Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра автономных информационных и управляющих систем

Паспорт
расчетно-графического задания

по дисциплине «Методы противодействия техническим разведкам», 8 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты изучить каналы утечки информации и меры противодействия потере информации и материальных ценностей.

При выполнении расчетно-графического задания студенты должны провести анализ текущей ситуации рассматриваемого вопроса разработать алгоритм противодействия, выбрать аппаратные средства.

Обязательные структурные части РГЗ. 1. Введение (рассмотрение текущего состояния вопроса). 2. Построение модели нарушителя (определение канала утечки). 3. Построение модели противодействия (разработка аппаратно-административных мет противодействия утечке информации). 4. Определение эффективности проведенных мереприятий.

Оцениваемые позиции: Оценивается качество и полнота выполнения каждой составной части РГЗ и всей работы в целом.

2. Критерии оценки.

• Работа считается **не выполненной,** если выполнены не все части РГЗ, отсутствуют 2е и более либо выполнена всего одна обязательная структурная часть, оценка составляет 2 балла.

• Работа считается выполненной **на пороговом** уровне, если выполнены не все части РГЗ, отсутствуют не более одной обязательной структурной части и остальные выполнены формально (присутствуют недочеты, при защите студент путается в терминах и определениях), оценка составляет 5 баллов.

• Работа считается выполненной **на базовом** уровне, если выполнены все части РГЗ, не более одной обязательной части выполнено формально (присутствуют недочеты, при защите студент путается в терминах и определениях), оценка составляет 10 баллов.

• Работа считается выполненной **на продвинутом** уровне, если выполнены все части РГЗ, все обязательной части выполнено без замечаний (недочеты в работе отсутствуют, при защите студент уверен в терминах и определениях), оценка составляет 15 баллов.

3. Шкала оценки

В общей оценке по дисциплине баллы за РГЗ учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. Примерный перечень тем РГЗ

1. Разработка предложений по защите конфиденциальной речевой информации от съёма с волоконно-оптических линий связи.

2. Разработка программно-аппаратного комплекса по изучению характеристик и методов маскирования речевых сигналов.

3. Разработка предложений по выбору технических средств системы контроля и управления доступом для защиты информации предприятия.

4. Разработка предложений по инженерно-технической защите информации предприятия с распределенной территориальной структурой.

5. Разработка предложений по защите данных в PLC-сетях.

6. Разработка метода защиты графических изображений от встраивания вредоносной информации стеганографическими средствами.

7. Разработка методики защиты персональных данных на предприятии и ее реализация.

8. Разработка методики анализа защищенности СУБД систем электронного документооборота от SQL-инъекций.

9. Разработка демонстрационной модели волоконного акустооптического технического канала утечки информации.

10. Разработка анализатора настроек безопасности узлов локальной сети.

11. Разработка метода низкоуровневого контроля целостности системных файлов.

12. Разработка способа защиты информации для доступа в компьютерную систему от утечки по оптическому каналу.

13. Построение системы контроля физического доступа посторонних лиц с помощью средств охранного телевидения.

14. Разработка модуля обнаружения вредоносного программного обеспечения в сетевом трафике по сигнатурам.

15. Разработка способа обнаружения и противодействия атакам типа ARP-spoofing.

16. Разработка предложений по использованию протоколов обеспечения анонимности абонентов связи в компьютерных сетях.

17. Разработка модели резервного комплекса для управления банком в кризисных ситуациях.

18. Разработка утилиты обфускации программ, написанных на скриптовых языках.

19. Разработка метода и программного средства деобфускации обфусцированных программ.

20. Разработка предложений по защите корпоративной сети на основе межсетевого экранирования.

21. Разработка предложений по проведению аудита информационной безопасности информационно-вычислительных систем организаций финансово-кредитной сферы.

22. Разработка предложений по защите мультимедийной продукции от несанкционированного копирования.

23. Разработка модуля оценки соответствия балансировщика нагрузки BIG-IP требованиям безопасности.

24. Разработка механизмов защиты информационного портала для органов государственной власти.

25. Автоматизация исследований защищенности объекта информатизации от утечки по каналам акустоэлектрических преобразователей.

26. Организация спецпроверок защищаемого помещения с использованием нелинейных радиолокаторов.

27. Разработка предложений по организации защиты конфиденциальных переговоров в необорудованном помещении.

28. Анализ способов оценки защищенности автоматизированных систем в соответствии с документами ФСТЭК России.

29. Сравнительный анализ протоколов, используемых для построения защищенных (частных) виртуальных сетей (VPN).

30. Моделирование защищенных (частных) виртуальных сетей с помощью программы Cisco Packet Tracer.

31. Сравнительный анализ систем обнаружения и предотвращения компьютерных атак.

32. Моделирование процессов межсетевого экранирования локальной вычислительной сети с помощью программы Cisco Packet Tracer.

33. Оценка защищенности межсетевых экранов в соответствии с документами ФСТЭК России.

34. Анализ угроз атак на клиентов в автоматизированных системах и методов противодействия им.

35. Моделирование процессов защиты в локальной вычислительной сети организации с внешним доступом в сеть Интернет.

36. Разработка предложений по противодействию деструктивным информационным воздействиям в социальных сетях.

37. Разработка предложений по контент-анализу данных социальных сетей.

38. Разработка многополосной шкалы для анализа тональности текстов в задачах информационной безопасности.