Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Защита информации в корпоративных сетях

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
А.Ю. Матросова

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ПК-2 Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИПК-2.1 Осуществляет проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем.

ИПК-2.2 Осуществляет разработку требований по защите, формирование политик безопасности компьютерных систем и сетей, проектирование программно-аппаратных средств защиты информации компьютерных систем.

ИПК-2.3 Осуществляет проведение анализа безопасности компьютерных систем, проведение сертификации программно-аппаратных средств защиты информации и анализ результатов, разработку и тестирование средств защиты информации компьютерных систем.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:
– тесты по лекционному материалу;
– контроль посещаемости;
– лабораторные работы;
– контрольная точка не менее одного раза в семестр.

1. Тесты по лекционному материалу оформлены в электронном курсе в LMS IDO в виде quiz-опросов, относящихся к игровым методам обучения: такие опросы проводятся в начале лекции или практического занятия по материалу предыдущей лекции и позволяют достаточно быстро вспомнить необходимый для текущего занятия материал.

Пример quiz-опроса.

Какие типы программ относятся к вредоносным?
вирусы √
троянские кони √
черви √
системные службы
операционные системы

2. Контрольная точка в середине семестра является комплексным контрольным мероприятием, включающим: 1) два теоретических вопроса; 2) выполнение двух первых лабораторных работ; 3) групповую работу.

Перечень теоретических вопросов:

1. Что такое информационная безопасность?
2. Какие компоненты входят в информационную безопасность?
3. Почему возникла необходимость в защите компьютеров?
4. Почему организации сталкиваются с проблемами при обеспечении информационной безопасности?

5. Являются ли системы, сертифицированные по уровню C2 правительства США, самыми защищенными?
6. Почему безопасность - это процесс, а не конечный продукт?
7. Сколько систем получили сертификат по уровню A1?
8. Почему "Оранжевая книга" утратила свою силу?
9. Была ли операционная система Microsoft Windows NT сертифицирована по уровню C2 "Оранжевой книги"?
10. Что значит TNI?
11. Почему физическая защита не может гарантировать безопасность?
12. Полагаются ли системы управления доступом на другие системы?
13. От какого нападения защищают межсетевые экраны?
14. Какие три вещи используются для установления подлинности личности?
15. Назовите два типа биометрических систем.
16. Назовите основные категории атак.
17. Какой тип доступа требуется для выполнения атак доступа к документам?
18. Почему атаки перехвата выполнить труднее, чем прослушивание?
19. Почему трудно выполнить атаки модификации документов, хранящихся в виде распечаток?
20. Для какого типа атак эффективным инструментом является разрыв кабеля?
21. Против каких свойств информации направлена атака на отказ от обязательств?
22. Если служащий открыл файл в домашнем каталоге другого служащего, какой тип атаки он выполнил?
23. Всегда ли атака модификации включает в себя атаку доступа?
24. Покупатель отрицает тот факт, что он заказал книгу на Amazon.com, - какая это атака?
25. Примером атаки какого рода является подслушивание служащим конфиденциальной информации из офиса босса?
26. К какому типу атак особенно уязвимы беспроводные сети?
27. Примером атаки какого рода является изменение заголовка электронной почты?
28. Что является целью атак на отказ в обслуживании?
29. Какие задачи решает злоумышленник при выполнении атаки на отказ в обслуживании?
30. Что является первым шагом при выполнении атаки модификации электронной информации?
31. Примером какого уязвимого места является в NFS установка разрешений корневой директории rw для всех пользователей?
32. Когда используются нетехнические средства для получения доступа в систему?
33. Какая часть памяти является объектом атаки на переполнение буфера?
34. Какой тип переменных используется при выполнении атаки на переполнение буфера?
35. Какая ошибка программирования позволяет выполнить атаку имитации IP-адреса?
36. Какой пакет не отправляется при выполнении синхронной атаки?
37. Существует ли способ защиты от грамотно разработанной DOS-атаки?
38. Что ищут хакеры, использующие ненаправленные методы атак?
39. Как хакер использует систему после взлома с помощью ненаправленной атаки?
40. Какой сайт используется для сбора информации об IP-адресах?

41. Какая часть предварительного исследования является наиболее опасной для хакера при подготовке направленной атаки?
42. Какой тип инструмента представляет собой программа Nmap?
43. С какой целью запускается атака DoS во время выполнения атаки имитации IP-адреса?
44. Чем представляется программа "троянский конь" для пользователя?
45. Для чего нужна программа nc?
46. Перечислите основные службы безопасности.
47. Какая служба полагается на службу конфиденциальности для обеспечения полной защиты информации?
48. Какие службы используются для противостояния атакам на модификацию?
49. В работе каких служб используется система контроля доступа?
50. Должны ли коммерческие организации соблюдать конфиденциальность потока данных?
51. Какой основной механизм обеспечивает конфиденциальность и целостность информации при передаче?
52. Для предотвращения перехвата должно использоваться шифрование - вместе с какой службой безопасности?
53. Может ли служба обеспечения доступности предотвратить атаки на отказ в обслуживании?
54. Назовите три типа аутентификационных факторов.
55. Почему двухфакторная аутентификация сильнее, чем однофакторная?
56. Зачем нужен аудит?
57. Какие службы позволяют предотвратить атаки на отказ от обязательств?
58. Какие службы позволяют предотвратить атаки доступа?
59. На какие три службы безопасности должен опираться аудит?
60. Примером работы какой службы безопасности является развертывание плана аварийного восстановления?
61. Назовите три раздела, которые должны присутствовать в каждой политике или процедуре.
62. Что определяет политика безопасности?
63. Должна ли политика безопасности определять конкретные требования реализации для каждого типа систем внутри самой политики?
64. Почему в политику безопасности включают отказы от защиты?
65. Что должна определять политика использования компьютеров?
66. Рекомендуется ли разрешать неограниченное использование компьютеров?
67. Для каких лиц должны указываться требования, содержащиеся в процедурах управления пользователями?
68. Когда сотрудник переходит с одной должности на другую внутри организации, кто должен нести ответственность за уведомление системных администраторов о необходимости изменения профиля доступа данного сотрудника?
69. Какова цель процедуры системного администрирования?
70. Почему необходимо соблюдать внимательность при определении целей IRP?
71. Назовите пять подразделений, сотрудники которых всегда должны входить в группу обработки инцидентов.
72. Назовите четыре ключевых раздела методологии разработки.
73. Назовите три типа событий, которые должны быть указаны в DRP.
74. Какие действия должен выполнять отдел безопасности в процессе создания политики?
75. Почему отдел безопасности должен работать совместно с отделом аудита?
76. Назовите две составляющих риска.

77. Каков уровень риска при отсутствии угроз?
78. Что такое уязвимость?
79. Назовите четыре цели для угроз.
80. Может ли угроза иметь более одной цели?
81. Какими характеристиками должен обладать агент, чтобы представлять собой угрозу?
82. Должен ли агент иметь физический доступ к системе, чтобы представлять собой угрозу?
83. Для какого типа организаций общественность рассматривается как угроза?
84. Только злонамеренные события являются угрозой?
85. После выявления уязвимых мест и угрозы что еще определяется для оценки риска в организации?
86. Назовите пять областей, которые нужно исследовать при оценке риска в организации.
87. С чего начинается определение реальных уязвимых мест?
88. Какая модель используется, если определение особых видов угроз является проблематичным?
89. Можно ли предположить, что большинство организаций в состоянии определить финансовые потери от различного рода инцидентов?
90. Какие затраты сложнее всего измерить?
91. Назовите пять этапов процесса информационной безопасности.
92. Для чего используются оценки?

Типовые варианты заданий для лабораторных работ:

Проект 1.

1.1. Проверьте наличие уязвимых мест.

- Проанализируйте информацию, относящуюся к вашему дому (можно выбрать другой объект исследования). Выявите самую важную.
- Определите место хранения этой информации.
- Определите типы атак, наиболее разрушительных для вас. Продумайте вероятность атаки доступа, атаки модификации, атаки на отказ в обслуживании.
- Продумайте способы обнаружения таких атак.
- Выберите тот тип атаки, которая, по вашему мнению, является наиболее разрушительной, и разработайте стратегию защиты.

1.2. Защитите свою информацию.

- Начните со списка атак и стратегий осуществления этих атак, разработанного в проекте.
- Для каждого метода атаки определите наиболее походящую службу безопасности, которая позволить предотвратить или обнаружить эту атаку.
- Для каждой выявленной службы примите решение о том, требуется ли ей для надежного функционирования служба идентификации. Если это так, то добавьте и эту службу к списку.
- Расположите список по приоритетам, начиная от самой важной (с вашей точки зрения).
- Если будут реализованы все службы безопасности, удастся ли вам обнаружить или предотвратить атаки, выявленные в проекте 2?

Проект 2.

Разработка политики использования интернета.

- Если вы работаете в группе, разделите группу на пары. Каждая пара будет разрабатывать свою собственную политику и представлять собой отдельную группу.

- Разработайте схему политики. Не забудьте включить раздел для входящих и исходящих соединений.

- Определите приемлемые типы входящих соединений.

- Определите приемлемые типы исходящих соединений. Если вам кажется, что все указано правильно, перейдите к определению типов сайтов, которые могу посещать сотрудники.

- Представьте политику другим членам группы. Некоторые из них должны выступать в роли сотрудников организации, а другие - в роли менеджеров.

- Как вариант, различные пары могут работать над разными политиками организации.

Проект 3.

Выявление различий между межсетевыми экранами различных типов.

- Сконфигурируйте сеть согласно архитектуре на рис. 1. Не подключайте эту сеть к интернету!

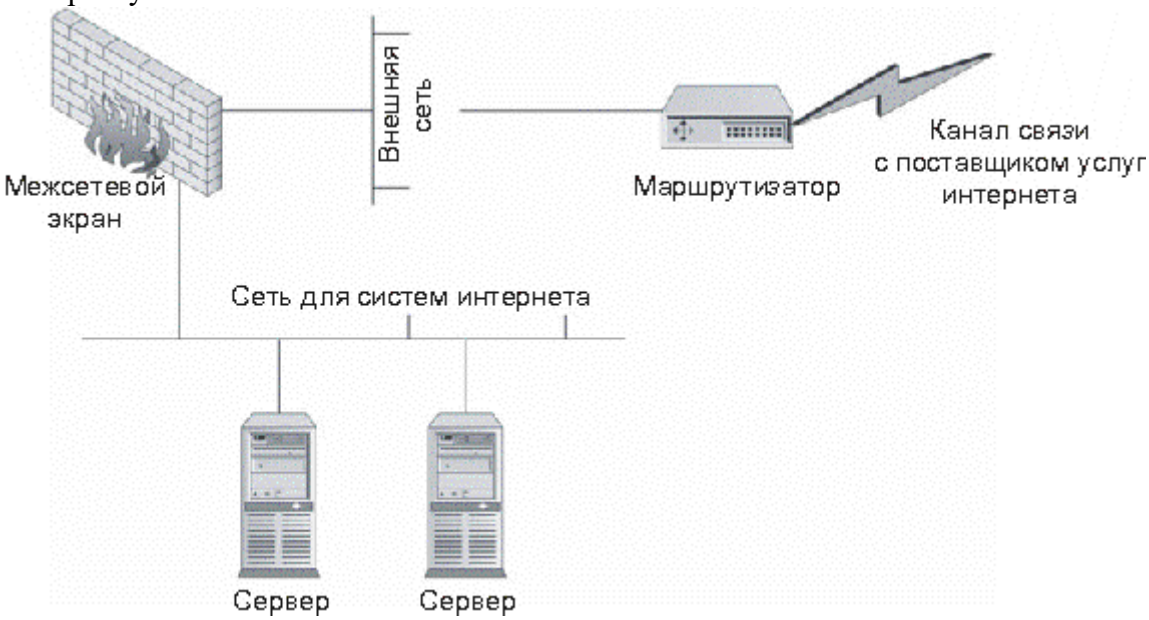

Рис. 1. Один межсетевой экран

- Создайте почтовый сервер и веб-сервер с настройками по умолчанию и оставьте в каждой системе уязвимости.

- Разместите межсетевой экран прикладного уровня в сети и настройте его согласно набору правил из табл. 1.

Таблица 1. Правила межсетевого экрана для архитектуры с одним межсетевым экраном

Номер	Исходный IP	Конечный IP	Служба	Действие
1	Любой	Веб-сервер	HTTP	Принятие
2	Любой	Почтовый сервер	SMTP	Принятие
3	Почтовый сервер	Любой	SMTP	Принятие
4	Внутренняя сеть	Любой	HTTP, HTTPS, FTP, telnet, SSH	Принятие
5	Внутренняя DNS	Любой	DNS	Принятие
6	Любой	Любой	Любая	Сброс

- Сконфигурируйте другую систему в качестве внешней системы (как если бы она располагалась вне межсетевого экрана в интернете) и запустите сканер уязвимостей.

- С помощью сканера уязвимостей просканируйте почтовый сервер и веб-сервер, а также межсетевой экран.

- Теперь замените межсетевой экран прикладного уровня межсетевым экраном с фильтрацией пакетов.

- Снова просканируйте серверы.

- Сравните полученные результаты. Различна ли информация, полученная при первом и втором сканировании? Одинаковы ли уязвимости, отображенные при подключении обоих межсетевых экранов? Если нет, то почему?

Проект 4.

Развертывание сетевой IDS.

- Определите, какие действия вы пытаетесь осуществить посредством развертывания датчика IDS. Это поможет четко обрисовать цели применения IDS.

- На основе целей применения IDS определите, какой сетевой трафик требуется отслеживать.

- Теперь решите, каким образом будут обрабатываться различные события, выявляемые IDS. Попробуйте определить, что будет разумнее - поручить выполнение некоторого действия системе IDS или оператору, который будет выполнять нужную процедуру.

- При отсутствии опыта работы с датчиком IDS вам придется нелегко при первой установке пороговых значений. Если в вашем обозрении есть уже функционирующая система IDS, можете посмотреть, какие пороговые значения установлены на этой системе для различных признаков атак.

- Составьте план развертывания IDS. Определите, кого в организации нужно задействовать для выполнения этой задачи.

- Если вы хотите попробовать осуществить развертывание датчика NIDS, выделите для этого компьютер и установите на него Linux, FreeBSD или другую версию операционной системы семейства Unix.

- Загрузите последнюю версию программы Snort (бесплатная IDS) с сайта http://www.snort.org/.

- Следуйте инструкциям по установке и выполните инсталляцию программы Snort. Можно также установить ряд дополнительных программных пакетов для упрощения процесса управления и конфигурации.

- Подключите датчик к сети. Лучше всего сделать это при помощи концентратора. Тем не менее, можно также использовать порт разветвителя на коммутаторе.

- Разместив датчик на нужном месте, просмотрите файлы журналов, чтобы выяснить, какие события в них фиксируются. Также можно использовать программу Acid для просмотра файлов журнала через веб-интерфейс. Acid - это веб-интерфейс, используемый для анализа данных программы Snort.

При подготовке к лабораторной работе студент обязан самостоятельно изучить методические рекомендации по проведению лабораторной работы, а также ответить на контрольные вопросы по лабораторной работе. Перед выполнением лабораторной работы преподавателем проводится инструктаж по достижению целей и решению задач лабораторной работы. По выполнению лабораторной работы студент готовит отчет, в котором указываются результаты выполнения лабораторной работы. При приеме лабораторной работы преподавателем задаются контрольные вопросы, позволяющие оценить уровень знаний студентов по теме лабораторной работы.

Выполнение лабораторной работы оценивается в 2 балла:

Критерии оценки выполнения лабораторных работ:

0 баллов. Студент слабо разбирается или не разбирается в задаче, не знает методов решения, не отвечает, либо отвечает, но с грубыми ошибками на вопросы преподавателя.

1 балл. Студент в целом удовлетворительно разбирается в задаче, использует методы решения при подсказке преподавателя, отвечает на вопросы, возможно, с негрубыми ошибками. Представляет работу на защите удовлетворительно.

2 балла. Студент отлично разбирается в задаче, знает и использует методы решения самостоятельно, отвечает на вопросы уверенно. Представляет работу на защите отлично.

Оцениваемая работа обучающегося по курсу в течение семестра разделена на три блока: 1) комплексная контрольная точка в середине семестра; 2) прохождение тестов по материалам лекций в течение семестра; 3) выполнение лабораторных работ.

Баллы по Блоку 1 формируются суммированием баллов за каждую из трех активностей в рамках комплексной контрольной точки: 1) ответ на два теоретических вопроса; 2) выполнение двух первых лабораторных работ 3) групповая работа.

Баллы по Блоку 2 формируются суммированием баллов за каждый тест (1 балл – тест пройден: 0 баллов – тест не пройден). Всего 13 тестов (по количеству лекционных тем).

Баллы по Блоку 3 формируются суммированием баллов за выполнение каждой лабораторной работы (всего четыре).

Критерии оценки ответа на теоретический вопрос:

3 балла: полно раскрыто содержание материала вопроса; материал изложен грамотно, в определенной логической последовательности; специальные термины используются правильно; определения приведены верно; допущены одна–две неточности при освещении вопросов, которые исправляются по замечанию преподавателя.

2 балла: вопрос изложен систематизировано и последовательно; продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; в изложении допущены небольшие пробелы, не исказившие содержание ответа, или допущены один–два недочета при освещении содержания ответа, исправленные по замечанию преподавателя.

1 балл: неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов.

0 баллов: полностью отсутствует ответ; не раскрыто основное содержание вопроса; обнаружено незнание или непонимание большей или наиболее важной части вопроса; допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов.

Оцениваемая работа обучающегося по курсу разделена на четыре блока: 1) комплексная контрольная точка в середине семестра; 2) прохождение тестов по материалам лекций в течение семестра; 3) выполнение лабораторных работ; 4) экзаменационное задание.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Экзамен проводится в письменной форме. Экзаменационное задание состоит из трех теоретических вопросов. Задания не сведены в один экзаменационный билет, а выбираются студентом в случайном порядке по каждой позиции экзаменационного задания. Продолжительность экзамена 1,5 часа.

Экзаменационное задание содержит три теоретических вопроса, проверяющих ИПК-2.1, ИПК-2.2, ИПК-2.3.

Перечень теоретических вопросов:

1. Что такое информационная безопасность?
2. Какие компоненты входят в информационную безопасность?

3. Почему возникла необходимость в защите компьютеров?
4. Почему организации сталкиваются с проблемами при обеспечении информационной безопасности?
5. Являются ли системы, сертифицированные по уровню C2 правительства США, самыми защищенными?
6. Почему безопасность - это процесс, а не конечный продукт?
7. Сколько систем получили сертификат по уровню A1?
8. Почему "Оранжевая книга" утратила свою силу?
9. Была ли операционная система Microsoft Windows NT сертифицирована по уровню C2 "Оранжевой книги"?
10. Что значит TNI?
11. Почему физическая защита не может гарантировать безопасность?
12. Полагаются ли системы управления доступом на другие системы?
13. От какого нападения защищают межсетевые экраны?
14. Какие три вещи используются для установления подлинности личности?
15. Назовите два типа биометрических систем.
16. Назовите основные категории атак.
17. Какой тип доступа требуется для выполнения атак доступа к документам?
18. Почему атаки перехвата выполнить труднее, чем прослушивание?
19. Почему трудно выполнить атаки модификации документов, хранящихся в виде распечаток?
20. Для какого типа атак эффективным инструментом является разрыв кабеля?
21. Против каких свойств информации направлена атака на отказ от обязательств?
22. Если служащий открыл файл в домашнем каталоге другого служащего, какой тип атаки он выполнил?
23. Всегда ли атака модификации включает в себя атаку доступа?
24. Покупатель отрицает тот факт, что он заказал книгу на Amazon.com, - какая это атака?
25. Примером атаки какого рода является подслушивание служащим конфиденциальной информации из офиса босса?
26. К какому типу атак особенно уязвимы беспроводные сети?
27. Примером атаки какого рода является изменение заголовка электронной почты?
28. Что является целью атак на отказ в обслуживании?
29. Какие задачи решает злоумышленник при выполнении атаки на отказ в обслуживании?
30. Что является первым шагом при выполнении атаки модификации электронной информации?
31. Примером какого уязвимого места является в NFS установка разрешений корневой директории rw для всех пользователей?
32. Когда используются нетехнические средства для получения доступа в систему?
33. Какая часть памяти является объектом атаки на переполнение буфера?
34. Какой тип переменных используется при выполнении атаки на переполнение буфера?
35. Какая ошибка программирования позволяет выполнить атаку имитации IP-адреса?
36. Какой пакет не отправляется при выполнении синхронной атаки?
37. Существует ли способ защиты от грамотно разработанной DOS-атаки?
38. Что ищут хакеры, использующие ненаправленные методы атак?

39. Как хакер использует систему после взлома с помощью ненаправленной атаки?

40. Какой сайт используется для сбора информации об IP-адресах?

41. Какая часть предварительного исследования является наиболее опасной для хакера при подготовке направленной атаки?

42. Какой тип инструмента представляет собой программа Nmap?

43. С какой целью запускается атака DoS во время выполнения атаки имитации IP-адреса?

44. Чем представляется программа "троянский конь" для пользователя?

45. Для чего нужна программа nc?

46. Перечислите основные службы безопасности.

47. Какая служба полагается на службу конфиденциальности для обеспечения полной защиты информации?

48. Какие службы используются для противостояния атакам на модификацию?

49. В работе каких служб используется система контроля доступа?

50. Должны ли коммерческие организации соблюдать конфиденциальность потока данных?

51. Какой основной механизм обеспечивает конфиденциальность и целостность информации при передаче?

52. Для предотвращения перехвата должно использоваться шифрование - вместе с какой службой безопасности?

53. Может ли служба обеспечения доступности предотвратить атаки на отказ в обслуживании?

54. Назовите три типа аутентификационных факторов.

55. Почему двухфакторная аутентификация сильнее, чем однофакторная?

56. Зачем нужен аудит?

57. Какие службы позволяют предотвратить атаки на отказ от обязательств?

58. Какие службы позволяют предотвратить атаки доступа?

59. На какие три службы безопасности должен опираться аудит?

60. Примером работы какой службы безопасности является развертывание плана аварийного восстановления?

61. Назовите три раздела, которые должны присутствовать в каждой политике или процедуре.

62. Что определяет политика безопасности?

63. Должна ли политика безопасности определять конкретные требования реализации для каждого типа систем внутри самой политики?

64. Почему в политику безопасности включают отказы от защиты?

65. Что должна определять политика использования компьютеров?

66. Рекомендуется ли разрешать неограниченное использование компьютеров?

67. Для каких лиц должны указываться требования, содержащиеся в процедурах управления пользователями?

68. Когда сотрудник переходит с одной должности на другую внутри организации, кто должен нести ответственность за уведомление системных администраторов о необходимости изменения профиля доступа данного сотрудника?

69. Какова цель процедуры системного администрирования?

70. Почему необходимо соблюдать внимательность при определении целей IRP?

71. Назовите пять подразделений, сотрудники которых всегда должны входить в группу обработки инцидентов.

72. Назовите четыре ключевых раздела методологии разработки.

73. Назовите три типа событий, которые должны быть указаны в DRP.

74. Какие действия должен выполнять отдел безопасности в процессе создания политики?

75. Почему отдел безопасности должен работать совместно с отделом аудита?
76. Назовите две составляющих риска.
77. Каков уровень риска при отсутствии угроз?
78. Что такое уязвимость?
79. Назовите четыре цели для угроз.
80. Может ли угроза иметь более одной цели?
81. Какими характеристиками должен обладать агент, чтобы представлять собой угрозу?
82. Должен ли агент иметь физический доступ к системе, чтобы представлять собой угрозу?
83. Для какого типа организаций общественность рассматривается как угроза?
84. Только злонамеренные события являются угрозой?
85. После выявления уязвимых мест и угрозы что еще определяется для оценки риска в организации?
86. Назовите пять областей, которые нужно исследовать при оценке риска в организации.
87. С чего начинается определение реальных уязвимых мест?
88. Какая модель используется, если определение особых видов угроз является проблематичным?
89. Можно ли предположить, что большинство организаций в состоянии определить финансовые потери от различного рода инцидентов?
90. Какие затраты сложнее всего измерить?
91. Назовите пять этапов процесса информационной безопасности.
92. Для чего используются оценки?
93. Что делает политика?
94. Включен ли план восстановления на случай чрезвычайных происшествий в разработку политики?
95. Что такое развертывание политики?
96. Назовите примерную длительность занятия по повышению осведомленности сотрудников.
97. Через какой тип учебных занятий по повышению осведомленности должны пройти руководители?
98. Являются ли учебные занятия лучшим и единственным способом для предоставления информации всем работникам?
99. Когда попытки нарушения защиты терпят неудачу?
100. Почему безопасность считается процессом, а не набора действий, совершаемых однократно?
101. Какие практические проблемы препятствуют последовательному выполнению процесса?
102. Сколько обычно длится период оценки?
103. Почему информационная политика и политика безопасности разрабатываются в первую очередь?
104. Какова основная проблема, связанная с развертыванием новых систем идентификации?
105. Почему организация должна первым делом браться за решение вопросов, связанных с меньшим уровнем риска?
106. Что такое "авторитетные рекомендации"?
107. Назовите четыре необходимых политики безопасности.
108. Назовите шесть навыков, которыми должны обладать сотрудники отделов безопасности.
109. Является ли закономерностью, что приобретение средств обеспечения безопасности снизит затраты на работу персонала отдела безопасности?

110. Кто должен нести ответственность за безопасность внутри организации?

111. Какова длительность занятия по изучению вопросов безопасности?

112. Должны ли планы восстановления после сбоев включать резервные "горячие сайты"?

113. Каким образом необходимо обеспечивать защиту постоянных соединений с внешними организациями?

114. На каких системах должны устанавливаться антивирусные программы?

115. Какой длины должны быть пароли?

116. Если информация очень секретна, какой метод аутентификации следует использовать?

117. Где должны храниться записи аудита в идеальном случае?

118. Должны ли программные обновления немедленно устанавливаться на все системы после их выпуска производителем?

119. Перечислите четыре аспекта защиты компьютерных систем, размещенных в информационном центре.

120. Что представляет собой стандарт ISO, в котором говорится об информационной безопасности?

121. Выделите два основных типа межсетевых экранов.

122. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика?

123. Является ли один из типов межсетевых экранов более безопасным, нежели другой?

124. Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?

125. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора?

126. Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией?

127. Что должен обеспечивать межсетевой экран для проверки состояния?

128. При каком условии межсетевой экран прикладного уровня может называться гибридным?

129. Где расположены доступные из интернета системы в архитектуре с одним межсетевым экраном?

130. Почему порядок правил в наборе правил межсетевого экрана играет важную роль?

131. Можно ли рассматривать использование SSH как реализацию VPN?

132. Почему пользовательские VPN требуют строгой аутентификации?

133. Может ли шифрование полностью защитить данные, передаваемые через VPN.

134. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?

135. Пригодны ли межузловые VPN для использования между организациями?

136. Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?

137. Какие два критерия должны использоваться для определения того, какое устройство следует использовать - межсетевой экран или VPN-сервер на отдельной системе?

138. Если используется отдельный VPN-сервер, должен ли он размещаться в демилитаризованной зоне интернета?

139. Почему процесс реализации VPN представляет собой гораздо большее, чем выбор алгоритма шифрования?

140. Какие механизмы аутентификации лучше всего использовать для пользовательской VPN?

141. На секретности какого элемента основана защита информации надежными алгоритмами шифрования?

142. Каковы три вида атак на схему шифрования?

143. Как иначе называется шифрование с секретным ключом?

144. Приведите пример раннего подстановочного шифра.

145. Может ли быть взломан правильно реализованный "одноразовый блокнот"?

146. Какую длину имеют ключи DES?

147. В чем заключается основной недостаток DES?

148. За счет чего тройной DES повышает уровень безопасности алгоритма DES?

149. Для чего предназначен алгоритм AES?

150. На сложности какой задачи базируется безопасность, обеспечиваемая алгоритмом Диффи-Хеллмана?

151. Можно ли использовать алгоритм Диффи-Хеллмана для шифрования трафика?

152. Назовите основную атаку, которой подвержен алгоритм Диффи-Хеллмана (с правильно выбранными a и b).

153. Что такое цифровая подпись?

154. Почему открытые ключи должны быть сертифицированными?

155. В чем заключается проблема, связанная с управлением ключами, которая вызывает сбои в большей части систем PKI?

156. Что подразумевается под обнаружением вторжений?

157. Назовите два основных типа IDS.

158. Может ли узловая IDS всегда определять успех или неудачу проведения атаки?

159. Может ли узловая IDS предотвращать атаку?

160. Возможно ли противостоять контролеру целостности файлов?

161. Назовите пять этапов реализации системы IDS.

162. Является ли идентификация действий пользователей корректной целью применения IDS?

163. Может ли сетевая IDS предотвращать достижение атаками их целей?

164. Что подразумевается под пассивными ответными действиями?

165. Что подразумевается под активными ответными действиями?

166. Должна ли применяться процедура выполнения ответных действий на инцидент в случае половинчатого IP-сканирования?

167. Почему оповещения о наличии в системе "черных ходов"часто оказываются ложными срабатываниями системы обнаружения вторжений?

168. О чем, как правило, говорит ситуация, при которой за небольшой промежуток времени наблюдается большое число различных атак?

169. Какой тип IDS следует применить в организации для защиты веб-сервера от причинения ущерба?

170. Какой тип системы IDS следует выбрать организации для защиты от атак, если в первую очередь рассматривается вопрос стоимости?

171. Каков приблизительный радиус действия беспроводной сети стандарта 802.11x на открытой местности и в помещении?

172. Какой тип серверов, помимо точки беспроводного доступа, как правило, доступен для подключения рабочей станции к WLAN?

173. Назовите три службы, предоставляемые WEP.

174. Опишите механизм криптографической аутентификации, имеющийся в WEP.

175. Реализация какого типа атак возможна по причине отсутствия обратной аутентификации AP по отношению к рабочей станции?

176. Какой алгоритм используется WEP для обеспечения конфиденциальности?

177. Что позволяет делать злоумышленнику недостаток в WEP, связанный с вектором инициализации?

178. Какой алгоритм используется WEP для обеспечения целостности?

179. Почему недостаточно использовать SSID или MAC-адреса для обеспечения аутентификации?

180. Почему аутентификация 802.1X сама по себе рассматривается как уязвимость в системе?

181. Назовите две цели, на которые направлены активные атаки в беспроводной сети.

182. Какой тип соединения следует использовать для управления точками беспроводного доступа?

183. Какой тип систем следует использовать для корректного обеспечения безопасности информации при передаче через WLAN?

184. К какому типу сетей следует относить WLAN?

185. Какую периодическую оценку необходимо проводить при работе с WLAN?

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Ответ на каждую часть экзаменационного задания оценивается по системе от 0 до 3 баллов. Экзамен считается состоявшимся, если в ходе экзамена студент набрал от 4 до 9 баллов. Экзаменационная оценка определяется суммой баллов, набранных студентом в течение семестра и в ходе экзамена.

Критерии оценки ответа на теоретический вопрос:

3 балла: полно раскрыто содержание материала вопроса; материал изложен грамотно, в определенной логической последовательности; специальные термины используются правильно; определения приведены верно; допущены одна–две неточности при освещении вопросов, которые исправляются по замечанию преподавателя.

2 балла: вопрос изложен систематизировано и последовательно; продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; в изложении допущены небольшие пробелы, не исказившие содержание ответа, или допущены один–два недочета при освещении содержания ответа, исправленные по замечанию преподавателя.

1 балл: неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов.

0 баллов: полностью отсутствует ответ; не раскрыто основное содержание вопроса; обнаружено незнание или непонимание большей или наиболее важной части вопроса; допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов.

Оцениваемая работа обучающегося по курсу разделена на четыре блока: 1) комплексная контрольная точка в середине семестра; 2) прохождение тестов по материалам лекций в течение семестра; 3) выполнение лабораторных работ; 4) экзаменационное задание.

Баллы по Блоку 1 формируются суммированием баллов за каждую часть в рамках комплексной контрольной точки: 1) ответ на два теоретических вопроса (критерии оценивания ответа на теоретический вопрос приведены выше); 2) выполнение первых двух лабораторных работ; 3) групповая работа (групповая работа оценивается по системе от 0 до 3 , критерии оценивания групповой работы доводятся до обучающихся в момент выдачи задания).

Баллы по Блоку 2 формируются суммированием баллов за каждый тест (1 балл – тест пройден: 0 баллов – тест не пройден). Всего 13 тестов (по количеству лекционных тем).

Баллы по Блоку 3 формируются суммированием баллов за выполнение каждой лабораторной работы (всего четыре).

Баллы по Блоку 4 формируются суммированием баллов за каждое экзаменационное задание (критерии оценивания ответа на теоретический вопрос приведены выше).

В таблице 1 приведена шкала оценивания каждого блока, а в таблице 2 – шкала формирования оценки за курс.

Таблица 1 – Оценивание каждого из трех блоков работы обучающегося по курсу

Оценка за блок	Количество баллов			
	Блок 1	Блок 2	Блок 3	Блок 4
«отлично»	7–9	11–13	6–8	8–9
«хорошо»	5–6	8–10	6–5	6–8
«удовлетворительно»	3–4	6–7	3–5	4–5
«неудовлетворительно»	0–2	0–5	0–2	0–3

Таблица 2 – Условия формирования оценки за курс

Оценка за курс	Условие формирования оценки за курс
«отлично»	За все блоки «отлично» Один или два блока «хорошо» остальные «отлично»
«хорошо»	Один блок «отлично» остальные «хорошо» За все блоки «хорошо» Один блок «удовлетворительно» остальные «хорошо» или «отлично»
«удовлетворительно»	Один блок «неудовлетворительно» остальные «хорошо» или «отлично» Все блоки «удовлетворительно» Да блока «удовлетворительно» остальные «хорошо» или «отлично»
«неудовлетворительно»	Все остальные случаи

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Примерный перечень контрольных вопросов для проверки остаточных знаний (при оценивании необходимо продемонстрировать достижение **всех** запланированных индикаторов достижения компетенций):

1. Почему физическая защита не может гарантировать безопасность?
2. Полагаются ли системы управления доступом на другие системы?
3. От какого нападения защищают межсетевые экраны?
4. Какие три вещи используются для установления подлинности личности?
5. Назовите два типа биометрических систем.
6. Назовите основные категории атак.
7. Какой тип доступа требуется для выполнения атак доступа к документам?
8. Почему атаки перехвата выполнить труднее, чем прослушивание?
9. Почему трудно выполнить атаки модификации документов, хранящихся в виде распечаток?
10. Для какого типа атак эффективным инструментом является разрыв кабеля?

11. Против каких свойств информации направлена атака на отказ от обязательств?
12. Что определяет политика безопасности?
13. Должна ли политика безопасности определять конкретные требования реализации для каждого типа систем внутри самой политики?
14. Почему в политику безопасности включают отказы от защиты?
15. Что должна определять политика использования компьютеров?
16. Рекомендуется ли разрешать неограниченное использование компьютеров?
17. Для каких лиц должны указываться требования, содержащиеся в процедурах управления пользователями?
18. Для какого типа организаций общественность рассматривается как угроза?
19. Только злонамеренные события являются угрозой?
20. После выявления уязвимых мест и угрозы что еще определяется для оценки риска в организации?
21. Назовите пять областей, которые нужно исследовать при оценке риска в организации.
22. С чего начинается определение реальных уязвимых мест?
23. Какая модель используется, если определение особых видов угроз является проблематичным?
24. Можно ли предположить, что большинство организаций в состоянии определить финансовые потери от различного рода инцидентов?

Информация о разработчиках

Останин Сергей Александрович, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности НИ ТГУ.