АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«Информационная безопасность»

по направлению подготовки 38.03.05 «Бизнес-информатика»
профиль «Цифровая экономика»

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность» посвящена изучению основ информационной безопасности. Рассматриваются основные понятия информационной безопасности, структура мер в области информационной безопасности, кратко описываются меры законодательного, административного, процедурного и программно-технического уровней. Излагаются взгляды на информацию, как объект защиты с выделением характерных свойств защищаемой информации. Рассматриваются виды угроз информационной безопасности; методы и средства борьбы с угрозами информационной безопасности; понятие политики безопасности, существующие типы политик безопасности; действующие стандарты информационной безопасности; нормативные руководящие документы.

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. То есть, задачами дисциплины является изучение основных теоретических положений и методов, формирование умений и привитие навыков применения теоретических знаний для решения прикладных задач, а также развитие новых подходов к обеспечению информационной безопасности в сфере экономики.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность» принадлежит вариативной части Блока Б1 «Дисциплины (модули)» основной профессиональной образовательной

программы (ОПОП), устанавливаемой вузом, и является обязательной. Данная дисциплина является одной из основополагающих дисциплин в системе подготовки бакалавра по направлению 38.03.05 «Бизнес-информатика». Вместе с другими курсами, посвященными трендам трансформации современной экономики, дисциплина «Информационная безопасность» составляет основу образования бакалавра в части ОПОП, касающейся современных тенденций становления и развития информационного общества. Она охватывает широкий круг проблем и поэтому связана практически со многими дисциплинами, которые преподают в рамках изучения современных информационных технологий, т.к. ее цель – получение студентом знаний, умений и навыков обеспечения информационной безопасности. Цифровая трансформация помогает не просто следовать тенденции, но и экономить время, деньги, ресурсы, то есть оставаться конкурентоспособными. Современные коммуникационные технологии помогают реализовать широкий набор бизнес-процессов предприятий и организаций различных видов деятельности, размеров и организационно-правовых форм. Общие тенденции информатизации экономики таковы, что информационные системы, обеспечивающие взаимодействие предприятия с другими субъектами хозяйственной деятельности, и их реализация на микроуровне становятся неразрывными, поэтому требования к уровню подготовки экономиста в области информационной безопасности постоянно повышаются. Информационная безопасность является важнейшей составляющей частью общей интегральной или комплексной безопасности, причем на любом возможном уровне рассмотрения – национальном, региональном, отраслевом, корпоративном и даже персональном. При этом информационная безопасность обладает специфической особенностью. При анализе необходимо учитывать, что сервисы защиты информации являются неотъемлемой частью информационных технологий, которые в настоящее время развиваются доселе невиданными темпами. Чтобы не отставать от технического прогресса, необходимо не просто внедрить некоторые готовые инструменты в сфере информационной безопасности, а разработать методологию генерации новых решений, отвечающих современному состоянию дел, а в идеале – работающих на перспективу

В рамках дисциплины изучаются основные направления развития современных информационных технологий и обеспечения безопасности информационных систем. Шифр дисциплины в рабочем учебном плане - Б1.В.ОД7.

Дисциплина читается в 6-ом семестре студентам 3-его курса очной формы обучения и базируется на отдельных компонентах компетенций, сформированных у обучающихся в ходе изучения предшествующих учебных дисциплин учебного плана.

Пререквизиты. Изучение курса «Информационная безопасность» базируется на компетенциях, сформированных у обучающихся в процессе изучения дисциплин:

- «Основы предпринимательского права»;
- «Программирование»;
- «Базы данных»;
- «Распределенные системы в цифровой экономике».

Дисциплина рассчитана на студентов, имеющих подготовку по предшествующим курсам, касающихся основ программирования с использованием алгоритмических языков, алгебры и теории чисел, теории вероятности. Предполагается, что студенты знакомы с основными понятиями алгебры, комбинаторики, теории вероятности, информатики, которые изучаются в рамках данной ОПОП перед изучением данной дисциплины.

Обучающиеся должны иметь подготовку (знания, умения, навыки и компетенции) в области информатики, информационных технологий и систем, глобальных сетей, организации и инфраструктуры предпринимательской деятельности, коммерции, менеджмента, производственных и бизнес-процессов. Для изучения раздела, касающегося криптографических средств защиты, студент также должен освоить курс «Вероятностные методы в экономике». Также, перед тем как приступить к изучению дисциплины «Анализ больших данных», студенту рекомендуется актуализировать знания по курсу

«Математические методы в экономике». Помимо этого, для успешного освоения данного курса студент должен иметь навык самостоятельной работы с различными источниками информации (интернет, печатные издания), умением обобщать информацию, полученную из разных источников, умением представлять результаты своих исследований. Материал курса «Программирование» необходим в части знания основных принципов объектно-ориентированного проектирования программных систем, основных алгоритмов обхода дерева, поиска и сортировки и др.

Постреквизиты. Результаты освоения дисциплины «Анализ больших данных» будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих специальных дисциплин:

– «Технология блокчейн и криптовалюта».

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, в процессе подготовки к сдаче и сдачи государственного экзамена, защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОСНОВЕНИЯ ДИСЦИПЛИНЫ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ПК-9 организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	**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. **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. **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.
ПК-11 умение защищать права на интеллектуальную собственность	**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.
ПК-13 умение проектировать и внедрять	**Знать:** понятие угроз безопасности; способы классификации угроз информационной безопасности; технологические возможности злоумышленников по преодолению систем защиты

компоненты ИТ-инфраструктуры предприятия, обеспечивающие достижение стратегических целей и поддержку бизнес-процессов	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:** 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:** 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.

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) – 5 ЗЕТ.

4.2. Объем дисциплины по видам учебной работы (в часах): 180.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии: лекции, лабораторный практикум с использованием активных и интерактивных форм и др.

Интерактивные формы проведения лекций:

- проблемная лекция;
- лекция - визуализация;
- лекция - дискуссия;
- лекция с разбором конкретных ситуаций.

Интерактивные формы практических и лабораторных занятий:

- использование специализированных и прикладных программ;
- решение конкретных профессиональных ситуаций, используя инструменты цифровой экономики;
- компьютерное моделирование ситуаций;
- групповая дискуссия;
- мозговой штурм.

При организации самостоятельной работы занятий используются следующие

образовательные технологии:

- систематизация информации из различных источников;
- работа со специализированной литературой и электронными ресурсами;
- написание реферата;
- регулярная проработка курса прослушанных лекций;
- подготовка к выполнению лабораторных работ.

6. КОНТРОЛЬ УСПЕВАЕМОСТИ

Программой дисциплины предусмотрены следующие виды текущего контроля:

- электронное тестирование;
- выполнение индивидуальных заданий (написание реферата);
- подготовка, выполнение и защита лабораторных работ.

По данной дисциплине предусмотрена форма отчетности: **экзамен**.

Промежуточная аттестация проводится в форме: **экзамен**.