АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Информационная безопасность

Автор: преподаватель кафедры теории и систем отраслевого управления Н.И. Пышков

Код и наименование направления подготовки, профиля:
27.03.05 Инноватика, «Технологическое предпринимательство»

Квалификация (степень) выпускника:
Бакалавр

Форма обучения:
Очно-заочная

Цель освоения дисциплины:
Сформировать способность оценивать уровень развития информационной и библиографической культуры и содействовать обеспечению информационной безопасности

План курса:
Тема 1. Информационная безопасность: предмет и содержание

Предмет и задачи теории информационной безопасности. Базовые термины и определения. Объекты защиты и объекты моделирования. Угрозы безопасности: разновидности и классификация. Принципы информационной безопасности. Триада CIA.

Процесс обеспечения защиты информации. Надежность системы безопасности: параметры, характеристики и требования. Уязвимости в защите информационных систем. Системы информационный защиты организации. Политика информационной безопасности. Защита от несанкционированного доступа: идентификация, аутентификация, управление доступом.

Тема 2. Технологии в сфере информационной безопасности

Уязвимости вычислительного оборудования. Методы и средства защиты информации. Криптографическая защита. Числовое программное управление. Управление разработкой ПО. Управление средствами ПО. Аппаратное управление. Программное управление

Модели безопасности: регламенты и критерии определения безопасности. Дискретные модели. Модель Харрисона-Рузо-Ульмана. Модель Белла ЛаПадула. Модель информационных потоков Грэхэма-Деннинга. Модель Биба. Модель Кларка-Уилсона. Модель «Китайской стены».

Криптография. Криптографический анализ: основы. Перестановка, транспозиция и диаграммы. Шифр Виженера. Стандарты DES. Алгоритмы IDEA, CAST и AES. Криптографическая система с открытым ключом. Аутентификация отправителя, Алгоритм RSA. Тенденции развития криптографической защиты. Квантовое шифрование. Блокчейн шифрование. Применение блокчейн-технологий.

Сетевая безопасность. Компьютерные сети: основные понятия. LAN, WAN, DNS-сервер и MAC-адрес. Протоколы TCP/UPD/IP. Сетевая модель OSI. Протоколы IPv4 и IPv6. Протокол UDP. Промежуточное ПО. Технологии VPN и Proxy. Системы IDS, IPS и SEIMs. Разновидности сетевых атак. Тенденции развития сетевой безопасности. Гипервизор. Виртуализация сервисов. Микросегментация сетей. Защищенные облачные вычисления. Модели SaaS, PaaS и IaaS.

Тема 3. Планирование системы информационной безопасности

Процесс планирования безопасности: основные этапы и принципы. Понятие системы информационной безопасности в организации. Основополагающие методы и абстрактные модели контроля доступа. Модели и методы ролевого и сессионного контроля доступа. Вопросы идентификации ролей и сессий. Задачи построения системы защиты информации. Уровни стратегии безопасности. Классы организационных решений в информационной безопасности. Альтернативные методы защиты информации.

Проектирование систем информационной безопасности. Служба информационной безопасности. Определение функциональных задач системы защиты информации. Определение требований к качеству разработки и технического сопровождения системы защиты информации. Экономическое обоснование проектных решений. Оценка производительности системы защиты информации. Эксплуатационное проектирование системы защиты информации. Служба информационной безопасности.

Тема 4. Управление рисками в сфере информационной безопасности

Управление рисками. Модель безопасности с полным перекрытием. Управление информационной безопасностью. Методики построения систем защиты информации. Методики и программные продукты для оценки рисков. Выбор проекта системы обеспечения информационной безопасности. Игровая модель конфликта «защитник-нарушитель».

Оценка рисков организации в сфере информационной безопасности. Снижение риска: методы. Анализ и экспертиза рисков. Оценка затрат и рисков. Модель для оценки стоимости программного обеспечения COBRA. Модель процесса управления рисками.

Тема 5. Руководства и стандарты в сфере информационной безопасности

Процесс построения и оценки систем информационной безопасности. Роль стандартов в безопасности информационных систем. Программное обеспечение для улучшения процессов. Стандарты ISO/IEC 17799/27002 и 27001. Модель SSE-CMM: ключевые конструкции и концепции. Архитектура SSE-CMM. Стандарты «Радужная серия». Общие критерии оценки защищённости информационных технологий (Common Criteria). Критерий оценки безопасности информационных технологий ITSEC. Гармонизация международных и российских стандартов.

Тема 6. Правовое обеспечение информационной безопасности: зарубежная и российская практика.

Зарубежная нормативно-правовая база в сфере информационной безопасности. Акт о компьютерном мошенничестве и злоупотреблении (CFAA). Закон о защите компьютерной информации (CSA). Закон об ответственности и переносе данных о страховании здоровья граждан (HIPAA). Закон Сарбейнса-Оксли (SOX). Федеральный закон об управлении информационной безопасностью (FISMA). Общий регламент по защите данных (GDPR).

Ограничение доступа к информации в целях защиты интересов личности, общества и государства. Правовые режимы тайн в системе организационного и правового обеспечение безопасности информации ограниченного доступа. Правовой режим защиты государственной тайны. Правовой режим коммерческой тайны. Правовой режим обеспечения безопасности персональных данных. Актуальные вопросы режима служебной тайны. Противодействие экстремистской деятельности в информационной сфере. Защита детей от информации, причиняющей вред их здоровью и развитию. Правовые проблемы обеспечения информационной безопасности в сети Интернет.

Тема 7. Нарушения и ответственность в сфере информационной безопасности

Понятие и виды юридической ответственности в области обеспечения информационной безопасности. Субъекты и объекты правоотношений в области обеспечения информационной безопасности. Компьютерная криминалистика: основные положения. Типы и область преступлений. Проблема отсутствия единого юридического пространства в сфере информационной безопасности: «за» и «против». Сбор доказательств в судебном порядке. Комплаенс в сфере информационной безопасности.

Формальная процедура сбора данных. Юридические основы соблюдения формальности процедуры и изъятие доказательств. Актуальные проблемы и угрозы мировой информационной безопасности.

Тема 8. Культура информационной безопасности

Информационное общество. Глобальные проблемы информатизации общества. Информационно-психологическая безопасность и манипулирование. Поведенческие аспекты безопасности информационных систем. Угрозы для сотрудников. Индивидуальная мотивация для предотвращения кибератак. Киберпреступность: преступники и средства массовой информации. Кибершпионаж и отслеживание.

Культура и информационная система безопасности. Понимание концепции культуры безопасности. Лидерство и культура безопасности. Принципы ОЭСР по культуре безопасности. Этические и профессиональные проблемы в управлении безопасностью ИС.

Формы текущего контроля и промежуточной аттестации:

В ходе реализации дисциплины используются следующие методы текущего контроля успеваемости обучающихся:

– при проведении занятий лекционного типа:
опрос, дискуссия;

– при проведении занятий семинарского типа:
контрольная работа, кейс;

- при контроле результатов самостоятельной работы студентов:
решение задач.

Зачет проводится в письменной и устной форме решением кейса.

Основная литература:

1. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: http://www.biblio-online.ru.ezproxy.ranepa.ru:3561/bcode/450371
2. Казарин, О. В. Надежность и безопасность программного обеспечения: учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: http://www.biblio-online.ru.ezproxy.ranepa.ru:3561/bcode/454453