Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный университет имени М.В.Ломоносова»
механико-математический факультет

УТВЕРЖДАЮ

Декан механико-математического
факультета, д.ф.-м.н.,
член-корр. РАН, профессор

_____/*А.И. Шафаревич*/

«30» сентября 2022 г.

ВРЕМЕННАЯ ПРОГРАММА-МИНИМУМ

кандидатского экзамена по специальности

2.3.6 Методы и системы защиты информации, информационная безопасность

Шифр и наименование области науки: 2.3. Информационные технологии и телекоммуникации

Наименование отраслей науки,

по которым присуждаются ученые степени: физико-математические науки

Рабочая программа утверждена
Ученым советом факультета
(протокол № 6 от 30 сентября 2022 г.)

Москва 2022

I. Описание программы:

Настоящая программа охватывает основополагающие разделы и области знания, в основе данной программы лежат следующие дисциплины: информационная безопасность и защита информации, а также смежные науки, включая алгебру, дискретную математику, теорию сложности, теорию алгоритмов, теорию автоматов, комбинаторику, теорию дискретных функций, математическую логику, теорию формальных языков, теорию вероятностей и математическую статистику.

II. Основные разделы и вопросы к экзамену:

Математические основы защиты информации

Алгебра логики. Функции алгебры логики. Задание функций таблицами истинности и формулами. Операция суперпозиции. Замыкание и замкнутые классы. Теорема Поста о полноте.

Теория автоматов. Понятие конечного абстрактного автомата. Отличимость состояний. Теоремы Мура об отличимости состояний. Регулярные и представимые множества. Теорема Клини. Связь сложности регулярных выражений и автоматов. Проблема экспоненциального взрыва. Понятие структурного автомата. Конечные полные системы относительно операции суперпозиции.

Схемы из функциональных элементов. Понятие схемы из функциональных элементов. Сложность и глубина схемы. Необходимое и достаточное условие полноты. Асимптотика функции Шеннона сложности и глубины схемы.

Теория алгоритмов. Понятие машины Тьюринга. Тезис Тьюринга. Существование универсальной машины Тьюринга. Теорема о структурном программировании. Теорема Райса. Понятие сложности вычисления. Классы сложности P, NP, BPP. Понятия сводимости и полноты. NP-полные задачи. Теорема Кука. Тезис Эдмондса (полиномиальный тезис Тьюринга).

Основы информационной безопасности

Основные понятия и подходы к защите ресурсов информационных систем. Информационная безопасность как наука, изучающая методы и средства защиты информационно-вычислительных систем и сетевых структур от деструктивных воздействий на их ресурсы, от использования таких систем и структур в целях, не совместимых с безопасностью личности, общества и государства. Основные составляющие информационной безопасности. Основные определения и подходы к классификации угроз безопасности информации. Примеры угроз доступности, целостности и конфиденциальности в информационных системах. Понятие о модели нарушителя. Подходы к

обеспечению информационной безопасности. Подходы к обеспечению безопасности объектов критически важных информационных инфраструктур. Комплексный подход. Объектно-ориентированный подход. Уровни комплексного подхода к обеспечению информационной безопасности. Основные понятия управления рисками информационной безопасности.

Законодательные и правовые основы защиты компьютерной информации и информационных технологий. Содержание и роль законодательного уровня обеспечения информационной безопасности. Анализ российского законодательства в области информационной безопасности; сравнение с зарубежным законодательством. Отдельные аспекты, рассматриваемые в законодательстве и связанные с обеспечением информационной безопасности: информация и доступ к ней; безопасность личности, общества и государства; информация ограниченного доступа и законодательно определенные виды тайн; персональные данные; интеллектуальная собственность; связь и передача информации; средства массовой информации; информационные технологии; информационные системы; защита информации; электронная подпись; техническое регулирование; лицензирование деятельности, связанной с информационной безопасностью; правонарушения, связанные с информационной безопасностью, неправомерное использование информации.

Нормативно-методические основы защиты информации. История отечественных, зарубежных и международных стандартов и руководящих документов в области информационной безопасности. Оценочные стандарты. Технические спецификации и рекомендации, связанные с информационной безопасностью. Стандарты в области организации и управления обеспечением информационной безопасности.

Содержание системы средств защиты компьютерной информации в информационных системах. Защищенная информационная система и система защиты информации; принципы построения систем защиты информации и их основы; законодательная, нормативно-методическая и научная база системы защиты информации.

Основные понятия административного уровня обеспечения информационной безопасности. Политика безопасности. Программа безопасности. Обеспечение информационной безопасность и жизненный цикл информационной системы. Особенности управления рисками информационной безопасности на административном уровне. Понятие об анализе защищенности.

Основные понятия процедурного уровня обеспечения информационной безопасности. Меры процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.

Основные понятия программно-технического уровня обеспечения информационной безопасности. Состав основных программно-технических мер, методов и средств защиты информации. Понятие об архитектурной безопасности.

Теоретические основы криптографии

Математические основы криптографии. Теория информации. Энтропия по Шеннону. Понятия информации, взаимной информации, условной энтропии.

Основные понятия криптографии. Три задачи криптографии: конфиденциальность, целостность, неотслеживаемость (на примерах). Понятие о криптографических системах, криптографических протоколах и криптографических примитивах. Модель противника. Атаки, угрозы, стойкость (на примерах).

Теоретическая криптография. Теория Шеннона секретной связи. Модель системы секретной связи. Неоднозначность ключа. Расстояние единственности. Идеальный шифр. Совершенная секретность. Шифр Вернама. Теория Симмонса аутентификации. Модель протокола аутентификации. Имитация и подмена. Безусловная целостность.

Элементы криптографических систем и протоколов. Односторонние (однонаправленные) функции: определение односторонней функции; гипотетические примеры односторонних функций. Криптографические хэш-функции; односторонние семейства хэш-функций; необходимые и достаточные условия существования. Генераторы псевдослучайных последовательностей в криптографии: два определения псевдослучайных генераторов; необходимые и достаточные условия их существования.

Криптографические системы. Принципы построения криптосистем с секретным ключом (симметричных криптосистем). Сети Файстеля и подстановочно-перестановочные сети (SP-сети). Криптосистемы с открытым ключом. Семейства функций с секретом. Криптосистема RSA. Криптосистемы на основе эллиптических кривых. Схемы разделения секрета: структуры доступа; доли секрета; пороговые схемы; схема Шамира.

Криптографические протоколы. Протоколы генерации ключей на примере протокола Диффи-Хеллмана. Протоколы электронной подписи: примеры протоколов; необходимые и достаточные условия существования стойких протоколов электронной подписи. Доказательства с нулевым разглашением: понятие протокола интерактивного доказательства; свойство нулевого разглашения; примеры; протоколы интерактивной аутентификации.

Методы и средства защиты информации

Модели защищенных систем. Модель «take-grant». Модель Белла-Лападулы. Модель невлияния.

Логическое разграничение доступа. Подход к определению безопасности в терминах доступов. Понятие о логическом разграничении доступа. Связь с идентификацией и аутентификацией. Модели логического разграничения доступа: дискреционные модели; мандатные многоуровневые модели; ролевые модели логического разграничения доступа. Анализ информационных потоков. Механизмы логического разграничения доступа в современных операционных системах.

Принципы реализации криптографических систем. Реализация симметричных криптосистем. Примеры режимов блочного шифрования. Примеры реа-

лизации потоковых криптосистем с секретным ключом. Принципы реализации алгоритма шифрования AES. Реализация криптосистем с открытым ключом. Совместное использование криптосистем с открытым ключом и симметричных криптосистем. Выбор длины ключа; функции формирования ключей; удлинение ключей. Отечественные криптосистемы.

Скрытые каналы. Понятие о скрытых каналах, подходы к классификации. Примеры реализации скрытых каналов по памяти и по времени. Сокрытие факта передачи информации. Стеганография. Примеры реализации методов стеганографии. Методы ограничения скрытых каналов.

Методы защиты от сетевых атак. Примеры сетевых атак. Подмена сетевых адресов, подмена доменных имен и «отравление» кэша доменных имен, источников отсылки сообщений. Использование подмены в проведении атак «человек посередине» и организации фишинга. Атаки на основные сетевые протоколы: IP; TCP; HTTP. Методы защиты от сетевых атак. Варианты защищенных сетевых проколов: IPsec; SSL/TLS; HTTPS. Инфраструктура открытых ключей, удостоверяющий центр, сертификат, путь доверия. Методы защиты от сетевых атак с использованием инфраструктуры открытых ключей или альтернативных моделей доверия (PGP).

Экранирование и туннелирование. Межсетевые экраны и их основные компоненты. Реализация функций межсетевых экранов в специализированном сетевом оборудовании. Программные реализации межсетевых экранов. Дополнительные функции межсетевых экранов. Основные схемы сетевой защиты на базе межсетевых экранов. Понятие о туннелировании и об организации виртуальных частных сетей. Применение криптографических методов в туннелировании и организации виртуальных частных сетей. Примеры реализации способов туннелирования в и организации виртуальных частных сетей в сетевом оборудовании и в программном обеспечении.

Протоколирование и аудит. Понятие о протоколировании, аудите, активном аудите. Подходы к организации архитектуры систем активного аудита. Методы мониторинга и обнаружения вторжений в распределенных информационно-вычислительных системах. Основные методы анализа регистрационной информации. Сигнатурные методы обнаружения вторжений и аномальной активности; использование регулярных выражений. Алгоритмы статистического анализа регистрационной информации.

Защита от вредоносного программного обеспечения. Понятие о вредоносном программном обеспечении. Подходы к классификации вредоносного программного обеспечения. Программные закладки. Троянские программы. Вирусы и черви. Способы внедрения вредоносного программного обеспечения в компьютерные системы. Воздействие вредоносного программного обеспечения на компьютерные системы. Взаимодействие компонентов вредоносного программного обеспечения. Вредоносное программное обеспечение и бот-сети. Методы защиты от вредоносного программного обеспечения. Обеспечение целостности. Изолированные программные среды. Методы антивирусной защиты. Алгоритмическая неразрешимость задачи выявления

вируса. Существование вирусов, не выявляемых алгоритмически.
Защита информации с точки зрения технологий программирования. Основные классы уязвимостей программных средств: ошибки типа «переполнение буфера» и ошибки управления памятью, ошибки типа «состояние гонки», арифметические переполнения, инъекции интерпретируемого кода. Примеры атак с использованием распространенных уязвимостей программных средств (переполнение буфера, состояние гонки, арифметическое переполнение, инъекции интерпретируемого кода). Подходы к предотвращению возникновения уязвимостей. Методы тестирования программных средств, методы верификации программных средств. Использование автоматических анализаторов исходного кода.

III. Критерии оценивания

Критерии и показатели оценивания ответа на экзамене			
1	2	3	4
Неудовлетворительно	**Удовлетворительно**	**Хорошо**	**Отлично**
Фрагментарные знания актуальных проблем и тенденций в развитии методов и систем защиты информации и информационной безопасности	Неполные знания актуальных проблем и тенденций в развитии методов и систем защиты информации и информационной безопасности	Сформированные, но содержащие отдельные пробелы знания актуальных проблем и тенденций в развитии методов и систем защиты информации и информационной безопасности	Сформированные и систематические знания актуальных проблем и тенденций в развитии методов и систем защиты информации и информационной безопасности

IV. Рекомендуемая основная литература:

1. Основы информационной безопасности: курс лекций / 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 защиты информации : учеб. пособие для студентов высш. учеб. заведений / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. — М.: Издательский центр «Академия», 2009. — 272 с.
3. Стандарты информационной безопасности : курс лекций : учеб. пособие / Второе издание / В. А. Галатенко. Под редакцией академика РАН В. Б. Бетелина — М.: ИНТУИТ.РУ «Интернет-университет информа-

ционных технологий», 2006. — 264 с.
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. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П. Н. Девянин. – М.: Радио и связь, 2006. — 176 с.
7. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений / П. Н. Девянин. — М.: Издательский центр «Академия», 2005. — 144 с.
8. Информационные компьютерные преступления: учебное пособие / В. В. Крылов. — М.: Изд-во РАГС, 2004. — 221 с.
9. Введение в криптографию. Издание 4-е, дополненное / Под общей редакцией В. В. Ященко. — М.: МЦНМО, 2012. — 352 с.
10. Методы дискретной математики в криптологии / В. М. Фомичев. — М.: Диалог-МИФИ, 2010. — 424 с.
11. Введение в дискретную математику / С. В. Яблонский. — М.: Высшая школа, 2010. — 384 с.
12. Введение в теорию автоматов / В. Б. Кудрявцев, С. В. Алешин, А. С. Подколзин. — М.: Наука. Гл. ред. физ.-мат. лит., 1985. — 320 с.
13. Дискретная математика для инженера / О. П. Кузнецов, Г. М. Адельсон-Вельский — 2-е изд., перераб. и доп. — М.: Энергоатомиздат, 1988. — 480 с.
14. Вычислительные машины и труднорешаемые задачи / М. Гэри, Д. Джонсон. — М.: «Мир», 1982. — 419 с.
15. Классические и квантовые вычисления / А. Китаев, А. Шень, М. Вялый. М.: МЦНМО, 1999. — 192 с.

V. Дополнительная литература:

1. Основы теории информации / А. Файнстейн ; пер. с англ. Коваленко И. Н., Ницкой Э. Р. ; под ред. Гихмана И. И. — М.: Издательство иностранной литературы, 1960. — Перевод изд.: Feinstein, Amiel. Foundations of Information Theory. New York: McGraw-Hill, 1958.
2. Математическая теория связи / К. Шеннон. // Работы по теории информации и кибернетике / К. Шеннон. — М.: Издательство иностранной литературы, 1963. — 832 с. — с. 243-332. — Перевод изд.: A Mathematical Theory of Communication / C. E. Shannon // The Bell

System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.
3. Теория связи в секретных системах / К. Шеннон. // Работы по теории информации и кибернетике / К. Шеннон. — М.: Издательство иностранной литературы, 1963. — 832 с. — с. 333-402. — Перевод изд.: Communication Theory of Secrecy Systems / C. E. Shannon // Bell System Technical Journal, Vol. 28, Issue 4, pp. 656–715, October 1949.
4. Обзор методов аутентификации информации / Г. Дж. Симмонс : пер. с англ. // Труды ИИЭР, 1988. — Т. 76, № 5. — Перевод изд.: Authentication Theory/Coding Theory / Gustavus J. Simmons // Proceedings of CRYPTO 84 on Advances in cryptology. — Springer-Verlag New York, Inc., New York, NY, USA, 1985. — Pages 411-431.
5. Foundations of cryptography. Volume 1 (Basic tools) / O. Goldreich. — Cambridge University Press, Cambridge, United Kingdom, 2001.
6. Foundations of cryptography. Volume 2 (Basic applications) / O. Goldreich. — Cambridge University Press, Cambridge, United Kingdom, 2004.
7. Pseudorandomness and cryptographic applications / M. Luby. — Princeton University Press, Princeton, New Jersey, USA, 1996.
8. Computational Complexity: A Modern Approach / S. Arora, B. Barak. — Cambridge University Press, New York, NY, USA, 2009.
9. О существовании скрытых каналов / А. А. Грушо. // Дискретная математика, т. 11, вып. 1, (1999). — с. 24-28.
10. О скрытых каналах и не только / А. В. Галатенко. // JetInfo, № 11, 2002. — с. 12-20.
11. Скрытые каналы / Е. Е. Тимонина. //JetInfo, № 11, 2002. — с. 2-11.
12. Активный аудит / А. В. Галатенко. // JetInfo, № 8, 1999. — с. 2-28.
13. The NIDES statistical component description and justification / H.S. Javitz, A. Valdes // Technical report, Computer Science Laboratory, SRI International, 1994. — URL: http://www.sdl.sri.com/papers/statreport
14. Computer Viruses / Cohen F. // Ph.D. Thesis, 1985.
15. An undetectable computer virus / D.M. Chess, S.R. White // Proceedings of Virus Bulletin Conference, 2000.

VI. Авторы временной программы:

1. д.ф.-м.н., профессор В.А. Васенин
2. к.ф.-м.н., ст.н.с. А.В.Галатенко
3. к.ф.-м.н., ст.н.с. А.В. Галатенко