Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное учреждение науки
Институт системного программирования им. В.П. Иванникова
Российской академии наук
(ИСП РАН)

Одобрено решением учёного совета ИСП РАН. **Протокол № 2022-14 - от 29 декабря 2022 г.**	**«УТВЕРЖДАЮ»** **Директор ИСП РАН** **д.ф.-м.н., академик РАН** **А.И. Аветисян** **«29» декабря 2022 г.**

ПРОГРАММА-МИНИМУМ

кандидатского экзамена

по специальности

1.2.4 - Кибербезопасность

по физико-математическим наукам.

Москва 2022

Вопросы кандидатского экзамена по специальности

1. Математические основы кибербезопасности

1.1. Криптография с секретным ключом и открытым ключом: области применения и основные алгоритмы. Методы передачи ключевой информации. Информационная безопасность технологии блокчейн. Защита информации для криптовалют. Хэш-функции. Основные понятия и методы реализации.

1.2. Стеганография. Основные понятия и направления использования для обеспечении информационной безопасности автоматизированных систем. Методы стеганографии для звуковых файлов и изображений.

2. Вычислительные машины и сети ЭВМ

2.1. Аппаратные средства защиты от эксплуатации ошибок, использование этих средств во время компиляции и при выполнении программ: защита стека, предотвращение выполнения данных, рандомизация адресного пространства, контроль целостности потока управления. Применение штатных средств защиты памяти для противодействия эксплуатации ошибок. Тегированная память, процессорная архитектура Эльбрус и ее зарубежные аналоги.

2.2. Аппаратные средства обеспечения безопасности информации: расширения архитектуры набора команд и специализированные криптопроцессоры. Примеры аппаратных средств: TPM, ARM TrustZone, Intel Boot Guard. Аппаратный корень доверия, доверенная загрузка.

3. Компьютерные атаки, их обнаружение, противодействие и ликвидация последствий

3.1. Сетевые атаки. Классификация сетевых атак. Сценарии и стадии проведения сетевых атак. Удаленное определение версии ОС. Методы сканирования портов. Методы выявлении пакетных снифферов. Десинхронизация TCP-соединений. Перехват сетевых соединений путем проведения атак, направленных на сетевую инфраструктуру. Методы перехвата сетевых соединений в сетях TCP/IP.

3.2. Безопасность веб-систем. Дефекты, приводящие к инъекциям. SQL-инъекции. Объектная модель DOM. Понятие HTTP-сессии. Инъекции JavaScript, cross site scripting (XSS). Получение удаленного доступа к веб-системе. Методы внедрения веб-шелла на удаленную веб-систему. Методы сокрытия веб-шелла.

3.3. Вредоносное программное обеспечение (ВПО). Предпосылки к внедрению, методы внедрения, средства и методы противодействия.

3.4. Механизмы эксплуатации уязвимостей: переполнение на стеке, целочисленное переполнение, неинициализированная переменная, использование памяти после освобождения.

4. Программно-аппаратные средства обеспечения кибербезопасности

4.1. Управление доступом пользователей: дискреционное мандатное, изолированная программная среда. Права, привилегии.

4.2. Идентификация и аутентификация пользователей. Парольная аутентификация. Аутентификация с использованием внешних носителей информации. Биометрическая аутентификация. Основные подходы к подбору паролей, средства, методы и практические приемы подбора паролей. Средства и методы защиты от подбора паролей. Оценки стойкости парольной защиты, методы ее повышения.

4.3. Сквозная аутентификация, протокол Kerberos, лесная доменная архитектура компьютерной сети. Активный каталог Windows, схема и классы объектов активного каталога. Назначение полномочий пользователям. Отношения доверия, управление доступои к объектам активного каталога, делегирование полномочий. Групповые политики.

4.4. Средства аудита и системы обнаружения вторжений (СОВ). Выявление атак на основе сигнатур атак и выявления аномалий. Архитектура и возможности СОВ.

4.5. Понятие безопасности БД. Угрозы безопасности БД: общие и специфичные. Средства обеспечения защиты информации в СУБД и многоуровневая защита. Угрозы конфиденциальности и целостности в СУБД, способы им противодействия.

4.6. Криптографические средства и методы сетевой безопасности. Понятие шифронабора. Протоколы, входящие в SSL/TLS. Схема рукопожатия: фазы, согласуемые параметры, вычисление сеансовых ключей. Понятие сессии, соединения и их состояний. Сокращенное и повторное рукопожатие.

4.7. Сертификаты и цепочки доверия. Модели инфраструктуры сертификатов. Организация защищённого канала связи на разных уровнях сетевого стека. End-to-End шифрование.

4.8. Пакетные фильтры и межсетевые экраны. Проблемы фильтрации на уровнях L3-L4 стека TCP/IP. Устройство и принцип работы ACL. Фильтрация на уровне приложения.

4.9. Виртуальные частные сети (VPN). Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Организация туннелирования на различных уровнях модели ISO/OSI. Особенности обеспечения сетевой безопасности при использовании VPN.

4.10. Понятие периметра и DMZ. Zero trust. Авторизация, аутентификация и аудит. UTM, NGFW. IDS,IPS и другие системы защиты.

5. Методы компиляции и статического анализа

5.1. Применения статического анализа. Актуальность поиска ошибок в программах, возможные методы. Понятия статического и динамического анализа программ. Ошибки, допускаемые анализатором. Выделение ошибочных ситуаций, причины появления различных ситуаций для одного класса ошибок.

5.2. Представления программы, подвергаемые анализу. Анализ программы на уровне абстрактных синтаксических деревьев. Примеры ошибочных ситуаций.

5.3. Анализ потоков данных. Потоковая чувствительность и нечувствительность. MOP-, MFP-, ideal-решения. Итеративный анализ, анализ на основе SSA-представления. Абстрактная интерпретация. Понятие решётки. Понятия конкретного и абстрактного состояний. Связь абстрактной интерпретации и анализа потока данных. Интервальный анализ.

5.4. Чувствительность к путям. Символьное выполнение. Символьное выполнение с объединением состояний. SMT-решатели.

5.5. Межпроцедурный анализ. Подходы к организации межпроцедурного анализа. Контекстная чувствительность. Межпроцедурный анализ на основе резюме.

6. Методы динамического анализа программ, методы анализа бинарного кода и исследований для поиска уязвимостей

6.1. Обфускация и защита от анализа программного кода. Методы защиты от статического и динамического анализа.

6.2. Динамическое символьное выполнение: основные понятия. Варианты использования. Схема работы системы символьного выполнения. Предикат пути, предикат безопасности. Ограничения подхода и способы их преодоления.

6.3. Программный слайсинг: определение, свойства, применение. Алгоритм обратного статического слайсинг. Виды зависимостей. Статический, динамический, условный слайсинг.

6.4. Межпроцедурный слайсинг. Методы вычисления слайса: анализ потоков данных и достижимость на графах. Выявление пути распространения ошибки.

6.5. Анализ помеченных данных: источники, распространение, обнаружение уязвимостей, варианты использования. Ограничения анализа помеченных данных. Поиск утечек конфиденциальных данных.

6.6. Анализ приложения для выявления уязвимостей. Этапы предварительного сбора данных.

6.7. Сетевые сканеры. Принцип работы, оптимизация времени работы для больших сетей.

6.8. Сбор данных из открытых источников (OSINT). Инструменты автоматизации.

7. Методы конструирования доверенных программных и программно-аппаратных систем

7.1. Общие критерии и гармонизированные стандарты Российской Федерации ГОСТ Р ИСО/МЭК 15408.

7.2. Уязвимость информационной системы. Классификация уязвимостей информационных систем по ГОСТ Р 56546.

7.3. Методологии разработки безопасного ПО: Microsoft SDL, CSDL, BSIMM, OWASP SAMM. Оценка зрелости жизненного цикла безопасного ПО.

7.4. Современное состояние сертификационной деятельности в области информационной безопасности в России.

7.5. Система национальных стандартов разработки безопасного ПО, ГОСТ Р 56939.
7.6. Технологии анализа кода, применяемые в жизненном цикле безопасного ПО, и требования, предъявляемые к ним.

8. Методы синтеза и верификации цифровой аппаратуры

8.1. Маршрут проектирования цифровой аппаратуры. Уровни представления аппаратуры. Логический и физический синтез. Верификация и ее разновидности. Специфика маршрута проектирования для ПЛИС (FPGA) и заказных СБИС (ASIC).
8.2. Безопасность аппаратуры. Закладки (hardware Trojans), их классификация. Пред- и пост-производственные методы обнаружения закладок. Доверенное проектирование и методы противодействия внесению закладок.
8.3. Проверка логической эквивалентности комбинационных схем (LEC). Сведение задачи LEC к задаче выполнимости (SAT). Адаптивная проверка эквивалентности для схем высокой размерности. Подходы к проверке эквивалентности последовательных схем (SEC).
8.4. Логический синтез. Представление и оптимизация булевых функций (BDD, AIG, MIG). Оптимизация структурных моделей конечных автоматов (кодирование состояний). Оптимизация временных характеристик (retiming). Технологическое отображение.
8.5. Высокоуровневый синтез и конструирование аппаратуры. Выделение ресурсов и планирование вычислений. Вычисления на основе потоков данных. Синтез потоковых вычислителей по высокоуровневым спецификациям.

9. Верификация программных и программно-аппаратных систем

9.1. Символическая проверка модели. Двоичные решающие диаграммы (BDD) и алгоритмы манипуляции с ними. Ограниченная проверка модели (bounded model checking). K-индукция.
9.2. Статическая верификация программ (software model checking). Задача проверки достижимости точки программы. Предикатная абстракция. Метод адаптивного уточнения абстракции по контрпримерам (CEGAR). Интерполяционная теорема Крейга.
9.3. Задача проверки выполнимости для логики высказываний (SAT). Кодировка Цейтина. Метод резолюций для логики высказываний. Алгоритм DPLL и его оптимизации. Формат DIMACS.
9.4. Задача проверки выполнимости в теориях первого порядка (SMT). Метод резолюций для логики первого порядка. Понятие разрешающей процедуры. Теория равенства неинтерпретируемых функций. Метод Нельсона-Оппена комбинирования разрешающих процедур разных теорий. Язык SMTLIB.

10. Методы интеллектуального анализа данных

10.1. Нейрон и нейронная сеть. Задачи, решаемые при помощи нейронных сетей.

10.2. Компоненты нейронной сети. Методы оптимизации. Сверточные нейронные сети.

10.3. Регуляризация, нормализация и метод максимального правдоподобия. Методы ускорения классификации при помощи нейросетей.

10.4. Естественный язык и текст. Векторная модель текста и классификация длинных текстов. Классификация новостных текстов.

10.5. Базовые методы работы с текстом при помощи нейронных сетей. Классификация коротких текстов. Распознавание структуры коротких текстов. Распознавание именованных сущностей.

Литература

1. Ахо,Лам,Сети,Ульман. Компиляторы. Принципы, технологии, инструменты. М., 2008, 2изд.
2. Cooper K., Torczon L. Engineering a Compiler, Second Edition.2011.
3. Flemming Nielson, Hanne R. Nielson, Chris Hankin. Principles of Program Analysis / Springer, 1999
4. Al Bessey, Ken Block, Ben Chelf, Andy Chou, Bryan Fulton, Seth Hallem, Charles Henri-Gros, Asya Kamsky, Scott McPeak, Dawson Engler. A Few Billion Lines of Code Later: Using Static Analysis to Find Bugs in the Real World // Comunications of the ACM, 2010, vol. 53, no. 2, pp. 66-75.
5. Brian Chess, Jacob West. Secure Programming with Static Analysis / Addison-Wesley Professional, 2007.
6. Nethercote N., Seward J. Valgrind: a framework for heavyweight dynamic binary instrumentation // ACM Sigplan notices. – ACM, 2007. – Т. 42. – №. 6. – С. 89-100.
7. Амини П., Саттон М., Грин А. Fuzzing: исследование уязвимостей методом грубой силы. — Символ-Плюс, 2009.
8. Edward J. Schwartz, Thanassis Avgerinos, David Brumley. All You Ever Wanted to Know about Dynamic Taint Analysis and Forward Symbolic Execution (but might have been afraid to ask), 2010
9. В.А. Падарян, А.И. Гетьман, М.А. Соловьев, М.Г. Бакулин, А.И. Борзилов, В.В. Каушан, И.Н. Ледовских, Ю.В. Маркин, С.С. Панасенко. Методы и программные средства, поддерживающие комбинированный анализ бинарного кода // Труды Института системного программирования РАН Том 26. Выпуск 1. - 2014 г. - С. 251-276
10. Balakrishnan G., Reps T. Analyzing memory accesses in x86 executables // International conference on compiler construction. – Springer Berlin Heidelberg, 2004. – С. 5-23 (https://research.cs.wisc.edu/wpis/papers/cc04.pdf)
11. M. Handley, V. Paxson. Network Intrusion Detection: Evasion Traffic Normalization And End-to-End Protocol Semantics//Proceedings of the 10th USENIX Security Symposium. - 2001.
12. Методика оценки угроз безопасности информации. ФСТЭК России. https://fstec.ru/tekhnicheskaya-zashchitainformatsii/dokumenty/114-spetsialnyenormativnye-dokumenty/2170-metodicheskij-dokument-utverzhdenfstek-rossii-5-fevralya-2021-g

13. Таненбаум Э., Уэзеролл Д. «Компьютерные сети». 5 издание. Питер, 2022.
14. Justin Schuh, John McDonald, Mark Dowd. The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. 2006.
15. Michael Bazzell. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. 2014.
16. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2007
17. Tobias Klein. A Bug Hunter's Diary: A Guided Tour Through the Wilds of Software Security. 2011.
18. Ian Goodfellow, Yoshua Bengio, and Aaron Courville. 2016. Deep Learning. The MIT Press.
19. Christopher M. Bishop. 2006. Pattern Recognition and Machine Learning (Information Science and Statistics). Springer-Verlag, Berlin, Heidelberg.
20. Sebastian Raschka. 2015. Python Machine Learning. Packt Publishing.
21. Daniel Jurafsky and James H. Martin. 2009. Speech and Language Processing (2nd Edition). Prentice-Hall, Inc., Upper Saddle River, NJ, USA.
22. К.А. Коньков, В.Е. Карпов Основы операционных систем. М.: Интернет университет информационных технологий. 2004.
23. Таненбаум Э. Современные операционные системы. - СПб.: Питер, 2002.
24. Рэндал Э. Брайант, Дэвид О'Халларон. Компьютерные системы: архитектура и программирование (Computer Systems: A Programmer's Perspective). Издательство: БХВ-Петербург, 2005 г. — 1186 стр.
25. Д.В. Буздалов, Е.В. Корныхин, А.А. Панфёров, А.К. Петренко, А.В. Хорошилов. Практикум по дедуктивной верификации программ: учебно-методическое пособие. М: МАКС Пресс, 2014.
26. А.С. Камкин. Введение в формальные методы верификации программ: учебное пособие. М: МАКС Пресс, 2018.
27. Ю.Г. Карпов. Model Checking. Верификация параллельных и распределенных программных систем. БХВ-Петербург, 2010.
28. K.R. Apt, F.S. de Boer, E.-R. Olderog. Verification of Sequential and Concurrent Programs. Springer, 2009.
29. C. Baier, J.-P. Katoen. Principles of Model Checking. The MIT Press, 2008.
30. M. Ben-Ari. Mathematical Logic for Computer Science. Springer, 2012.
31. Цифровой синтез: практический курс / под общ. ред. А.Ю. Романова, Ю.В. Панчула. М.: ДМК Пресс, 2020.
32. S. Bhunia, M. Tehranipoor. Hardware Security A Hands-on Learning Approach. Morgan Kaufmann, 2019.
33. Д. Харис, С. Харис. Цифровая схемотехника и архитектура компьютера: RISC-V. М.: ДМК Пресс, 2021.
34. К. Максфилд. Проектирование на ПЛИС. Архитектура, средства и методы. Курс молодого бойца. М.: Додэка XXI, ДМК Пресс, 2015.
35. Web Application Security A Beginner's Guide. Bryan Sullivan, Vincent Liu. 2011
36. Основные понятия PKI. http://www.cryptocom.ru/articles/pki.html
37. Ключи, шифры, сообщения: как работает TLS. А. Венедюхин. https://tls.dxdt.ru/tls.html