АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

СОВРЕМЕННАЯ ПРАКТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(название дисциплины)

10.04.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

(код направления (специальности) подготовки)

1

(семестр)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- Целями освоения дисциплины «Современная практика информационной безопасности» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.04.01 «Информационная безопасность»; формирование у бакалавров профессиональных навыков по эксплуатации и обслуживанию аппаратуры, оборудования и программного обеспечения, связанных с: -обеспечением безопасности данных; - шифрованием и защитой от несанкционированного доступа; -профессиональных навыков выявления и уничтожения компьютерных вирусов; - противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; -навыков работы со специальной технической литературой; -создание представления о принципах, методах и средствах выявления угроз безопасности информационных систем; - развитие способностей к логическому и алгоритмическому мышлению и осуществлению проверки защищенности объектов на соответствие требованиям нормативных документов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО (ВПО)

- Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.16). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.
- Дисциплина изучается на четвертом курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Основы информационной безопасности», «Аппаратные средства вычислительной техники», «Криптографические методы защиты информации», «Техническая защита информации» по направлению подготовки 10.03.01 «Информационная безопасность», квалификации - бакалавр. Кроме того, для грамотного использования полученных знаний в профессиональной деятельности, требуется изучение курсов «Математика», «Информатика».
- Курс тесно взаимосвязан с другими дисциплинами. Он является полезным для изучения таких дисциплин как «Управление информационной безопасностью», «Организационное и правовое обеспечение информационной безопасности», «Система защиты информации на предприятии», «Защита информации в корпоративных ИС», «Служба информационной безопасности на предприятии».

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

- ПК-1 – способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
- ПК-6 – способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

- Введение (предмет и задачи современной практики информационной безопасности; методы и средства защиты информации и предотвращения несанкционированного доступа)
- Идентификация и аутентификация (идентификация пользователей (субъектов доступа к данным); процедура идентификации и аутентификации; однофакторная и двухфакторная идентификации; биометрические методы идентификации и аутентификации; технологии автоматической идентификации; протоколы идентификации/аутентификации (обобщенный алгоритм, на основе алгоритма RSA, схемы Фейге-Фиата-Шамира, Эль-Гамаля, Шнорра); протоколы идентификации с нулевой передачей знаний; протоколы Kerberos, S/Key (RFC 1760), PAP и CHAP, OpenID, WindowsLive ID, LDAP, OpenLDAP.)
- Системы разграничения доступа к информации (архитектура системы; концепция построения систем разграничения доступа; модели разграничения доступа; надежность систем разграничения доступа)

- Методы и средства защиты программ от компьютерных вирусов (характеристика и классификация компьютерных вирусов; характеристика средств нейтрализации компьютерных вирусов; технологии обнаружения вирусов; антивирусные комплексы; оценка антивирусов; требования к средствам антивирусной защиты ФСТЭК России; классификация методов защиты от компьютерных вирусов)
- Общая характеристика программно-аппаратных средств защиты информации (классификация средств защиты; государственный реестр сертифицированных средств защиты информации; краткая характеристика средства защиты СЗИ SecretNet, ПАК Криптон, HoneypotManager, КИБSearchInform, SecretDisk и т.д.)
- Общая характеристика электронных идентификаторов (идентификаторы eToken, JaCarta, Maxim (iButton), Sentinel, Guardant, Rutoken, CmDongle, WibuKey, SenseLock, LOCK и т.д.)
- Защите программ от программных закладок (способы внедрения закладок; классификация недекларированных возможностей
- программного обеспечения;
- методы вскрытия недекларированных возможностей; подходы выявления дефектов
- в программном обеспечении; возможные методы защиты)
- Методы и способы защиты программ от исследования
- Подходы к защите программ от несанкционированного копирования
- Архитектура СПИБ (конфигурации средств защиты; методы реализации; функционал и особенности использования)

Составитель: доцент кафедры ИЗИ к.т.н. Воронин А.А.
должность, ФИО, подпись

Заведующий кафедрой ИЗИ М.Ю. Монахов
ФИО, подпись

Директор института ИТР А.А. Галкин
ФИО, подпись

Дата, Печать института (факультета)