Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ / Д.С. Гуц /
«10» марта 2023 г.

ПРОГРАММА
кандидатского экзамена по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Красноярск 2023

ПРОГРАММА-МИНИМУМ
кандидатского экзамена по специальности
2.3.6 «Методы и системы защиты информации. Информационная безопасность»
по техническим наукам

1 Основы теории защиты информации

Особенности информатизации общества на современном этапе. Основные характеристики современных информационных систем. Необходимость обеспечения информационной безопасности систем и объектов.

Возникновение проблемы защиты информации. Развитие и становление способов защиты. Этапы развития и их характеристики.

Определение, особенности и общее содержание теории защиты информации.

Научно-методологический базис теории защиты. Система моделей защиты информации.

Определение и основные понятия стратегии защиты информации. Факторы, влияющие на формирование стратегий защиты. Классификационная структура множества необходимых стратегий защиты. Общая характеристика основных стратегий.

Определение и назначение инструментально-методологического базиса защиты информации. Требования к инструментально-методологическому базису.

Пути и способы реализации основных положений теории защиты информации.

Перспективы и проблемы развития теории и практики защиты.

2 Угрозы информации и методология оценки ее уязвимости

Определение и природа угроз информации в современных системах ее обработки.

Классификация и общая характеристика основных угроз.

Понятие уязвимости информации. Подходы к определению значений показателей уязвимости.

Эмпирические методы определения значений показателей уязвимости. Примеры эмпирических моделей. Способы определения параметров моделей. Особенности использования моделей.

Теоретико-вероятностные методы определения значений показателей уязвимости, подходы к построению моделей. Примеры моделей. Особенности и проблемы практического использования.

Теоретико-эмпирические методы определения значений показателей. Подходы к построению теоретико-эмпирических моделей. Понятие базового показателя уязвимости, аналитическая и статистическая модели его определения.

Методы и модели прогнозирования значений показателей уязвимости.

Определение, значение, структура и способы формирования инструментальных средств оценки уязвимости информации.

3 Методы обеспечения информационной безопасности

Защита автоматизированных систем от удаленных атак через сеть Internet. Режим функционирования межсетевых экранов и их основные компоненты; маршрутизаторы; шлюзы сетевого уровня; усиленная аутентификация; основные схемы сетевой защиты на базе межсетевых экранов; применение межсетевых экранов для организации виртуальных корпоративных сетей; программные методы защиты.

Защита информации от несанкционированного доступа (НСД). Каналы утечки информации. Защита компонентов автоматизированных систем от НСД. Антивирусная защита. Системы анализа защищённости и обнаружения вторжений. Модель и источники каналов утечки информации.

Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Классификация способов защиты; защита от отладок и дизассемблирования; способы встраивания защитных механизмов в программное обеспечение; понятие разрушающего программного воздействия; модели взаимодействия прикладной программы и программной закладки; методы перехвата и навязывания информации; методы внедрения программных закладок; компьютерные вирусы как особый класс разрушающих программных воздействий; защита от разрушающих программных воздействий; понятие изолированной программной среды.

Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов. Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации. Парольные системы опознавания, их сущность, содержание, достоинства и недостатки. Способы повышения надежности парольных систем. Другие системы опознавания. Средства опознавания аппаратуры, программ, массивов данных.

Методы идентификации и проверки подлинности пользователей автоматизированных систем. Основные понятия и концепции; идентификация и механизмы подтверждения подлинности пользователя; взаимная проверка подлинности пользователей; протоколы идентификации с нулевой передачей знаний; упрощенная схема идентификации с нулевой передачей знаний; проблема аутентификации данных.

Биометрическая идентификация и аутентификация пользователей: основные понятия и механизмы. «Fuzzy extractors». Искусственные нейронные сети в преобразователях биометрия-код. Алгоритм быстрого обучения искусственной нейронной сети. Алгоритм ускоренного тестирования нейросетевого преобразователя биометрия-код (НПБК). Алгоритм полного тестирования НПБК. Базы биометрических образов: назначение, виды, требования к формированию. Нейросетевой биометрический контейнер (НБК): назначение, виды. Наиболее вероятные атаки на НБК, защита от них.

Программные средства разграничения доступа, их сущность, достоинства и недостатки. Модели разграничения доступа. Разграничение доступа по уровням и кольцам секретности, матрицам полномочий и мандатам. Способы и средства повышения надежности разграничения. Примеры систем разграничения доступа. Другие программные средства защиты: регистрации, сигнализации, реагирования и т.п. Программы защиты ЭВМ от электронных вирусов.

Способы организации и использования программных средств защиты.

Организационно-правовые средства защиты, их сущность, возможности, достоинства и недостатки. Критерии классификации организационно-правовых средств, классификационная структура и общая характеристика.

Система законов, регламентирующих защиту информации в РФ. Перечень основных законов, основное их содержание и порядок действия.

Руководящие методические материалы (РММ) по защите информации. Назначение и состав необходимых РММ. Перечень и содержание имеющихся РММ.

Организационные мероприятия по защите информации, их сущность и назначение.

Системная классификация организационных мероприятий. Мероприятия, проводимые на различных этапах жизненного цикла систем обработки данных.

Стеганография. Основы стеганографии. Основные понятия. Компьютерная стеганография.

4 Управление информационной безопасностью

Необходимость, сущность и основные понятия управления информационной безопасностью.

Служба информационной безопасности на объекте. Назначение и организационно-правовой статус службы. Функции и задачи службы, способы и методы их решения.

Создание, поддержка, оценка эффективности, совершенствование системы управления информационной безопасности.

Методы и модели управления рисками информационной безопасности. Формирование критериев влияния, оценивания, принятия рисков. Итерационные процедуры управления рисками информационной безопасности.

Методы и модели оценки рисков информационной безопасности. Методы идентификации рисков информационной безопасности активов. Методы формирования сценариев инцидентов, модели сценариев инцидентов. Методы идентификации и анализа последствий инцидентов различного вида. Оценка ущерба в результате нарушения безопасности. Методы оценивания рисков информационной безопасности. Методы обработки рисков информационной безопасности. Оценка вариантов обработки рисков.

Оценка эффективности выбранных защитных мер. Методы управления изменениями систем.

Управление инцидентами информационной безопасности. Обнаружение и анализ инцидентов. Методы реагирования на инциденты информационной безопасности.

Управление непрерывностью функционирования систем и объектов

Методы и модели мониторинга информационной безопасности. Структура систем мониторинга.

Методы аудита информационной безопасности. Оценка соответствия защитных мер, процессов обеспечения информационной безопасности. Методы выявления и анализа свидетельств оценки.

Организация обучения и осведомления персонала информационной безопасности.

Основная литература

1. Информационная безопасность предприятия: Учебное пособие / Н. В. Гришина. - 2-е изд. доп. - Москва: Форум; Москва: НИЦ ИНФРА-М, 2015. - 240 с. (доступ из электронной библиотеки).

2. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва: РИОР, 2013. - 222 с. (доступ из электронной библиотеки).

3. Защита информации [Электронный ресурс]: учебное пособие / А. П. Жук [и др.]. - 2-е изд. - Москва: ИЦ РИОР; Москва: НИЦ ИНФРА-М, 2015. - 392 с. (доступ из электронной библиотеки).

4. Организация и технологии защиты информации [Текст]: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учеб. пособие / В. А. Сердюк; Гос. ун-т - Высш. шк. экономики. - Москва: ГУ - ВШЭ, 2011. - 572 с.: ил. - Библиогр.: с. 541-567.

5. Сычев, Ю. Н. Защита информации и информационная безопасность: учебное пособие / Ю.Н. Сычев; Российский экономический университет им. Г.В. Плеханова. - 1. - Москва: ООО "Научно-издательский центр ИНФРА-М".

6. Зайцев А.П. Технические средства и методы защиты информации: Рекомендовано УМО вузов по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям 090102 - "Компьютерная безопасность", 090105 - "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 - "Информационная безопасность телекоммуникационных систем" / Зайцев А.П. ; Шелупанов А.А., Мещеряков Р.В., Голубятников И.В., Солдатов А.А., Скрыль С.В. – 2012 (доступ из электронной библиотеки).

7. Методы и средства защиты информации в компьютерных системах: учеб. пособие для студентов вузов / П. Б. Хорев. - 4-е изд., стер. - Москва: Академия, 2008. - 256 с.

8. Васильева И. Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата по инженерно-техническим направлениям и специальностям / И. Н. Васильева; Санкт-Петербург. гос. эконом. ун-т. – 2016.

9. Гашков С. Б. Криптографические методы защиты информации: учеб. пособие для студентов вузов / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. – 2010.

10. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. - 586 с.

11. Бузов, Г.А. практическое руководство по выявлению специальных технических средств несанкционированного получения информации: Учебное пособие/ Г.А. Бузов. - М.: ГЛТ, 2010. – 240.

Дополнительная литература

1. Конституция Российской Федерации.

2. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).

3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями).

4. Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1 (с изменениями).

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями).

6. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями).

7. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» (с изменениями).

8. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» (с изменениями).

9. Закон Российской Федерации от 29.07.04 № 98-ФЗ «О коммерческой тайне» (с изменениями).

10. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (с изменениями).

11. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями).

12. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (с изменениями).

13. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (с изменениями).

14. Постановление Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» (с изменениями).

15. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

16. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.05.2019) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

17. приказом ФСТЭК России от 02.06.2020 № 76 «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий».

18. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», М.: Стандартинформ, 2007г.

19. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.).

20. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (с изменениями).

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

- Электронный каталог научной библиотеки СФУ. URL: https://bik.sfu-kras.ru
- Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России): URL: https://fstec.ru
- Некоммерческая интернет-версии системы КонсультантПлюс: URL: http://www.consultant.ru

Составители:

канд.физ.-мат.наук, доцент,
заведующий кафедрой
Информационной безопасности  Вайнштейн В.И.