

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего
образования

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

«Утверждаю»
Директор ИнЭИ
_____ **А. Ю. Невский**

**ПРОГРАММА
ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ
ДЛЯ ПОСТУПАЮЩИХ В МАГИСТРАТУРУ**

Направление подготовки:
10.04.01 - «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Профиль магистерской программы:
«УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

Москва, 2019 год

I. Содержание дисциплин базовой части

1. Теория информационной безопасности и методология защиты информации

1.1. Содержание разделов дисциплины

Значение и цели защиты информации в современной России.

Общая характеристика целей защиты информации. Соответствие целей защиты информации характеру защищаемой информации и характеристикам субъектов информационных отношений. Анализ положений Федерального Закона РФ №149-ФЗ 2006 года «Об информации, информационных технологиях и защите информации»: сфера действия закона, информация как объект правовых отношений, правовая регламентация доступа к информации, государственное регулирование в сфере применения информационных технологий, ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

Угрозы безопасности информации.

Понятие «угроза безопасности информации». Причины возникновения угроз безопасности информации. Классификация и характеристика угроз. Разработка моделей угроз безопасности информации в конкретной организации. Определение актуальности угроз. Ущерб организации в результате реализации угроз безопасности информации. Виды ущерба. Структура прямых и косвенных потерь при реализации угроз безопасности информации.

Уязвимость информации в информационных системах.

Понятие уязвимости информации в информационных системах. Причины возникновения уязвимости информации. Классификация уязвимостей информации. Понятие «утечка информации». Общая характеристика каналов утечки информации из информационных систем. Порядок оценки уязвимости информации в информационных системах.

Риски информационной безопасности.

Понятие «риск информационной безопасности». Менеджмент рисков информационной безопасности на основе положений стандарта ГОСТ Р ИСО/МЭК 27005-2010: задачи системы менеджмента информационной безопасности организации, процесс управления рисками, критерии оценки риска, порядок оценки рисков, технология обработки рисков.

Механизмы защиты государственной тайны.

Правовой режим государственной тайны в соответствии с требованиями Федерального Закона РФ №5485-1 1993 года «О государственной тайне»: сфера действия Закона, отнесение сведений к государственной тайне и их засекречивание, принципы отнесения, степени секретности и грифы.

Перечень сведений, отнесенных к государственной тайне в соответствии с требованиями Указа Президента РФ № 1203 1995 года «Об утверждении Перечня сведений, отнесенных к государственной тайне».

Механизмы защиты, основанные на разделении конфиденциальной информации на виды тайны.

Понятие «коммерческая тайна». Правовой режим коммерческой тайны и порядок его установления в организации на основе требований Федерального Закона

РФ №98-ФЗ 2004 года «О коммерческой тайне»: охрана конфиденциальности информации при осуществлении трудовых отношений, при предоставлении информации, ответственность за нарушения Закона. Основания и методика отнесения сведений к коммерческой тайне на основе требований Указа Президента РФ № 188 1997 года «Об утверждении Перечня сведений конфиденциального характера».

Понятие «служебная тайна» в соответствии с требованиями Указа Президента РФ № 188 1997 года «Об утверждении Перечня сведений конфиденциального характера». Правовой режим «служебной информации ограниченного распространения» в соответствии с Постановлением Правительства РФ №1233 от 3.11.1994 г. «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии» (с изменениями и дополнениями): порядок отнесения сведений, порядок обращения с документами, содержащими служебную информацию ограниченного доступа.

Понятие «персональные данные». Обеспечение безопасности персональных данных граждан РФ в соответствии с требованиями Федерального Закона РФ №152-ФЗ 2006 года «О персональных данных»: сфера действия Закона, обеспечение конфиденциальности персональных данных, специальные категории персональных данных, особенности обработки персональных данных в государственных и муниципальных информационных системах персональных данных, права субъектов и обязанности операторов персональных данных. Структура федеральных органов исполнительной власти, участвующих в организации защиты персональных данных в РФ: ФСТЭК РФ, ФСБ России, Роскомнадзор РФ и выполняемые ими функции.

1.2. Литература

Основная:

1. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности. М.: Изд. «Академия», 2008.
2. Белов Е.Б. Основы защиты информации. М.: Изд. «Горячая линия – Телеком», 2006.

Вспомогательные материалы:

1. Федеральный Закон РФ №5485-1 1993 года «О государственной тайне».
2. Федеральный Закон РФ № 149-ФЗ 2006 года «Об информации, информационных технологиях и защите информации».
3. Федеральный Закон РФ №63-ФЗ 2011 года «Об электронной подписи»:
4. Федеральный Закон РФ № 98-ФЗ 2004 года «О коммерческой тайне».
5. Федеральный Закон РФ № 152-ФЗ 2006 года «О персональных данных».
6. Указ Президента РФ № 1203 1995 года «Об утверждении Перечня сведений, отнесенных к государственной тайне».
7. Указ Президента РФ № 188 1997 года «Об утверждении Перечня сведений конфиденциального характера».

2. Криптографическая защита информации

2.1. Содержание разделов дисциплины

Методы криптографической защиты информации.

Методы криптографического преобразования информации. Классификация и характеристика методов: шифрование, кодирование, стеганография, сжатие информации. Требования к современным методам шифрования: по стойкости, объему шифртекста; времени и стоимости шифрования. Правило Керкхоффа.

Симметричные алгоритмы шифрования.

Модель симметричной криптосистемы. Примеры алгоритмов симметричного шифрования: DES, AES и их основные характеристики. Последовательность и режимы алгоритма симметричного шифрования в соответствии с отечественным стандартом ГОСТ 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Асимметричные алгоритмы шифрования.

Модель асимметричной криптосистемы. Последовательность алгоритма асимметричного шифрования RSA, его основные характеристики. Сравнительный анализ симметричных и асимметричных алгоритмов шифрования.

Электронная подпись.

Порядок практического использования электронной подписи в соответствии с отечественным стандартом ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной подписи»: параметры, формирование и проверка электронной подписи.

2.2. Литература

Основная:

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М.: Изд. «Горячая линия - Телеком», 2005.

2. Хорев П.Б., Методы и средства защиты информации в компьютерных системах. М.: Серия «Учебная литература для ВПО», 2005.

3. Программно-аппаратная защита информации

3.1. Содержание разделов дисциплины

Средства защиты информации, встроенные в системное программное обеспечение.

Общая характеристика системы защиты информации, встроенной в современную операционную систему. Понятие, сущность и общая характеристика процессов аутентификации, авторизации и аудита.

Прикладные программные средства защиты информации.

Межсетевые экраны. Понятие, назначение, принцип действия, перечень выполняемых функций, основы применения и настройки межсетевых экранов. Типы межсетевых экранов и особенности их защитного действия. Программные и программно-аппаратные межсетевые экраны, основные отличия, примеры программной (программно-аппаратной) реализации, преимущества и недостатки.

Средства создания виртуальных частных сетей. Понятие, возможности, принцип действия и область использования технологии VPN. Состав сети и основные функциональные возможности VPN.

Средства предотвращения утечки информации. Понятие и принцип действия DLP-систем. Возможности DLP-систем по предотвращению утечки информации в информационной системе предприятия. Примеры программных решений DLP-систем. Практическая работа по внедрению DLP-системы в информационную систему организации.

Средства защиты от компьютерных вирусов. Понятие компьютерного вируса, классификация и основы деструктивного воздействия. Антивирусная система: понятие, принцип действия, классификация, примеры. Общая характеристика современных методов обнаружения компьютерных вирусов и защиты от них: эвристические методы детектирования вирусов; проактивная защита от вирусов; поведенческий анализатор. Интегрированные антивирусные решения и их общая характеристика: защита от спама, межсетевое экранирование, защита от использования опасных сетевых ресурсов. Организация антивирусной защиты информационной системы предприятия.

Системы резервного копирования.

Понятие системы резервного копирования и требования, предъявляемые к ним. Основы политики резервного копирования. Виды резервирования. Общая характеристика программных и программно-аппаратных средств резервного копирования. Практическая организация резервного копирования в информационной системе организации.

3.2. Литература

Основная:

1. Хорев П.Б. Программно-аппаратная защита информации. - М.: Высшее образование. Инфра-М, 2009.

2. Зайцев А.П., Голубятников И.В. Программно-аппаратные средства обеспечения информационной безопасности. - М.: Машиностроение, 2006.

3. Семенов В. А., Федоров Н. В. Программно-аппаратная защита информации. М.: Изд. Московского государственного индустриального университета, 2007

II. Содержание дисциплин вариативной части

1. Инженерно-техническая защита информации

1.1. Содержание разделов дисциплины

Инженерно-техническая защита территорий и помещений.

Средства предупреждения угроз безопасности: инженерно-технические средства физической защиты, средства контроля и управления доступом. Технические средства обнаружения угроз: средства видеонаблюдения (ССТV) и контроля, охранно-пожарная сигнализация. Технические средства нейтрализации угроз: средства

тревожной сигнализации, средства противопожарной защиты, средства электропитания и освещения.

Защита информации от утечки по техническим каналам.

Классификация, структура и основные характеристики технических каналов утечки информации: оптические, радиоэлектронные, акустические, возникающие при работе вычислительной техники; материально-вещественные. Средства выявления основных технических каналов утечки информации и их характеристика. Средства защиты технических каналов утечки информации и их характеристика: средства пассивной и активной защиты.

Комплекс мероприятий по защите информации от утечки по техническим каналам: специальные проверки технических средств приема, обработки, хранения и передачи информации; специальное обследование защищаемых помещений; специальные исследования технических каналов с использованием контрольно-измерительной аппаратуры.

1.2. Литература

Основная:

1. Халяпин Д.Б. Защита информации. Вас подслушивают? Защищайтесь. М.: Изд. «Школа охраны «Баярд»», 2004.

2. Зайцев А.П. Техническая защита информации. М.: Изд. «Горячая линия-Телеком», 2009.

Программу составили:

Руководитель
магистерской программы
д.т.н., профессор

А.С. Минзов