АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ/ПРАКТИКИ

Б1.В.ДВ.3.1 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ

наименование дисциплины/практики

Автор: к.т.н., доцент кафедры
Информационных систем и математического моделирования 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 компетенции УК ОС-2 Способность применять проектный подход при решении профессиональных задач, ПК-1 Способность подготавливать исходные данные, необходимые для расчета экономических и социально-экономических показателей, характеризующих деятельность хозяйствующих субъектов

План курса:

Тема 1. Понятие информации, защиты информации и информационной безопасности. Основные составляющие.

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. 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. Классификация атак. Понятие угрозы. Модель угроз. Рекомендации по обеспечению информационной безопасности.

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. 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. Криптография с открытым ключом. Системы шифрования, не требующие передачи ключа. 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. 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 «**Основы информационной безопасности хозяйственной деятельности»** проводится в соответствии с учебным планом: *в 4 семестре – в виде зачета.* Формы текущего контроля: устный опрос, тестирование.

Дисциплина **Б1.В.ДВ.3.1 Основы информационной безопасности хозяйственной деятельности** 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-2.4.1	Способность использовать программные продукты для формирования и анализа баз данных и правовой информации с целью обеспечения информационной безопасности
ПК-1	Способность подготавливать исходные данные, необходимые для расчета экономических и социально-экономических показателей, характеризующих деятельность хозяйствующих субъектов	ПК-1.4.3	Способность ориентироваться в данных финансовой отчетности экономического субъекта для проведения экспресс-анализа его финансовой деятельности

В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ/ трудовые или профессиональные действия	Код этапа освоения компетенции	Результаты обучения
	УК ОС-2.4.1	На уровне знаний: Назвать международные стандарты информационного обмена; дать определение понятия угрозы, защиты, видов противников или “нарушителей”; перечислить модели безопасности и их применение; назвать методы криптографии; назвать методы и способы обеспечения информационной безопасности в профессиональной деятельности; идентифицировать информационные технологии в системе мер защиты информации; назвать нормативные документы по защите информации и организации соответствующих отделов в организациях; назвать руководящие документы, касающиеся государственной тайны
		На уровне умений: Демонстрировать способность самообучения в современных компьютерных средах; выделить 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
		На уровне навыков: Демонстрировать навыки криптографической и стеганографической защиты информации; применять основные методы и средства защиты информации
Составление и представление финансовой отчетности экономического субъекта/	ПК-1.4.3	На уровне знаний: Демонстрация знаний основных методов криптографии, моделей безопасности, понятия угрозы, защиты и способов обеспечения информационной безопасности в профессиональной деятельности

проведение финансового анализа, бюджетирование и управление денежными потоками (Проф. стандарт «Бухгалтер», утв. Приказом Минтруда России от 22 декабря 2014 г. N 1061н)		На уровне умений: Умение применять знания в современных компьютерных средах и выделять опасности угроз информационной безопасности. Применять основные методы и программы защиты информации
		На уровне навыков: Свободное владение навыками криптографической и стенографической защиты информации, основными методами и средствами защиты информации

Основная литература:

1. 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.
2. Платонов В. В. Программно-аппаратные средства защиты информации: учебник. / М.: Изд. центр "Академия". 2014.
3. Малюк, А.А. Введение в информационную безопасность: учебное пособие. Горячая линия-Телеком.2011. Режим доступа: http://www.iprbookshop.ru/11979.- ЭБС «IPRbooks»