ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВА

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕГОРОДА МОСКВЫ

«КОЛЛЕДЖ СВЯЗИ №54»

ИМЕНИ П.М.ВОСТРУХИНА

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

ПО ПРОВЕДЕНИЮ ЛАБОРАТОРНО-ПРАКТИЧЕСКИХ ЗАНЯТИЙ

для МДК 03.01Применение инженерно-технических средств обеспечения информационной безопасности

специальность:**090305 Информационная безопасность автоматизированных систем**

Москва 2016.

|  |  |
| --- | --- |
| РАССМОТРЕНЫПредметной цикловой комиссиейПротокол № \_\_\_1\_\_Председатель ПЦК\_\_\_\_\_\_\_\_\_\_\_« 31 » августа 2016г. |  |

Разработчик:

Чагмавели Н.В., преподаватель ГБПОУ КС №54

**Содержание**

1. Общие положения.

2. Методика и средства выполнения практических работ

3. Этапы выполнения практических работ

4.Правила выполнения практических работ

5.Критерии оценки практических работ

6.Правила внутреннего распорядка и техника безопасности при выполнении практических работ

7. Тематика практических работ и задания к ним

8. Учебно-методическое и информационное обеспечение МДК

1. **ОБЩИЕ ПОЛОЖЕНИЯ**

Методические указания для выполнения практических работ по МДК 03.01**При­ме­не­ние ин­же­нер­но-тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти**в соответствии с рабочей программой ПМ 03.

Данные методические указания предназначены для закрепления теоретических знаний, полученных в рамках лекционного курса, и приобретения необходимых практических навыков и умений в решении профессиональных задач по программе модуля.

В сборнике содержатся методические указания по выполнению следующих лабораторно-практических работ:

1. Виды информации и основные методы ее защиты

2. Виды угроз информационной̆ безопасности Российской̆ Федерации.

3. Источники угроз информационной̆ безопасности Российской̆ Федерации.

4. Анализ информационной̆ инфраструктуры государства.

5. Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации.

6. Виды, каналы утечки и искажения информации

7. Технические средства и методы защиты информации.

8. Программно-аппаратные средства обеспечения информационной̆

безопасности.

9. Испытания программных средств защиты.

10. Защита от утечек по каналу ПЭМИН, по акустическому и виброаккустическому каналам. (4 часа)

11. Классификация программ по защите информации

12. Создание зашифрованного канала передачи данных

13. Сетевое сканирование

14. Анализ трафика и сбор критичной информации программами пассив-

ного анализа

15. Дистанционное управление компьютером.

16. Обнаружение уязвимостей по сигнатурам

17. Сетевые помехоподавляющие фильтры

18. Анализ угроз и рисков комплексной защиты информации на объекте с использованием системы «Гриф»

19. Анализ и управление политикой информационной безопасности на объекте с использованием системы «Кондор»

20. Аудит комплексной защиты информации предприятия

21. Технические средства защиты информации в телефонных линиях

22. Технические средства обнаружения, локализации средств негласного получения информации.

23. Нейтрализациирадиоизлучающих специальных технических

24. Контроль эффективности защиты речевой информации с помощью программно-аппаратного комплекса «СПРУТ- МИНИ»

25. Поиск и измерение побочных электромагнитных излучений и наводок с помощью программно-аппаратного комплекса «НАВИГАТОР-П3Г».(4 часа)

26. Акустические и виброакустические каналы утечки

27. Побочные эми от средств обработки информации

28. Исследование оптоэлектронного канала утечки информации

29. Технические средства защиты от утечек информации по проводным линиям

30. Идентификация с помощью биометрических устройств

31. Применение активных и пассивный пластиковых карт

32. Применение парольных систем различного типа

33. Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладныхустройств в защищаемом помещении (4 часа)

34. Обнаружение сигналов линейных и сетевыхзакладок

35. Обнаружение оптических сигналов передатчиков ик-диапазона

36. Программирование арифметических алгоритмов

37. Программирование алгебраических алгоритмов

38. Защита от закладок при разработке программ

39. Программирование алгоритмов криптосистем с открытом ключом

40. Профилактика заражения вирусами компьютерных систем

41. Биометрическая аутентификация пользователя по клавиатурному подчерку»

42. «Элементы криптоанализа. Оценка частотности символов в тексте»

43. Шифрование методами перестановки.

44. Шифрование методом замены

45. Шифрование методом гаммирования.

46. Методы криптографической защиты информации.

47. Простейшие алгоритмы шифрования

48. Шифр многоалфавитной замены — шифрование методом Вернама.

49. Зашифровать и расшифровать выданное сообщение с помощью алгоритма шифрования RSA.

50. Методы и алгоритмы стеганографического сокрытия данных

51. Оценка уязвимости коммутируемого доступа

52. Произвести защиту вымышленного помещения (8 часов )

53. Программно-аппаратный комплекс «спрут-7»

54. Оценка защищенности ограждающих конструкций помещения от утечки информации (6 часа )

55. Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласногополучения информации, использующих силовые линии сети переменного тока и линии систем охранной̆ (пожарной̆) сигнализации

56. Анализ систем видеонаблюдения

57. Анализ систем защиты от прослушивания

58. Скрытые функции диктофоны

59. «Построение зависимости состояния защищенности от уровня экономического развития организации»(4часа )

60. Изучение международных стандартов во ИБ

61. Требования к средствам обеспечения безопасности.

62. «Планирование безопасности организации».(10 часов )

63. «Изучение основных направлений деятельности СУИБ»

64. «Взаимодействие отдела обеспечения безопасности информации с другими подразделениями».

65. «Изучение этапов разработки КСЗИ»

66. «Построение зависимости вида защищаемой информации от формы собственности предприятия»

67. «Конструктивные особенности организации, как фактор, влияющий на КСЗИ»

68. «Качественные показатели ресурс обеспечения, как факторы, влияющие на КСЗИ»

69. Степень автоматизации основных процедур обработки защищаемой информации.

70. Виды защищаемой информации на предприятии.(4 часа)

Целью выполнения практических работ является овладение указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями.В ходе освоения профессионального модуля обучающийсядолжен:

**иметь прак­ти­че­ский опыт:**

* выявлениятех­ни­че­ских ка­на­лов утеч­ки
ин­фор­ма­ции;
* использования основных ме­то­дов и сред­ст­в ин­же­нер­но-тех­ни­че­ской за­щи­ты ин­фор­ма­ции;
* ди­аг­но­сти­ки, уст­ра­не­ния от­ка­зов и вос­ста­нов­ле­ния ра­бо­то­спо­соб­но­сти ин­же­нер­но-тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти;
* участия в мо­ни­то­рин­ге эф­фек­тив­но­сти ин­же­нер­но-
тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти;
* ре­ше­ния ча­ст­ных тех­ни­че­ских за­дач, воз­ни­каю­щих при ат­те­ста­ции
* объ­ек­тов, по­ме­ще­ний, тех­ни­че­ских средств;

**уметь:**

* при­ме­нять тех­ни­че­ские сред­ст­ва защиты информации;
* использовать средства ох­ра­ны и безо­пас­но­сти, ин­же­нер­ной за­щи­ты и тех­ни­че­ской ох­ра­ны объ­ек­тов, сис­тем ви­део­наб­лю­де­ния;
* использовать средства за­щи­ты ин­фор­ма­ции от несанкционированного съёма и утеч­ки по тех­ни­че­ским ка­на­лам;
* при­ме­нять нор­ма­тив­ные пра­во­вые ак­ты, нор­ма­тив­ные ме­то­ди­че­ские до­ку­мен­ты по обес­пе­че­нию ин­фор­ма­ци­он­ной безо­пас­но­сти тех­ни­че­ски­ми сред­ст­ва­ми;

**знать:**

* физику воз­ник­но­ве­ния технических каналов утеч­ки ин­фор­ма­ции, спо­со­бы их вы­яв­ле­ния и ме­то­ды оцен­ки опас­но­сти, клас­си­фи­ка­цию су­ще­ст­вую­щих фи­зи­че­ских по­лей и тех­ни­че­ских ка­на­лов утеч­ки ин­фор­ма­ции;
* но­менк­ла­ту­ру и ха­рак­те­ри­сти­ки ап­па­ра­ту­ры,
ис­поль­зуе­мой для съе­ма, пе­ре­хва­та и ана­ли­за
сиг­на­лов в тех­ни­че­ских ка­на­лах утеч­ки ин­фор­ма­ции;
* основные ме­то­ды и сред­ст­ва технической за­щи­ты ин­фор­ма­ции, но­менк­ла­ту­ру при­ме­няе­мых средств за­щи­ты ин­фор­ма­ции от несанкционированного съёма и утеч­ки по тех­ни­че­ским ка­на­лам;
* но­менк­ла­ту­ру при­ме­няе­мых средств ох­ра­ны и безо­пас­но­сти, ин­же­нер­ной за­щи­ты и тех­ни­че­ской ох­ра­ны объ­ек­тов, сис­тем ви­део­наб­лю­де­ния

**Выполнение практическихработспособствуютформированию:**

Профессиональных и общих компетенций:

|  |  |
| --- | --- |
| **Код** | **Наименование результата обучения** |
| ПК 3.1. | При­ме­нять ин­же­нер­но-тех­ни­че­ские сред­ст­ва обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти. |
| ПК 3.2.  | Уча­ст­во­вать в экс­плуа­та­ции ин­же­нер­но-тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, уст­ра­не­нии от­ка­зов и вос­ста­нов­ле­нии ра­бо­то­спо­соб­но­сти. |
| ПК 3.3.  | Уча­ст­во­вать в мо­ни­то­рин­ге эф­фек­тив­но­сти при­ме­няе­мых ин­же­нер­но-тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти. |
| ПК 3.4.  | Ре­шать ча­ст­ные тех­ни­че­ские за­да­чи, воз­ни­каю­щие при проведении всех видов плановых и внеплановых контрольных проверок, при ат­те­ста­ции объ­ек­тов, по­ме­ще­ний, технических средств. |
| ПК 3.5.  | При­ме­нять нор­ма­тив­ные пра­во­вые ак­ты, нор­ма­тив­но-ме­то­ди­че­ские до­ку­мен­ты по обес­пе­че­нию ин­фор­ма­ци­он­ной безо­пас­но­сти ин­же­нер­но-тех­ни­че­ски­ми сред­ст­ва­ми. |
| ОК 1.  | Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности. |
| ОК 2.  | Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. |
| ОК 3.  | Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях. |
| ОК 4.  | Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития. |
| ОК 5.   | Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности. |
| ОК 6. | Работать в коллективе и команде, обеспечивать их сплочение, эффективно общаться с коллегами, руководством, потребителями. |
| ОК 7.  | Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий. |
| ОК 8. | Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. |
| ОК 9.  | Быть готовым к смене технологий в профессиональной деятельности. |
| ОК 10.  | Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей). |
|  |  |
| ОК 11. | Формулировать задачи логического характера и применять средства математической логики для их решения. |
| ОК 12.  | Владеть основными методами и средствами разработки программного обеспечения. |
| ОК 13. | Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах. |

1. **МЕТОДИКА И СРЕДСТВА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ**

Выбор содержания и объем конкретной практической работы обусловлен сложностью учебного материала для усвоения, междисциплинарными связями и учетом значения конкретной практической работы для приобретения обучающимися соответствующих умений и компетенций, предусмотренных ФГОС.

Методика выполнения каждой практической работы определяется моделью соответствующей задачи, решаемой студентом на занятии по заданию преподавателя.

Средством проведения практических работ являются:

* Комплект персональных ЭВМ в компьютерных классах, с выходом в ГКС Интернет;

Комплекс программного обеспечения:

* операционная система WindowsХР, Vista и др.;

Практические работы проводятся в компьютерных классах, расположенных на учебных площадках.

Процедурным обеспечением практических работ является:

* настоящие Методические указания.
1. **ЭТАПЫ ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ**

Выполнение каждой из практических работ включает в себя пять (5) основных этапов.

1. Постановка задачи практической работы

На первом практическом занятии со студентами проводится общая постановка задач практических работ. Преподаватель может давать необходимые пояснения по методике предстоящих практических работ. После ознакомления с программным комплексом преподаватель проводит постановку задачи конкретного практического занятия. Здесь разъясняется группе студентов содержание и объем работ, предусмотренных конкретной практической работой. Прежде всего, формулируются цели, задачи, основные этапы работы, последовательность и ход решения задачи практической работы. Определяются содержание и форма представления результатов работы. Необходимо пояснить, что каждая практическая работа студента должна быть оформлена в виде отчета о практической работе. Поясняется методика составления и оформления отчета по практической работе. Проводится инструктаж по Охране труда с записью в журнал.

2. Ознакомление студента с содержанием и объемом практической работы.

На этом этапе студент должен тщательно изучить содержание и объем предстоящей практической работы. Если постановка задачи недостаточно ясна, он может обратиться к преподавателю за дополнительными разъяснениями. Затем студент приступает к выполнению задания практической работы.

1. Порядок выполнения практической работы.

Студент включает ПК и, при необходимости, запускает соответствующую программу. В соответствии с установленной последовательностью этапов работы студент выполняет объем работ, предусмотренных заданием практической работы.

При условии выполнения полного объема практической работы студент проверяет правильность результатов и предъявляет преподавателю результаты работы, выведенные на монитор. В случае замеченных ошибок, студент принимает меры к их исправлению и затем снова предъявляет результаты преподавателю для контроля и приема результатов работы. Если в работе ошибок не содержится, то приступает к составлению и оформлению отчета по практической работе.

1. Регистрация результатов и оформление отчета по практической работе.

По мере того, как выполняются этапы практическойработы, студент регистрирует все результаты своей работы в собственном файле. Этот файл в будущем должен быть оформлен как отчет студента по практической работе. Файл должен храниться в папке соответствующего студента. На основе полученных результатов практической работы, составить соответствующий отчет и сдать его преподавателю. Оформление отчета выполнить по следующим правилам. Отчет по практической работе должен содержать следующие обязательные разделы – номер и тема ПР, цель, задание, основные этапы практической работы, выводы по выполненной работе.

Отчет по каждой практической работе составляется по следующей обобщенной структуре:

* Наименование идентифицирующих признаков: «Отчет по практической работе №\_\_\_\_\_ по теме (наименование темы)».
* Студента (указываются фамилия и инициалы, курс, группа).
* Цель работы. Формулируется в соответствии с содержанием раздела «Цель работы», соответствующей практической работы.
* Необходимые принадлежности, задание.

Определяется в соответствии с указанной выше формулировкой и при необходимости уточняется в зависимости от содержания конкретной практической работы.

* Этапы выполнения работы. Последовательно по каждому из этапов приводится характеристика содержания выполненных по этапу работ.
* Выводы по работе. К этой части работы студент должен быть особенно внимательным. Формулируются выводы теоретического и практического характера о выполненной практической работе. Не следует указывать в выводах содержание и объем выполненных работ.

Текст отчета должен быть изложен лаконично и вместе с тем информативно с соблюдением правил грамматики. В конце отчета может быть указана литература, которую студент применил в практической работе. Библиографические описания литературных источников должны быть оформлены в соответствии с ГОСТ 7.1-84. Правила библиографического описания документации.

1. Заключительная часть практической работы.

После окончания составления отчета студент проверяет его правильность и устраняет ошибки. При условии отсутствия ошибок предъявляет экранный отчет преподавателю. Преподаватель читает текст отчета и принимает его. При условии замеченных ошибок преподаватель указывает студенту на эти ошибки. После этого студент исправляет ошибки и повторно предъявляет отчет преподавателю.

После завершения полного объема работ, исправления ошибок по замечаниям преподавателя, сохраняет отчет, выходит из системы и выключает компьютер.

1. **ПРАВИЛА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ**

При выполнении практических работ (ПР), студенты должны соблюдать и выполнять следующие правила:

1. Прежде, чем приступить к выполнению работы, обучающийся должен подготовить ответы на теоретические вопросы к ПР.
2. Перед началом каждой работы проверяется готовность обучающегося к ПР.
3. После выполнения ПР студент должен представить отчет о проделанной работе в собственном файле (в ПК) и подготовиться к обсуждению полученных результатов и выводов.
4. Студент (обучающийся), пропустивший выполнение ПР по уважительной или неуважительной причинам, обязан выполнить работу в дополнительно назначенное время.
5. Оценка за практическую работу выставляется с учетом предварительной подготовки к работе, доли самостоятельности при ее выполнении, точности и грамотности оформления отчета по работе.

**5. КРИТЕРИИ ОЦЕНКИ ПРАКТИЧЕСКИХ РАБОТ**

Практические работы оцениваются по пятибалльной шкале.

* оценка «5» (отлично) ставится, если работа выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, необходимые программы запущены и работают без ошибок; работа оформлена аккуратно;
* оценка «4» (хорошо) ставится, если работа выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, частично с помощью преподавателя, присутствуют незначительные ошибки при запуске и эксплуатации (работе) необходимых программ; работа оформлена аккуратно;
* оценка «3» (удовлетворительно) ставится, если работа выполнена в полном объеме, в соответствии с заданием, частично с помощью преподавателя, присутствуют ошибки при запуске и работе требуемых программ; по оформлению работы имеются замечания;
* оценка «2» (неудовлетворительно) ставится, если обучающийся не подготовился к работе, при запуске и эксплуатации (работе) требуемых программ студент допустил грубые ошибки, по оформлению работы имеются множественные замечания.
1. **ПРАВИЛА ВНУТРЕННЕГО РАСПОРЯДКА И ТЕХНИКА БЕЗОПАСНОСТИ ПРИ ВЫПОЛНЕНИИ ПРАКТИЧЕСКИХ РАБОТ**

При выполнении практических работ во избежание несчастных случаев, а также преждевременного выхода из строя персональных компьютеров и оборудования студент должен выполнять следующие правила внутреннего распорядка и техники безопасности:

1. К работе в кабинете (лаборатории) допускаются студенты, знакомые с правилами внутреннего распорядка и техники безопасности, изучившие содержание предстоящей практической работы, представившие отчет за предыдущую практическую работу.
2. После ознакомления с правилами внутреннего распорядка и инструктажа по технике безопасности каждый студент должен расписаться в специальном журнале.
3. При работе в кабинете (лаборатории) запрещается приносить собой вещи и предметы, загромождающие рабочие места.
4. Приступая к работе, каждый студент занимает место за «своим» ПК
5. В кабинете (лаборатории) запрещается громко разговаривать, покидать рабочие места без разрешения преподавателя и переходить от одного ПК к другому.
6. Во время небольших перерывов в работе не обязательно выключать компьютер.
7. При появлении запаха гари или при обнаружении повреждения изоляции, обрыва провода следует немедленно сообщить о неисправности преподавателю.
8. Прикасаться к задней панели работающего системного блока (процессора) запрещается.
9. Недопустимо попадание влаги на системный блок, дисплей, клавиатуру и другие устройства.
10. При выполнении практической работы необходимо занять правильную рабочую позу:
* следует сидеть прямо (не сутулясь) и опираться спиной о спинку кресла. Прогибать спину в поясничном отделе нужно не назад, а, наоборот, немного вперед. Недопустимо работать, развалившись в кресле. Такая поза вызывает быстрое утомление, снижение работоспособности.
* Необходимо найти такое положение головы, при котором меньше напрягаются мышцы шеи. Рекомендуемый угол наклона головы – до 20°. В этом случае значительно снижается нагрузка на шейные позвонки и на глаза.
* Положение рук и ног: во время работы за компьютером необходимо расслабить руки, держать предплечья параллельно полу, на подлокотниках кресла, кисти рук – на уровне локтей или немного ниже, запястья – на опорной планке. Тогда пальцы получают наибольшую свободу передвижения. Колени должны располагаться на уровне бедер или немного ниже. При таком положении ног не возникает напряжение мышц. Нельзя скрещивать ноги, класть ногу на ногу – это нарушает циркуляцию крови из-за сдавливания сосудов. Лучше держать обе стопы на подставке или на полу. Необходимо сохранять прямой угол (90°) в области локтевых, тазобедренных, коленных и голеностопных суставов.
* При ощущении усталости глаз нужно в течение 2—3 мин. окинуть взглядом аудиторию (лабораторию), устремлять взгляд на разные предметы, смотреть вдаль (в окно).
1. Если резко возникло общее утомление, появилось дрожание изображения на экране дисплея (покачивание, подергивание, рябь), следует сообщить об этом преподавателю.
2. Выполнение практической работы должно происходить в соответствии с правилами выполнения практических работ (п. 4).

**7. ТЕМАТИКА ЛАБОРАТОРНО-ПРАКТИЧЕСКИХ РАБОТ И ЗАДАНИЯ К НИМ**

**Лабораторная работа 1.**

**Тема**:. 1. Виды информации и основные методы ее защиты

Цель занятия: Приобрести навыки анализа требований к информационной безопасности

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить теоретический̆ материал по курсу «Основы информационной̆ безопасности».

2. Изучить соответствующий̆ теоретический̆ материал по курсу «Програм-мирование».

3. Написать на языке Си программу, реализующую поставленную задачу.

4. Проанализировать проделанную работу и предложить свой метод проти- воздействия реализованной̆ атаке.

5. Результат отразить в отчете.

**Контрольные вопросы**

1. Кратко сформулируйте виды безопасности для соответствующих сфер жизнедеятельности личности, общества и государства.

2. В чем состоят источники угроз интересам личности?

3. В чем состоят источники угроз интересам общества?

4. В чем состоят источники угроз интересам государства?

5. Перечислите виды информации и основные методы ее защиты.

6. В чем состоят национальные интересы Российской Федерации в информационной̆ сфере и их что собой̆ представляет их обеспечение.

7. Раскройте понятие информационно-безопасного шифрования.

8. В чем состоит сложность использования симметричных криптографических систем?

9. В чем заключаются слабости решения с помощью псевдослучайных генераторов чисел? 10. Приведите несколько примеров применения одноразовых блокнотов.

11. Расскажите о методах противодействия данной̆ атаке.

**Лабораторно-практическая работа 2.**

**Тема**:Виды угроз информационной̆ безопасности Российской̆ Федерации.

Цель занятия: Приобрести знания по основным видам угроз

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Виды угроз информационной безопасности »

2. Проанализировать проделанную работу и предложить свой метод защиты от угрозы.

3. Результат отразить в отчете.

Содержание отчета

Отчет должен содержать:

1. Виды угроз.

2. Вывод, в котором предлагаются методы защиты от основных видов угроз.

**Контрольные вопросы**

1. Какие виды угроз вы знаете?

2. В чем состоят источники угроз?

3. Перечислите виды информации.

4. В чем состоят основные способы защиты от угроз?

**Лабораторно-практическая работа 3.**

**Тема**: Источники угроз информационной̆ безопасности Российской̆ Федерации.

Цель занятия: Ознакомиться с алгоритмами оценки риска информационной безопасности Российской̆ Федерации.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Ч а с т ь 3 «Методы менеджмента безопасности информационных технологий»

2. Ознакомьтесь с Приложениями C, D и Е ГОСТа.

3. Выберите три различных информационных актива организации (см. вариант).

4. Из Приложения D ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

5. Пользуясь Приложением С ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

6. Пользуясь одним из методов (см. вариант) предложенных в Приложении Е ГОСТа произведите оценку рисков информационной безопасности.

7. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

**Контрольные вопросы**

1. Классифицировать способы воздействия угроз?

2. Описать подходы к оценки риска?

3. Цели безопасности согласно ISO.

4. Понятие политики безопасности?

**Лабораторно-практическая работа 4.**

**Тема**:Анализ информационной̆ инфраструктуры государств

Цель занятия: Ознакомление с основными принципами обеспечения информационной безопасности в ведущих странах.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

 1. Подготовить краткий доклад по заданному вопросу, используя учебное пособие Аверченкова, В.И. "Системы защиты информации в ведущих зарубежных странах" и другие доступные источники информации.

Вариант – номер по списку в журнале.

|  |  |  |  |
| --- | --- | --- | --- |
| **Страна** | **Основныепринципыобеспечения ИБ** | **Основные документы в области обеспечения ИБ** | **Структура государственных****органов обеспечения национальной ИБ** |
| **США** | 1 | 2 | 3 |
| **Евросоюз** | 4 | 5 | 6 |
| **Великобритания** | 7 | 8 | 9 |
| **Швеция** | 10 | 11 | 12 |
| **Франция** | 13 | 14 | 15 |
| **Германия** | 16 | 17 | 18 |
| **Китай** | 19 | 20 | 21 |
| **Япония** | 22 | 23 | 24 |
| **Швейцария** | 25 | 26 | 27 |

2. Заполнить таблицу " Системы обеспечения ИБ в ведущих зарубежных странах "(см. вариант) на основе подготовленного материала, а также докладов других студентов.

3. Провести анализ собранной информации и сделать выводы.

**Контрольные вопросы**

1. Виды организации организационно –правовых угроз?

2. Понятие субъекта и объекта безопасности?

3. Перечислите основные виды тайн?

4. В чем состоят основные способы защиты Информационной безопасности?

**Лабораторно-практическая работа 5.**

**Тема**:. 5.Исследование атаки переполнения буфера как примера нарушения

конфиденциальности, целостности и доступности информации

Цель занятия: Получить представление о возникновении и механизме эксплуатации уязвимости переполнения буфера.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Найти или написать программу, уязвимую с точки зрения переполнения буфера.

2. Описать, в какой именно функции содержится ошибка, приведшая к возникновению уязвимости, и каков алгоритм эксплуатации этой уязвимости.

3. Исследовать программу с точки зрения нарушителя (путем подачи различных аргументов на вход по реакции программы.

4. Написать программу-exploit, выполняющую формирование входных данных для уязвимой программы (с подбором длины буфера) таким образом, чтобы передать управление на произвольный код (для этого необходимо сформировать этот shellcode для подачи на вход уязвимой программы с тем, чтобы затем передать управление на этот shellcode).

5. Подробно описать в отчете процесс поиска и эксплуатации уязвимости, используемые для этого методы и инструменты (включая формирование shellcode).

**Контрольные вопросы**

1. Методы противодействия атакам по переполнению буфера?

2. Что такое программа exploit?

3. Каковы могут быть последствия атаки в различных операционных систе- мах?.

4. Какие основные способы защиты от угроз информационной безопасности внутри операционной системы?

**Лабораторно-практическая работа 6.**

**Тема**:Виды, каналы утечки и искажения информации

Цель занятия: Приобрести знания по основным каналам утечки информации

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Каналы утечки информации»

3. Проанализировать проделанную работу и предложить свой метод защиты от различных каналов утечки информации .

4. Результат отразить в отчете.

Содержание отчета

Отчет должен содержать:

1. Виды каналов .

2. Вывод, в котором предлагаются методы защиты от основных каналов утечки информации.

**Контрольные вопросы**

1. Основные каналы утечки информации?

2. В чем заключается проблема защиты от основных каналов утечки информации?

3. Перечислите способы защиты от каналов утечки информации .

4. В чем состоят основные способы защиты?

**Лабораторно-практическая работа 7.**

**Тема**:Технические средства и методы защиты информации.

Цель занятия: Получить практический опыт в классификации методов и средств защиты информации

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу

2. Составить таблицу в электронном документе с описание средств защиты и способов защиты от технических каналов утечки информации .

4. Результат отразить в отчете.

Содержание отчета

Отчет должен содержать:

1. Виды технических каналов утечки информации .

2. Вывод.

**Контрольные вопросы**

1. Перечислите основные каналы утечки информации

2. В чем состоят источники угроз?

3. Перечислите виды информации которые требуют защиты от утечки данных.

4. В чем состоят основные способы защиты от угроз по техническим каналам утеки информации?

**Лабораторно-практическая работа 8.**

**Тема**:Программно-аппаратные средства обеспечения информационной̆

безопасности.

Цель занятия: Изучение функционирования программного обеспечения для информационной безопасности

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить основные программные средства для защиты информации

2. Составить таблицу и заполнить таблицу с помощью программы Microsoftword

|  |  |
| --- | --- |
| **Тип угрозы информационной безопасности**  | **Программа для предотвращения угроз** |
|  |  |

**Контрольные вопросы**

1. Что представляет собой межсетевой экран?

2. Как защитить информацию от несанкционированного доступа ?

3. В чем заключаются функции системы обнаружения атак?

**Лабораторно-практическая работа 9.**

**Тема**:Испытания программных средств защиты

Цель занятия: Изучение функционирования программного обеспечения для информационной безопасности и в частности программного обеспечения VIPNET OFFICE FIREWALL, приобретение навыков по работе с данным продуктом.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить назначение, основные возможности ПО VIPNET OFFICE FIREWALL

2. Систему окон и меню ПО VIPNET OFFICE FIREWALL

**Контрольные вопросы**

1. Что представляет собой внешний интерфейс?

2. Что представляет собой внутренний интерфейс?

3. Что представляют собой режимы безопасности интерфейса?

4. Что такое антиспуфинг?

5. В чем заключаются функции режима «Бумеранг»?

6. В чем заключаются правила фильтрации IP-трафика?

**Лабораторно-практическая работа 10.**

**Тема**:Защита от утечек по каналу ПЭМИН, по акустическому и виброаккустическому каналам.

Цель занятия: Получить практический опыт получения данных по каналу ПЭМИН, по акустическому и виброаккустическому каналам.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 4часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу

2. Составить таблицу в электронном документе с описание технических средств излучающих побочные электромагнитные сигналы.

3. Описать различные источники получения данных по акустическому каналу

**Контрольные вопросы**

1. Что такое Побочные электромагнитные излучения

2. В чем состоят угроз канала ПЭМИН?

3. Перечислите виды информации которые можно получить по виброакустическому каналу

4.Основные способы защиты от угроз по техническим каналам утеки информации?

**Лабораторно-практическая работа 11.**

**Тема**:Классификация программ по защите информации.

Цель занятия: Изучить основные программы по защите данных

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу

2. Составить таблицу в электронном документе с описание основных программ по защите от вредоносного ПО и несанкционированного доступа при передачи данных.

3. Описать различные источники заражения ПК вредоносными программами

**Контрольные вопросы**

1. Что такое антивирус и для каких целей применяется

2. В чем состоят угроз несанкционированного доступа к данным?

3. Перечислите виды информации ?

4.Основные способы защиты данных?

**Лабораторно-практическая работа 12.**

**Тема**:Создание зашифрованного канала передачи данных.

Цель занятия: Изучить основы программы PGP для шифрования данных

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

Работа выполняется группами по два-три человека. Каждый̆ член группы должен:

1 Создать пару ключей̆ для использования шифрации с открытым ключом;

2 Выполнить экспорт своего открытого ключа и передачу его всем членам

группы;

3 Выполнить шифрацию произвольного сообщения для каждого члена груп-

пы и отправку зашифрованного сообщения адресатам;

**Контрольные вопросы**

1. Что такое открытый ключ, поясните механизм работы шифрования с открытым ключом.

2. Что такое цифровая подпись.

3. Кем была создана программа PGP.

4. Почему программа PGP обеспечивает очень высокую степень защиты за-

шифрованных файлов.

5. Что такое электронный сертификат, может ли электронный̆ сертификат со-

задаваться с помощью программы PGP.

**Лабораторно-практическая работа 13.**

**Тема**: Сетевое сканирование

Цель занятия: Изучить основные возможности сетевого сканирования

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Установите программу LanSurfer;

2. После установки запустите программу.

3. Создайте LANprofiles. Для этого выберите пункт меню OptionsВ раскрывшемся окне выберите пункт LANprofiles

5. Щелкните мышкой̆ по кнопке Greate

6. Вверху справа активируется строка ввода диапазона адресов для сканирования компьютеров, расшаренных папок и серверов влокальной̆ сети и составления списка сети, содержащего исчерпывающую информацию икомпьютерах и ресурсах сети.

7. Щелкните кнопкой̆ мыши по зеленому плюсу

8. Появиться окно, в котором необходимо ввести начальныӗ IP-адрес и последний̆ адрес диапазона IP-адресов

9. Введите диапазон адресов вручную или используя кнопки Local IP или 1..254

10. Нажмите кнопку ADD

11. Вверху в пункте Lanprofilecaption введите имя вашего профиля и нажмите Save

12. После этого выйдите из режима настройки профиля нажав кнопку Close

13. Выполните сканирование сети. Для этого нажмите кнопку StartLanScaning

14. После сканирования на экран выведется список ПК, серверов, маршрутизаторов, общедоступных папок.

15. Для поиска необходимого файла в сети используется Кнопка SearchonLan

16. В поисковой̆ строке программы вводите имя файла и нажимаете кнопку Start

17. Ниже будет выведен список искомых файлов

**Контрольные вопросы**

1. Что такое IP адрес?

2. Для каких целей следует применять сетевое сканирование

4. Опишите алгоритм нахождения файла программы MyTestXSetup.exe

**Лабораторно-практическая работа 14.**

**Тема**:Анализ трафика и сбор критичной̆ информации программами пассив-

ного анализа

Цель занятия: Применение методов и технологий испытания программного и аппаратного уровней̆ комплексной̆ защиты информации для проведения атаки на КИС с целью установления уязвимостей̆.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить теоретический̆ материал по курсу «Основы информационной̆ безопасности».

2. Изучить соответствующий̆ теоретический материал по теме лабораторной̆ работы.

3. Провести проверку, реализующую поставленную задачу.

4. Проанализировать проделанную работу и предложить возможный̆ метод

противодействии атаке.

5. Результат с рекомендациями по защите анализируемой̆ сети и ПЭВМ от- разить в отчете

**Контрольные вопросы**

1. В чем заключается угроза пассивного анализа?

2. Что положено в основу атаки?

3. Раскройте понятие «трафик» в вычислительной̆ системе.

4. Какова роль анализа трафика системе?

5. Какие средства позволяют реализовать пассивный анализ?

6. Расскажите о методах противодействия данной атаке.

7. Какие недостатки присущи пассивному анализу?

**Лабораторно-практическая работа 15.**

**Тема**:Дистанционное управление компьютером.

Цель занятия: Получить практический опыт управления компьютером по сети по средствам программы TeamViewer.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 4часа.

**Задание:**

Работа состоит из следующих этапов:

1. Установить программу на ПК

2. Получить адрес, пароль для удаленного подключения.

3. Войти в мой компьютер ПК к которому был получен удаленный доступ

**Контрольные вопросы**

1. Для каких целей можно использовать удаленный доступ

2. В чем состоят угрозы при получение несанкционированного доступа?

3. Перечислите виды информации которые можно получить по средства НСД

4.Основные способы защиты от угроз?

**Лабораторно-практическая работа 16.**

**Тема**:Обнаружение уязвимостей̆ по сигнатурам.

Цель занятия: применение методов и технологий испытания программного и аппаратного уровней̆ комплексной̆ защиты информации для проведения атаки на КИС с целью установления уязвимостей̆.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Описание атак по анализу топологии сети,

2. Описание определения внутренней доменной структуры и установленных

сервисов.

3. Описание определения средств межсетевого экранирования, признаков работы сервисов по нестандартным портам и типов примененных операци-онных систем.

4. Алгоритм, функциональная схема и функциональный состав проверки. 5. Вывод, в котором предлагаются решения повышения защищенности КИС.

Контрольные вопросы

1. В чем заключается угроза уязвимости по сигнатурам?

2. Что положено в основу определения уязвимости по сигнатурам?

3. Раскройте понятие «Сигнатура» в контексте защиты информации в вы-

числительной системе.

4. Какова роль сигнатуры в операционной системе?

5. Какие средства позволяют реализовать атаку на уязвимость?

6. Расскажите о методах противодействия данной атаке.

**Лабораторно-практическая работа 17.**

**Тема**:Сетевые помехоподавляющие фильтры

Цель занятия: Изучение принцип действия сетевых помехоподавляющих фильтров.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить назначение сетевых помехоподавляющих фильтров

2. Создать в электронном документе таблицу с описанием моделей сетевых помехоподавляющих фильтров

3. Составить отчет по выбору помехоподавляющего фильтра для защиты информации

**Контрольные вопросы**

1. Что представляет собой сетевой фильтр?

2. Какие угрозы могут быть реализованы при отсутствие сетевого помехоподавляющего фильтра?

3. Что представляют собой помехи на линиях связи?

4. В чем заключаются правила фильтрации IP-трафика?

**Лабораторно-практическая работа 18.**

**Тема**:Анализ угроз и рисков комплексной̆ защиты информации на объекте с

использованием системы «Гриф»

Цель занятия: Применение принципов организации, проектирования и анализа систем защиты информации и основ их комплексного построения на различных уровнях защиты.

 Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить теоретический̆ материал по курсу «Основы информационной̆ безопасности».

2. Выполнить работу по анализу угроз и рисков с использованием системы «Гриф».

3. Проанализировать проделанную работу и предложить метод внедрения системы «Гриф» на предприятии.

4. Результат отразить в отчете.

Отчет должен содержать:

1. Описание организации проведения анализа угроз и рисков на предпри-ятии.

2. Формальный̆ отчет по результатам анализа.

3. Вывод, в котором предлагаются методы решения проблемы защиты ин-

формации.

**Контрольные вопросы**

1. В чем заключается угроза раскрытия информации? Какие еще угрозы Вы знаете?

2. Что положено в основу системы «Гриф»?

3. Какова роль руководителя системе «Гриф»?

4. Какие средства позволяют реализовать систему «Гриф» на предприятии?

5. Приведите несколько примеров расчета рисков при изменении системы

защиты информации.

6. Какие недостатки присущи системе «Гриф»?

**Лабораторно-практическая работа 19.**

**Тема**:Анализ и управление политикой̆ информационной̆ безопасности на

объекте с использованием системы «Кондор»

Цель занятия: Применение принципов организации, проектирования и анализа систем защиты информации и основ их комплексного построения на различных уровнях защиты.

 Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».

2. Выполнить работу по анализу угроз и рисков с использованием системы «Кондор».

3. Проанализировать проделанную работу и предложить метод внедрения системы «Кондор» на предприятии.

4. Результат отразить в отчете.

Отчет должен содержать:

1. Описание организации проведения анализа и управления информационной̆ безопасности на предприятии.

2. Формальный̆ отчет по результатам анализа.

3. Вывод, в котором предлагаются методы решения проблемы защиты ин-

формации.

**Контрольные вопросы**

1. Перечислите источники угроз безопасности информации предприятия.

2. В чем заключается угроза НСД?

3. Что положено в основу санкционированного доступа?

4. Раскройте понятие «Управление политикой̆ безопасности» в контексте

защиты информации в вычислительной̆ системе.

5. Какие средства позволяют реализовать систему «Кондор»? 6. Какие недостатки присущи системе «Кондор»?

**Лабораторно-практическая работа 20.**

**Тема**:Аудит комплексной̆ защиты информации предприятия

Цель занятия: Применение принципов организации, проектирования и анализа систем защиты информации и основ их комплексного построения на различных уровнях защиты.

 Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить теоретический̆ материал по курсу «Основы информационной̆ безопасности».

2. Выполнить работу по аудиту комплексной̆ защиты информации предприятия.

3. Проанализировать проделанную работу и предложить свой метод проведения аудита комплексной̆ защиты информации на предприятии.

4. Результат отразить в отчете.

1. Описание организации проведения Аудита на предприятии.

2. Формальный̆ отчет по результатам Аудита.

3. Вывод, в котором предлагаются методы решения проблемы защиты ин-

формации.

**Контрольные вопросы**

1. Кратко сформулируете виды Аудита КЗИ.

2. В чем состоят источники успеха Аудита?

3. Раскроите понятие «Сюрвей».

4. В чем состоит сложность применения Аудита КЗИ?

5. В чем заключаются слабости внутреннего Аудита силами предприятия?

6. Приведите несколько примеров успешного применения Аудита.

**Лабораторно-практическая работа 21.**

**Тема**:Технические средства защиты информации в телефонных линиях

Цель занятия: Получение студентами навыков работы с аппаратурой̆ защиты речевой информации в телефонных линиях.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить основные приборы и принцип их работы

2. Составить таблицу отличий основных приборов

3. Проанализировать проделанную работу.

4. Результат отразить в отчете.

**Контрольные вопросы**

1.Опишите принципы работы аппаратуры на линиях связи.

2. Опишите прибор «ПРОКРУСТ-2000»

3. В чем состоит сложность применения технические средства защиты информации в телефонных линиях?

4. Опишите основные виды угроз на линиях связи.

**Лабораторно-практическая работа 22.**

**Тема**:Технические средства обнаружения, локализации

средств негласного получения информации.

Цель занятия: Ознакомление студентов с работой̆ аппаратуры

защиты информации, работающей̆ в радиодиапазоне.

 Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Лабораторная работа является демонстрационной̆ и представляет собой̆ рассказ и показ преподавателем принципов работы и применения современных технических средств обеспечения информационной̆ безопасности

Работа состоит из следующих этапов:

1. Работа с прибором РRОТЕСТ 1203.

2. Работа с прибором D 008

3. Работа с прибором МFР-8000.

4. Работа с прибором SТ031Р

5.Составить отчет

**Контрольные вопросы**

1.Опишите принципы работы аппаратуры для обнаружения подслушивающих устройств.

2. Опишите основные отличия приборов для защиты от негласного получения информации

3. В чем состоит сложность применения технические средства защиты?

**Лабораторно-практическая работа 23.**

**Тема**:Нейтрализации радиоизлучающих специальных технических устройств.

Цель занятия:Ознакомление студентов с работой̆ аппаратуры защиты информации, работающей̆ в проводных линиях различного назначения

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить основные приборы и принцип их работы

2. Составить таблицу отличий основных приборов

3. Проанализировать проделанную работу.

4. Результат отразить в отчете.

**Контрольные вопросы**

1.Опишите принципы работы аппаратуры в проводных линиях.

2. Для каких целей служит генератор СОНАТА-РС1

3. В чем состоит сложность применения устройств в проводных линиях связи?

4. Опишите основные виды угроз в проводных линиях связи.

**Лабораторно-практическая работа 24.**

**Тема**:Контроль эффективности защиты речевой̆ информации с помощью программно-аппаратного комплекса «СПРУТ- МИНИ»

Цель занятия: ознакомление студентов с работой̆ программно- аппаратного комплекса «СПРУТ-МИНИ».

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия –2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Провести оценку эффективности защиты речевой̆ информации от утечки по акустическому каналу.

2.Оценка эффективности защиты речевой̆ информации от утечки по виброакустическому каналу

3. Анализ результатов измерений.

4. Результат отразить в отчете.

**Контрольные вопросы**

1.Опишите принципы работы программно-аппаратного комплекса «СПРУТ- МИНИ».

2. Опишите угрозы против которых выступает программно-аппаратный комплекс «СПРУТ- МИНИ»

4. Опишите основные технические каналы утечки информации.

**Лабораторно-практическая работа 25.**

**Тема**:Поиск и измерение побочных электромагнитных излучений и наводок с помощью программно-аппаратного комплекса

«НАВИГАТОР-П3Г».

Цель занятия: ознакомление студентов с работой̆ программно-

аппаратного комплекса «НАВИГАТОР-П3Г».Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 4 часа.

**Задание:**

Работа состоит из следующих этапов:

Лабораторная работа проводится преподавателем в демонстрационном режиме.

1.Устанавливается оборудование

2.Запускается программа «Измерительная задача»

3.Поиск и измерение сигналов ПЭМИН монитора методом разности панорам.

3. Анализ результатов измерений.

4. Результат отразить в отчете.

**Контрольные вопросы**

1.Опишите принципы работы программно-аппаратного комплекса «НАВИГАТОР-П3Г».

2. Опишите угрозы против которых выступает программно-аппаратный комплекс«НАВИГАТОР-П3Г».

3. Опишите основные технические каналы утечки информации способы противодействия?

**Лабораторно-практическая работа 26.**

**Тема**:Акустические и виброакустические каналы утечки

Цель занятия: ознакомление студентов с акустическим и выброакустическим каналом утечки данных

.Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

Лабораторная работа проводится преподавателем в демонстрационном режиме.

1.Составить список основных источников акустических и выброакустических каналов утечки информации

2.описать средства для защиты от акустических и выброакустических каналов утечки информации

3. описать приборы и их возможности для защиты от акустических и выброакустических каналов утечки информации

4. Результат отразить в отчете.

**Контрольные вопросы**

1.Опишите принципы работы систем защиты от акустических и выброакустических каналов утечки информации».

2. Опишите основные источники возникновения акустических и выброакустических каналов утечки информации

3. В чем состоит сложность применения технические средства защиты информации в телефонных линиях?

4. Опишите основные виды угроз на линиях связи.

**Лабораторно-практическая работа 27.**

**Тема**:Побочные ЭМИ от средств обработки информации

Цель занятияисследовать возможности защиты информации посредством применения генераторов шума «ГНОМ-3»

.Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

Лабораторная работа проводится преподавателем в демонстрационном режиме.

1.Составить таблицу возможностей

2.Научиться управлять ГШ-Гном 3.

3 .Подготовить ответы на вопросы

**Контрольные вопросы**

1.Для чего служит элементарный магнитный излучатель

2.Опишите электромагнитные каналы утечки информации ТСПИ

3. Опишите электрические каналы утечки информации

4. Какие средства защиты от ЭМИ вы знаете?

**Лабораторно-практическая работа 28.**

**Тема**:Исследование оптоэлектронного канала утечки информации

Цель занятия: Исследовать лазерные акустические локационные системы.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Составить таблицу возможностей лазерных акустических локационных систем

2.Описать модели лазерных акустических локационных систем

3 .Подготовить ответы на вопросы

**Контрольные вопросы**

1.Для чего служат лазерные акустические локационные системы?

2.Опишите Акустический канал утечки информации?

3. Опишите электрические каналы утечки информации

4. Какие средства защиты от акустического канала утечки информации вы знаете?

**Лабораторно-практическая работа 29.**

**Тема**:Технические средства защиты от утечек информации по проводным линиям

Цель занятия: Исследовать системы защиты информации на проводных линиях.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Составить таблицу различных угроз на проводных линиях

2. Описать модели приборов и систем для защиты данных на проводных линиях

3.Подготовить ответы на вопросы

**Контрольные вопросы**

1. Для чего служат проводные линии связи?

2. Какие угрозы возможны осуществить в проводных линиях связи?

3. Опишите технические каналы утечки информации?

4. Какие средства защиты проводных линий вы знаете?

**Лабораторно-практическая работа 30.**

**Тема**:Идентификация с помощью биометрических устройств

Цель занятия: Исследовать системы контроля доступа и разграничения доступа по средствам биометрии человека.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Составить таблицу биометрических способов , которые могут применяться для защиты данных в системах контроля и управления доступа

2. Описать модели приборов и систем для защиты данных

3. Подготовить ответы на вопросы

**Контрольные вопросы**

1. Для чего системы контроля и управления доступом ?

2. Какие способы защиты с помощью биометрических данных применяются чаще всего?

3. Опишите технические каналы утечки информации?

4. Опишите технические средства защиты, в которых применяются биометрические параметры?

**Лабораторно-практическая работа 31.**

**Тема**:Применение активных и пассивный пластиковых карт

Цель занятия: Исследовать различия между пассивными и активнами картами.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Изучить материал по картам использующихся в системах контроля и управления доступом

2. Описать основные отличия пассивных и активных карт

3. Подготовить ответы на вопросы

**Контрольные вопросы**

1. Для каких целей системы контроля и управления доступом используют активные карты?

2. Какие способы защиты данных с помощью пластиковых карт применяются чаще всего?

3. Опишите технические каналы утечки информации от которых защищают активные пластиковые карты?

4. Опишите технические средства защиты, в которых применяются пассивные пластиковые карты?

**Лабораторно-практическая работа 32.**

**Тема**:Применение парольных систем различного типа

Цель занятия: Исследовать парольные системы используемые для контроля и разграничения доступа

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить материал парольным системам и различным видам моделей безопасности

2. Описать основные правила генерации паролей

3. Подготовить ответы на вопросы

**Контрольные вопросы**

1. Для каких целей применяются парольные системы в нутри операционных систем?

2. Какие модели защиты данных и разграничения вы знаете?

3. Опишите технические каналы утечки информации от которых защищают парольные системы ?

4. Опишите технические средства защиты, в которых применяются парольные системы защиты данных ?

**Лабораторно-практическая работа 33.**

**Тема**: Статистический анализ загрузки заданного радиодиапазона и обнаружение радио закладных устройств в защищаемом помещении

Цель занятия: Изучить методы статистического анализа заданного радиодиапазона и обнаружения радио микрофонных закладок с помощью компьютеризированных комплексов RS turbo.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 4 часа.

**Задание:**

Работа состоит из следующих этапов:

Работа проводиться в режиме демонстрации

1. Ознакомиться с видами радио закладок и изучить методы их обнаружения.

2. Изучить работу комплексов в режиме обнаружения радио закладок.

3. Произвести настройку программы для работы в режиме «Радио». Выполнить один или несколько циклов сканирования заданного радиодиапазона. Обнаружить излучения без учета априорных данных за один цикл сканирования.

4. Посмотреть и проанализировать списки обнаруженных сигналов.

5. Для интересующего сигнала выполнить:

− спектральный̆ анализ сигналов излучений;

− анализ гармонического состава сигналов излучений;

− корреляционный̆ анализ откликов на акустические импульсы.

6. Выявить наличие радио закладногоустройства в контролируемом помещении.

**Контрольные вопросы**

1 Приведите определение закладочного устройства.

2 Перечислите демаскирующие признаки автономных не камуфлированных

акустических закладок.

3 Перечислите демаскирующие признаки полуактивных акустических радио закладок.

4 Какие технические средства применяют для выявления радио закладочных устройств?

5 Назначение комплекса «RS turbo». Перечислите состав комплекса «RS

turbo».

6 Радио закладки с каким видом модуляции обнаруживает комплекс «RS

turbo»?

7 Назовите базовую операцию в комплексе «RS turbo», предшествующую

обнаружению и идентификации источников излучений. 16

8 Как на следующем цикле сканирования формируется новая (текущая) таблица и модифицируются значения уровней̆ в таблице предыдущей̆ панорамы в соответствии с выбранным методом обработки?

9 С помощью каких операций выполняется автоматически или в ручном режиме идентификация (опознавание) сигналов подслушивающих устройств в программе «RS turbo»?

**Лабораторно-практическая работа 34.**

**Тема**:Обнаружение сигналов линейных и сетевых

закладок

Цель занятия: Изучить методы обнаружения сетевых и линейных закладок с помощью комплексов «RS turbo», «RS turboMobile-L»

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Изучить способы внедрения сетевых и линейных закладок.

3. Изучить принцип действия и порядок работы комплекса «RS turboMobile-L» на выявление сетевых и линейных закладок.

3. Подготовить ответы на вопросы

**Контрольные вопросы**

1. Для каких целей применяются линейные закладки?

2.Для каких целей применяются сетевые закладки ?

3. Опишите технические каналы утечки данных в которых применяются линейные закладки ?

4. Опишите технические средства защиты от сетевые закладки ?

**Лабораторно-практическая работа 35.**

**Тема**:35. Обнаружение оптических сигналов передатчиков ик-диапазона

Цель занятия: Обнаружение оптических сигналов передатчиков ИК – диапазона и анализ загрузки заданного радиодиапазона с помощью комплекса RS turboMobile-L.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Сформирование список «опасных» излучений, которые могут быть созданы передатчиками.

2. Выполнить операции анализа, необходимые для выявления среди множества обнаруженных сигналов подслушивающих устройств.

3. Подготовить ответы на вопросы

**Контрольные вопросы**

1. Приведите определение нелинейного объекта.
2. Приведите определение нелинейной локации.
3. На чем основан принцип действияоптического сигнала?
4. Как отличить полупроводниковой соединение от ложного?
5. Определите понятии эффекта затухания.
6. Для чего предназначен режим «20К»?

**Лабораторно-практическая работа 36.**

**Тема**:Программирование арифметических алгоритмов

Цель занятия: Исследование и разработка основных методов симметричных криптосистем.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. На языке DELPHI, VBA С++ или C# написать программу шифрования и дешифрования текстового файла методом, указанным преподавателем.

2. Составить отчет и ответить на вопросы

**Контрольные вопросы**

1. Цель и задачи криптографии.

2. Шифры одиночной перестановки и перестановки по ключевому слову.

3. Шифры двойной перестановки. Шифрование с помощью магического квадрата.

4. Отличия симметричной и ассиметричной криптосистемы

**Лабораторно-практическая работа 37.**

**Тема**:Программирование алгебраических алгоритмов

Цель занятия: Исследование и разработка классических методов симметричных криптосистем

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Используя шифры простой замены. Систему шифрования Цезаря произвести зашифровку и расшифровку сообщения

2. Используя шифры сложной замены. Шифр Гронсфельда произвести зашифровку и расшифровку сообщения

3. Составить отчет и ответить на вопросы

**Контрольные вопросы**

1. Цель и задачи криптографии.

2. Шифры простой замены ?

3. что представляет собой шифрование с помощью магического квадрата?

4. Отличия простой и сложной замены в шифровании?

**Лабораторно-практическая работа 38.**

**Тема**:Защита от закладок при разработке программ

Цель занятия: Исследование и анализ служебных программ Windows XP для повышения эффективности работы компьютера

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Установите проверку подлинности доступа к ресурсам компьютера из локальной сети.

2. Запретите доступ к ресурсам вашего компьютера из Интернета.

3Разрешить удаленный доступ к ресурсам вашего компьютера.

4. Защита и восстановление данных на компьютере

3. Составить отчет и ответить на вопросы

**Контрольные вопросы**

1. Цель и задачи закладок при разработке программ?

2. Основные способы защиты от закладок при разработке программ ?

3.Для каких целей следует использовать архивацию?

4.Назовите служебные программы Windows XP?

**Лабораторно-практическая работа 39.**

**Тема**:Программирование алгоритмов криптосистем с открытом ключом

Цель занятия: Исследование и анализ основных методов ассимметричных криптосистем

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Получить от пользователя ключ, имя входного и выходного файла.

2. Инициализировать генератор случайных чисел с помощью ключа. Открыть указанные файлы.

3. Прочитать строку из файла.

4. Получить случайное число.

5. Получить ASCII-код очередного символа строки и увеличить его на случайное число, полученное на шаге 4.

6. Проверить правильность (допустимый диапазон) нового ASCII-кода.

7. В выходную строку записать очередной символ, соответствующий ASCII-коду, полученному на шаге 6.

8. Если не достигли конца входной строки, то перейти к шагу 4.

9. Записать полученную строку в выходной файл.

10. Если не достигнут конец файла, то перейти к шагу 3.

11. Закрыть файлы

**Контрольные вопросы**

Вопросы для самопроверки

1. Алгоритм шифрации двойным квадратом. Шифр Enigma.

2. Алгоритм шифрования DES.

3. Алгоритм шифрования ГОСТ 28147-89.

4. Алгоритм шифрования RSA.

5. Алгоритм шифрования Эль Гамаля.

6. Задачи и алгоритмы электронной подписи.

7. Задачи распределения ключей.

**Лабораторно-практическая работа 40.**

**Тема**:Профилактика заражения вирусами компьютерных систем

Цель занятия: Исследование и анализ основных методов асимметричных криптосистем

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

 1. Выключить ЭВМ для уничтожения резидентных вирусов.

 2. Осуществить загрузку эталонной операционной системы со сменного носителя информации, в которой отсутствуют вирусы.

 3. Сохранить на сменных носителях информации важные для вас файлы, которые не имеют резервных копий.

4. Использовать антивирусные средства для удаления вирусов и восстановления файлов, областей памяти. Если работоспособность ЭВМ восстановлена, то осуществляется переход к шагу 8, иначе - к шагу 5.

5. Осуществить полное стирание и разметку (форматирование) несъемных внешних запоминающих устройств. В ПЭВМ для этого могут быть использованы программы MS-DOS FDISK и FORMAT. Программа форматирования FORMAT не удаляет главную загрузочную запись на жестком диске, в которой может находиться загрузочный вирус.

6. Восстановить ОС, другие программные системы и файлы с дистрибутивов и резервных копий, созданных до заражения.

7. Тщательно проверить файлы, сохраненные после обнаружения заражения, и, при необходимости, удалить вирусы и восстановить файлы;

8. Завершить восстановление информации всесторонней проверкой ЭВМ с помощью всех имеющихся в распоряжении пользователя антивирусных средств.

**Контрольные вопросы**

1. Назовите признаки классификации компьютерных вирусов.

2. Поясните принцип действия "стелс" - вирусов и полиморфных вирусов.

3. Приведите структуру файлового вируса и поясните алгоритм его работы.

4. В чем заключаются особенности алгоритмов функционирования макровирусов и загрузочных вирусов?

5. Дайте характеристику методов обнаружения вирусов.

6. Назовите методы удаления последствий заражения вирусами.

7. Перечислите профилактические меры предотвращения заражения вирусами КС.

8. Приведите порядок действий пользователя при заражении ЭВМ вирусами.

**Лабораторно-практическая работа 41.**

**Тема**:Биометрическая аутентификация пользователя по клавиатурному подчерку

Цель занятия: Исследование программы для распознания клавиатурного подчерка

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

 1. Составить таблицу параметров для распознавания клавиатурного подчерка

1. Скоростьввода
2. Динамикаввода
3. Частотавозникновениеошибокпривводе
4. Использованиеклавиш

2. Ответить на вопросы

**Контрольные вопросы**

1. Для каких целей следует применять аутентификацию по клавиатурного подчерку

2. Цель и задачи закладок при разработке программ?

3. Основные параметры клавиатурного подчерка?

4. Основные технические каналы утечки информации?

**Лабораторно-практическая работа 42.**

**Тема**:«Элементы криптоанализа. Оценка частотности символов в тексте»

Цель занятия: Исследование программы для распознания клавиатурного подчерка

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

 1. Открыть текстовый документ

 2. Запустить программу “частота символов”

 3. Исследовать частность символов в тексте

 2. Ответить на вопросы

**Контрольные вопросы**

1. Что понимают под криптоанализом?

2. Сформулируйте правило Керхоффа

3. Основные параметры клавиатурного подчерка ?

4. Основные технические каналы утечки информации?

**Лабораторно-практическая работа 43.**

**Тема**:Шифрование методами перестановки

Цель занятия: Ознакомление с историей становления криптографии, освоение алгоритма шифрования «двойными перестановками», криптоанализа сообщений, зашифрованных указанным алгоритмом.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Зашифровать предложение из 16 символов методом двойной перестановки и показать преподавателю.

2. Произвести криптоанализ перехваченного сообщения (выдает преподаватель).

3. Сравнить полученный и исходные ключи.

4. Разработать программы, позволяющие максимально автоматизировать процесс криптоанализа (автоматизированное рабочее место криптоаналитика).

**Контрольные вопросы**

1. Что понимают под криптоанализом?

2. Сформулируйте правило Керхоффа

3. Что представляет собой метод Виженера ?

4. Основные способы и методы криптографического закрытия данных?

**Лабораторно-практическая работа 44.**

**Тема**:Шифрование методами перестановки

Цель занятия: Отработать навыки применение различных шифров

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.В работе необходимо зашифровать свою фамилию с помощью следующих шифров:

- шифра Цезаря;

- лозунгового шифра;

- полибианского квадрата;

- шифрующей системы Трисемуса;

- шифра Playfair;

**Контрольные вопросы**

1. Что понимают под криптоанализом?

2. Чем отличается тметодТрисемуса и Виженера

3. Что представляет собой метод Playfaiа ?

4. Основные способы и методы криптографического закрытия данных ?

**Лабораторно-практическая работа 45.**

**Тема**:Шифрование методом гаммирования

Цель занятия: Отработать навыки применение шифрование методом гаммирования

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Используя один из алгоритмов гаммирования, составить программу, выполняющую шифрование и дешифрование текста.

2. Ответить на контрольные вопросы

**Контрольные вопросы**

1. В чем заключается принцип шифрования гаммированием?
2. Поясните, как происходит построение гаммы.
3. В чем слабость шифра гаммирования с неравновероятной гаммой?
4. Почему наложение на открытыйтектс гаммы, представляющей собой периодическую последоваетельность небольшого периода, не дает надежной защиты?

**Лабораторно-практическая работа 46.**

**Тема**:Методы криптографической защиты информации

Цель занятия: Отработать навыки применение различных шифров

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Создать таблицу с описанием и сравнением известных методов криптографического преобразования информации:

- шифрование;

- стеганография;

- кодирование;

- сжатие.

2 Ответить на вопрос

**Контрольные вопросы**

1. Объясните выражение – «совершенно стойкий шифр».

2. Почему недопустимо использовать дважды одну и ту же гамму для защиты открытых текстов?

3. Назовите преимущества и недостатки шифра Вернама?

4. Какие условия необходимы для обеспечения криптостойкости шифра гаммирования?

**Лабораторно-практическая работа 47.**

**Тема**:Простейшие алгоритмы шифрования

Цель занятия: Получить практический навык работы с криптографической системой шифрования данных, базирующейся на алгоритме шифровании ГОСТ

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Описать криптографическую систему шифрования данных, которая базируется на алгоритме шифровании ГОСТ, являющимся первым российским симметричным алгоритмом блочного шифрования данных.

2. Ответить на вопросы

**Контрольные вопросы**

1. Перечислить принципы формирования шифров, которые сформулировал Шеннон.
2. Какое правило Кергоффса является актуальным для современной криптографии.

3. Дать определение шифру замены.
4. Дать определение шифру перестановки.
5. Каким принципам должны удовлетворять преобразования, которые обеспечивают шифрование информации.
6. Какие арифметические операции используются в алгоритме ГОСТ.
7. Что является ключом шифра простой замены.
8. Число ключей в шифре замены.
9. Привести примеры шифров простой замены.
10. Привести примеры шифров многоалфавитной замены.
11. Существуют ли абсолютно стойкие шифры?
12. Чему равна длина ключа в абсолютно стойком шифре?
13. Перечислить режимы работы ГОСТ.

**Лабораторно-практическая работа 48.**

**Тема**:Шифр многоалфавитной замены — шифрование методом Вернама.

Цель занятия: Получить практический навык работы с многоалфавитной заменой

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Для многоалфавитного шифрования с фиксированным ключом определите, сколько одноалфавитных методов и с каким смещением используется в программе. Для этого нужно создать свой файл, состоящий из строки одинаковых символов, выполнить для него шифрование и по гистограмме определить способ шифрования и набор смещений.

2. Для многоалфавитного шифрования с ключом фиксированной длины: выполните шифрование и определите по гистограмме, какое смещение получает каждый символ для файла, состоящего из строки одинаковых символов;

3. Выполните шифрование и расшифрование для файла произвольного текста; просмотрите и опишите гистограммы исходного и зашифрованного текстов; ответьте, какую информацию можно получить из гистограмм.

4.Ответить на вопросы

**Контрольные вопросы**

1. Какие вы знаете методы криптографической защиты файлов?
2. В чем преимущества и недостатки одноалфавитных методов?

3. Если необходимо зашифровать текст, содержащий важную информацию, какой метод из рассмотренных вы выберете? Обоснуйте свой выбор
4. Дать определение шифру перестановки.

**Лабораторно-практическая работа 49.**

**Тема**:Зашифровать и расшифровать выданное сообщение с помощью алгоритма шифрования RSA.

Цель занятия: изучение и реализация алгоритма шифрования RSA. Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Составьте программное обеспечение, реализующее алгоритм RSA. Исходные данные должны передаваться через файлы: файл с открытым ключом, закрытым ключом и шифруемая информация.

2. Для созданного программного обеспечения проведите тестирование не менее чем на 10 различных наборах данных.

3.Ответить на вопросы

**Контрольные вопросы**

1. Какие вы знаете методы криптографической защиты файлов?
2. В чем преимущества и недостатки метода RSA?

3. Опишите алгоритм шифрования RSA?
4. Дать определение шифру перестановки.

**Лабораторно-практическая работа 50.**

**Тема**:Методы и алгоритмы стеганографического сокрытия данных

Цель занятия: Применение и реализация стенографического метода закрытия данных

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.в программе документах редактора MicrosoftWord за счет специфицеского форматирования символов текста использую таблицу кодировки зашифровать текст.

2.Ответить на вопросы

**Контрольные вопросы**

1. Число ключей в шифре замены.

2. Привести примеры шифров простой замены.

3. Привести примеры шифров многоалфавитной замены.

4. Существуют ли абсолютно стойкие шифры?

5. Чему равна длина ключа в абсолютно стойком шифре?

**Лабораторно-практическая работа 51.**

**Тема**: Оценка уязвимости коммутируемого доступа коммутируемого доступа коммутируемого доступа

Цель занятия: Применение методов и технологий испытания программного и аппаратного уровней̆ комплексной̆ защиты информации для проведения атаки на КИС с целью установления уязвимостей̆.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Изучить теоретический материал

2. Провести проверку сети, реализующую поставленную задачу.

3. Проанализировать проделанную работу и предложить возможный метод

противодействия атаке.

4. Результат с рекомендациями по защите анализируемой сети и ПЭВМ от- разить в отчете

**Контрольные вопросы**

Перечислите виды коммутируемого доступа.

2. Раскройте понятие коммутируемый доступ.

3. В чем состоит сложность использования коммутируемого доступа?

4. В чем заключаются слабости коммутируемого доступа ?

5. Приведите несколько примеров применения уязвимости коммутируемого

доступа.

6. Расскажите о методах противодействия данной атаке.

**Лабораторно-практическая работа 52.**

**Тема**: Произвести защиту вымышленного помещения

Цель занятия: Применение методов и технологий защиты для организации защиты вымышленного выделенного помещения

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 8 часов.

**Задание:**

Работа состоит из следующих этапов:

1. C помощью программы Visio составить схему этажа здания с указанием выделенного помещения

2. Создать вторую схему с указанием потенциальных путей утечки информации.

3. Указать методы и способы защиты выделенного помещения от указанных путей утечек информции .

4. Результат отразить в отчете

5. Ответить на вопросы

**Контрольные вопросы**

1.Для чего служат лазерные акустические локационные системы?

2.Опишите акустический канал утечки информации?

3. Опишите электрические каналы утечки информации

4. Какие средства защиты от акустического канала утечки информации вы знаете?

5. На какие группы делятся злоумышленники

**Лабораторно-практическая работа 53.**

**Тема**: Программно-аппаратный комплекс «спрут-7

Цель занятия: Изучить назначение комплекса Спрут-7, его состав и возможности. Изучить возможности управления комплексом при помощи специального программного обеспечения.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часов.

**Задание:**

Работа состоит из следующих этапов:

1. Составить описание работы программно-аппаратного комплекса «спрут-7.

2. Ответить на вопросы.

**Контрольные вопросы**

1. Перечислите источники угроз безопасности информации предприятия.

2. В чем заключается угроза НСД?

3. Что положено в основу санкционированного доступа?

4. Раскройте понятие «Управление политикой̆ безопасности» в контексте

защиты информации в вычислительной̆ системе.

**Лабораторно-практическая работа 54.**

**Тема**: Оценка защищенности ограждающих конструкций помещения от утечки информации

Цель занятия:Освоить навыки защиты помещения с помощью инженерных средств.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 6 часов.

**Задание:**

Работа состоит из следующих этапов:

1. Ознакомиться с материалами курса .

2. Проанализировать состояние физической защиты вымышленного помещения.

3. С учетом проделанной работы, предложить модернизацию системы инженерной защиты информации

2. Ответить на вопросы.

**Контрольные вопросы**

1. Кратко сформулируйте виды Аудита КЗИ.

2. В чем состоят источники успеха Аудита?

3. Раскройте понятие «Сюрвей».

4. В чем состоит сложность применения Аудита КЗИ?

5. В чем заключаются слабости внутреннего Аудита силами предприятия?

6. Приведите несколько примеров успешного применения Аудита.

**Лабораторно-практическая работа 55.**

**Тема**: Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласного

получения информации, использующих силовые линии сети переменного тока и линии систем охранной (пожарной̆) сигнализации

Цель занятия:Получить практические навыки работы с средствами обнаружения локализации и нейтрализации специальных технических средств негласногополучения информации

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Составить таблицу основных угроз и сопоставить средство защиты,обнаружения локализации и нейтрализации специальных технических средств

2. Проанализировать проделанную работу и предложить свой метод проведения комплексной̆ защиты информации.

2. Ответить на вопросы.

**Контрольные вопросы**

1. Для каких целей используется прибор D 008

2. В чем состоят источники успеха Аудита?

3. Назовите основные средства для негласного получения информации?

4. В чем заключаются слабости внутреннего Аудита силами предприятия?

**Лабораторно-практическая работа 56.**

**Тема**: Анализ систем видеонаблюдения

Цель занятия:Изучение назначения, основных характеристик и принципа подключения устройств видеонаблюдения

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Составить таблицу основных средств для скрытого видеонаблюдения с описанием характеристик

2. Составить отчет, ответить на вопросы

**Контрольные вопросы**

1. Для каких целей используется видеонаблюдения?

2. В чем заключается защита от скрытого видеонаблюдения?

3. Что называется демаскирующими признаками?

**Лабораторно-практическая работа 57.**

**Тема**: Анализ систем защиты от прослушивания

Цель занятия:Изучение назначения, основных характеристик и принципа подключения устройств для прослушивания

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Составить таблицу основных средств для прослушивания с описанием характеристик и сопоставить методы защиты для каждого устройства

2. Составить отчет, ответить на вопросы

**Контрольные вопросы**

1. Для каких целей используется прослушивание ?

2. В чем заключается защита от прослушивания

3. Что такое генератор шума?

4. Для чего служит лазерный микрофон и принципы его действия

**Лабораторно-практическая работа 58.**

**Тема**: Скрытые функции диктофонов

Цель занятия:Изучение назначения, основных характеристик и принципа работы диктофонов

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Составить таблицу с описанием характеристик диктофонов.

2. Составить отчет, ответить на вопросы

**Контрольные вопросы**

1. Для каких целей используется прослушивание ?

2. Какие средства для защиты от прослушивания с помощью диктофонов вы знаете?

3. Для каких целей используются зашумляющие устройства?

**Лабораторно-практическая работа 59.**

**Тема**: Построение зависимости состояния защищенности от уровня экономического развития организации

Цель занятия:Приобретение практический навыков для составления зависимости экономического развития предприятия и способов защиты информации от несанкционированного доступа

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 4 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Ознакомиться с материалами курса

2. Оценить соответствия состояния защищенности вымышленного предприятия

3. Сформулировать рекомендации по повышению безопасности информации в обследуемой̆ организации

4. Смоделировать действия злоумышленника

4. Составить отчет, ответить на вопросы

**Контрольные вопросы**

1. Для каких целей используется прослушивание ?

2. В чем состоит сложность применения Аудита КЗИ?

3. В чем заключаются слабости внутреннего Аудита силами предприятия?

4. Приведите несколько примеров успешного применения Аудита.

**Лабораторно-практическая работа 60.**

**Тема**: Изучение международных стандартов во ИБ

Цель занятия:Закрепить знания по международным стандартам информационной безопасности

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 4 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Определение целей обеспечения информационной безопасности компьютерных систем;

2. Определить принципы создание эффективной системы управления информационной безопасностью;

 3. Ответить на вопросы

**Контрольные вопросы**

1. Виды организации организационно –правовых угроз?

2. Понятие субъекта и объекта безопасности?

3. Перечислите основные виды тайн?

4. В чем состоят основные способы защиты Информационной безопасности?

**Лабораторно-практическая работа 61.**

**Тема**: Требования к средствам обеспечения безопасности.

Цель занятия:Закрепить знания по методам и средства для обеспечения безопасности

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Определение целей обеспечения безопасности

2. Определить принципы создание эффективной системы безопасности

 3. Ответить на вопросы

**Контрольные вопросы**

1. Виды организационной защиты?

2. Виды технической защиты?

3. Виды инженерной защиты?

4. В чем состоят основные способы защиты информации?

**Лабораторно-практическая работа 62.**

**Тема**: Планирование безопасности организации.

Цель занятия:Получить практический опыт планирования безопасности организации

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 10 часов.

**Задание:**

Работа состоит из следующих этапов:

1. Определить состав и содержание основных руководящих и планирующих документов, определяющих структуру, функции и должностные обязанности сотрудников службы защиты информации

2. Сформулировать замысел защиты информации с помощью ответов на вопросы:

Замысел защиты информации: каковы состав и структура информационной подсистемы организации на каких этапах цикла управления организацией и в каких звеньях управления возможны утрата и утечка информации;

Какие возможности по утечке и утрате информации допускают используемые технические средства обеспечения управления, административной и хозяйственной деятельности;

Кого из конкурентов и какая информации может заинтересовать;

Кого они могут привлечь для получения информации, какие средства и способы могут быть использованы при этом;

3. Ответить на вопросы

**Контрольные вопросы**

 1. Чем руководствуется служба защиты информации в своей деятельности

2. Принципы создания и функционирования службы защиты информации

 3. Условия и факторы, влияющие на организацию работы службы защиты информации

 4. Порядок создания службы защиты информации.

**Лабораторно-практическая работа 63.**

**Тема**: Изучение основных направлений деятельности СУИБ.

Цель занятия:Получить практический опыт работы с СУИБ

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Изучения этапов создания СУИБ

 2.Принятие решения о создании СУИБ

3.Подготовка к созданию СУИБ

4.Анализ рисков

 5. Ответить на вопросы

**Контрольные вопросы**

 1. Разработка политик и процедур СУИБ?

2. Принципы создания и функционирования службы защиты информации

 3. Основные этапы создания СУИБ?

 4. Порядок создания службы защиты информации.

**Лабораторно-практическая работа 64.**

**Тема**: «Взаимодействие отдела обеспечения безопасности информации с другими подразделениями».

Цель занятия:Провести связь между отделом обеспечения безопасности и другими подразделениями

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. Составить схему взаимосвязи между отделом обеспечения защиты и другими отделами вымошленной организации

 2. Ответить на вопросы

**Контрольные вопросы**

1. В чем состоит сложность применения Аудита КЗИ?

2. В чем заключаются слабости внутреннего Аудита силами предприятия?

3. Приведите несколько примеров успешного применения Аудита.

**Лабораторно-практическая работа 65.**

**Тема**: Изучение этапов разработки КСЗИ

Цель занятия:Приобрести навык проектирования комплексной системы защиты информации

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1. В электронном документа описать основные стадии разработки КСЗИ вымышленного предприятия

 2. Ответить на вопросы

**Контрольные вопросы**

1. Применения Аудита КЗИ?

2. Что следует учитывать при разработки КСЗИ

3. Как правильно спроектировать систему защиты.

**Лабораторно-практическая работа 66.**

**Тема**: Построение зависимости вида защищаемой информации от формы собственности предприятия.

Цель занятия:Получить практический опыт построение зависимости вида защищаемой информации от формы собственности предприятия.

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Изучение вида информации на вымышленном предприятии

 2.Построить схему взаимосвязи вида информации и собственности предприятия

 3. Ответить на вопросы

**Контрольные вопросы**

 1. Виды защищаемой информации?

2. Принципы создания службы защиты информации

 4. Как зависит способ защиты информации от вида информации.

**Лабораторно-практическая работа 67.**

**Тема**: «Конструктивные особенности организации, как фактор, влияющий на КСЗИ»

Цель занятия: Провестикласификацию факторов влияющих на создание системы безопасности предприятия

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Изучение вида информации на вымышленном предприятии

 2.Построить схему взаимосвязи вида информации и собственности предприятия

 3. Ответить на вопросы

**Контрольные вопросы**

1. Применения Аудита КЗИ?

2. Что следует учитывать при разработки КСЗИ

3. Как правильно спроектировать систему защиты.

**Лабораторно-практическая работа 68.**

**Тема**: «Качественные показатели ресурс обеспечения, как факторы, влияющие на КСЗИ»

Цель занятия: Провести классификацию ресурсов обеспечения, влияющих на создание системы безопасности предприятия

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

1.Изучение вида ресурсов обеспечения на вымышленном предприятии

 2.Построить схему взаимосвязи ресурса обеспечения, влияющего на создание системы безопасности

 3. Ответить на вопросы

**Контрольные вопросы**

1. Что такое ресурсы обеспечения организации?

2. Что следует учитывать при разработки КСЗИ по мимо ресурсов обеспечения?

3. Что такое система защиты информации?

4.Что такое комплексная система защиты информации?

**Лабораторно-практическая работа 69.**

**Тема**: Степень автоматизации основных процедур обработки защищаемой информации.

Цель занятия: Получить практический опыт работы с автоматизированными системами обработки информации

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 2 часа.

**Задание:**

Работа состоит из следующих этапов:

 Работа проводиться в демонстрационном режиме

1.Составить таблицупроцессов защиты информации, которые могут производиться в автоматическом режиме

 2. Ответить на вопросы

**Контрольные вопросы**

1. Что такое автоматизированная система безопасности?

2. Что следует учитывать при разработке автоматизированной системы?

3. Что такое система защиты информации?

**Лабораторно-практическая работа 70.**

**Тема**: Виды защищаемой информации на предприятии

Цель занятия: Разработать классификацию видов защищаемой информации

Оснащение рабочего места:Персональный компьютер

Продолжительность занятия – 4 часа.

**Задание:**

Работа состоит из следующих этапов:

 Работа проводиться в демонстрационном режиме

1.Составить таблицу видов информации , которые могут подвергаться попытке несанкционированного доступа

 2. Составить схему защиты предприятия от потенциальных угроз в зависимости от вида информации

 2. Ответить на вопросы

**Контрольные вопросы**

1.Что такое информация?

2. Какие технические каналы утечки информации вам известны?

3. Что такое комплексная система защиты информации?

4. Какими способами можно противостоять грозам по акустическим каналам утечки информации

**8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ МДК**

**Основная литература**

**Информационное обеспечение обучения. Основные источники (ОИ):**

Таблица 2б

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование | Автор | Издательство, год издания |
| ОИ 1 | Комплексная система защиты информации на предприятии | Грибунин В.Г., Чудовский В.В. | М. Издательский центр «Академия», 2014. |
| ОИ 2 | Организация комплексной системы защиты информации | Гришина Н.В. | М.: Гелиос АРВ, 2013. |
| ОИ 3 | Информационная безопасность предприятия  | Конеев И. Р.  | СПб.: БХВ-Петербург, 2013 |

**Дополнительные источники (ДИ):**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование | Автор | Издательство, год издания |
| ДИ 1 | Основы информационной безопасности.  | Галатенко В.А. | М.: Интуит.Ру, 2010. |
| ДИ 2 | Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел: Учебн. пособие | Под ред. Чекалина А.А. | М.: Горячая линия-Телеком, 2012. |
| ДИ 4 | Инженерно-техническая защита информации: Учеб.пособие для студентов, обучающихся по специальностям в обл. информ. безопасности | Торокин А. А. | М.: Гелиос АРВ, 2010. |
| ДИ 5 | Техническая защита информации: Учеб.пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации | **Хорев А.А.** | М.: НПЦ «Аналитика», 2011. |

**Интернет-ресурсы (ИР):**

|  |  |
| --- | --- |
| ИР 1 | <http://www.pandia.ru/> |
| ИР 2 | <http://www.twirpx.com/> |
| ИР 3 | http://www.infsec.ru/ |
| ИР 4 | <http://www.booksshare.net/> |