Годовой спецкурс по выбору кафедры для студентов 2-4 курсов

«Комплексный подход к обеспечению информационной безопасности»

(«Integrated approach to information security enforcement»)

д.ф.-м.н., проф. В. А. Васенин, к.ф.-м.н., с.н.с. А. В. Галатенко,

Форма отчетности: экзамен (в конце года).

Цели дисциплины: дать слушателям представление о современной методологии обеспечения информационной безопасности (ИБ), о роли математических методов и программно-технических средств в обеспечении информационной безопасности; подготовить студентов в области применения методов обеспечения информационной безопасности на этапах проектирования, разработки и эксплуатации сложно организованных компьютерных систем.

Дисциплина базируется на знаниях в области других дисциплин: информатики, программирования, дискретной математики, математической логики, теории вероятностей.

В результате освоения дисциплины обучающийся должен:

- владеть понятийным аппаратом информационной безопасности и знать основные положения методологии комплексного подхода к обеспечению информационной безопасности;
- знать общие положения формирования политики безопасности компьютерной системы;
- владеть навыками применения положений современных нормативных документов и стандартов в области информационной безопасности;
- знать и уметь применять математические методы в обеспечении информационной безопасности, в том числе знать типовые математические модели безопасных информационных систем и уметь строить на их основе модели безопасности компьютерных комплексов;
- знать основные методы криптографии и криптоанализа, применяемые в обеспечении информационной безопасности компьютерных систем;
- знать основные программно-технические методы и программные реализации средств обеспечения информационной безопасности подконтрольных объектов, их роль и место в программной архитектуре компьютерных систем;
- знать основные принципы обеспечения информационной безопасности с позиции технологии программирования, владеть навыками проектирования программных систем защиты и «безопасного» программирования, знать типовые ошибки программирования, приводящие к уязвимостям компьютерным систем, уметь применять методы аудита программного обеспечения для поиска таких уязвимостей.

Первый семестр

Лекция 1. Уровни комплексного подхода к обеспечению ИБ. Законодательные документы и стандарты в области обеспечения ИБ. Административный уровень обеспечения ИБ. Политика информационной безопасности. Операционные меры обеспечения ИБ. Обзор программно-технических мер обеспечения ИБ. Обзор математических методов в ИБ.

Лекция 2. Анализ защищенности. Распространенные угрозы и атаки. Стратегия нарушителя при атаке системы. Учет ресурсов противника и подходы к определению состава и архитектуры системы защиты. Вопросы применения методов анализа рисков. Методы обеспечения высокой доступности.

Лекция 3. Безопасность в терминах доступов. Принцип монитора обращений. Дискреционный принцип разграничения доступа. Матрица доступов. Списки прав доступа. Элементы дискреционного разграничения доступа в операционных системах на примере моделей «Unix permissions» и «POSIX ACLs».

Лекция 4. Безопасность в терминах доступов. Анализ допустимых информационных потоков по модели разграничения доступа. Модель «take-grant».

Лекция 5. Мандатный принцип разграничения доступа. Многоуровневые модели разграничения доступа. Модели разграничения доступа, основанные на решетках. Модель Белла-Лападула. Модель Биба. Модели «Low Watermark» и «High Watermark».

Лекция 6. Ролевые модели разграничения доступа. Ролевые модели разграничения доступа с административными привилегиями. Связь ролевых моделей разграничения доступа с типовыми дискреционными и многоуровневыми моделями.

Лекция 7. Разграничение доступа в операционных системах. Модель «Type Enforcement» и механизм разграничения доступа SELinux. Разграничение доступа в сетевой среде и экранирование.

Лекция 8. Разграничение доступа в системах управления базами данных (СУБД). Место механизмов разграничения доступа в архитектуре типовых систем, использующих СУБД. Пример реализации многоуровневой модели разграничения доступа в реляционной СУБД.

Лекция 9. Математические модели безопасных систем. Скрытые каналы. Модель невлияния в детерминированной постановке.

Второй семестр

Лекция 10. Криптография и криптоанализ. Обзор решаемых задачи и основных методов. Понятия криптографической системы, криптографического алгоритма, криптографического протокола. Методы криптографии с симметричным ключом.

Лекция 11. Методы криптографии с открытым ключом.

Лекция 12. Примеры криптографических систем и протоколов.

Лекция 13. Идентификация и аутентификация. Общие положения создания систем и механизмов идентификации и аутентификации. Реализация устойчивых схем аутентификации.

Лекция 14. Протоколирование и активный аудит. Вероятностные модели и задачи.

Лекция 15. Протоколирование и активный аудит. Детерминированные модели и задачи.

Лекция 16. Информационная безопасность с точки зрения технологии программирования. Распространенные уязвимости программного обеспечения. Подходы к классификации уязвимостей. Основные принципы безопасного программирования.

Лекция 17. Методы обнаружения уязвимостей программного обеспечения.

Лекция 18. Методы верификации программного обеспечения. Часть 1.

Лекция 19. Методы верификации программного обеспечения. Часть 2.

Рекомендуемая литература

1. Основы информационной безопасности: учебное пособие. / В. А. Галатенко. Под редакцией академика РАН В. Б. Бетелина – 4-е изд. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. – 205 с.: ил. – (Серия «Основы информационных технологий»).

2. Теоретические основы компьютерной безопасности: учеб. пособие для студентов высш. учеб. заведений. / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. – М.: Издательский центр «Академия», 2009. – 272 с.

3. Проблемы математического, алгоритмического и программного обеспечения компьютерной безопасности в Интернет. / В. А. Васенин. // Математика и безопасность информационных технологий. Материалы конференции в МГУ 23-24 октября 2003 г. – М: МЦНМО, 2004. – С. 111-141.

4. Критически важные объекты и кибертерроризм. Часть 1. Системный подход к организации противодействия. / О. О. Андреев и др. Под ред. В. А. Васенина. М.: МЦНМО, 2008. – 398 с.

5. Критически важные объекты и кибертерроризм. Часть 2. Аспекты программной реализации средств противодействия. / О. О. Андреев и др. Под ред. В. А. Васенина. М.: МЦНМО, 2008. – 607 с.

6. Б. Шнайер. Прикладная криптография: протоколы, алгоритмы и исходные тексты на языке С. 2-е изд. / Под редакцией П. В. Семьянова. – М.: Триумф, 2002.

7. Методы дискретной математики в криптологии. / В. М. Фомичев. – М. Диалог-МИФИ, 2010. – 424 с.