МЕЖДУНАРОДНАЯ ПОЛИЦЕЙСКАЯ АКАДЕМИЯ
Автономная некоммерческая организация высшего образования
АНО ВО МПА

Правовое обеспечение информационной безопасности

Фонд оценочных средств дисциплины (модуля)

Учебный план 40.03.02 Обеспечение законности и правопорядка
Год начала подготовки 2026-2027

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Виды контроля в семестрах:
экзамены 5

1. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ОПК-12: Информационно-коммуникационные технологии для профессиональной деятельности
ОПК-12.1: Ориентируется в принципах работы современных информационных технологий
ОПК-12.2: Использует современные информационные технологии для решения задач профессиональной деятельности
ОПК-12.3: Применяет основные способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации
УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
УК-1.1: Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними
УК-1.2: Критически оценивает надежность информации, работает с противоречивой информацией из разных источников
УК-1.3: Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов

В результате освоения дисциплины обучающийся должен

1.1	**Знать:**
1.1.1	- основные правовые понятия, категории, конструкции, используемые в сфере обеспечения информационной безопасности Российской Федерации;
1.1.2	- компетенцию органов государственной власти в сфере обеспечения информационной безопасности Российской Федерации;
1.1.3	- правовой режим защиты государственной тайны и информации ограниченного доступа в Российской Федерации;
1.1.4	- правовое регулирование денежного обращения в Российской Федерации;
1.1.5	- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.
1.2	**Уметь:**
1.2.1	- избирать наиболее эффективные правовые способы защиты информации;
1.2.2	- использовать полученные навыки по реализации технологий, направленных на обеспечение информационной безопасности в условиях операционной системы Windows, ее приложений, локальных и общемировых сетей.
1.3	**Владеть:**
1.3.1	- навыками разработки локальных нормативных документов в области защиты информации;
1.3.2	- опытом (навыком) работы с антивирусными пакетами, настройки параметров информационной безопасности в приложениях – браузерах сети Internet.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО КРИТЕРИЯМ ОЦЕНИВАНИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Уровень сформированности профессиональных компетенций каждого обучающегося оценивается по следующей шкале (от 1 до 5):
1 – не справляется с выполнением типовых профессиональных задач, не проявляет ни один из навыков, входящих в компетенцию;
2 – не справляется с выполнением типовых профессиональных задач, проявляет отдельные навыки, входящие в компетенцию;
3 – выполняет типовые профессиональные задачи при консультационной поддержке: пороговый (критический) уровень готовности;
4 – самостоятельно выполняет типовые профессиональные задачи. Для решения нестандартных задач требуется консультационная помощь: пороговый (допустимый) уровень готовности;
5 – все профессиональные (типовые и нестандартные) профессиональные задачи выполняет самостоятельно: повышенный уровень готовности.
Бально-рейтинговая оценка по промежуточной аттестации проводимой в форме экзамена и (или) дифференцированного зачета выставляется в соответствии со следующей шкалой:
50–71 – «удовлетворительно»;
71–92 – «хорошо»;
92–100 – «отлично».
Далее приводятся критерии оценки результатов ответов. Например:
Оценка "ОТЛИЧНО" ставится обучающемуся, показавшему повышенный уровень готовности.
Оценка "ХОРОШО" ставится обучающемуся, показавшему пороговый (допустимый) уровень готовности.
Оценка "УДОВЛЕТВОРИТЕЛЬНО" ставится обучающемуся, показавшему пороговый (критический) уровень готовности.
Бально-рейтинговая оценка по промежуточной аттестации проводимой в форме зачета выставляется в соответствии со следующей шкалой:
51–100 – «зачтено».
Далее приводятся критерии оценки результатов ответов. Например:
Оценка "зачтено" ставится обучающемуся, минимально показавшему пороговый (критический) уровень готовности.

3. ОЦЕНОЧНЫЕ СРЕДСТВА

3.1. Вопросы для самоконтроля и текущей аттестации

Понятие информационной безопасности.
Концепция информационной безопасности.
Место информационной безопасности экономических систем в национальной безопасности страны.
Важность и сложность проблемы информационной безопасности.
Информационная безопасность в условиях функционирования в России глобальных сетей.
Теория информационной безопасности информационных систем, ее основные составляющие и задачи.
Моделирование процессов защиты информации.
Модели безопасности и их применение.
Понятие стратегии защиты. Виды стратегий защиты.
Критерии обоснования стратегии защиты.
Понятие угрозы безопасности информации и общие подходы к ее классификации.
Классификация угроз безопасности информации по способам их возможного негативного воздействия.
Угрозы доступности, целостности, конфиденциальности.
Происхождение угроз безопасности информации.
Предпосылки появления угроз.
Понятие нарушителя безопасности информации.
Виды противников или нарушителей безопасности информации.
Виды возможных нарушений информационной системы.
Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
Анализ способов нарушений информационной безопасности.
Вирус как типичное нарушение информационной безопасности. Виды вирусов.
Понятие системы защиты информации.
Типизация и стандартизация систем защиты информации.
Центры защиты информации и их функции.
Основные технологии построения защищенных ЭИС.
Использование защищенных ЭИС.
Понятие криптографии. Методы криптографии.
Политика безопасности.
Программа безопасности.
Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
Международные стандарты информационного обмена.
Стандарты и спецификации в области информационной безопасности и их классификация.
«Оранжевая книга».

Гармонизированные критерии европейских стран.
Спецификация internet-сообщества RFC 1510 «сетевой сервис аутентификации kerberos (v5)».
Руководящие документы (РД) Гостехкомиссии России.
X.800 «архитектура безопасности для взаимодействия открытых систем».
Технические спецификации IPSEC, TLS.
Рекомендация «как выбирать поставщика internet-услуг».
Британский стандарт BS 7799 «управление информационной безопасностью. Практические правила».
Безопасность операционных систем.
Безопасность систем управления базами данных.
Безопасность виртуальных частных сетей.
Безопасность виртуальных локальных сетей.
Безопасность смарт – карт.
Архитектура средств безопасности IP-уровня.
Контексты безопасности и управление ключами.
Обеспечение аутентичности IP-пакетов.
Обеспечение конфиденциальности сетевого трафика.
Роль поставщика internet-услуг в реагировании на нарушения безопасности.
Меры по защите internet-сообщества.
Обеспечение безопасности маршрутизаторов.
Особенности использования управляющих протоколов.
Безопасное размещение сетевого оборудования потребителя.
Защита системной инфраструктуры.

3.2. Темы письменных работ (контрольных и курсовых работ, рефератов)

1 Развитие законодательства в области защиты информации.
2 Сравнительный анализ положений Доктрин информационной безопасности.
3 Информационное оружие – миф или реальность?
4 Основные вызовы в Стратегии развития информационного общества до 2030 года.
5 Трансформация поля угроз в киберпространстве.
6 Система информационного законодательства в области защиты информации.
7 Персональные данные как социальная и правовая категория.
8 Классификация видов тайн в современном российском законодательстве.

3.3. Оценочные средства для промежуточной аттестации

1 Основные этапы формирования и реализации государственной политики в информационной сфере.
2 Стратегия развития информационного общества.
3 Понятие «информационной безопасности».
4 Место информационной безопасности в системе национальной безопасности РФ. Стратегия национальной безопасности РФ.
5 Доктрина информационной безопасности РФ.
6 Основные положения государственной политики обеспечения информационной безопасности Российской.
7 Характеристика информационного законодательства.
8 Основные положения федерального закона «Об информации, информационных технологиях и о защите информации», касающиеся вопросов информационной безопасности.
9 Государственная программа РФ «Информационное общество (2011– 2020 годы)».
10 Виды и источники угроз информационной безопасности Российской Федерации.
11 Методы обеспечения информационной безопасности Российской Федерации: классификация и общая характеристика.
12 Основные функции системы обеспечения информационной безопасности Российской Федерации.
13 Структура организационной основы системы обеспечения информационной безопасности Российской Федерации.
14 Защита информации. Место защиты информации в информационной безопасности.
15 Системный подход к защите информации. Правовые, организационно-технические и экономические методы защиты информации.
16 Стандартизация и сертификация в сфере информационной безопасности: российский и зарубежный опыт.
17 Система национальных стандартов в сфере защиты информации.
18 Руководящие документы ФСТЭК России в сфере защиты информации.
19 Понятие электронного обмена данными и электронного документооборота.
20 Понятие электронного документа и его особенности.
21 Понятие электронной подписи.
22 Виды электронной подписи: простая, усиленная неквалифицированная, усиленная квалифицированная.
23 Аппаратные и программные средства электронной подписи.
24 Удостоверяющие центры.
25 Требования к удостоверяющим центрам.
26 Аккредитация удостоверяющих центров.
27 Предмет и задачи криптографии. Основные определения.
28 Требования к криптографическим системам защиты информации.
29 Криптографические атаки.
30 Простейшие методы шифрования с закрытым ключом. Методы замены.
31 Понятие «хеш-функции» и её назначение.
32 Методы шифрования с открытым ключом.
33 Цифровая подпись на основе алгоритмов с открытым ключом.

34 Требования к алгоритмам шифрования с открытым ключом.
35 Классификация угроз информационной безопасности в вычислительных сетях.
36 Использование антивирусных программ.
37 Обеспечение безопасности в сети Интернет.
38 Межсетевые экраны: понятие и принципы использования.