

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)/ПРАКТИКИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ *наименование дисциплин (модуля)/практики*

Автор: Ковальчук Н. Н.

Код и наименование направления подготовки, профиля:

38.03.05 Бизнес-информатика, профиль Бизнес-аналитика

Квалификация (степень) выпускника: Бакалавр

Форма обучения: Очная

Цель освоения дисциплины:

Сформировать компетенции:

- способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-ОС-1)
- организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия (ПК-9)
- умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия (ПК-21)

План курса:

Вводная лекция. Роль и место информационной безопасности в развитии современного общества.

Информация как стратегический ресурс государства и общества. Необходимость изучения вопросов информационной безопасности. Предмет курса, его цели, задачи, структура и порядок изучения.

Исторические аспекты вопроса. Основные факторы, влияющие на процесс обеспечения информационной безопасности в ретроспективе глобального исторического процесса и на современном этапе. Информатизация государства и общества. Эволюция приоритетов угроз информационной безопасности в XXI веке. Теории информационного общества. Концепции информационных войн иностранных государств. Последствия глобализации для информационной безопасности.

Раздел 1. Теоретические основы информационной безопасности.

Тема 1.1. Основные понятия и определения, сущность и содержание информационной безопасности.

Основные понятия и определения теории информационной безопасности в соответствии с действующими нормативно-правовыми документами Российской Федерации и международным правом, а также современными научными взглядами.

Информационная безопасность как составная часть национальной безопасности страны. Составляющие национальных интересов в информационной сфере. Сущность и содержание информационной безопасности с позиций системного подхода.

Цели, задачи, направления (составные части), закономерности и принципы обеспечения информационной безопасности.

Тема 1.2. Угрозы и уровни обеспечения информационной безопасности в условиях глобализации.

Системный подход к построению иерархии последовательно вложенных уровней глобальных угроз информационной безопасности. Особенности форм и содержания угроз на каждом уровне применительно к России. Фасетно-иерархическая классификация угроз информационной безопасности. Специфика информационных угроз на региональном, ведомственном и муниципальном уровнях.

Возможности по нейтрализации угроз информационной безопасности на различных уровнях применительно к существующему состоянию рассматриваемых аспектов в Российской Федерации. Сравнительный анализ проводимых мероприятий по обеспечению информационной безопасности в России и других развитых странах.

Тема 1.3. Нормативно-правовое и концептуальное обеспечение информационной безопасности.

Структура правового обеспечения Российской Федерации в области информационной безопасности: Конституция, Федеральные законы, законы, подзаконные нормативно-правовые акты (Указы Президента, Постановления Правительства, концептуальные и доктринальные документы), государственные стандарты, правовые акты, организационно-распорядительные и методические документы соответствующих федеральных министерств и ведомств. Концепция национальной безопасности, Доктрина информационной безопасности России. Нормативные документы РФ по стандартизации.

Международная нормативно-правовая база по вопросам информационной безопасности. Международные стандарты обеспечения информационного обмена.

Тема 1.4. Система обеспечения информационной безопасности Российской Федерации (региона, муниципального образования).

Состав и структура системы обеспечения информационной безопасности России. Функции и взаимосвязь системообразующих элементов. Особенности обеспечения информационной безопасности на федеральном, региональном, ведомственном и муниципальном уровнях. Основные механизмы обеспечения информационной безопасности: организационный, нормативно-правовой, методическое и технологическое обеспечение, кадровое и научное обеспечение.

Тема 1.5. Информационная безопасность различных сфер жизнедеятельности общества.

Составляющие национальных интересов в информационной области для различных сфер жизнедеятельности общества: политической, экономической, социальной, духовной. Специфика информационных угроз, особенности решения вопросов обеспечения информационной безопасности в различных сферах жизнедеятельности общества. Субъекты, объекты, цели и задачи, механизмы обеспечения информационной безопасности. Защита интеллектуальной собственности. Роль и место вопросов обеспечения информационной безопасности в ходе реализации Федеральных целевых программ в области информационных технологий.

Тема 1.6. Информационная безопасность отраслей социально-трудовой сферы Российской Федерации.

Система обеспечения информационной безопасности социально-трудовой сферы России. Особенности формирования и развития жизненно-важных интересов и ценностей, угроз и опасностей в информационной области для различных отраслей социально-трудовой сферы: образования, здравоохранения, культуры, рынка труда, процессов обеспечения занятости, жилищно-коммунального хозяйства и др. Специфика рассматриваемых вопросов применительно к проблемам демографии, миграции и эмиграции населения, этническим вопросам. Роль и место вопросов обеспечения информационной безопасности в ходе реализации Приоритетных национальных проектов.

Тема 1.7. Применение методов системных исследований при анализе процессов обеспечения информационной безопасности.

Основные положения современной теории системных исследований. Методология применения системного подхода при анализе процессов обеспечения информационной безопасности, соотношение гуманитарных, естественнонаучных и технических аспектов.

Проблема информационно-аналитического обеспечения в достижении опережающего информационного эффекта при осуществлении реформ. Анализ возможностей использования методов математического моделирования при исследовании проблем обеспечения информационной безопасности.

Особенности прогнозирования информационной обстановки. Основные показатели и критерии обеспечения информационной безопасности. Особенности оценки эффективности мероприятий по обеспечению информационной безопасности. Модель принятия управленческого решения, вопросы обеспечения его информационной безопасности.

Раздел 2. Подготовка и проведение мероприятий по обеспечению информационной безопасности организации (предприятия).

Тема 2.1. Основы информационной безопасности организации (предприятия).

Роль и место информационной безопасности в системе комплексной безопасности организации (предприятия). Анализ способов нарушения информационной безопасности. Информационные угрозы, цели и задачи обеспечения информационной безопасности. Принципы, методы и способы обеспечения информационной безопасности. Концепция информационной безопасности организации (предприятия). Модели безопасности и их применение.

Тема 2.2. Особенности нормативно-правового обеспечения информационной безопасности в государственном секторе и бизнесе.

Нормативно-правовая база обеспечения информационной безопасности организации (предприятия). Закон РФ “О государственной тайне”. Федеральный закон РФ “О коммерческой тайне”.

Лицензирование деятельности в области информационной безопасности, сертификация средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.

Структура внутреннего нормативно-правового обеспечения информационной безопасности в организации. Разрабатываемые в организации документы по вопросам информационной безопасности и требования по их корректировке. Содержание руководства по обеспечению информационной безопасности в организации.

Создание защищенного документооборота в организации.

Тема 2.3. Организация мероприятий по обеспечению информационной безопасности предприятия (фирмы).

Основные этапы процесса организации мероприятий по обеспечению информационной безопасности на предприятии (фирме).

Органы обеспечения информационной безопасности организации (предприятия): состав, структура и функции. Порядок действий должностных лиц по вопросам обеспечения информационной безопасности в различных условиях обстановки.

Тема 2.4. Информационный аудит организации (предприятия).

Организация и проведение анализа информационной уязвимости предприятия (фирмы). Роль и место информационного аудита в ходе комплексного аудита организации (предприятия), в процессе информационной санации. Виды информационного аудита, условия их проведения, содержание и взаимосвязь. Нормативно-правовая база проведения аудита.

Этапы алгоритма анализа и оценки информационных рисков. Основные направления управления рисками.

Тема 2.5. Информационно-технические аспекты обеспечения информационной безопасности.

Демаскирующие признаки информационных объектов. Органы, принципы, методы, способы и средства добывания информации. Технические каналы утечки информации. Способы и средства предотвращения утечки информации.

Угрозы и объекты обеспечения информационно-технической безопасности, принципы, методы и способы ее обеспечения. Технология процесса обеспечения информационно-технической безопасности. Контроль состояния технической защиты информации.

Тема 2.6. Методы, способы и средства защиты информации в автоматизированных информационных системах.

Анализ способов нарушений информационной безопасности в сетях и их таксономия. Способы и средства защиты информации от утечки по техническим каналам в автоматизированных информационных системах. Средства программно-математического и программно-технического воздействия. Виды “вирусов” и защита от них. Использование защищенных компьютерных систем. Системы обнаружения и предотвращения атак. Методы и средства защиты данных, применяемые в сетях. Методы криптографии. Электронная цифровая подпись.

Тема 2.7. Информационно - психологические аспекты обеспечения информационной безопасности.

Теоретические основы межличностной коммуникации, скрытного информационно-психологического управления. Методы и приемы информационно-психологического воздействия на должностных лиц: продуктивного общения, приемы ведения дискуссии, методы и приемы “жесткого” информационно-психологического воздействия. Психологический анализ учебных видеофрагментов. Алгоритмы информационно-психологической защиты: активная защита, пассивная защита.

Формы текущего контроля и промежуточной аттестации:

Форма промежуточной аттестации – экзамен.

В результате освоения дисциплины обучающийся знает, умеет, владеет:

Код этапа освоения компетенции	Результаты обучения
ОПК ОС 1.3	На уровне знаний знать: основные положения теории информационной безопасности (основные понятия и определения, интересы и ценности в области информационной безопасности, основные факторы и угрозы, закономерности и принципы, направления обеспечения информационной безопасности; состав, структуру и основные функции органов обеспечения информационной безопасности организации); основные нормативно-правовые документы Российской Федерации и международного права в изучаемой области.
	На уровне умений уметь: определять интересы и ценности в информационной сфере, ранжировать их по приоритетности; выявлять и оценивать угрозы интересам в информационной сфере при различных условиях обстановки, осуществлять прогноз их развития; принимать управленческие решения по вопросам обеспечения информационной безопасности и реализовывать их на практике.
	На уровне навыков владеть: механизмами принятия решений по обеспечению информационной безопасности в условиях риска и

	<p>неопределенности, вопросах информационно-аналитического обеспечения процессов принятия решений в области информационной безопасности, с существующими и перспективными возможностями по недопущению возникновения и нейтрализации угроз в информационной сфере.</p>
9.3	<p>На уровне знаний знать: основные положения теории информационной безопасности (основные понятия и определения, интересы и ценности в области информационной безопасности, основные факторы и угрозы, закономерности и принципы, направления обеспечения информационной безопасности; состав, структуру и основные функции органов обеспечения информационной безопасности организации); основные нормативно-правовые документы Российской Федерации и международного права в изучаемой области.</p> <p>На уровне умений уметь: определять интересы и ценности в информационной сфере, ранжировать их по приоритетности; выявлять и оценивать угрозы интересам в информационной сфере при различных условиях обстановки, осуществлять прогноз их развития; принимать управленческие решения по вопросам обеспечения информационной безопасности и реализовывать их на практике.</p> <p>На уровне навыков: владеть механизмах принятия решений по обеспечению информационной безопасности в условиях риска и неопределенности, вопросах информационно-аналитического обеспечения процессов принятия решений в области информационной безопасности, с существующими и перспективными возможностями по недопущению возникновения и нейтрализации угроз в информационной сфере.</p>
21.3	<p>На уровне знаний знать: основные положения теории информационной безопасности (основные понятия и определения, интересы и ценности в области информационной безопасности, основные факторы и угрозы, закономерности и принципы, направления обеспечения информационной безопасности; состав, структуру и основные функции органов обеспечения информационной безопасности организации); основные нормативно-правовые документы Российской Федерации и международного права в изучаемой области.</p> <p>На уровне умений: уметь определять интересы и ценности в информационной сфере, ранжировать их по приоритетности; выявлять и оценивать угрозы интересам в информационной сфере при различных условиях обстановки, осуществлять прогноз их развития; принимать управленческие решения по вопросам обеспечения информационной безопасности и реализовывать их на практике.</p> <p>На уровне навыков: владеть навыками применения механизмах принятия решений по обеспечению информационной безопасности в условиях риска и неопределенности, вопросах информационно-аналитического обеспечения процессов принятия решений в области информационной безопасности с существующими и</p>

	перспективными возможностями по недопущению возникновения и нейтрализации угроз в информационной сфере.
--	---

Информационные технологии, программное обеспечение, материально-техническая база, оценочные средства, необходимые для освоения дисциплины, адаптированы для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья.

Основная литература:

1. Мельников, В. П. Информационная безопасность и защита информации: учебное пособие: гриф УМО / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 7-е изд., стер. - М.: Академия, 2012.