МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Ф. УТКИНА

Кафедра «Автоматики и информационных технологий в управлении»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки – 27.03.04 Управление в технических системах

«Управление в технических системах»

ОПОП
«Управление в технических системах»

Квалификация выпускника – бакалавр
Формы обучения – очная

Рязань 2024

Оценочные материалы – это совокупность учебно-методических материалов (контрольных заданий, описаний форм и процедур), предназначенных для оценки качества освоения обучающимися данной дисциплины как части основной профессиональной образовательной программы.

Цель – оценить соответствие знаний, умений и уровня приобретенных компетенций обучающихся целям и требованиям основной профессиональной образовательной программы в ходе проведения текущего контроля и промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности общекультурных, общепрофессиональных и профессиональных компетенций, приобретаемых обучающимся в соответствии с этими требованиями.

Контроль знаний проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости проводится с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся и принятия необходимых мер по совершенствованию методики преподавания учебной дисциплины, организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков, приобретенных обучающимися в ходе выполнения индивидуальных заданий на практических занятиях. При оценивании результатов освоения практических занятий применяется шкала оценки «зачтено – не зачтено». Количество практических работ и их тематика определена рабочей программой дисциплины, утвержденной заведующим кафедрой.

Результат выполнения каждого индивидуального задания должен соответствовать всем критериям оценки в соответствии с компетенциями, установленными для заданного раздела дисциплины.

Промежуточный контроль по дисциплине осуществляется проведением зачета.

Форма проведения теоретического зачета – устный ответ по утвержденным билетам, сформулированным с учетом содержания учебной дисциплины. В билет включается два вопроса по темам курса. Объем знаний и степень освоения компетенций на зачете оценивается по двухбалльной системе: «зачтено» и «не зачтено».

Паспорт оценочных материалов по дисциплине

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по темам)	Код контролируемой компетенции (или её части)	Вид, метод, форма оценочного мероприятия
1	2	3	4
1	**Тема 1. Стохастическая компьютерная вирусология**	ОПК-11.1 ОПК-11.2 ОПК-5.1 ОПК-5.2 ОПК-5.3	Зачет
2	**Тема 2. Тенденции развития угроз информационной безопасности**	ОПК-11.1 ОПК-11.2 ОПК-5.1 ОПК-5.2 ОПК-5.3	Зачет
3	**Тема 3. Скрытые каналы передачи данных**	ОПК-11.1 ОПК-11.2 ОПК-5.1 ОПК-5.2 ОПК-5.3	Зачет
4	**Тема 4. Технология безопасного программирования**	ОПК-11.1 ОПК-11.2 ОПК-5.1 ОПК-5.2 ОПК-5.3	Зачет

Критерии оценивания компетенций (результатов)

1). Уровень усвоения материала, предусмотренного программой.

2). Умение анализировать материал, устанавливать причинно-следственные связи.

3). Ответы на вопросы: полнота, аргументированность, убежденность, умение

4). Качество ответа (его общая композиция, логичность, убежденность, общая эрудиция)

5). Использование дополнительной литературы при подготовке ответов.

В рамках текущего контроля на протяжении семестра в качестве оценочных средств используются устные и письменные ответы студентов на индивидуальные вопросы, доклады на практических занятиях.

Оценка степени формирования контролируемых компетенций у обучающихся на различных этапах их формирования проводится

преподавателем во время лекций по шкале оценок «зачтено», «не зачтено».

Устанавливаются следующие уровни сформированности компетенций в рамках текущего контроля:

1) 0%-70% оценок «зачтено» соответствует неудовлетворительному уровню сформированности компетенций.

2) 71%-85% оценок «зачтено» соответствует пороговому уровню сформированности компетенций.

3) 86%-100% оценок «зачтено» соответствует продвинутому уровню сформированности компетенций.

Уровень сформированности компетенций не ниже порогового является основанием для допуска обучающегося к промежуточной аттестации по данной дисциплине.

Формой промежуточной аттестации по данной дисциплине является зачет.

Зачет организуется и осуществляется в форме устного собеседования. Средством, определяющим содержание собеседования студента с экзаменатором, является утвержденный билет, в который включается два вопроса по темам курса согласно настоящей рабочей программе. Оценке на заключительной стадии зачета подвергаются устный ответ студента на вопросы билета, ответы на дополнительные вопросы экзаменатора.

В процессе оценки знаний, умений и навыков студента, производимой на этапе промежуточной аттестации в форме зачета, используется оценочная шкала «зачтено», «не зачтено», что соответствует шкале «компетенции студента соответствуют требованиям ФГОС ВО», «компетенции студента не соответствуют требованиям ФГОС ВО»:

Для получения оценки «**зачтено**» обучающийся должен ответить на теоретический вопрос билета и дать корректный ответ на практическое задание; продемонстрировать общее знание изучаемого материала; знать основную рекомендуемую программой дисциплины учебную литературу; уметь строить ответ в соответствии со структурой излагаемого вопроса; показать общее владение понятийным аппаратом дисциплины. Допускается наличие погрешностей в ответе на теоретические вопросы и при выполнении практического задания в случае коррекции неточностей по указанию преподавателя.

Оценка «**не зачтено**» ставится в случае незнания обучающимся значительной части программного материала; не владения понятийным аппаратом дисциплины; при наличии существенных ошибок в изложении учебного материала; неумения построить ответ на заданный вопрос и делать выводы по излагаемому материалу. Оценка ставится обучающимся, которые не могут продолжить обучение по образовательной программе без дополнительных занятий по соответствующей дисциплине (формирования и развития компетенций, закрепленных за данной дисциплиной).

Отметка «**не зачтено**» выставляется также, если обучающийся после начала зачета отказался его сдавать или нарушил правила сдачи зачета (списывал, обманом пытался получить более высокую оценку и

т.д.).

Типовые контрольные задания или иные материалы

Вопросы к зачету по дисциплине
(ОПК-11.1, ОПК-11.2)

1. Чем полиморфные вирусы отличаются от самошифрующихся?
2. Сформулируйте принцип обнаружения компьютерного вируса методом сигнатурного анализа.
3. Сформулируйте принцип обнаружения компьютерного вируса методом эвристического анализа.
4. Какой метод используется для обнаружения компьютерного вируса в момент их активизации?
5. Какой метод используется для обнаружения последствий вирусной активности?
6. Какие методы используются для обнаружения компьютерного вируса до момента их активизации?
7. Какие существуют типы программных средств антивирусной защиты?
8. Что такое вирусная сигнатура? Приведите пример.
9. Что такое эвристический признак компьютерного вируса? Приведите пример.
10. Что такое ошибка 1-го рода при работе программных средств антивирусной защиты?
11. Что такое ошибка 2-го рода при работе программных средств антивирусной защиты?
12. Что такое ошибка 3-го рода при работе программных средств антивирусной защиты?
13. Что такое клептографическая атака на криптоалгоритм?
14. Какие криптоалгоритмы могут являться объектом клептографической атаки?
15. Приведите пример клептографической атаки на криптоалгоритм RSA.
16. Как можно защититься от клептографической атаки?
17. Опишите клептографическую атаку на криптосистему Эль-Гамаля.
18. Опишите возможную клептографическую атаку на генератор ПСЧ.
19. Как вы понимаете термин «клептография»? Приведите примеры, иллюстрирующие данное понятие.
20. Что такое недоказуемое шифрование?
21. Что такое криптовычисления?
22. Каким образом можно получить запись из базы данных таким образом, чтобы не раскрывать, какая именно запись была получена?
23. Что такое отрицаемое шифрование?
24. Какие программы называют симбиотическими?
25. Приведите примеры симбиотических разрушающих программных воздействий.
26. Каким образом можно использовать сетевые разрушающие программные

воздействия для проведения распределенных вычислений?
27. Предположим, что улучшенный криптотроян применяет плохой генератор случайных чисел и сеансовые ключи, сформированные на разных компьютерах, оказываются одинаковыми. Какие последствия это может иметь?
28. Какие методы противодействия автоматической рассылке сообщений вы знаете?
29. В чем различие между принципами недоказуемого и отрицаемого шифрования?
30. Какому риску подвергаются вредоносные программы, участвующие в протоколе информационного шантажа, при использовании ими некачественных генераторов случайных чисел?
31. Какую роль в протоколе контроля работоспособности узлов распределенных вычислений играет случайный бит b?
32. С какой вероятностью для достижения своих целей в протоколе безопасного выкупа жертве придется купить не более k сообщений ($1 \leq k \leq 2S$)?
33. Дайте определение скрытого канала передачи данных.
34. Дайте определение потайного канала передачи данных.
35. Дайте определение побочного канала передачи данных.
36. Перечислите типы скрытых каналов передачи данных.
37. Что такое скрытый канал по памяти?
38. Что такое скрытый канал по времени?
39. Какие основные характеристики скрытых каналов используются при их описании?
40. Укажите различия между синхронными и асинхронными скрытыми каналами.
41. Какое влияние оказывает синхронизация на емкость канала?
42. Укажите особенности применения скрытых каналов в системах обработки информации.
43. Перечислите методы организации локальных скрытых каналов.
44. Перечислите методы организации сетевых скрытых каналов.
45. Каким образом можно организовать скрытые каналы на базе стека протоколов TCP/IP: IP и ICMP?
46. Каким образом можно организовать скрытые каналы на базе стека протоколов TCP/IP: TCP и UDP?
47. Каким образом можно использовать протоколы уровня приложений HTTP и DNS для организации скрытых каналов?
48. Укажите методы противодействия угрозе организации скрытых каналов?
49. В чем состоят главные отличия компилятора от транслятора?
50. Перечислите преимущества трансляторов?
51. Какие интерпретируемые языки вы знаете?
52. Укажите основные особенности скрипт-вирусов.
53. Укажите методы обнаружения скрипт-вирусов.
54. Какие возможности предоставляет утилита awk?
55. Почему присутствие команды «rm» является одним из наиболее характерных признаков скрипт-вируса?

56. Какими свойствами должен обладать скрипт-файл, чтобы быть классифицированным как вирус?
57. Что такое уязвимость программного кода?
58. К каким последствиям может привести существование уязвимости в программном коде?
59. Каковы основные причины появления уязвимости в программном коде?
60. В чем суть уязвимости, вызванной переполнением буфера на стеке?
61. Укажите основные способы борьбы с уязвимостями переполнения буфера на стеке.
62. К каким последствиям может привести существование уязвимости класса «переполнение кучи»?
63. Укажите основные методы борьбы с уязвимостями класса «переполнение кучи».
64. К каким последствиям может привести существование уязвимостей класса «целочисленное переполнение»?
65. Каковы последствия существования уязвимостей в программах, написанных с использованием интерпретируемых языков?
66. В чем суть уязвимости внедрения команд?
67. К каким последствиям может привести существование уязвимости внедрения SQL-кода?

Тестовые задания к зачёту (ОПК-11.1, ОПК-11.2)

1) Техническая защита информации - это:
   а) Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;
   б) Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением;
   в) Защита информации с помощью ее криптографического преобразования;
   г) Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.
2) Защита информации от несанкционированного воздействия - это:
   а) Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному

перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

б) Защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации;

в) Защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях;

г) Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

3) Политика безопасности - это:

а) Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности;

б) Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации;

в) Состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

4) Объект защиты информации - это:

а) Информация или носитель информации, которые необходимо защищать в соответствии с целью защиты информации;

б) Активы организации и финансовые процессы, которые необходимо защищать в соответствии с целью защиты информации.

5) Угроза безопасности информации - это:

а) Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;

б) Совокупность информационных ресурсов, технических, программных и методических средств, обеспечивающих хранение, накопление, обновление, поиск и выдачу данных по запросу пользователей, а также персонал;

в) Совокупность защитных механизмов вычислительной системы, включая программные и аппаратные компоненты, ответственные за поддержание политики безопасности.

6) Вредоносная программа - это:

а) Программа, предназначенная для осуществления несанкционированного доступа к информации и воздействия на информацию;
б) Антивирусная программа;
в) Программа, предназначенная для осуществления санкционированного доступа к информации и воздействия на информацию;

7) Ошибка 1-го рода при работе программных средств антивирусной защиты:
а) Не обнаружение компьютерного вируса в зараженном информационном объекте: имеет место, например, в случае неполноты вирусных баз или появления компьютерного вируса с новым механизмом функционирования, неучтенным при разработке эвристических признаков;
б) Ошибочное обнаружение компьютерного вируса в незараженном информационном объекте, иначе говоря, ложная тревога: имеет место, например, в случае некачественного выделения сигнатуры или эвристики из тела компьютерного вируса и включения этой некачественной сигнатуры или эвристики в вирусную базу;
в) Обнаружение не того компьютерного вируса в зараженном файле; имеет место, например, в случае, когда искусственно вводят в тело компьютерного вируса сигнатуру или эвристический признак другого вируса.

8) Программная закладка - это:
а) Преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения;
б) Функциональные возможности программного обеспечения, неописанные в документации;
в) Программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.

9) Компьютерный вирус - это:
а) Вредоносная программа, способная создавать свои копии или другие вредоносные программы;
б) Программное обеспечение, некорректно выполняющее свои функции, описание которых приведено в программной документации;
в) Вредоносная программа, появившаяся при выполнении неверно написанного программного обеспечения.

10) Компьютерная атака - это:
а) Целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств;
б) Несанкционированное воздействие на ресурсы автоматизированной

информационной системы, осуществляемое с использованием вредоносных программ.

11) Сетевая атака - это:
   а) Компьютерная атака с использованием протоколов межсетевого взаимодействия;
   б) Компьютерная атака с использованием вредоносного программного обеспечения, распространяемого на USB-носителях.
12) К защищаемой информации относят:
   а) Секретные сведения, содержащие государственную тайну;
   б) Конфиденциальную информацию, содержащую коммерческую тайну;
   в) Персональные данные о личной жизни или деятельности граждан;
   г) Все перечисленные выше варианты верны.
13) Свойства информации:
   а) Доступность, целостность и конфиденциальность;
   б) Надежность, доступность;
   в) Актуальность, конфиденциальность.
14) Целостность информации - это:
   а) Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
   б) Состояние информации, при котором отсутствует любое ее изменение;
   в) Состояние информации, при котором пользователи могут беспрепятственно её распространять.
15) Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации?
   а) Угроза;
   б) Опасность;
   в) Атака;
   г) Уязвимость.
16) Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации:
   а) Источник угрозы;
   б) Защитник от угрозы.
17) Воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации:
   а) Несанкционированное воздействие на информацию;
   б) Преднамеренное воздействие на информацию;
   в) Защита информации.
18) Неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического

средства
а) Утечка;
б) Перехват;
в) Уязвимость.

19) Средство защиты информации может быть:
а) Техническим;
б) Программным;
в) Программно-техническим;
г) Все перечисленные выше варианты верны.

20) Деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ.
а) Лицензирование в области защиты информации;
б) Сертификация в области защиты информации;
в) Мониторинг в области защиты информации;
г) Аккредитация в области защиты информации.

21) Вредоносная программа, зашифровывающая данные пользователя-жертвы:
а) Криптотроян;
б) Макро-вирус;
в) Логическая бомба;
г) Макрос.

22) CRC-код может быть применен для контроля целостности файлов:
а) При обнаружении случайных искажений данных;
б) Для выявления компьютерных вирусов.

23) Преимущество скрипт-вируса заключается в то, что он:
а) не зависит от версии операционной системы и от версии программного обеспечения;
б) для его запуска подходит любой компилятор;
в) простота распространения с использованием сетевых технологий.

24) Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов:
а) Перехват;
б) Утечка;
в) Уязвимость.

25) Создание условий, препятствующих доступу к информации субъекту, имеющему право на него:
а) Несанкционированное блокирование доступа к информации;
б) Санкционированное блокирование доступа к информации;
в) Ограничение на использование информации.

26) Разновидностями угроз безопасности относятся :
а) Программные, технические, организационные, технологические;
б) Серверные, клиентские, спутниковые, наземные;

в) Личные, корпоративные, социальные, национальные.

27) Несанкционированный доступ к информации:
   а) Преднамеренное обращение пользователя к данным, доступ к которым ему не разрешен, с целью их чтения, обновления или разрушения.
   б) Доступ к информации, нарушающий установленные правила ее получения.
   в) Доступ субъектов к информации или действия с информацией с использованием штатных средств объекта информатизации (сети передачи данных), нарушающий установленные правила получения и работы с информацией.
   г) Получение информации без соответствующего разрешения на доступ.

28) Виды информационной безопасности:
   а) Персональная, корпоративная, государственная;
   б) Клиентская, серверная, сетевая;
   в) Локальная, глобальная, смешанная.

29) Программные меры защиты заключаются в:
   а) использовании антивирусных средств;
   б) написании собственного программного кода с учетом известных уязвимостей.
   в) разработке регламентирующих программ и методик для персонала.

30) Процесс, в ходе которого на основании пароля, ключа или какой-либо иной информации, пользователь подтверждает, что является именно тем, за кого себя выдает:
   а) Аутентификация;
   б) Идентификация;
   в) Классификация.

31) Антивирусных программы способные находить только известные им вирусы:
   а) Программы-детекторы;
   б) Программы-доктора;
   в) Программы-ревизоры;
   г) Программы-фильтры.

32) Антивирусные программы, которые осуществляют автоматическую проверку всех используемых файлов в масштабе реального времени:
   а) Антивирусные мониторы;
   б) Антивирусные сканеры;
   в) программа-брандмауэр.

33) Основные объекты информационной безопасности:
   а) Компьютерные сети, базы данных;
   б) Информационные системы, психологическое состояние пользователей;
   в) Бизнес-ориентированные, коммерческие системы.

34) Основными рисками информационной безопасности являются:
   а) Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов - это:

б) Политика информационной безопасности;
в) Политика «закрытых дверей».

35) Метод поиска вирусов, который заключается в поиске характерных команд и участков кода:
а) Сигнатурный метод;
б) Эвристический метод;
в) Контроль целостности;
г) Метод резидентного сторожа.

36) Вирус, не имеющий сигнатуры, так как в нем нет ни одного постоянного участка кода:
а) Полиморфный вирус;
б) Самошифрующийся вирус.

37) Полезная или кажущаяся полезной программа или командная процедура, содержащая скрытый код, который после запуска программы-носителя выполняет нежелательные или разрушительные функции:
а) Троянская программа;
б) Вирус-червь;
в) Бэкдор;
г) Баннер-блокировщик.

38) Создание «закладки», внедряемой в разрабатываемую криптосистему, которая может быть реализована в виде аппаратного устройства или программы:
а) Клептографическая атака;
б) Атака путем подделки записей кэша DNS.

39) Вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи, называется:
Запишите ответ:_____

40) Сохранение конфиденциальности, целостности и доступности информации называется:
Запишите ответ:_____

41) Системы аутентификации, основанная на распознавании людей по одной или более физическим чертам (трёхмерная фотография лица, образец голоса, отпечатки пальцев, и т. д.), называется:
Запишите ответ:_____

42) Специализированное программное обеспечение для обнаружения вредоносных программ, называется:
Запишите ответ:_____

43) Обратимое преобразование информации в целях сокрытия от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней, называется:
Запишите ответ:_____

44) Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, называется:

Запишите ответ:_____

45) Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации:

Запишите ответ:_____

Практикум по дисциплине

№ п/п	№ темы дисциплины	Наименование практического занятия	Трудоемкость, час
1	1	Анализ механизмов функционирования компьютерных вирусов, использующих стохастические методы для сокрытия и выполнения деструктивных функций.	2
2	2	Клептографическая атака на алгоритм выработки общего секретного ключа. Защита от клептографических атак.	4
3	3	Классификация скрипт-вирусов. Поиск скрипт-вирусов на основе анализа кода. Выделение эвристических признаков скрипт-вирусов	4
4	4	Уязвимость переполнения буфера. Уязвимость строки формата. Уязвимость целочисленного переполнения. Уязвимость индексации массива. Уязвимость подключения внешних файлов. Уязвимость использования глобальных переменных. Уязвимость внедрения команд. Уязвимость внедрения SQL кода.	6

Типовые задания для самостоятельной работы

1. Анализ механизмов функционирования компьютерных вирусов, использующих стохастические методы для затруднения своего обнаружения.
2. Анализ механизмов функционирования компьютерных вирусов, использующих стохастические методы для выполнения деструктивных функций.
3. Элементы теории игр. Информационный шантаж. Распределенные вычисления. Безопасный выкуп.
4. Угроза проведения атак на Unix-системы с использованием скрипт-вирусов для командных интерпретаторов.
5. Интерпретатор и компилятор. Преимущества вирусов на интерпретируемых языках.
6. Скрипт-вирусы на языке Shell. Классификация технических приемов, используемых скрипт-вирусами.
7. Перспективные методы противодействия вредоносным программам.
8. Иммунологический подход к антивирусной защите. Понятие иммунной системы.

9. Архитектура компьютерной иммунной системы.
10. Автономность надежной системы защиты.
11. Стохастический подход к защите информации.
12. Поведенческий анализ программ. Поведение по определению. Определение по поведению.
13. Иммунологический подход. Распределенное обнаружение изменений.
14. Современные тенденции в динамическом анализе кода.