АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«Информационная безопасность»
по специальности 38.05.01 «Экономическая безопасность»
специализация «Финансовый учет и контроль в правоохранительных органах»

1. Цели и задачи освоения дисциплины

Цель дисциплины – формирование у будущих специалистов и руководителей системных знаний по проблеме обеспечения комплексной защиты информационных ресурсов и управлению информационными рисками, а также практических навыков безопасной работы в информационных системах.

Задачи дисциплины:

- формирование системных представлений об управлении информационными рисками;
- изучение методов и средств комплексной защиты информации в информационных системах коммерческих предприятий и государственных учреждений;
- формирование практических навыков анализа защищенности информационных систем, использования встроенных возможностей ОС, MS Office, Брандмауэра Windows, Internet Explorer, а также антивирусных и криптографических средств для обеспечения безопасности информации;
- получение теоретических знаний и практических навыков при решении типовых задач по обеспечению информационной безопасности;
- изучение проблем защиты информации, стоящих перед современной вычислительной техникой;
- формирование навыков использования полученных знаний для правильного выбора решений при разработке криптографических, организационных, технических средств защиты информации.

В результате изучения курса студенты должны ознакомиться с методикой и инструментами построения комплексной, эшелонированной системы информационной безопасности.

2. Место дисциплины в структуре ОПОП

Очная форма

В рамках дисциплины изучаются основные направления развития современных информационных технологий и обеспечения безопасности информационных систем. Шифр дисциплины в рабочем учебном плане - Б1.Б.51.

Дисциплина читается в 9-ом семестре студентам 5-го курса очной формы обучения и базируется на отдельных компонентах компетенций, сформированных у обучающихся в ходе изучения предшествующих учебных дисциплин учебного плана.

Вместе с другими курсами, посвященными трендам трансформации современной экономики, дисциплина «Информационная безопасность» составляет основу образования специалиста в части ОПОП, касающейся современных тенденций становления и развития информационного общества. Она охватывает широкий круг проблем и поэтому связана со многими дисциплинами, которые преподают в рамках изучения современных информационных технологий, т.к. ее цель – получение студентом знаний, умений и навыков обеспечения информационной безопасности.

Дисциплина читается в 9-ом семестре студентам 5-го курса очной формы обучения

и базируется на отдельных компонентах компетенций, сформированных у обучающихся в ходе изучения предшествующих учебных дисциплин учебного плана.

До изучения данной дисциплины студенты изучают :

- Информационные технологии в экономике и управлении (ОК-12; ПК-29)
- Инструменты цифровой экономики (ОК-12; ПК-29)
- Автоматизация обработки учётной информации (ОК-12; ПК-29)
- Контроллинг (ПК-32; ПК-43; ПСК-8)
- Оценка рисков (ОПК-1; ПК-32; ПК-43)
- Методы оптимизации производственных процессов (ПК-32; ПК-43; ПСК-8).

Знания, навыки и умения, приобретенные в результате прохождения курса «Информационная безопасность», также будут востребованы при прохождении практик, осуществлении проектной деятельности, выполнении курсовых и выпускной квалификационной работ, связанных с обеспечением защиты информационных систем, ИТ-инфраструктуры, безопасной работы в сети Интернет, защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

заочная форма

Дисциплина «Информационная безопасность» охватывает широкий круг проблем и поэтому связана со многими дисциплинами, которые преподают в рамках изучения современных информационных технологий, т.к. ее цель – получение студентом знаний, умений и навыков обеспечения информационной безопасности.

В рамках дисциплины изучаются основные направления развития современных информационных технологий и обеспечения безопасности информационных систем. Шифр дисциплины в рабочем учебном плане - Б1.Б.51.

Дисциплина читается в 9-ом семестре студентам 5-го курса очной формы обучения и базируется на отдельных компонентах компетенций, сформированных у обучающихся в ходе изучения предшествующих учебных дисциплин учебного плана.

До изучения данной дисциплины студенты изучают :

- Информационные технологии в экономике и управлении (ОК-12; ПК-29)
- Инструменты цифровой экономики (ОК-12; ПК-29)
- Автоматизация обработки учётной информации (ОК-12; ПК-29)
- Контроллинг (ПК-32; ПК-43; ПСК-8)
- Оценка рисков (ОПК-1; ПК-32; ПК-43)
- Методы оптимизации производственных процессов (ПК-32; ПК-43; ПСК-8).

Студенты заочной формы обучения дисциплину «Информационная безопасность» изучают параллельно с курсом «Судебная экономическая экспертиза» (ОПК-3; ПК-32; ПК-33).

Знания, навыки и умения, приобретенные в результате прохождения курса, также будут востребованы при прохождении практик, осуществлении проектной деятельности, выполнении курсовых и выпускной квалификационной работ, связанных с обеспечением защиты информационных систем, ИТ-инфраструктуры, безопасной работы в сети Интернет, защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Перечень планируемых результатов освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование	Перечень планируемых результатов обучения по дисциплине

реализуемой компетенции	**(модулю), соотнесенных с индикаторами достижения компетенций**
ОК-12 способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	**Знать:** понятие информации, способы ее представления, основные приемы получения, хранения, обработки информации; стандартные программные средства набора текста и баз данных; правовые акты в области защиты государственной тайны и информационной безопасности; правовые основы организации защиты государственной тайны и конфиденциальной информации; основные понятия информационной безопасности; основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках; возможности применения в работе современных системных программных средств: операционных систем, операционных оболочек, обслуживающих программ; основные принципы организации и алгоритмы функционирования операционных систем и оболочек; проблемы и направления развития системных программных средств; понятие угроз безопасности; способы классификации угроз информационной безопасности; технологические возможности злоумышленников по преодолению систем защиты информации; характеристики и механизмы реализации типовых удаленных атак; понятие типовой удаленной атаки; уязвимости сетевых протоколов ARP, ICMP, DNS, TCP, FTP, TELNET; принципы создания защищенных систем связи в распределенных вычислительных системах; понятие сервиса безопасности; понятие архитектурной безопасности; назначение списков управления доступом; принципы функционирования системы S/KEY и сервера аутентификации Kerberos. **Уметь:** использовать программные и аппаратные средства персонального компьютера; ориентироваться в современной системе источников информации; использовать современные информационные технологии в своей профессиональной деятельности; применять средства антивирусной защиты; анализировать информационную безопасность многопользовательских систем; пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа; видеть и формулировать проблему, видеть конкретную ситуацию, прогнозировать и предвидеть, рассчитывать риски, ставить цели и задачи; проектировать и использовать средства идентификации и аутентификации пользователей; использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; использовать алгоритмы генерации, хранения и распределения ключей; использовать методы активного аудита; использовать межсетевые экраны для обеспечения безопасности межсетевого взаимодействия; обеспечивать комплексную защиту информации. **Владеть:** навыками применения аппаратных и программных средств обеспечения информационной безопасности; навыками противостояния типовым удаленным атакам; навыками обеспечения безопасной работы на компьютере; навыками безопасного поиска информации в глобальной информационной сети Интернет, работы с базами данных и Интернет-ресурсами; современной терминологией и методологией в области информационной безопасности; идеологией произвольного (дискреционного) управления доступом, принудительного (мандатного) управления доступом, ролевого управления доступом; технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет; инструментами ОС семейства Windows для настройки политики аудита;

	методикой и стандартами построения защищённых виртуальных частных сетей VPN; навыками антивирусной борьбы и использования антивирусного ПО.
ПК-32 способностью проводить анализ возможных экономических рисков и давать им оценку, составлять и обосновывать прогнозы динамики развития основных угроз экономической безопасности	**Знать:** основные понятия, изложенные в Доктрине информационной безопасности РФ и Федеральном Законе «Об информации, информационных технологиях и защите информации»; интересы личности, общества и государства в информационной области; понятие ценности информации, защиты информации, системы защиты информации; цели и концептуальные основы защиты информации; основные виды угроз безопасности информации и их классификацию; классификацию стандартов в области информационной безопасности; руководящие документы Гостехкомиссии России; направления защиты от несанкционированного доступа. **Уметь:** производить анализ типов информации в зависимости от порядка ее предоставления; делать разбор методов обеспечения информационной безопасности; классифицировать в соответствии с уровнями обеспечения национальной безопасности группы субъектов; подразделять основные средства защиты по видам деятельности; пользоваться в своей профессиональной деятельности основными нормативными правовыми актами в сфере обеспечения информационной безопасности. **Владеть:** методами классификации конфиденциальной информации; навыками работы с документами в сфере обеспечения информационной безопасности; методами классификации угроз безопасности информации в распределенных вычислительных системах; основными сетевыми командами ОС Windows, используемыми для обеспечения безопасности распределенных вычислительных систем; методами и способами управления персоналом; организации физической защиты; поддержания работоспособности; реагирования на нарушения режима безопасности; планирования восстановительных работ.

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет **3** зачетных единицы (**108** часов).

5. Образовательные технологии

В ходе изучения дисциплины используются как традиционные методы и формы обучения (лекции, практические занятия, самостоятельная работа), так и интерактивные формы проведения занятий (кейс-задания).

При организации самостоятельной работы используются следующие образовательные технологии: самостоятельная работа, сопряженная с основными аудиторными занятиями (проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины); подготовка к тестированию; самостоятельная работа под контролем преподавателя в форме плановых консультаций; внеаудиторная самостоятельная работа при выполнении студентом домашних заданий, подготовки докладов.

6. Контроль успеваемости

Программой дисциплины предусмотрены виды текущего контроля: собеседование, заслушивание докладов, проверка решения практических задач, кейс-заданий (ситуационного практикума), проверка тестовых заданий.

Промежуточная аттестация проводится в форме: зачет.