Правила их использования. Принципы построения криптосистем с открытым ключом. Известные криптосистемы с открытым ключом и их алгоритмы. Система RSA. Длина ключа в криптографии с открытым ключом. Односторонняя функция, возможность ее использования. Электронная подпись и принципы ее применения.

#### **Тема 6. Интернет в юридической деятельности. Основные технологии построения защищенных ИС. Межсетевые экраны.**

Основные технологии построения защищенных ИС. Понятие межсетевого экрана. Правила фильтрации и принципы их применения. Пакетные фильтры. Политика сетевой безопасности. Политика реализации межсетевых экранов. Функциональные требования к межсетевым экранам и их компоненты. Шлюзы сеансового и прикладного уровня. Новые функции брандмауэров. Схемы организации межсетевых экранов. Особенности различных схем реализации, их преимущества и недостатки. Проблемы, связанные с межсетевыми экранами. Требования к межсетевым экранам

#### **Тема 7. Технология VPN-сетей.**

Технология объединения локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи данных в единую виртуальную сеть, обеспечивающую защиту информационных потоков или технология VPN-сетей. Особенности VPN. Туннель VPN. Туннелирование и его особенности. Основные разновидности VPN-устройств по технической реализации. Роли VPN-устройств. Варианты построения защищенных каналов VPN. Угрозы для VPN. Варианты защищенных соединений. Классификация VPN-сетей. Совмещение VPN-технологий и межсетевого экрана. Недостатки VPN.

#### **Тема 8. Защита информации в Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей.**

Проблема обеспечения информационной безопасности при работе с глобальной сетью Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей. Указ президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена». Угрозы информационной безопасности при работе с Интернет. Вирусы, исполняемые модули, всплывающие окна и реклама. Использование антивирусных программ и межсетевых экранов при работе с Интернет. Программные средства проверки трафика и борьбы с несанкционированным использованием ресурсов информационной системы.

## Тема 9. Типовая структура защиты от НСД. Управление доступом.

Архитектура типовой системы защиты от несанкционированного доступа. Идентификация и аутентификация. Парольная аутентификация. Правила применения паролей. Одноразовые пароли. Сервер аутентификации. Подсистема управления доступом, подсистема регистрации и учета. Принципы контроля доступа. Матрица доступа и списки доступа. Произвольное и принудительное управление доступом. Ограничивающий интерфейс. Ролевое управление доступом. Статическое и динамическое распределение ролей. Подсистема обеспечения целостности. Криптографическая подсистема.

Программно-аппаратные средства защиты информации от НСД. Устройства ввода идентификационных признаков. Классификация устройств ввода идентификационных признаков. Биометрические устройства ввода идентификационных признаков и их классификация. Преимущества и недостатки их использования. Комбинированные устройства. Электронные замки.

### Формы текущего контроля и промежуточной аттестации:

Промежуточная аттестация по дисциплине «**Правовая информатика**» проводится в соответствии с учебным планом: *в 4 семестре – в виде зачета.*

1.1. Дисциплина Б1.В.ДВ.3.2 Правовая информатика обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
УК ОС-2	Способность применять проектный подход при решении профессиональных задач	УК ОС-2.4.2	Способность использовать программные продукты для формирования и анализа баз данных и правовой информации с целью обеспечения информационной безопасности

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ <sup>1</sup> (при наличии профстандарта)/ трудовые или профессиональные действия	Код этапа освоения компетенции	Результаты обучения
УК ОС-2 направлена на формирование глубоких знаний в области информационных технологий, необходимых для приобретения навыков и умений управления информацией, как взаимосвязанной и соответствующим образом сформированной совокупности: организационных, управленческих, экономических, информационных, методических, программно-технологических аспектов деятельности по удовлетворению информационных потребностей с целью принятия эффективного решения, и по наращиванию интеллектуального потенциала в виде информационных баз данных и баз знаний.	УК ОС-2.4.2	Сформулировать базовые теоретические представления о правовой информации, процессах оборота информации и информатизации в правовой сфере; определить средства, методы и технологии решения профессионально-ориентированных задач с применением новейших компьютерных и коммуникационных технологий; назвать основные методы обеспечения информационной безопасности; дать определение основных положений теории информационной безопасности информационных систем; характеризовать модели безопасности и их применение; назвать способы нарушений информационной безопасности. Определить опасности и угрозы информационной безопасности; применять основные методы и программы защиты информации; использовать методы и способы обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты служебной информации; применять новые информационные и телекоммуникационные технологии правовой информатики.

<sup>1</sup> Для образовательных программ, реализуемых по ФГОС, и для универсальных компетенций первая колонка может не заполняться

	Демонстрировать навыки криптографической и стеганографической защиты информации; применять основные методы и средствами защиты информации; демонстрировать навыками работы с нормативными документами по защите информации и организацией соответствующих отделов в организациях; осуществлять самостоятельное решение задач предметной области на персональном компьютере с помощью новых информационных технологий и современных информационных систем
--	--

### **Основная литература:**

1. Гаврилов О.А. Курс правовой информатики: Учебник для вузов / О.А.Гаврилов; Ин-т государства и права РАН; Акад. правовой унт. – М.: Норма, 2015. – 419 с.: ил.
2. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.
3. Малюк, А.А. Введение в информационную безопасность: учебное пособие. Горячая линия-Телеком.2011. Режим доступа: <http://www.iprbookshop.ru/11979>.- ЭБС «IPRbooks»