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

УТВЕРЖДАЮ
Проректор по учебной работе
_____/Д.С. Гуц/
«28» марта 2022 года

ПРОГРАММА
вступительного испытания для поступающих в аспирантуру
2.3 Информационные технологии и телекоммуникации
шифр и наименование группы научных специальностей

2.3.6 Методы и системы защиты информации, информационная безопасность
шифр и наименование научной специальности

Красноярск 2022

Перечень вопросов вступительного испытания

1. Информация как предмет защиты. Основные свойства защищаемой информации. Принципы категоризации информации. Охарактеризуйте категории. Понятия «Защита информации» и «Информационная безопасность». Основные направления защиты информации.
2. Угрозы безопасности. Что такое объекты угроз ИБ? Каковы основные источники угроз защищаемой информации? Каковы цели угроз со стороны злоумышленников? Классификации угроз безопасности (по различным критериям). Понятие уязвимости. Базы данных уязвимостей. Взаимосвязь уязвимостей и угроз безопасности.
3. Модели управления доступом. Базовые понятия и их взаимосвязь (объекты и субъекты, преобразование информации, информационные потоки и т.д.). Классификация задач, решаемых механизмами управления доступом (с примерами).
4. Структура государственной системы защиты информации. Понятия: тайна и конфиденциальность. Государственные регуляторы в области защиты информации. Полномочия и сфера компетенции. Юридическая ответственность за нарушения в области ИБ (кодексы, статьи, виды ответственности).
5. Закон №5485-1 «О государственной тайне». Сфера деятельности, основные понятия. Отнесение сведений к государственной тайне и засекречивание этих сведений. Порядок засекречивания и рассекречивания сведений и их носителей. Грифы секретности. Реквизиты носителей сведений, составляющих государственную тайну.
6. Понятие конфиденциальной информации. Категории конфиденциальной информации. Юридические основания ограничения доступа к информации. Информация, доступ к которой не может быть ограничен (законодательно). Основные нормативно-правовые документы, регламентирующие защиту конфиденциальной информации.
7. Определите понятие НСД. Что такое канал НСД? Назовите типовые причины возникновения. Основные руководящие документы ФСТЭК России в области защиты информации от несанкционированного доступа: классификация и их назначение.
8. Основные понятия федерального закона «О персональных данных» (152-ФЗ): персональные данные (ПДн), оператор, обработка персональных данных, обезличивание, согласие субъекта на обработку ПДн и др.
9. Требования к защите персональных данных при их обработке в ИСПДн. Нормативно-правовая база. Категории Пдн. Актуальные угрозы безопасности ПДн. Уровень защищённости ИСПДн.
10. Лицензирование в области защиты информации. Нормативно-правовая база. Основные виды лицензий в области защиты информации и лицензирующие органы. Понятие лицензионных требований. Сроки действия лицензии и её приостановление.
11. Сертификация средств защиты информации. Структура государственной системы сертификации и её нормативно-правовая база. Сертификат соответствия, сроки действия, возможность и условия продления.
12. Понятие объекта информатизации. Аттестация объектов информатизации. Основные нормативные и методические документы. Участники системы аттестации. Мероприятия, проводимые при аттестации. Понятия аттестата соответствия, условия и сроки его действия.

13. Понятие государственной информационной системы (ГИС). Основные нормативно-правовые документы. Классификация и перечень мероприятий для обеспечения защиты информации ГИС.
14. Электронная подпись (ЭП). Нормативно-правовая база. Виды ЭП. Признание ЭП (юридическая значимость). Удостоверяющий центр и его аккредитация. Квалифицированный сертификат и его выдача. Средства ЭП
15. Аутентификация и авторизация. Классификация методов аутентификации. Достоинства и недостатки методов аутентификации. Технические устройства аутентификации. Парольная защита: угрозы преодоления, способы усиления.
16. Системы защиты информации от несанкционированного доступа (СЗИ от НСД). Основные функциональные возможности. Классы защищённости АС от НСД и область применения.
17. Системы предотвращения утечек информации (DLP-системы). Основные функциональные возможности. Оценка DLP-систем на соответствие требованиям ФСТЭК. Примеры.
18. Средства антивирусной защиты (САВЗ). Классификация. Основные функциональные возможности. Классы защищенности согласно Требованиям ФСТЭК России. Примеры.
19. Средства криптографической защиты информации (СКЗИ). Принципы функционирования, общая схема и особенности применения СКЗИ. Лицензирование деятельности в области КЗИ и сертификация СКЗИ.
20. Понятие утечки информации по техническому каналу (технические каналы утечки информации, ТКУИ). Причины и условия образования ТКУИ. Классификация и основные характеристики ТКУИ.
21. Актуальность проблематики обеспечения безопасности компьютерных сетей. Угрозы безопасности (различные подходы к классификации). Классификация антропогенных, технических и техногенных угроз компьютерным сетям. Понятие атаки на компьютерную сеть (цель, типовой сценарий, конечная цель).
22. Атаки на транспортную подсистему компьютерной сети. Пассивные атаки. Методы противодействия пассивным атакам (описание подходов и средств). Атаки типа Отказ в обслуживании (DoS). Общая концепция таких атак и конечная цель. Классификация DoS-атак по уровню OSI и применяемые техники.и на транспортную подсистему компьютерной сети.
23. Безопасность беспроводных сетей Wi-Fi. Протоколы шифрования WEP, TKIP и CCMP (разбор в общем виде, ключевые характеристики. Безопасность данных протоколов и принципиальные отличия друг от друга. Программы сертификации WPA/WPA2. Сравнение безопасности протокола WEP от программ WPA и WPA2.
24. Межсетевые экраны (МЭ). Типовая архитектура сетей, защищаемых МЭ. Классификация МЭ согласно документам ФСТЭК России. Понятия: класс защиты, тип МЭ и профиль защиты.
25. Системы обнаружения вторжений (СОВ, IDS). Классификация. Основные функциональные возможности. Классы защищенности согласно Требованиям ФСТЭК России. Примеры.

Список рекомендованных источников

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.

Нормативно-правовые документы

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

Составитель программы:
к.ф.-м.н., доцент,
руководитель НУЛ ИБ каф. ПМКБ ИКИТ  В.И. Вайнштейн