

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Безопасность в сетевом обществе

Автор: кандидат социол. наук Магадиев М.Ф.

Код и наименование направления подготовки, профиля:

38.04.04 Государственное и муниципальное управление

Направленность (профиль) Безопасность сферы государственных услуг

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Цель освоения дисциплины:

Формирование у бакалавров основных знаний и понятий в области безопасности в сетевом обществе, ознакомление с современными проблемами информационной безопасности, основными концептуальными положениями системы защиты информации, а также овладение теоретическими знаниями и практическими навыками по использованию современных методов защиты информации в компьютерных системах; изучение опасностей и рисков в процессе жизнедеятельности человека и способов защиты от них в любых средах обитания; изучение комфортных условий жизнедеятельности и методов достижения таких условий, как необходимая предпосылка для эффективной профессиональной деятельности, повышения производительности труда, сохранения здоровья и работоспособности, активного долголетия человека.

План курса:

Тема 1. Безопасность и развитие: сущность, содержание, взаимосвязь.

Взаимосвязанные процессы развития и самосохранения систем различной природы. Понятие опасности и безопасности. Риск как интегральная характеристика опасности. Понятие приемлемого риска. Философское осмысление безопасности и развития. Проблема функционирования и проблема развития. Проблема обеспечения безопасности как проблема развития.

Роль и место безопасности в жизнедеятельности человека и общества. Безопасность в системе «природа-человек-общество». Понятие безопасности жизнедеятельности. Структура безопасности жизнедеятельности. Безопасность существования человека. Современное понимание безопасности. Функции, задачи и содержание обеспечения безопасности. Соотношение процессов обеспечения безопасности и развития.

Тема 2. Угрозы социальной безопасности молодёжи. Концептуальные основы социализации молодёжи в условиях социальной трансформации.

Сущность понятия “угроза”. Источники угроз социальной безопасности молодёжи. Виды угроз безопасности. Классификация угроз безопасности по местонахождению источника опасности, по степени сформированности угрозы, по характеру проявления, по сферам и областям жизнедеятельности, по степени субъективного восприятия. Социально-психологическое «самочувствие» населения и уровень конфликтности общества как индикаторы результативности социальной политики и обеспечения социальной

безопасности личности. Система социальной защиты в обществе и возможности повышения уровня социальной безопасности личности.

Неформальные молодежные объединения и организации. Типы молодежных субкультур по направлениям деятельности; по степени комфортности; по ценностным ориентациям; по принадлежности; по взаимоотношениям; по региональным и национальным различиям. Деструктивные молодежные организации.

Социальные деформации и их источники в трансформирующемся российском обществе. Социально-экономические источники социальных деформаций. Сущность девиантного поведения. Социальный аспект наркомании и алкоголизма. Игромания. Бытовые конфликты. Детская безнадзорность: причины и профилактика.

Образование и социальная культура как основа обеспечения социальной безопасности молодежи. Духовно-нравственное воспитание современной российской молодёжи как фактор противодействия внешним угрозам в условиях обеспечения национальной безопасности.

Тема 3. Источники угроз и рисков информационной безопасности, методы и средства обеспечения информационной безопасности.

Национальные интересы личности, общества и государства в информационной сфере и их обеспечение. Понятие и виды угроз, отраженные в Доктрине информационной безопасности. Основные виды угроз информационно-технического и информационно-психологического характера. Роль СМИ в информационно – психологической борьбе. Технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации. Принципы и методы противодействия несанкционированному информационному воздействию на информационно-коммуникационные системы и системы передачи информации.

Информационное общество и система обеспечения информационной безопасности. Понятие «системы обеспечения информационной безопасности». Основные элементы системы и уровни взаимодействия. Значение государственного и негосударственного секторов в области обеспечения информационной безопасности. Защита личных имущественных и неимущественных прав личности в информационной сфере. Авторское право. Доменные имена: проблемы правового регулирования.

Тема 4. Финансовая безопасность личности, общества, государства в современных условиях.

Финансовая система и финансовые резервы, их значение для сбалансированного развития экономики. Финансовая безопасность, ее сущность. Необходимость финансовой безопасности государства. Система финансовой безопасности. Меры по укреплению финансовой безопасности государства. Безопасность системы налогообложения. Безопасность государственного бюджета. Дефицит государственного бюджета как угроза финансовой безопасности государства. Основные меры по укреплению безопасности государственного бюджета. Безопасность финансово-денежной системы государства и меры по ее обеспечению. Устойчивость банковской системы как фактор обеспечения финансовой безопасности. Инфляционная безопасность и ее обеспечения. Внешний долг как угроза финансовой и экономической безопасности страны. Оценка влияния внутреннего и внешнего долга на финансовую систему страны.

Мошенничество и иные финансовые преступления в сфере денежного обращения. Вывоз (бегство) и ввоз капитала: сущность, масштабы и угрозы. Безработица и финансовые трудности как социальная опасность. Проблема бедности. Потребительский бюджет человека и семьи. Защита от финансовых преступлений.

Финансовый рынок. Валютная безопасность государства и деятельность по ее обеспечению. Конвертируемость национальной валюты как фактор обеспечения финансовой безопасности страны. Безопасность фондового рынка. Основные угрозы безопасности российского фондового рынка. Основные направления деятельности по устранению угроз безопасности фондового рынка в России.

Формы текущего контроля и промежуточной аттестации:

Промежуточная аттестация – зачёт с оценкой; форма текущего контроля – опрос, ситуационные задачи, защита презентаций.

Этапы освоения компетенции:

ОПК-6 – способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности.

На уровне знаний:

- способов и правил использования информационно-коммуникационных технологий для решения профессиональных задач в рамках профессиональной деятельности на основе информационной и библиографической культуры;
- содержание информационных угроз организации / органу власти;
- основных принципов использования информационных баз данных и Интернет-ресурсов для решения стандартных задач профессиональной деятельности с учётом основных требований информационной безопасности;
- роль и место системы обеспечения информационной безопасности в общем процессе функционирования организации / органа власти.

На уровне умений:

- работы с основными пакетами прикладных программ информационно-коммуникационных технологий, используемых для решения стандартных задач в рамках профессиональной деятельности на основе информационной и библиографической культуры;
- применять методы анализа и управления состояниями и процессами информационной безопасности;
- осуществлять аудит угроз информационного характера;
- выявлять и анализировать источники информационных рисков деятельности организации / органа власти.

На уровне навыков:

- использования информационно-коммуникационных технологий для интенсификации процесса получения, обработки и оценки информации в рамках решения стандартных задач профессиональной деятельности с учётом основных требований информационной безопасности;
- обеспечивать цикл управления с помощью средств ИКТ;
- оценки информационных угроз организации / органа власти;
- использования информационно-коммуникационных технологий для повышения эффективности деятельности организации.

ПК-26 – владение навыками сбора, обработки информации и участия в информатизации деятельности соответствующих органов власти и организаций.

На уровне знаний:

- способов и правил использования информационно-коммуникационных технологий для решения задач в рамках профессиональной деятельности, а также участия в информатизации деятельности соответствующих органов власти и организаций;
- корпоративных и информационных систем и баз данных, структуры, принципов работы и основных возможностей ЭВМ;
- содержания информационных угроз организации / органу власти;
- мер противодействия конкурентной разведки конкурентов с использованием информационно-коммуникационных технологий;
- роли и места системы обеспечения информационной безопасности в общем процессе функционирования организации / органа власти.

На уровне умений:

- использования информационных баз данных, электронных библиотек и ресурсов для решения различных задач в рамках профессиональной деятельности с видением их взаимосвязей и перспектив использования;
- применять методы сбора, обработки информации и участия в информатизации деятельности соответствующих органов власти и организаций;
- применения пакетов офисных программ и сетевых технологий для работы с информацией, связанной с профессиональной деятельностью;
- выявлять и анализировать источники информационных рисков деятельности организации / органа власти.

На уровне навыков:

- использования информационно-коммуникационных технологий для интенсификации процесса получения, обработки и оценки информации в рамках решения различных задач профессиональной деятельности;
- сбора и обработки первичной информации о социальных, экономических и политических процессах и явлениях современной российской социально-экономической и общественно-политической действительности;
- обеспечивать цикл управления с помощью средств ИКТ;
- использования информационно-коммуникационных технологий для повышения эффективности деятельности организации.

Основная литература:

1. Аверченков В.И. Организационная защита информации: учебное пособие для вузов 3-е изд., стер. – М.: Флинта, 2018. – <http://www.biblioclub.ru>
2. Данжани Н., Кларк Д. Средства сетевой безопасности / Пер. с англ. – СПб.: КУДИЦ-ПРЕСС, 2017.
3. Колисниченко Д.Н. Анонимность и безопасность в интернете. От чайника к пользователю. – СПб., БХВ-Петербург, 2015.
4. Максим М., Поллино Д. Безопасность беспроводных сетей. – М.: ДМК Пресс, 2008. - <http://www.biblioclub.ru>
5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Учебное пособие. – М.: ДМК-Пресс, 2017.
6. Маньков В.Д. Безопасность общества и человека в современном мире: учебное пособие. – СПб: Политехника, 2015.