НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
МОСКОВСКИЙ ИНСТИТУТ ЭЛЕКТРОНИКИ И МАТЕМАТИКИ

«Утверждаю»
Заместитель директора
МИЭМ по учебной работе

_____ С.Р. Тумковский

«___» _____ 2022 г.

ПРОГРАММА
государственного экзамена
по специальности 10.05.01 - «Компьютерная безопасность»

Раздел 1. Теоретические основы защиты информации

1. *Основные принципы современной концепции обеспечения защиты информации*. Исходные предположения о возможностях злоумышленника. Требования к защите с позиции пользователя. Основные методы защиты.
2. *Роль законодательного и организационного обеспечения защиты информации*. Законы Российской Федерации, составляющие основу правовой базы защиты информации в стране. Особенности российского законодательства в части защиты государственной тайны, коммерческой тайны и авторских прав. Порядок лицензирования и сертификации деятельности в области защиты информации.
3. *Основные элементы теории компьютерной безопасности.* Проблема построения защищенной КС. Модели ценности информации: аддитивная модель, порядковая шкала, решетка многоуровневой безопасности. Методы аппаратной защиты от несанкционированного доступа. Доверенная загрузка и контроль защищенности. Примеры аппаратных средств защиты. Технологии аутентификации. Парольные системы. Выбор, хранение, передача паролей по сети.
4. *Математические модели формальной теории защиты информации*. Угрозы информации и политика безопасности. Классификация систем защиты. Стандарты в области защиты информации в вычислительной системе, «Оранжевая книга» США, российские стандарты. Расширенная модель Take-Grant. Классическая модель Белла-Ла Падулы. Субъектно-ориентированная модель изолированной программной среды (ИПС). Объекты, функционально ассоциированные с субъектами. Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ).
5. *Криптографические методы защиты информации*. Основные понятия криптографии. Исторические шифры. Теоретическая, практическая и временная стойкость системы криптографической защиты. Криптографические параметры узлов и блоков шифрующих автоматов. Методы получения псевдослучайных последовательностей. Генераторы псевдослучайных последовательностей и их свойства. Современные поточные и блочные алгоритмы шифрования. Системы ассиметричного шифрования, открытый ключ, электронная подпись. Вопросы генерации и распределения ключей. Атаки на криптографические алгоритмы: алгоритмические, алгебраические, статистические. Методология обоснования надежность криптографической защиты.
6. *Криптографические протоколы*. Криптографические протоколы с использованием симметричного и асимметричного шифрования. Криптографические протоколы с использованием цифровой подписи. Криптографические протоколы генерации и распределения ключей. Протоколы разделения секрета и доказательства без разглашения. Протокол подбрасывания монеты по телефону.
7. *Теоретико-числовые методы в криптографии*. Оценка сложности арифметических операций. Непрерывные дроби и их свойства, квадратичные вычеты, асимптотический закон распределения простых чисел. Арифметические алгоритмы, (вычисление НОД, Символа Якоби), решение квадратных уравнений в конечных простых полях, алгоритмы построения

и проверки простоты чисел, алгоритмы факторизации и дискретного логарифмирования. Криптосистема RSA, выбор параметров и взаимосвязь между ними.

8. *Программно-аппаратные средства обеспечения информационной безопасности*. 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. Средства обеспечения безопасности в ОС семейств Windows и UNIX, критерии защищенности ОС. Средства обеспечения безопасности в сетях. Протоколы аутентификации при удаленном доступе. Средства защиты серверов и рабочих станций. Средства защиты локальных сетей при подключении к Internet. Межсетевые экраны, электронные замки, криптофильтры, криптороутеры. Области применения, достоинства, недостатки, реализуемые политики безопасности. Методы оценки качества применяемых средств защиты. Методы и средства защиты информации в СУБД. Средства идентификации и аутентификации, управление доступом, средства контроля, аудит безопасности. Критерии защищенности БД и АИС. Методы и системы обнаружения компьютерных атак. Экспресс-анализ защищенности сетевого компьютера от удаленных атак через сеть.
9. Протоколы аутентификации при удаленном доступе. Протоколы семейства TLS, протокол SSH, область применения, методы оценки безопасности. Протокол SESPAKE выработки общего ключа на основе пароля, область его применения, принципы обоснования сложности перебора паролей. Протокол защищенного взаимодействия SP-FIOT. Обоснование свойств безопасности, отличия от других протоколов. Криптографические механизмы протокола IPSec, обеспечиваемые им свойства безопасности.
10. *Защита информации от технической разведки*. Основные физические каналы утечки информации о функционировании информационной системы. Узлы и блоки оборудования информационной системы, уязвимые для технической разведки. Технические параметры современных средств перехвата побочных сигналов. Математические модели побочных каналов утечки. Выделение полезных сигналов на фоне помех. Методы и средства защиты от инженерно-технической разведки. Методика оценки качества инженерно-технической защиты.
11. *Особенности защиты информации в вычислительной системе*. Перечень типовых угроз вычислительной системе со стороны потенциального злоумышленника. Основные принципы защиты вычислительной системы от несанкционированного доступа (проверка полномочий, разграничение доступа, аудит). Защита информации в локальных и глобальных вычислительных сетях и ее особенности. Роль и задачи администратора вычислительной системы и службы безопасности.
12. *Разрушающие программные воздействия*. Компьютерные вирусы как особый класс разрушающих программных воздействий. Классификация вирусов. Методы выявления и защиты от вирусов. Изолированные программные среды. Защита программных продуктов от изменения и контроль целостности, защита от изучения.
13. *Методика анализа программных реализаций алгоритмов защиты информации*. Методы восстановления алгоритмов защиты в программных продуктах. Оценка уровня криптографической защиты типовых программных продуктов. Анализ особенностей выработки и распределения ключей. Анализ возможности внедрения криптографических закладок.

Раздел 2. Теория вероятностей и математическая статистика

1. Вероятность: аксиомы и свойства (дискретный, абсолютно-непрерывный и общий случаи).
2. Случайные величины и их характеристики: определение, свойства (дискретный, абсолютно-непрерывный и общий случаи, функции распределения, моменты).
3. Основные вероятностные распределения, их свойства (нормальное, биномиальное, экспоненциальное, пуассоновское, связь между ними)

4. Предельные теоремы: закон больших чисел, теоремы Хинчина, Чебышева; усиленный закон больших чисел, теорема Колмогорова; центральная предельная теорема, теорема Муавра-Лапласа.
5. Характеристические функции, их свойства, связь с моментами.
6. Выборка, эмпирическая функция распределения, гистограмма.
7. Критерии отношения правдоподобия, его основные асимптотические свойства, его связь с критерием хи-квадрат для полиномиального распределения.
8. Лемма Неймана-Пирсона; равномерно наиболее мощные (р.н.м.) критерии для моделей с монотонным отношением правдоподобия в случае односторонних гипотез; двусторонние гипотезы, несмещенные критерии для них.
9. Критерии согласия Колмогорова, хи-квадрат, Смирнова и др. для гипотез о виде распределения, односторонности, независимости, случайности.
10. Доверительные интервалы (д.и.) и множества, построение д.и. с помощью центральной статистики, примеры; асимптотические д.и.
11. Случайные подстановки, методы генерации. Циклы в случайных подстановках, распределение числа циклов.
12. Элементы теории случайных процессов. Марковский, винеровский, пуассоновский процессы и их свойства.
13. Применение вероятностных методов в теории защиты информации: построение вероятностных моделей процессов, возникающих в задачах защиты информации, проверка качества псевдослучайных последовательностей и др.

Раздел 3. Алгебра.

1. Группа, подгруппа, нормальный делитель, фактор-группа. Циклическая группа; абелева группа (определения, примеры), гомоморфизм групп. Группа подстановок.
2. Идеал кольца, гомоморфизм колец, кольцо многочленов, разложение на множители, интерполяционная формула Лагранжа. Разложение кольца вычетов по заданному модулю в прямую сумму колец.
3. Простое поле, расширение поля, примитивный элемент конечного поля, описание множества примитивных элементов через степени одного из них. Алгоритмы построения примитивных элементов. «Китайская» теорема об остатках, методы разложения многочленов на неприводимые множители.
4. Линейные рекуррентные последовательности над конечным полем. Характеристический и минимальный многочлен, сопровождающая матрица. Оценка длины периода.
5. Применение алгебраических методов в задачах защиты информации.

Раздел 4. Основы теории чисел

1. Понятие эвклидового кольца. Примеры эвклидовых колец.
2. Понятие наибольшего общего делителя. Алгоритм Эвклида. Оценка алгоритмической сложности алгоритма Эвклида.
3. Простые числа. Основная теорема арифметики. Примеры колец, в которых теорема не верна. Элементарные алгоритмы разложения чисел на множители.
4. Методы доказательства простоты целого числа.
5. Целостные кольца. Кольцо классов вычетов. Примеры конечных и бесконечных колец классов вычетов.
6. Решение уравнений первой степени в кольцах вычетов. Расширенный алгоритм Эвклида. Китайская теорема об остатках.
7. Понятие показателя элемента. Функция и критерий Эйлера. Понятие примитивного элемента. Примеры
8. Алгоритмы поиска корней многочленов старших степеней.
9. Понятие цепной и подходящих дробей. Вычисление действительных чисел с заданной точностью.

Раздел 5. Основы дискретной математики

1. Перечислительная комбинаторика, сочетания, размещения, перестановки
2. Подстановки и их свойства, циклы подстановок. Применение в задачах защиты информации.
3. Автоматы, определения, свойства. Применение в задачах защиты информации
4. Латинские квадраты и конфигурации. Композиции
5. Задачи линейного программирования и оптимального квадратичного назначения

Раздел 6. Теория информации и кодирование

1. Основы теории информации. Аксиоматика Хинчина и Фаддеева. Энтропия вероятностной схемы, условная энтропия, взаимная информация. Энтропия источника сообщений. Применение в задачах защиты информации.
2. Математические модели источника сообщений. Марковские, стационарные, эргодические источники и источники без памяти. Методы вычисления энтропии указанных источников.
3. Первая теорема Шеннона для дискретных источников без памяти. Следствие. Вторая теорема Шеннона для дискретных источников без памяти (без доказательства). Практические приложения.
4. Основы теории кодирования. Кодирование дискретных источников сообщений. Алгоритмы построения префиксных кодов. Алгоритм Фано и его свойства, алгоритм Шеннона, доказательство его корректности, алгоритм Хаффмана. Примеры.
5. Основные свойства и параметры кодов. Теорема о верхней и нижней оценке средней длины префиксного кода.
6. Коды, исправляющие ошибки. Процедура декодирования с помощью таблицы стандартного расположения. Понятие синдрома вектора. Основные свойства. Декодирование с помощью синдромов. Декодирование по методу максимума правдоподобия.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА.

1. Кабанов А.С., Лось А.Б., Першаков А.С., Теоретические основы компьютерной безопасности, Учебное пособие, М: РИО МИЭМ, 2012 г.
2. Лось А.Б., Нестеренко А.Ю., Рожков М.И.. Криптографические методы защиты информации — 2-е изд., испр. — М.: Издательство Юрайт, 2021. — 473 с. — Серия: Бакалавр. Академический курс.
3. Шелухин О.И., Сакалема Д.Ж., А.С. Филинова, Обнаружение вторжений в компьютерные сети, М., Горячая линия – Телеком, 2013, 220 с.
4. Девянин П.Н., Ивашко А.М., Першаков А.С., Проскурин В.Г., Черемушкин А.В Программно - аппаратные средства защиты от НСД к компьютерным криптографическим системам обработки информации (учебное пособие), МИЭМ, 2003.
5. Проскурин В.Г., Защита программ и данных, ИД «Академия», 2011 г.
6. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2005.
7 . Духин А.А. Теория информации (учебное пособие), МИЭМ, 2005 г.
8. Зубов А.Ю. Математика кодов аутентификации // М.: Гелиос АРВ, 2007.
9. Законы РФ «О государственной тайне», «Об информации, информационных технологиях и защите информации», «О стандартизации». Положения о лицензировании ФСБ и ФСТЭК.
10. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем, М: горячая линия – Телеком, 2000 г.
11. Девянин П.Н. Модели безопасности компьютерных систем. – М.: Издательский центр «Академия», 2005.
12. Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004.

13. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008.
14. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему? / Под ред. Д.П. Зегжды и В.В. Платонова. – СПб: Мир и семья, 1997.
15. Мамаев М., Петренко С. Технология защиты информации в Интернете. Специальный справочник. – СПб: Питер, 2002.
18. Петраков А.В. Основы практической защиты информации. – М.: Радио и связь. 2000.
19. Петров А.А. Компьютерная безопасность. криптографические методы защиты. – М.: ДМК, 2000.
20. Трубачев А.П., Егоркин И.В. Общие критерии оценки безопасности информационных технологий. История вопроса // «Защита информации. Конфидент», №2, 2002.

Порядок проведения государственного экзамена в 2022 году.

В соответствии с учебным планом образовательной программы «Компьютерная безопасность», государственный экзамен по данной программе проводится на 6 курсе после окончания преддипломной практики на последней неделе октября 2022 года.

Для сдачи экзамена допускаются студенты 6 курса, не имеющие академических задолженностей к моменту его проведения.

Государственный экзамен проводится в устной форме, для его проведения из числа членов государственной комиссии организуются 4 локальные комиссии, в каждой из которых принимает участие не менее 3 членов комиссии.

В экзаменационном билете сформулированы два теоретических вопроса и указывается номер комиссии для ответа студента.

Объявление итоговых оценок проводится по завершении процедуры экзамена и обсуждении их всеми членами комиссии.

В процессе подготовки к экзамену студентам запрещено пользоваться литературой, конспектами, любыми электронными устройствами.

Процедура проведения государственного экзамена фиксируется на видеокамеру, соответствующие записи хранятся на кафедре Компьютерной безопасности не менее 3 лет.

Программа государственного экзамена и порядок его проведения в 2022 году утверждены на заседании кафедры «Компьютерная безопасность» 30 августа 2022 г., протокол № 6.

Формула оценивания и формирования итоговой оценки:

Q = 0.5 (оценка за первый вопрос билета) + 0,5 (оценка за второй вопрос билета).

Правила округления для формирования итоговой оценки: округление происходит на конечном этапе, путем отбрасывания дробной части.

Заведующий кафедрой
«Компьютерная безопасность А.Б. Лось

30. 08. 2022 г.