МИНОБРНАУКИ РОССИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«Санкт-Петербургский политехнический университет Петра Великого»

ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

УТВЕРЖДАЮ:
Проректор по образовательной
деятельности
Е.М. Разинкина
«30» сентября 2019 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА СПЕЦИАЛЬНАЯ ДИСЦИПЛИНА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ

10.06.01 – Информационная безопасность

Направленность (профиль):

1. Методы и системы защиты информации, информационная безопасность

Директор
Института прикладной математики и механики М.Е. Фролов

Руководитель основных
образовательных программ ИПММ Е.Ю. Павленко

г. Санкт-Петербург
2019

ВВЕДЕНИЕ

Программа вступительного экзамена в аспирантуру по направлению 10.06.01 «Методы и системы защиты информации, информационная безопасность» включает в себя перечень выносимых на экзамены вопросов и список рекомендуемой литературы по профилю:

1. Методы и системы защиты информации, информационная безопасность

На вступительном экзамене в аспирантуру по направлению 10.06.01 «Методы и системы защиты информации, информационная безопасность» соискатель должен продемонстрировать владение категориальным аппаратом по направлению и выбранному профилю, знание основных теорий и концепций разделов по учебным планам по профильным программам магистерской подготовки.

Соискатель также должен показать умение использовать теории и методы информационной науки для анализа современных IT-проблем

Целью подготовки аспирантов по направлению 10.06.01 «Методы и системы защиты информации, информационная безопасность» является обеспечение различных сфер экономики РФ научными и научно-педагогическими кадрами, а также высококвалифицированными специалистами, владеющими современными научными методами анализа и принятия управленческих решений в области IT-технологий.

Основу настоящей программы составили ключевые положения специальных дисциплин учебных планов подготовки магистров и специалистов по соответствующим программам по направлению 10.03.01 «Информационная безопасность», 10.05.01 «Компьютерная безопасность», 10.05.03 «Информационная безопасность автоматизированных систем», 10.05.04 «Информационно-аналитические системы безопасности».

Методы и системы защиты информации, информационная безопасность

Теоретические вопросы безопасности компьютерных систем

1.Современное состояние проблемы информационной безопасности. Причины нарушения безопасности. Основные направления создания информационных систем.

2.Политика безопасности. Неформальное и формальное описание политики безопасности. Понятие монитора безопасности пересылок. ТСВ системы. Пример ТСВ системы.

3.Модели дискреционного доступа. Матрица доступа. Пятимерное пространство безопасности Хартстона. Модель Харрисона-Руззо-Ульмана. Способы реализации системы распространения прав.

4.Троянские кони. Уровни безопасности. Секретность и степень доверия. Мандатная модель доступа. Модель Белла и Лападула. Критика модели Белла и Лападула.

5.Информационные модели. Модели невыводимости и невмешательства. Вероятностные модели. Модель системы безопасности с полным перекрытием. Базовая система безопасности Клеменса.

6.Модель Биба и ее вариации. Объединение модели Белла и Лападула с моделью Биба. Модель Кларка-Вилсона. Объединение модели Кларка-Вилсона с моделью Биба.

7.Модели защиты от угрозы отказа в обслуживании. Мандатная модель защиты от угрозы отказа в обслуживании. Модель Миллена распределения ресурсов.

8.Сравнение выразительной мощности моделей контроля доступа.

9.Подсистема идентификации - аутентификации. Подсистема аудита и подсистема обнаружения нарушителя.

Операционные системы и их защита. Функции и основные понятия.

1.Процессы и потоки. Межпроцессное взаимодействие. Распределение времени процессора.

2.Управление памятью. Сегментация и страничная организация памяти. Виртуальная память. Адресное пространство задачи. Ресурсы. Совместное использование ресурсов.

3.Защита в операционной системе. Проблемы внедрения политики безопасности. Требования к подсистеме взаимодействия с ресурсами для корректного внедрения абстрактной модели безопасности.

4.Достоинства и недостатки микроядерных операционных систем.

5.Аппаратные средства защиты современных процессоров и материнских плат.

6.Состав и правила взаимодействия компонент в подсистеме обеспечения безопасности.

7.Современные типы операционных систем, преимущества и недостатки различных подходов к построению ОС.

8.Эталонная модель взаимодействия открытых систем. Основные службы и протоколы вычислительных сетей.

9.Типовые удаленные воздействия на распределенные вычислительные системы, понятие удаленной атаки. Причины успеха удаленных воздействий на распределенные вычислительные системы

10.Принципы создания защищенных систем связи в распределенных вычислительных системах.

11.Типовая структура подсистемы безопасности ОС и выполняемые ей функции; идентификация и аутентификация, разграничение доступа, аудит, подотчетность действий, повторное использование объектов, точность и надежность обслуживания, защита обмена данных; реализация подсистем безопасности; средства обеспечения безопасности ОС семейств UNIX, Windows и Linux; домены безопасности; критерии защищенности ОС; средства защиты от атак переполнения буфера.

12.Технология виртуализации операционных систем, классификация и особенности. Архитектура гипервизоров и особенности их защиты.

Защита программ и данных

1.Программно-аппаратные средства защиты ПЭВМ; методы и средства ограничения доступа к компонентам ЭВМ; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; защита программ от изучения; защита от разрушающих программных воздействий; защита от изменения и контроль целостности; методы обфускации программ; применение аппаратных средств для защиты программ и данных.

Вычислительные сети

1.Задачи и проблемы распределенной обработки данных; классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей; основы организации и функционирования сетей; сетевые операционные системы; основные сетевые стандарты; средства взаимодействия процессов в сетях; распределенная обработка информации в системах клиент-сервер; одноранговые сети; средства идентификации и аутентификации; средства повышения надежности функционирования сетей; интеграция локальных сетей в региональные и глобальные сети; неоднородные вычислительные сети; организация сетей на базе операционных систем UNIX, Windows и Linux; глобальные сети: Internet, основные службы и предоставляемые услуги, стандарты, перспективы развития; организация корпоративных сетей интранет.

2.Защита в сетях. Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях; протоколы аутентификации при удаленном доступе; средства и методы обеспечения целостности и конфиденциальности; защита серверов и рабочих станций; средства защиты локальных сетей при подключении к Интернет; межсетевые экраны; системы обнаружения и предупреждения вторжений, виртуальные защищенные сети, защита виртуальных локальных сетей.

3.Облачные вычисления, организация внутренней инфраструктуры систем облачных вычислений, использование традиционных средств защиты для систем облачных вычислений, безопасность средств виртуализации. Специфика построения грид-систем и особенности их защиты.

4.Основные сетевые атаки. Классическая модель системы обнаружения вторжений (СОВ). Требования к СОВ. Модель СОВ как системы распознавания образов. Байесовская модель обнаружения вторжений. Информационные преобразования в СОВ. ROC-анализ.

5.Сигнатурный метод обнаружения атак. Свойства сигнатур. Методы обнаружения сигнатур. Системы автоматического создания сигнатур. Модуль сбора данных. Сетевые и хостовые системы. Методы выявления аномалий. Применение методов Data Mining для выявления аномалий.

Защита в СУБД

1.Средства обеспечения защиты информации в СУБД; средства идентификации и аутентификации объектов баз данных, управление доступом; средства контроля целостности информации, организация аудита; типы контроля безопасности: потоковый, контроль вывода, контроль доступа; многоуровневая защита; модели безопасности, применяемые при построении защиты в СУБД; использование транзакции для

изолирования действий пользователей; блокировки; ссылочная целостность; триггерная и событийная реализация правил безопасности; причины, виды, основные методы нарушения конфиденциальности в СУБД; получение несанкционированного доступа к конфиденциальной информации путем логических выводов.

Криптографические методы защиты информации

1.Понятия алгоритма и исчисления. Сложность алгоритма. Основные алгебраические структуры: группа, кольцо, поле. Гомоморфизмы групп и колец. Идеалы и классы вычетов. Кольцо полиномов Жегалкина. Простые поля. Расширения полей. Конечные поля. Квадратичные вычеты и невычеты. Квадратичный закон взаимности. Модульное умножение. Проверка чисел и полиномов на простоту. Умножение с помощью быстрого преобразования Фурье. Эллиптические кривые. Аффинная и проективная плоскость. Закон сложения точек эллиптической кривой. Гомоморфизмы эллиптических кривых. Дивизоры и якобиан гиперэллиптической кривой. Порядок якобиана.

2.Понятие стойкости криптографических алгоритмов. Симметричное и несимметричное шифрование. Цифровая подпись. Задачи, положенные в основу безопасности криптографических алгоритмов (задача о выполнимости, разложение на множители, дискретное логарифмирование в конечном поле и на эллиптической кривой).

3.Криптографические протоколы и методы их анализа. Протокол Диффи–Хеллмана. Протоколы шифрования с открытым ключом и цифровой подписи RSA и Эль-Гамаля, их безопасность. Генераторы псевдослучайных последовательностей. Доказательства с нулевым разглашением. Протоколы управления ключами. Отечественные стандарты криптографической защиты информации.

4.Основные положения теории секретности Шеннона. Объем текстов, однозначно определяющих ключ. Аффинно эквивалентные булевы функции и подстановки. Алгебраические и статистические методы криптоанализа. Выбор подстановок для шифров.

Управление информационной безопасностью

1.Проблема защиты информации в условиях информационного конфликта: понятия информационного оружия, информационного конфликта, формы информационного воздействия. Угрозы безопасности. Классификация источников, характеров и механизмов угроз. Классификация уязвимостей и мер защиты.

2.Современные технологии защиты ресурсов от программных атак. Комплекс средств защиты и управления безопасностью. Задача управления безопасностью. Обобщенная структура системы управления защитой информации, ее компоненты. Элементы теории управления информационной безопасностью.

3.Цикл управления безопасностью: анализ систем, реализация, контроль, оценка безопасности. Непрерывность обеспечения безопасности.

4.Управление рисками информационной безопасности. Этапы процесса управления рисками. Оценка рисков. Определение уязвимостей. Определение рисков. Качественные и количественные методы.

5.Общая модель управления безопасностью. Макропроцессы управления: планирование, кратко-, средне-, долгосрочное управление, оценка безопасности. Поиск оптимального решения проблемы безопасности. Методы оптимизации управленческих решений. Контроль защищенности информации, контроль функционирования механизмов защиты. Адаптивные модели и саморегулирующиеся модели. Динамические методы и алгоритмы противодействия и предупреждения НСД. Контроль целостности информационных систем с помощью модельного анализа настроек безопасности.

Литература

1. Блэк У. Интернет: протоколы безопасности. Учебный курс. Спб.: Питер, 2001.
2. Введение в криптографию / Под общ. ред.В.В. Ященко. М.: МЦНМО-ЧеРо, 2000.
3. Гарсиа-Молина Г., Ульман Д.Д., Уидом Д. Системы баз данных. М., 2003.
4. Городецкий А.Е., Тарасова И.Л. Управление и нейронные сети. СПб.: Изд-во СПбГПУ, 2005.
5. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. М. Горячая линия-Телеком, 2011.
6. Запечников С.В., Милославская Н.Г, Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем: Учеб. для вузов. В 2-х тт. М.: Горячая линия – Телеком, 2006.
7. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем: Учебное пособие. М.: Горячая линия-Телеком, 2000.
8. Зегжда Д.П., Калинин М.О., Безопасность операционных систем. Модели контроля и управления доступом (в 2-х частях), 2002/2003.
9. Зегжда Д.П., Никольский А.В. Безопасность современных высокопроизводительных систем. Часть 1. Безопасность облачных вычислений. Учебное пособие. 2013.
10. Зегжда П.Д., Калинин М.О. Управление безопасностью компьютерных систем. 2012.
11. Касперски К. Компьютерные вирусы изнутри и снаружи. М.[и др.]: Питер, 2007.
12. Корт С.С. Теоретические основы защиты информации. М. Гелиос АРВ, 2004.
13. Олифер В., Олифер Н. Сетевые операционные системы. СПб. Питер, 2009.
14. Платонов В.В. Программно-аппаратные средства защиты информации: учебник. 2013.
15. Ростовцев А.Г. Алгебра и теория чисел. СПб. Изд-во Политехн. ун-та, 2011.
16. Ростовцев А.Г. Эллиптические кривые в криптографии. Теория и вычислительные алгоритмы. СПб.: АНО «Профессионал», 2010.
17. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. СПб.: АНО «Профессионал», 2005.
18. Столингс В. Основы защиты сетей. Приложения и стандарты: Пер. с англ. М.: Изд. Дом «Вильямс», 2002.
19. Ховард М., Леблан Д. Защищенный код: пер. с англ. М.: Рус. ред., 2004.