МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Дагестанский государственный университет»

Колледж

УТВЕРЖДАЮ
директор Колледжа ДГУ
_____ Д.Ш. Пирбудагова
«31» 08 2021 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

профессионального модуля

ПМ.02. ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММАМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Махачкала – 2021

Составитель/ составители:

Шахбанова М.И. - преподаватель кафедры естественно-научных и гуманитарных дисциплин Колледжа ФГБОУ ВО «Дагестанский государственный университет»

Шахбанова З.И. - к.э.н., доцент кафедры прикладной информатики в экономике факультета информатики и информационных технологий ФГБОУ ВО «Дагестанский государственный университет»

Фонд оценочных средств рассмотрен и рекомендован к утверждению на заседании кафедры специальных дисциплин колледжа ДГУ

Протокол №_1_ от «31» _____08_____ 2021г.

Зав. кафедрой _____/Магомедова А.М./

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

профессионального модуля

ПМ.02. ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММАМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

№	Контролируемые разделы, темы, модули	Код контролируемой компетенции	Наименование оценочного средства
МДК.02.01. ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ			
1.	**Раздел 1.** Основные принципы программной и программно-аппаратной защиты информации	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 2.1, ПК. 2.4, ПК. 2.5.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы тестирование рефераты составление и оформление письменных документов подготовка и защита рефератов экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
2.	**Раздел 2.** Защита информации в локальных сетях	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 2.1, ПК. 2.4, ПК. 2.5.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы тестирование рефераты составление и оформление письменных документов подготовка и защита рефератов экспертная

			оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
3.	**Раздел 3.** Мониторинг систем защиты	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 2.1, ПК. 2.4, ПК. 2.5.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы тестирование рефераты составление и оформление письменных документов подготовка и защита рефератов экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
МДК.02.02. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ			
1.	**Раздел 1.** Основные понятия и характеристика шифров	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 2.2, ПК. 2.3, ПК. 2.5.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.

2.	**Раздел 2.** Симметричная криптография	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 2.2, ПК. 2.3, ПК. 2.5.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
3.	**Раздел 3.** Криптография с открытым ключом	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 2.2, ПК. 2.3, ПК. 2.5.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
4.	**Раздел 4.** Электронная подпись.	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 2.2, ПК. 2.3, ПК. 2.5.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов;

			экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
5.	**Раздел 5.** Применение криптографических методов и средств для обеспечения информационной безопасности	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 2.2, ПК. 2.3, ПК. 2.5.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
МДК.02.03. КОРПОРАТИВНАЯ ЗАЩИТА ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ			
1.	**Раздел 1.** Основные понятия и характеристика шифров	ОК 1, ОК 2, ОК 3, ОК 4, ПК. 2.1, ПК. 2.2, ПК. 2.6.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.

Примерный перечень оценочных средств

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	2	3	4
1.	Деловая и/или ролевая игра	Совместная деятельность группы обучающихся и педагогического работника под управлением педагогического работника с целью решения учебных и профессионально-ориентированных задач путем игрового моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.	Тема (проблема), концепция, роли и ожидаемый результат по каждой игре
2.	Кейс-задача	Проблемное задание, в котором обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы.	Задания для решения кейс-задачи
3.	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования педагогического работника с обучающимися.	Вопросы по темам/разделам дисциплины
4.	Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Комплект контрольных заданий по вариантам
5.	Круглый стол, дискуссия, полемика, диспут, дебаты	Оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения.	Перечень дискуссионных тем.
6.	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах.	Структура портфолио

7.	Рабочая тетрадь	Дидактический комплекс, предназначенный для самостоятельной работы обучающегося и позволяющий оценивать уровень усвоения им учебного материала.	Образец рабочей тетради
8.	Проект	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умение обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированное аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся.	Темы групповых и/или индивидуальных проектов
9.	Разно-уровневые задачи и задания	*Различают задачи и задания:* – репродуктивного уровня, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины; – реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей; – творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.	Комплект разно-уровневых задач и заданий
10.	Расчетно-графическая работа	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом.	Комплект заданий для выполнения расчетно-графической работы

11.	Реферат	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.	Темы рефератов

КРИТЕРИИ ОЦЕНКИ
по дисциплине

МДК.02.01. ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Критерии оценки:

Оценка «отлично»: студент владеет знаниями предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы, подчеркивал при этом самое существенное, умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделять в нем главное: устанавливать причинно-следственные связи. Четко формирует ответы, решает ситуационные задачи повышенной сложности, хорошо знаком с основной литературой, увязывает теоретические аспекты предмета с задачами практического характера.

Оценка «хорошо»: студент владеет знаниями дисциплины почти в полном объеме программы (имеются пробелы знаний только в некоторых, особенно сложных разделах). Самостоятельно и отчасти при наводящих вопросах дает полноценные ответы, не всегда выделяет наиболее существенное, не допускает вместе с тем серьезных ошибок в ответах, умеет решать легкие и средней тяжести ситуационные задачи.

Оценка «удовлетворительно»: студент владеет основным объемом знаний по дисциплине проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками. В процессе ответов допускаются ошибки по существу вопросов. Студент способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом методов исследований.

Оценка «неудовлетворительно»: студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал, отмечаются такие недостатки в подготовке студента, которые являются серьезным препятствием к успешному овладению последующим материалом.

Вопросы к экзамену по дисциплине «Программные и программно-аппаратные средства обеспечения информационной безопасности»:

1. Цели, задачи и содержание курса. Основные понятия.
2. Предмет и задачи программно-аппаратной защиты информации.
3. Автоматизированная система.
4. Структура и компоненты АС. Сети ЭВМ.
5. Способы защиты конфиденциальности.
6. Проблема защиты программного обеспечения информационных систем.
7. Объекты защиты.
8. Жизненный цикл программного обеспечения информационных систем.
9. Технологическая и эксплуатационная безопасность программного обеспечения.
10. Основные принципы обеспечения безопасности программного обеспечения.
11. Защита программного обеспечения как система научных дисциплин.
12. Уязвимости программного обеспечения.
13. Угрозы безопасности программного обеспечения.
14. Вредоносные программы.
15. Несанкционированные исследование
16. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.
17. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты).
18. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.
19. Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.
20. Работа с содержанием нормативных правовых актов.
21. Автоматизация процесса обработки информации.Понятие автоматизированной системы.
22. Особенности автоматизированных систем в защищенном исполнении.
23. Основные виды АС в защищенном исполнении. Методы создания безопасных систем.
24. Методология проектирования гарантированно защищенных КС Дискреционные модели Мандатные модели.
25. Учет, обработка, хранение и передача информации в АИС
26. Ограничение доступа на вход в систему.

27. Идентификация и аутентификация пользователей
28. Разграничение доступа. Регистрация событий (аудит).
29. Контроль целостности данных. Уничтожение остаточной информации.
30. Управление политикой безопасности. Шаблоны безопасности
31. Криптографическая защита. Обзор программ шифрования данных.
32. Управление политикой безопасности. Шаблоны безопасности
33. Организация доступа к файлам. Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД.
34. Понятие несанкционированного доступа к информации.
35. Основные подходы к защите информации от НСД.
36. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.
37. Доступ к данным со стороны процесса Особенности защиты данных от изменения. Шифрование. Сети, работающие по технологии коммутации пакетов.
38. Стек протоколов TCP/IP. Особенности маршрутизации.
39. Штатные средства защиты информации стека протоколов TCP/IP.
40. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.
41. Виртуальная частная сеть. Функции, назначение, принцип построения.
42. Виртуальная частная сеть. Функции, назначение, принцип построения.
43. Криптографические и некриптографические средства организации VPN.
44. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.
45. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки.
46. Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки.
47. Методы защиты информации при работе в сетях общего доступа. 16 Межсетевые экраны типа firewall.
48. Достоинства, недостатки, реализуемые политики безопасности Основные типы firewall.
49. Симметричные и несимметричные firewall. Уровень 1. Пакетные фильтры Уровень 2.
50. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3.
51. Proxy-сервера прикладного уровня.
52. Однохостовые и мультихостовые firewall.
53. Основные типы архитектур мультихостовых firewall.
54. Требования к каждому хосту исходя из архитектуры и выполняемых функций.
55. Требования по сертификации межсетевых экранов.
56. Сертификация средств защиты информации по требованиям безопасности информации.
57. Проверка соответствия реальных и декларируемых функциональных возможностей. Проверка отсутствия недекларируемых возможностей.

58. Методы проведения испытаний. Документация, представляемая на испытания.
59. Статический анализ исходных текстов и исполняемых модулей ПО.
60. Контроль полноты и отсутствия избыточности исходных текстов на уровне файлов.
61. Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду.
62. Контроль связей функциональных объектов по управлению и информации.
63. Синтаксический контроль наличия заданных конструкций.
64. Формирование и анализ маршрутов выполнения функциональных объектов.
65. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации.
66. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25.
67. Классификация отслеживаемых событий.
68. Особенности построения систем мониторинга.
69. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.
70. Классификация сетевых мониторов.
71. Системы управления событиями информационной безопасности (SIEM).
72. Обзор SIEM-систем на мировом и российском рынке.
73. Изучение требований о защите информации, не составляющей государственную тайну.
74. Изучение методических документов ФСТЭК по применению мер защиты.
75. Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов
76. Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol или других аналогов.
77. Изучение типовых решений для построения VPN на примере VipNet или других аналогов.
78. Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов.
79. Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов.
80. Классификация вредоносных программ.
81. Защита от вредоносных программ.
82. Методы тестирования программного обеспечения на его защищенность.
83. Методы тестирования программ.
84. Фаззинг программ.
85. Методы защиты программ от несанкционированного исследования.
86. Классификация средств несанкционированного исследования программ.

87. Способы защиты программ от несанкционированного исследования.
88. Обфускация программ. Способы встраивания защитных механизмов в программное обеспечение.
89. Методы защиты программ от несанкционированного копирования. Криптографические методы защиты от копирования.
90. Метод привязки к идентификатору. Методы, основанные на работе с переходами и стеком.
91. Манипуляции с кодом программы.
92. Методы противодействия динамическим способам снятия защиты программ от копирования.

Примерные задачи:

Дано: описание алгоритма хэширования паролей в базах данных аутентификации

Windows NT/2000 (Lan manager):

Для формирования хэша пароля все буквенные символы исходной строки пользовательского пароля приводятся к верхнему регистру, и если пароль содержит меньше 14 символов, то он дополняется нулями. Из каждой 7-байтовой половины преобразованного таким образом пароля пользователя (длина пароля в Windows NT/2000/XP ограничена 14 символами), отдельно формируется ключ для шифрования некоторой фиксированной 8-байтовой последовательности по DES-алгоритму с ключом 64(56)бит. При этом в качестве ключа используется PID (персональный идентификатор) пользователя). Полученные в результате две 8- байтовые половины хешированного пароля Lan Manager еще раз шифруются по DESалгоритму и помещаются в базу данных SAM.

Проанализируйте уровень защищенности баз данных аутентификации операционных систем, связанную с описанным алгоритмом.

1. Дано: имеется сервер, работающий под управлением ОС Windows Server 2003. На сервере запущена СУБД Oracle 9i.

   С помощью каких программных средств можно составить список возможных уязвимостей и определить уровень угроз? Опишите известные Вам виды уязвимостей, присущие предложенной конфигурации сервера и способы защиты от них.
2. Дано: Имеется процедура добавления (регистрации) нового покупателя на PL/SQL следующего содержания:

```
Create procedure NewCustomer(CName varchar2,CPassword varchar2,CInfo varchar2) as
Begin
Insert into CustomersTable (Name,Password,Info) values('||CName||' ,*||CPassword||'
,'||CInfo||');
End;
```

Какой способ SQL Injection необходимо применить, чтобы в поле CInfo занести пароль

пользователя «Иванов» из этой же таблицы. Как обнаружить и предотвратить попытку

SQL Injection

3. Дано: имеется функция проверки аутентификации покупателя по имени пользователя и

паролю на PL/SQL следующего содержания:

```
Create function GetCustomerInfo(CName varchar2,CPassword varchar2) return varchar2 as
CInfo varchar2(200);
Begin
Select Info into CInfo from CustomersTable where
Name='||CName||' and Password='||CPassword||';
Return CInfo;
End;
```

17

Какой способ SQL Injection необходимо применить, чтобы злоумышленник зарегистрировался под пользователем «Иванов» из этой же таблицы без знания пароля. Как обнаружить и предотвратить попытку SQL Injection

Дано: Как известно, мера информационной энтропии измеряется по формуле Шэннона:

n

H = -^p(i)log2p(i).. В то же время, по формуле Хартли, на один символ алфавита

источника сообщений (со стандартным объемом в 256 символов) приходится

H=log2256=8bit.

Проанализируйте применимость формул для случая парольной защиты с паролем, запоминаемым пользователем, и для случая парольной защиты с паролем, запоминаемым в аппаратном устройстве хранения паролей. В каких случаях формула Шэннона будет давать такой же результат, что и формула Хартли.

Критерии оценки эссе (рефератов, докладов, сообщений)

Оценка «отлично»: выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка «хорошо»: основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

Оценка «удовлетворительно»: имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы.

Оценка «неудовлетворительно»: тема освоена лишь частично; допущены грубые ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Темы для эссе (рефератов, докладов, сообщений) по дисциплине «Программные и программно-аппаратные средства обеспечения информационной безопасности»:

1. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей.
2. Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей.
3. Анализ методов и средств анализа защищенности беспроводных сетей.
4. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения.
5. Виброакустические средства современных систем обеспечения информационной безопасности.
6. Средства защиты от ПЭМИН, современное состояние, проблемы и решения.
7. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений.
8. Средства обеспечения информационной безопасности банков данных.
9. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса).
10. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации.

11. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота.
12. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа.
13. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации.
14. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела.
15. Инструментальные средства анализа рисков информационной безопасности.
16. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками.
17. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности).
18. Контроль работы и регистрации пользователей и технических средств
19. Идентификация имеющихся технических средств, пользователей и файлов
20. Защита операционных ресурсов ЭВМ и пользовательских программ
21. Обслуживания различных режимов обработки данных
22. Уничтожение данных после ее использования в элементах системы
23. Сигнализирование при нарушениях
24. Анализ аппаратных средств защиты ПК
25. Разработка ПС на основе асимметричного шифрования для защиты ОС.
26. Разработка ПС для защиты ОС с помощью цветовой схемы.
27. Разработка программно-аппаратного комплекса для защиты ОС.
28. Разработка электронного ключа для защиты от несанкционированного доступа к ПК.
29. Разработка ПС для защиты от спама.
30. Разработка ПС для защиты ПК от несанкционированного сканирования портов.
31. Анализ существующих методов защиты ОС.
32. Разработка ПС для защиты от фишинговых атак.
33. Разработка ПС для защиты ПК от несанкционированного сканирования портов.
34. Разработка электронного ключа для доступа к ПК.
35. Разработка межсетевого экрана.
36. Создание системы защиты локальной сети от несанкционированного доступа.
37. Разработка системы управления сайтом с дополнительной аутентификацией пользователя.
38. Разработка ПС для аутентификации пользователя с помощью графического изображения.
39. Разработка аппаратно-программного комплекса защиты ПК.
40. Анализ существующих ПС по защите локальных сетей от внешних атак.

СТРУКТУРА ИТОГОВОГО ТЕСТА:

Тест содержит 20 вопросов случайным образом выбранных их списка. Тест проводиться на персональном компьютере в оболочке для тестирования MyTest. Результат выдается сразу после тестирования и формируется отчет протестированных студентов на сервере.

Время на подготовку и выполнение:

Выполнение – 20 минут. За правильный ответ выставляется по 1 баллу, затем результаты суммируются, и выставляется оценка. За неправильный ответ 0 баллов.

Критерии оценки промежуточной аттестации:

Оценка «отлично» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «отлично», средний балл по аттестациям не ниже 4,5.

Оценка «хорошо» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «хорошо», средний балл по аттестациям не ниже 3,5.

Оценка «удовлетворительно» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «удовлетворительно», средний балл по аттестациям не ниже 2,5.

Оценка «неудовлетворительно» выставляется, если имеются все конспекты лекции обучающимися выполнено менее 100% практических работ, оценка за итоговое тестирование – «неудовлетворительно», средний балл по аттестациям ниже 2,5.

Цель итогового тестирования:

Тестирование по учебной дисциплине **«Программные и программно-аппаратные средства обеспечения информационной безопасности»** предназначено для проверки теоретических знаний и понятийного аппарата, которые лежат в основе профессионального образования и найдут самое широкое применение в будущей профессиональной деятельности учащихся по специальности 10.02.05.Обеспечение информационной безопасности автоматизированных систем.

Критерии оценки знаний:

Процент правильных ответов, %	Оценка знаний
90-100	5 «отлично»
75-89	4 «хорошо»
60-74	3 «удовлетворительно»
Менее 60	2 «неудовлетворительно»

Список теоретических заданий для подготовки к итоговому тестированию (ТЗ) по дисциплине «Программные и программно-аппаратные средства обеспечения информационной безопасности»

1. Под СВТ понимается:
   а) совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем
   б) электронные компоненты, из которых строятся вычислительные системы
   в) совокупность программных и технических элементов систем передачи информации, используемая для построения компьютерных систем
2. Под АС понимается:
   а) система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций
   б) локальная ПЭВМ или компьютерная сеть с установленным системным программным обеспечением и средствами коммуникации
   в) автоматизированная система управления обработкой информации с целью выполнения производственных функций организации
3. Под несанкционированным доступом в компьютерной системе понимается:
   а) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС
   б) доступ к информации с преодолением парольной защиты, фальсификации аутентификационной информации с использованием штатных средств, предоставляемых СВТ или АС
   в) реализация угроз безопасности информации с целью ознакомления и/или уничтожения информации с использованием штатных или специальных СВТ
4. К основным функциям СРД относятся:
   а) регистрация действий субъекта и активизированного им приложения

б) контроль целостности программной и аппаратной части СРД
в) реакция на попытки НСД
г) управление потоками информации в целях предотвращения записи её н носители несоответствующего уровня конфиденциальности.

5. К основным функциям СРД не относятся:
а) реализация правил разграничения доступа субъектов и их процессов к информации и устройствам создания её твердых копий
б) изоляция процесса, выполняемого в интересах субъекта доступа, от других субъектов
в) идентификация и аутентификация субъектов и поддержание привязки субъекта к процессу, выполняемому для него

6. К функциям обеспечивающих средств для СРД не относятся:
а) учет выходных печатных и графических форм и твердых копий в КС
б) очистка оперативной памяти после завершения работы пользователя с защищаемыми данными
в) реализация правил обмена информацией между субъектами в компьютерных сетях.

7. Идентификация это:
а) однозначное определение уникального имени, под которым пользователь зарегистрирован в КС
б) генерация уникального имени, под которым пользователь будет зарегистрирован в КС
в) проверка уникальности имени зарегистрированного в КС пользователя при запросе доступа к ресурсам КС

8. Аутентификация это:
а) подтверждение подлинности имени, предъявленного пользователем
б) подтверждение заявленных пользователем прав доступа к ресурсам КС
в) проверка наличия введенного имени пользователя в регистрационной базе КС.

9. Авторизация это:
а) процесс наделения пользователя индивидуальным набором привилегий в системе и определение его прав доступа к объектам КС
б) процесс определения набора информационных ресурсов, доступ к которым разрешен пользователю
в) проверка соответствия введенного пользователем пароля его идентификатору.

10. Аудит безопасности КС это:
а) учет возникающих при работе системы событий, связанных с безопасностью информации в ней, и регистрация этих событий в системном журнале
б) учет попыток НСД и регистрация их в системном журнале

в) проверка соответствия защитных функций установленных в АС СЗИ требованиям, предъявляемым к СЗИ в АС
г) учет неудачных попыток ввода пароля и регистрация этих попыток в системном журнале.

11. Укажите наиболее правильную формулировку требований к «идеальной» системе защиты информации (СЗИ).
а) СЗИ должна быть прозрачна для легальных пользователей и создавать непреодолимые трудности для реализации НСД.
б) СЗИ должна обеспечивать уровень защищенности информации, соответствующий требованиям для данного класса АС.
в) СЗИ должна обеспечивать защищенность информации на программном и аппаратном уровне, включать в себя подсистемы, использующие разные технологии ЗИ.

12. Выберите наиболее полное правило, которым следует руководствоваться при выборе паролей:
а) пароли должны трудно подбираться и легко запоминаться
б) в паролях следует использовать буквы и цифры, причем длина пароля должна быть не менее 4 символов
в) в качестве паролей не следует использовать простые слова, имена собственные и т.п.

13. Выберите наиболее правильное описание начального этапа модели «рукопожатия».
а) система генерирует случайное значение , вычисляет и сообщает пользователю.
б) пользователь генерирует случайное значение , вычисляет и вводит в ответ на запрос системы.
в) система генерирует случайное значение , вычисляет и сообщает пользователю.
г) система генерирует случайное значение , вычисляет и сообщает и пользователю.

14. К пассивным устройствам аутентификации не относятся:
а) пластиковые карты с магнитной полоской
б) элементы Touch Memory
в) USB-ключи

15. Уязвимость информационной системы это:
а) любая характеристика, использование которой нарушителем может привести к реализации угрозы
б) ошибки в программном обеспечении, возникновение которых может привести к реализации угрозы
в) количественная и качественная недостаточность средств ЗИ, которая может привести к реализации угрозы.

16. Угрозой информационной системе называется:
а) потенциально возможное событие, действие, процесс или явление, которое может вызвать нанесение ущерба ресурсам системы

б) совокупность программно-аппаратных средств осуществления НСД при наличии методов их использования для нанесения ущерба ресурсам системы
в) возможность использования информации, штатных и нештатных технических средств АС для нанесения ущерба ресурсам системы.

17. Под информационной безопасностью понимается:
а) защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры
б) комплекс программно-аппаратных средств направленных на защиту от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры
в) совокупность мер организационно-технического характера, направленных на защиту от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры

18. Сущность комплексного подхода к ЗИ заключается в:
а) сочетании различных мер обеспечения безопасности на законодательном, административном, процедурном и программно-техническом уровнях
б) сочетании различных мер обеспечения безопасности на законодательном и программно-техническом уровнях
в) сочетании различных программно-аппаратных средств защиты АС от НСД.

19.Аспекты обеспечения ИБ:
а) формальный и практический
б) общий и частный
в) программный и аппаратный.

20. Укажите, что не является контекстом ЗИ и соответствующих бизнес-процессов:
а) конфиденциальность
б) целостность
в) доступность
г) достоверность.

21. Основная цель сетевой ПБ:
а) контроль сетевого трафика и его использования
б) противодействие попыткам НСД с использованием сетевой инфраструктуры
в) установка и правильная настройка программно-аппаратных СЗИ.

22. Под доверенными понимаются сети, …

а) …над которыми специалисты организации имеют полный административный контроль
б) …на компьютерах которых установлены средства удаленного администрирования
в) …оснащенные программно-аппаратными СЗИ и проходящие регулярные проверки на предмет вирусной активности.

23. Ресурсы (в контексте задачи управления рисками) это:
а) то, что организация ценит и хочет защитить
б) финансовые и информационные активы организации
в) файлы и бумажные документы.

24. Политика информационной безопасности определяет:
а) способы развертывания систем безопасности и поведение пользователей при использовании КС
б) способы настройки межсетевых экранов и антивирусных средств
в) порядок получения доступа пользователей к ресурсам КС организации.

25. Основная цель сетевой ПБ:
а) описание топологии ЛВС и определение мест установки МЭ
б) контроль сетевого трафика и его использования
в) формирование требований к настройке МЭ и антивирусных систем
г) разрешить то, что явно не запрещено
д) запретить то, что явно не разрешено.

26. Выберите пункт из перечисленного ниже, который не относится к службам безопасности:
а) аутентификация
б) целостность
в) информированность.

27. Под доверенными понимаются сети, …
а) …на компьютерах которых установлены средства удаленного администрирования
б) …над которыми специалисты организации имеют полный административный контроль
в) оснащенные программно-аппаратными СЗИ и проходящие регулярные проверки на предмет вирусной активности.

29. Ресурсы (в контексте задачи управления рисками) это:
а) информация и поддерживающие средства для ведения бизнеса
б) базы данных корпоративных информационных систем (бухгалтерских, аналитических и т.п.)
в) файлы и бумажные документы
г) описания устройств и технологических процессов, являющиеся «ноу-хау» организации.

30. Угроза – это …
а) …потенциальная причина нежелательного события, которое может нанести ущерб

б) организации и её объектам
в) …сетевая атака, влекущая нарушение работоспособности КС организации
г) …потенциальная возможность НСД к конфиденциальной информации организации
д) …совокупность вредоносного ПО, распространяющаяся по компьютерным сетям.

31. По характеру воздействия угрозы могут быть…
а) …против доступности, целостности, конфиденциальности
б) …внутренними, внешними
в) …преднамеренными, случайными.

32. Риск безопасности это …
а) …возможность реализации сетевой атаки на ресурсы КС
б) вероятность преодоления системы защиты за произвольный период времени
в) …возможность данной угрозы реализовать уязвимости для нанесения ущерба организации
г) …вероятность начала вредоносного воздействия на ресурсы КС злоумышленником.

33. Классы межсетевых экранов по функционированию на уровнях модели OSI:
а) пакетный фильтр, программно-аппаратный, программный.
б) пакетный фильтр, экранирующий транспорт, прикладной шлюз
в) контроллер состояния протокола, экранирующий транспорт, прикладной шлюз.

34. Список доступа маршрутизатора – это…
а) …набор строк, описывающих доверенные адреса хостов
б) …набор строк, определяющих некие образцы, на соответствие которым проверяются пакеты IP
в) …набор строк, описывающих конфигурацию интерфейсов маршрутизатора.

35. Выберите наиболее правильное утверждение.
а) стандартный ACL может проверять адреса отправителей, получателей и ряд параметров
б) нумерация стандартных ACL выполняется в диапазоне от 100 до 199
в) стандартный ACL может выполнять контроль состояния соединения
г) стандартный ACL может проверять только адреса отправителей.

36. Выберите наиболее правильное утверждение.
а) ключевое слово host означает любой IP-адрес хоста
б) обратная маска 255.255.255.255 определяет единственный IP-адрес
в) обратная маска 0.0.0.0 определяет единственный IP-адрес
г) ключевое слово any соответствует WildCard-маске 0.0.0.0.

37. В чем заключается смысл следующего списка доступа?
    а) access-list 45 permit 192.168.20.0 0.0.0.255
    б) access-list 45 deny host 192.168.20.13
    в) трафику сети 192.168.20.0 разрешено проходить через маршрутизатор, за исключением хоста192.168.20.13
    г) трафику сети 192.168.20.0 разрешено проходить через маршрутизатор
    д) трафику сети 192.168.20.0 запрещено проходить через маршрутизатор, за исключением хоста 192.168.20.13
    е) трафику хоста 192.168.20.13 запрещено проходить через маршрутизатор, а остальным хостам сети 192.168.20.0 – разрешено.
38. Выберите наиболее правильное утверждение.
    а) расширенный ACL может проверять адреса источников, получателей, тип протокола и порты.
    б) расширенный ACL обеспечивает более быструю проверку пакетов, чем стандартный ACL.
    в) допускается размещать более 1 расширенного ACL на интерфейс, на протокол, на направление.
    г) расширенный ACL не может проверить состояние соединения TCP.
39. В чем заключается смысл следующего выражения?
    а) запрещение доступа к хосту с IP-адресом 130.120.110.100
    б) разрешение доступа к хосту с IP-адресом 130.120.110.100
    в) запрещение доступа к подсети 130.120.110.0 0.0.0.255.
    г) access-list 101 deny ip 0.0.0.0 255.255.255.255 130.120.110.100 0.0.0.0
40. Межсетевой экран (Брандмауэр, firewall) – это…
    а) Комплекс аппаратных средств
    б) Комплекс программных средств
    в) Комплекс аппаратных или программных средств
    г) Комплекс аппаратных и программных средств

Основная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. - Москва: Издательство Юрайт, 2021. - 312 с. - (Профессиональное образование). - ISBN 978-5-534-13221-2. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL:
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. - Москва: Издательство Юрайт, 2020. - 312 с. - (Профессиональное

образование). - ISBN 978-5-534-13221-2. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/449548

Дополнительная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. - Москва : Издательство Юрайт, 2019. - 312 с. - (Специалист). - ISBN 978-5-9916-9043-0. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/
2. Долозов Н. Л., Гультяева Т. А. Программные средства защиты информации: конспект лекций Новосибирск: Новосибирский государственный технический университет, 2015. – 63 с. https://biblioclub.ru/index.php?page=book_red&id=438307&sr=1
3. Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков Программно-аппаратные средства защиты информационных систем : учебное пособие Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2017. – 194 с. https://biblioclub.ru/index.php?page=book_red&id=499013&sr=1
4. Рецензируемый научный журнал «Проблемы информационной безопасности».
5. ГОСТ Р ИСО/МЭК ТО 12182-2002. Информационная технология. Классификация программных средств. 2002 г.www.standartgost.ru

Интернет-ресурсы:

1. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. URL: http://elibrary.ru
2. Национальная электронная библиотека [Электронный ресурс]. URL: https://нэб.рф/.
3. Электронно-библиотечная система «Университетская библиотека онлайн» [Электронный ресурс]. URL: http://biblioclub.ru
4. Юридический вестник ДГУ. URL: www.jurvestnik.dgu.ru
5. Федеральный портал «Российское образование» [Электронный ресурс]. URL: http://www.edu.ru
6. Электронно-библиотечная система Юрайт [Электронный ресурс]. URL: https://urait.ru/.
7. http://www.tehlit.ru, свободный. – Загл. с экрана

КРИТЕРИИ ОЦЕНКИ

по дисциплине

МДК.02.02. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Критерии оценки:

Оценка «отлично»: правильно выполнены все задания практической работы, правильно даны ответы на все контрольные вопросы, выполнены задания самостоятельной работы в полном объеме. Студент отвечает на вопросы, демонстрируя глубокие знания.

Оценка «хорошо»: выполнены все задания практической и контрольной работы с наличием несущественных ошибок, выполнены задания самостоятельной работы в неполном объеме, не противоречащих основным понятиям дисциплины. Студент уверенно отвечает на вопросы, демонстрируя достаточно высокий уровень знаний

Оценка «удовлетворительно»: выполнены все задания практической и контрольной работы с наличием грубых ошибок, выполнены задания самостоятельной работы в неполном объеме, противоречащих или искажающих основные понятия дисциплины. Студент демонстрирует достаточный уровень знаний, однако затрудняется отвечать на некоторые вопросы

Оценка «неудовлетворительно»: выполнены не все задания практической работы, даны не все ответы на контрольные вопросы, имеются грубые ошибки в выполнении практических заданий и/или ответах на контрольные вопросы, противоречащие или искажающие основные понятия дисциплины, самостоятельная работа не выполнена, либо выполнена на 50%. Студент затрудняется отвечать на вопросы.

Вопросы к экзамену по дисциплине «Криптографические средства и методы защиты информации»:

1. Криптография. Цели криптографии. История развития криптографии.
2. Классификация криптографических методов.
3. Обеспечение конфиденциальности, целостности, неотказуемости, аутентичности, неотслеживаемости информации.
4. Основные понятия: шифр, открытый текст, шифр текст, электронная подпись, хэш-функция.
5. Математические примитивы. Криптографические алгоритмы.
6. Криптографическая схема. Криптографическая система.
7. Классификация шифров.
8. Алгебраическая модель шифра.
9. Алгебраическая модель шифра замены.
10. Алгебраическая модель шифра перестановки.
11. Алгебраическая модель шифра гаммирования.
12. Вероятностная модель шифра.
13. Распределения на множествах открытых текстов, ключей, шифр текстов.
14. Математические модели открытых текстов
15. Атаки на шифры.
16. Понятие стойкости шифров.
17. Классификация атак на шифры.
18. Виды атак на схемы шифрования.
19. Цели криптоанализа.
20. Теоретико-информационная стойкость.
21. Условная вероятность.
22. Энтропия. Понятие абсолютно стойкого шифра.
23. Теоретико-сложностная стойкость шифров.
24. Понятие практической стойкости шифра.
25. Модель противника.
26. Классификация симметричных криптографических систем.
27. Требования к блочным шифрам.
28. Требования к поточным шифрам.
29. Криптографические параметры узлов и блоков блочных шифров.
30. Базовые криптографические преобразования блочных шифров.
31. Способы реализации блочных шифров.
32. Процедура развертывания ключа
33. Сеть Фейстеля.
34. Шифр DES.
35. Основные преобразования.
36. Алгоритм зашифрования.
37. Алгоритм расшифрования. Процедура развертывания ключа.
38. Типовые методы построения поточных шифров.
39. Синхронные и самосинхронизирующиеся поточные шифры.
40. Генераторы псевдослучайных последовательностей.

41. Статистические характеристики генераторов псевдослучайных последовательностей. Методы усложнения последовательностей.
42. Элементы теории сложности.
43. Односторонние функции.
44. Односторонние функции с секретом.
45. Примеры односторонних функций с секретом.
46. Алгебраическая модель асимметричного шифра.
47. Понятие открытого ключа.
48. Схема шифрования RSA.
49. Процедура генерации ключей.
50. Процедура шифрования.
51. Схема Эль-Гамаля.
52. Стойкость схем шифрования RSA и Эль-Гамаля.
53. Понятие электронной подписи.
54. Связь с понятием электронной подписи ФЗ-63.
55. Процессы формирования и проверки электронной подписи.
56. Алгебраическая модель схемы электронной подписи.
57. Конструкция схемы электронной подписи на односторонней функции с секретом.
58. Электронная подпись на основе схемы шифрования с открытым ключом, электронная подпись с извлечением сообщения, электронная подпись с дополнением.
59. Криптографическая хэш-функция без ключа.
60. Слабая хэш-функция. Сильная хэшфункция.
61. Стойкость криптографической хэш-функции.
62. Применение хэш-функций.
63. Типовые конструкции криптографических хэш-функций.
64. Хэш-функция ГОСТ Р 34.11–94.
65. Конструкция хэш-функции на основе алгоритма шифрования.
66. Шаговая функция хэширования.
67. Коды аутентификации сообщений.
68. Методы построения кодов аутентификации сообщений.
69. Основные понятия. Цели безопасности криптографических протоколов. Протоколы передачи сообщений.
70. Протоколы передачи ключей.
71. Протоколы аутентификации.
72. Универсальная модель жизненного цикла ключа.
73. Управление ключами.
74. Службы управления ключами.
75. Назначение инфраструктуры открытых ключей.
76. Удостоверяющий центр.
77. Функции удостоверяющего центра.
78. Сертификат открытого ключа
79. Общие принципы построения СКЗИ.
80. Принципы применения криптографических механизмов защиты.

81. Принципы применения инженерно-криптографических механизмов защиты. Положение ПКЗ-2005.
82. Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств. Приказ ФАПСИ 152. Приказ ФСБ РФ 378.

Правила выполнения лабораторных работ:

При выполнении лабораторных работ (ЛР), студенты должны соблюдать и выполнять следующие правила:

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

Критерии оценки лабораторных работ

Лабораторные работы оцениваются по пятибалльной шкале.

Оценка «отлично»: ставится, если ЛР выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, необходимые программы запущены и работают без ошибок; работа оформлена аккуратно;

Оценка «хорошо»: ставится, если ЛР 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 «удовлетворительно»: частично с помощью преподавателя, присутствуют ошибки при запуске и работе требуемых программ; по оформлению работы имеются замечания.

Оценка «неудовлетворительно»: ставится, если обучающийся не подготовился к ЛР, при запуске и эксплуатации (работе) требуемых программ студент допустил грубые ошибки, по оформлению работы имеются множественные замечания.

Лабораторная работа № 1.
Шифрование данных методамиподстановки, перестановки и полиалфавитными шифрами

Цель работы: Приобретение навыков шифрования информации с использованием простейших методов шифрования.

Криптографические методы защиты информации

Проблемой защиты информации путем ее преобразования занимается криптология (kryptos - тайный, logos - наука). Криптология разделяется на два направления - криптографию и криптоанализ. Цели этих направлений прямо противоположны:

– криптография занимается поиском и исследованием математических методов преобразования информации.

– сфера интересов криптоанализа - исследование возможности расшифровывания информации без знания ключей.

Криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа. В качестве информации, подлежащей шифрованию и дешифрованию, рассматриваются тексты, построенные на некотором алфавите. Алфавит - конечное множество используемых для кодирования информации знаков. Примеры алфавитов, используемых в современных информационных системах:

- алфавит Z_{33} - 32 буквы русского алфавита и пробел;
- алфавит Z_{256} - символы, входящие в стандартные коды ASCII и КОИ-8;
- бинарный алфавит - $Z_2 = \{0,1\}$.

Шифрование – процесс преобразования исходного или открытого текста в зашифрованный. Выполняется на основе ключа и используется для защиты сообщений от несанкционированного прочтения. Дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов. Обычно ключ представляет собой последовательный ряд символов того же алфавита, в котором набрано информационное сообщение

По характеру используемого ключа криптографические методы делятся на:

- симметричные: для шифрования и дешифрования используется

один и тот же секретный ключ;

- асимметричные: для шифрования и дешифрования используют разные ключи, открытый – для шифрования, секретный – для дешифрования.

К симметричным криптографическим алгоритмам относят простейшие методышифрования (подстановки, перестановки), потоковые и блочные шифры.

Метод подстановки

Шифр подстановки или замены - наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие символы того же либо другого алфавита по определенному правилу.

Историческим примером шифра подстановки является шифр Цезаря, в котором каждый символ открытого текста заменяется другой буквой, которая определяется путем смещения по алфавиту от исходной буквы влево или вправо на k букв. При достижении конца алфавита выполняется циклический переход к его началу. Цезарь использовал шифр замены при смещении вправо при $k = 3$.

Для произвольного ключа k шифр имеет вид:

$$x_i \to y_j, \qquad i = (j + k) mod\, n, \qquad i = \overline{1,n}$$

где i – номер в алфавите символа открытого текста,

j –номер зашифрованного символа,

k –величина смещения - ключ,

n –количество букв в алфавите.

Обратная подстановка осуществляется по правилу

$$i = (j + n - k) mod\, n$$

Условием для успешной реализации этого метода является совпадение размера множеств открытого текста и шифротекста. Это условие в современных криптосистемах называется гомоморфизмом.

Другим вариантом метода подстановки является задание соответствия между буквами исходного алфавита и буквами подстановочного алфавита. Это позволяет заменять буквы в открытом тексте буквами из подстановочного алфавита Подстановочный алфавит может задаваться как множество символов, либо составляться по определенному правилу.

Пусть подстановочный алфавит составлен по следующему правилу:

$$y_{2k-1} = x_{2k}, y_{2k} = x_{33-2k} \quad k = \overline{1,16} \qquad (1.3)$$

где x- исходный подстановочный алфавит; y - подстановочный алфавит;

В формуле (1.3) буквы с четными и нечетными номерами в

алфавите, заменяются по разным правилам.

Воспользуемся новым алфавитом для шифрования фразы:

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Каждая буква в этой фразе имеет порядковый номер в исходном алфавите. При шифровании методом подстановки необходимо заменить буквы исходного алфавита соответствующими буквами подстановочного алфавита (О - П, С - О, Н - Т и т.д.). Так буква О в исходном алфавите имеет номер 16, k=8. По правилу $x(2\square 8)=y(33\text{-}2\square 8)$ буква О заменяется буквой с номером 17, т.е. П.

В шифрованном виде эта фраза примет следующий вид:

ПОТПГЭ ШБЖЙУЭ ЙТХПСНБЧЙЙ.

Шифрование простой подстановкой на коротких алфавитах обеспечивает слабую защиту открытого текста. Подстановочные криптограммы можно раскрыть, составляя частотные таблицы для букв, пар букв (биграмм) и троек букв (триграмм). Большие частоты появления одних букв и малые других, а также частые ассоциации гласных с согласными позволяют найти буквы открытого текста. С увеличением размера алфавита применение частотного анализа становится все более дорогим, однако, принцип подстановки теряет свою практическую значимость.

Метод перестановки

При шифровании этим методом переставляются не буквы алфавита, а буквы открытого текста в пределах группы, называемой таблицей перестановки. Например, сообщение разбито на группы знаков, включая пробелы, и в каждой группе буквы переставлены в соответствии с правилом:

1	2	3	4
2	4	1	3

В этом случае вторая буква исходного текста буде стоять на первом месте, четвертая –на втором и т.д. Если сообщение не кратно количеству символов в группе перестановки, последняя группа дополняется определенными символами, чаще всего пробелами.

Если задана фраза: ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ, то после шифрования она примет вид: СООНЫЗВ ЩТАИ НЫИОМФРИАИ.

В случае перестановки таблицы частот для пар и трех букв показывают наличие стандартных буквенных пар, позволяя реконструировать открытый текст путем поиска тех перестановок, которые их воссоединяют. Следовательно, ключ, используемый для преобразования открытого текста, может быть восстановлен по одной криптограмме. Используется, как правило, в сочетании с другими методами.

Многоалфавитные шифры

Слабая криптостойкость моноалфавитных подстановок преодолевается с применением подстановок многоалфавитных. Для защиты от частотного анализа были разработаны многоалфавитные шифры, в которых для шифрования сообщения периодически используется несколько различных подстановочных алфавитов. Если задано *r* подстановочных алфавитов, то исходное сообщение разбивается на группы по *r* символов, для шифрования *i*-го символа группы используется *i*-ый подстановочный алфавит. Например, для *r*=4 буквы с номерами 1,5,9,13, ... шифруются 1 алфавитом, буквы с номерами 2,7,10,14, ... - 2 алфавитом, и т.д.

Для получения открытого текста выделяются повторяющиеся группы знаков, и определяется период повторения. Предполагаемый период проверяется составлением частотного распределения для каждой n-й буквы зашифрованного текста. Если каждое из n частотных распределений имеет сильную неоднородность, характерную для моноалфавитной подстановки, то предполагаемый период является правильным. Затем задача решается как n различных простых подстановок.

Задание на лабораторную работу

1. Разработать алгоритм и составить программу, позволяющую закодировать любой текст одним из вышеизложенных методов и выполнить обратное преобразование. Метод, которым необходимо зашифровать исходную информацию, выбирается в соответствии с вариантом из таблиц 1.1, 1.2, 1.3. Язык программирования выбирается произвольно.
2. Осуществить вывод на экран или принтер полученной криптограммы.
3. Провести дешифрование данной криптограммы, в результате должен бытьполучен исходный текст.
4. Результаты работы оформить в виде отчета.

Таблица 1.1 - Методы шифрования

Ном вар.	Метод шифрования	Таблица	Номер задания в таблице	Представление исходного текста
1	Подстановка	2	3	Английский алфавит
2	Перестановка	3	1	ASCII-код
3	Многоалфавитные шифры	2	1, 2, 5	Русский алфавит
4	Перестановка	3	2	Русский алфавит

5	Подстановка	2	4	Английский алфавит
6	Многоалфавитные шифры	2	1, 3	Русский алфавит
7	Подстановка	2	1	Английский алфавит
8	Многоалфавитные шифры	2	2, 5	Английский алфавит
9	Перестановка	3	3	ASCII-код

Продолжение таблицы 1.1				
10	Подстановка	2	2	Русский алфавит
11	Перестановка	3	4	ASCII-код
12	Многоалфавитные шифры	2	1, 3, 4	Русский алфавит

Таблица 1.2 – Подстановочные алфавиты

Ном симв	Исходный алфавит		Подстановочный алфавит								
			1		2		3		4		5
1	А	А	Б	V	С	С	О	Z	Ю	С	М
2	Б	В	Ю	W	О	D	П	ппро-ббел	Я	D	Н
3	В	С	Г	Х	У	А	М	.	Ы	А	О
4	Г	D	Ы	Y	М	В	Н	Х	Э	В	П
5	Д	Е	Е	Z	К	Н	Х	Y	Ь	Н	Р
6	Е	F	Ь	про-бел	Х	І	Л	,	Ъ	І	С
7	Ё	G	З	.	Ч	J	И	!	Ш	J	Т
8	Ж	Н	Ш	,	И	Е	Й	S	Щ	Е	У
9	З	І	Й	!	Щ	F	Ж	Т	Ц	F	Ф
10	И	J	Ц	:	Ж	G	З	:	Ч	G	Х
11	Й	К	Л	;	Ъ	О	Д	;	Ф	О	Ц
12	К	L	Ф	?	Д	Р	Е	Q	Х	Р	Ч
13	Л	М	Н	-	Э	Q	В	R	Т	Q	Ш
14	М	N	Т	К	В	R	Г	?	У	R	Щ
15	Н	О	П	L	Я	К	А	-	Р	К	Ъ
16	О	Р	Р	М	А	L	Б	N	С	L	Ь

17	П	Q	C	N	Б	M	Ю	O	O	M	Ы
18	Р	R	O	O	Ю	N	Я	P	П	N	Э
19	С	S	У	P	Г	U	Ы	L	M	U	Ю
20	Т	T	M	Q		V	Э	M	H	V	Я
21	У	U	X	R	E	W	Ь	N	К	W	про-бел
22	Ф	V	К	S	Ь	:	про-бел	O	Л	:	А
23	Х	W	Ч	T	З	S	Ш	P	про-бел	S	Б
24	Ц	X	И	U	Ш	T	Щ	A	Й	T	В
25	Ч	Y	Щ	A	Й	Z	Ц	B	Ж	Z	Г
26	Ш	Z	Ж	B	Ц	про-бел	Ч	C	З	про-бел	Д
27	Щ	про-бел	Ъ	C	Ё	X	Ф	D	Д	X	Е
28	Ъ	.	Д	D	Ф	Y	К	E	E	Y	Ё
29	Ь	,	Э	E	H	;	T	F	B	;	Ж
30	Ы	!	B	F	T	?	У	G	Г	?	З
31	Э	:	Я	G	П	-	P	H	A	-	И
32	Ю	;	про-бел	H	P	.	C	I	Б	.	Й
33	Я	?	A	I	Ы	,	Ъ	J	Ё	,	К
34	про-бел	-	Ё	J	Л	!	Ё	K	И	!	Л

Таблица 1.3 - Группы перестановок

Номер вар.	Группа перестановки	Номер вар.	Группа перестановки
1	□1 2 3 4 5 6□ □3 5 2 6 1 4□	4	□1 2 3 4 5 6□ □2 6 3 5 1 4□
2	□1 2 3 4 5□ □5 4 1 2 3□	5	□1 2 3 4 5□ □2 5 4 3 1□
3	□1 2 3 4 5 6□ □2 5 3 4 1 6□	6	□1 2 3 4 5 6□ □3 5 2 6 1 4□

Содержание отчета:

- цель работы, постановка задачи,
- описание исходных данных,

– алгоритм работы программы,
– текст программы,
– результаты работы программы,
– анализ результатов
– выводы.

Контрольные вопросы

1. Почему метод подстановки имеет слабую надежность?
2. Что такое частотный анализ?
3. Что является криптографическим ключом в методе перестановки?
4. Как связаны метод подстановки и многоалфавитные шифры?
5. В чем отличие криптографии от криптоанализа?
6. По какому признаку шифры делят на симметричные и асимметричные?

Лабораторная работа №2.
Шифр гаммирования

Цель работы: Освоение принципов шифрования гаммированием, изучение свойств генератора псевдослучайных чисел, программная реализация метода гаммирования.

Теоретические основы метода гаммирования

Принцип шифрования гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной гаммы шифра на открытые данные обратимым образом (используя операцию сложения по модулю 2).

$$y_i = x_i \oplus g_i$$

где x_i - бит исходного текста;

y_i - бит зашифрованного текста;

g_i - бит гаммы.

Процесс дешифрования сводится к повторной генерации гаммы шифра при известном ключе и наложении такой же гаммы на зашифрованные данные.

Гамма шифра генерируется независимо от исходного текста.

Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей и изменяется случайным образом для каждого шифруемого слова. Если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то шифр можно раскрыть только прямым перебором (подбором ключа). В этом случае криптостойкость определяется размером ключа.

Метод гаммирования становится бессильным, если известен фрагмент исходного текста и соответствующая ему шифрограмма. В

этом случае простым сложением по модулю 2 получается отрезок псевдослучайной последовательности и по нему восстанавливается вся эта последовательность.

Линейные конгруэнтные датчики ПСЧ

Чтобы получить линейные последовательности элементов гаммы, длина которых не превышает размер шифруемых данных, используют датчики ПСЧ. Одним из хороших конгруэнтных генераторов является линейный конгруэнтный датчик ПСЧ. Он вырабатывает последовательности псевдослучайных чисел $T(i)$, описываемые соотношением

$$T_i = (A \cdot T_{i-1} + C) mod\ M, \quad (2.2)$$

где A, C, M - константы, T_0 - исходная величина, выбранная в качестве порождающего числа. Очевидно, что эти три величины и образуют ключ.

Такой датчик ПСЧ генерирует псевдослучайные числа с определенным периодом повторения, зависящим от выбранных значений A и C. Значение M обычно устанавливается равным 2^b , где b -длина машинного слова в битах. Необходимо выбирать числа A и C так, чтобы период M был максимальным.

Как показано Д.Кнуттом, линейный конгруэнтный датчик имеет максимальную длину
M тогда, когда C нечетное и A mod 4 = 1.

В качестве примера использования линейного конгруэнтного датчика ПСЧ рассмотрим процесс шифрования исходного текста «абв». Пусть b = 5, т.е. для представления буквы исходного текста используется 5 двоичных разрядов. В соответствии с номером в алфавите буква «а» имеет двоичный код 00001; буква «б» имеет двоичный код 00010; буква «в» имеет двоичный код 00011. Исходный текст будет представлен в виде последовательности 00001 00010 00011.

Для формирования гаммы шифра выберем параметры датчика ПСЧ: A=5; C=3; T(0)=7; M=2^b; b=5; M=2^5=32. Сформируем три псевдослучайных числа:

T(1) = (5□7+3) mod 32 = 6 (00110);
T(2) = (5□6+3) mod 32 = 1 (00001);
T(3) = (5□1+3) mod 32 = 8 (01000).

Полученная гамма шифра 00110 00001 01000. Зашифрованный текст получается путем наложения гаммы шифра на исходный текст (путем сложения по модулю 2):

```
  00001 00010 00011
  00110 00001 01000
  -----------------
  00111 00011 01011
```

что соответствует шифрограмме «жвк», «ж» (седьмая буква в алфавите) имеет код 00111,
«в» (третья буква в алфавите) имеет код 00011, «к» (одиннадцатая буква

в алфавите) имееткод 01011.

Дешифрование производится путем наложения той же гаммы на зашифрованныйтекст с помощью операции сложения по модулю 2. В результате получаем исходный текст
«абв».

00111 00011 01011
<u>00110 00001 01000</u>
00001 00010 00011

Метод гаммирования с обратной связью

При использовании обратной связи значение зашифрованного символа зависит не только от гаммы, но и от предыдущих символов.

Для получения сегмента гаммы можно использовать контрольную сумму определенного участка шифруемых данных. Процесс шифрования в этом случае представляется следующими шагами:

1. Генерация сегмента гаммы $H(1)$ и наложение его на соответствующий участокшифруемых данных.
2. Подсчет контрольной суммы участка, соответствующего сегменту гаммы $H(1)$.
3. Генерация с учетом контрольной суммы уже зашифрованного участка данныхследующего сегмента гамм $H(2)$.
4. Подсчет контрольной суммы участка данных, соответствующего сегменту данных

$H(2)$ и т.д.

Под контрольной суммой понимают функцию $f(t(1), \ldots t(n))$, где $t(i)$ - i-е словошифруемых данных.

Зашифруем исходный текст «абв», представленный в виде последовательности 0000100010 00011. Пусть A=5; C=3; b=5; M=32;T(0)=7. Тогда T(1)=(5□7+3) mod 32 = 6 (00110).

В качестве контрольной суммы участка данных, выберем количество единиц на этомучастке. Тогда сегменту H(1) соответствует участок 00001, количество единиц равно 1.

T(2)=(5□1+3) mod 32 = 8 (01000).

Контрольная сумма следующего участка (00010) равна 1.T(3)=(5□1+3) mod 32 = 8 (01000).

Полученная шифрограмма: соответствует тексту «жик».

00001 00010 00011
<u>00110 01000 01000</u>
00111 01010 01011

Задание на лабораторную работу

1. Выбрать в таблице 2.1 параметры генератора ПСЧ: A, C, T_0, b в соответствии с вариантом.

2. Разработать программу шифрования и дешифрования текста.

3. Произвести шифрование исходного текста, получить шифрограмму, осуществить ее дешифрование и сравнение с исходным текстом. Рекомендуется для представления символов исходного текста использовать стандартную кодировку символов.

4. Произвести изменение одного или несколько параметров генератора случайных чисел, осуществить получение шифрограммы и сравнение ее с предыдущим вариантом.

5. Результаты работы оформить в виде отчета.

Таблица 2.1 – Генераторы ПСЧ

№ варианта	Вид генератора ПСЧ	Количество разрядов b
1	Линейные конгруэнтные датчики ПСЧ	6
2	Гаммирование с обратной связью	7
3	Линейные конгруэнтные датчики ПСЧ	8
4	Гаммирование с обратной связью	6
5	Линейные конгруэнтные датчики ПСЧ	7
6	Гаммирование с обратной связью	8
7	Линейные конгруэнтные датчики ПСЧ	6
8	Гаммирование с обратной связью	7
9	Линейные конгруэнтные датчики ПСЧ	8
10	Гаммирование с обратной связью	6
11	Линейные конгруэнтные датчики ПСЧ	7
12	Гаммирование с обратной связью	8
13	Линейные конгруэнтные датчики ПСЧ	6
14	Гаммирование с обратной связью	7
15	Линейные конгруэнтные датчики ПСЧ	8

Содержание отчета:

- цель работы, постановка задачи,
- описание используемого метода,
- описание исходных данных,
- алгоритм работы программы,
- текст программы,
- результаты работы программы,
- анализ результатов

– выводы.

Контрольные вопросы

1. Какие параметры конгруэнтного генератора необходимо выбрать для получениямаксимальной длины последовательности псевдослучайных чисел?
2. От чего зависит длина псевдослучайной последовательности?
3. Каков принцип действия генераторов с обратной связью?
4. Какую операцию используют для шифрования в методе гаммирования?
5. Каковы достоинства и недостатки метода гаммирования?
6. Что является ключом в шифрах гаммирования?

Критерии оценки эссе (рефератов, докладов, сообщений)

Оценка «отлично»: выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка «хорошо»: основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

Оценка «удовлетворительно»: имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы.

Оценка «неудовлетворительно»: тема освоена лишь частично; допущены грубые ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Темы для эссе (рефератов, докладов, сообщений) по дисциплине «Криптографические средства и методы защиты информации»:

1. Применение алгоритма ГОСТ Р34.11-2012 для хэширования ключевой информации.
2. Разработка диспетчера доступа для типовой информационной системы.
3. Разработка диспетчера доступа для реляционных СУБД.
4. Аутентификация ОС МСВС.
5. Разработка системы аутентификации Windows для типового предприятия.
6. Разработка стеганографической подсистемы защиты информации предприятия на основе методов скрытия информации в изображении.
7. Разработка стеганографической подсистемы защиты информации предприятия на основе методов скрытия информации в аудиофайлах.
8. Разработка подсистемы разграничения доступа СУБД предприятия.
9. Разработка подсистемы защиты электронного документооборота предприятия.
10. Разработка подсистемы разграничения доступа к информации на основе модели
11. Харрисона-Руззо-Ульмана.
12. Разработка подсистемы защиты сайта от SQL-инъекции.
13. Разработка системы аутентификации для информационной системы типового предприятия.
14. Безопасность обработки данных облачными сервисами.
15. Модель администрирования ролевого управления доступом предприятия.
16. Реализация арифметических операций с числами большой разрядности (больше 64 бит).
17. Алгоритмы с открытым ключом. Схема Полига-Хелмана.
18. Реализация алгоритма Евклида для решения уравнения сравнения 1-й степени на 64-разрядных
19. Взлом криптографической защиты RSA. «Time Attac
20. Реализация быстрого поиска и проверки простоты чисел.
21. Взлом криптографической защиты RSA. Факторинг разложение открытого ключа N на простые множители (факторы) и отыскание закрытого ключа.
22. Подсчет частотных вероятностей для k-грамм русского текста.
23. Алгоритмы с открытым ключом. Схема Эль-Гамаля.
24. Алгоритмы с открытым ключом. Схема Рабина.
25. Алгоритмы симметричного шифрования. Rijndael.
26. Афинная криптосистема.
27. Алгоритмы с открытым ключом. Схема Вильямса.
28. Шифрование в аналоговой телефонии (частотное и временное преобразование).
29. Алгоритмы с открытым ключом. Задача об укладке ранца.
30. Электронное голосование.
31. Метод безключевого чтения RSA.
32. Разработка программного обеспечения, реализующего криптозащиту данных с использованием нескольких методов.

33. Проведение анализа применения блочных криптосистем в системе защиты информации предприятия.
34. Применение алгоритмов электронной цифровой подписи в автоматизированной системе управления делопроизводством.
35. Проведение сравнительного анализа эффективности современных программных, программно-аппаратных и аппаратных средств криптографической защиты.
36. Оценка эффективности криптографических генераторов, основанных на алгоритмах Фибоначчи.
37. Проведение сравнительного анализа алгоритмов формирования хэш-функций.
38. Исследование практического применения криптографических протоколов распределения ключей.
39. Разработка системы аутентификации сотрудников производственного предприятия.

Структура итогового теста:

Тест содержит 20 вопросов случайным образом выбранных их списка. Тест проводиться на персональном компьютере в оболочке для тестирования MyTest. Результат выдается сразу после тестирования и формируется отчет протестированных студентов на сервере.

Время на подготовку и выполнение:

Выполнение – 20 минут. За правильный ответ выставляется по 1 баллу, затем результаты суммируются, и выставляется оценка. За неправильный ответ 0 баллов.

Критерии оценки промежуточной аттестации:

40.

Оценка «отлично» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «отлично», средний балл по аттестациям не ниже 4,5.

Оценка «хорошо» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «хорошо», средний балл по аттестациям не ниже 3,5.

Оценка «удовлетворительно» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «удовлетворительно», средний балл по аттестациям не ниже 2,5.

Оценка «неудовлетворительно» выставляется, если имеются все конспекты лекции обучающимися выполнено менее 100% практических работ, оценка за итоговое тестирование – «неудовлетворительно», средний балл по аттестациям ниже 2,5.

Цель итогового тестирования:

Тестирование по учебной дисциплине **«Криптографические средства и методы защиты информации»** предназначено для проверки теоретических знаний и понятийного аппарата, которые лежат в основе профессионального образования и найдут самое широкое применение в будущей профессиональной деятельности учащихся по специальности 10.02.05.Обеспечение информационной безопасности автоматизированных систем.

Критерии оценки знаний:

Процент правильных ответов, %	Оценка знаний
90-100	5 «отлично»
80-89	4 «хорошо»
70-79	3 «удовлетворительно»
Менее 70	2 «неудовлетворительно»

Список теоретических заданий для подготовки к итоговому тестированию (ТЗ) по дисциплине «Криптографические средства и методы защиты информации»

1. Шифрование – это…
    а) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
    б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
    в) удобная среда для вычисления конечного пользователя
2. Кодирование – это…
    а) преобразование обычного, понятного текста в код
    б) преобразование
    в) написание программы
3. Что требуется для восстановления зашифрованного текста
    а) ключ
    б) матрица
    в) Вектор
4. Когда появилось шифрование
    а) четыре тысячи лет назад

б) две тысячи лет назад
в) пять тысяч лет назад

5. Первым известным применением шифра считается
   а) египетский текст
   б) русский
   в) нет правильного ответа
6. Какую секретную информацию хранит Windows
   а) пароли для доступа к сетевым ресурсам
   б) пароли для доступа в Интернет
   в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере
7. Самый распространенный метод шифрования, используемый в компьютерных сетях
   а) ГОСТ 28147-89
   б) RSA
   в) DES
   г) Rijndael
8. Алфавит – это…
   а) конечное множество используемых для кодирования информации знаков
   б) буквы текста
   в) нет правильного ответа
9. Текст – это…
   а) упорядоченный набор из элементов алфавита
   б) конечное множество используемых для кодирования информации знаков
   в) все правильные
10. Примеры алфавитов:
    а) Z_{256} – символы, входящие в стандартные коды ASCII и КОИ-8
    б) восьмеричный и шестнадцатеричный алфавиты
    в) AEE
11. Шифрование – это…
    а) преобразовательный процесс исходного текста в зашифрованный
    б) упорядоченный набор из элементов алфавита
    в) нет правильного ответа
12. Дешифрование – это…
    а) на основе ключа шифрованный текст преобразуется в исходный
    б) пароли для доступа к сетевым ресурсам
    в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере
13. Криптографическая система представляет собой…
    а) семейство T преобразований открытого текста, члены его семейства индексируются символом k
    б) Программу

в) систему

14. Пространство ключей k – это…
    а) набор возможных значений ключа
    б) длина ключа
    в) нет правильного ответа
15. Криптосистемы разделяются на:
    а) симметричные
    б) Ассиметричные
    в) с открытым ключом
16. Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования
    а) 1
    б) 2
    в) 3
17. Сколь ключей используется в системах с открытым ключом
    а) 2
    б) 3
    в) 1
18. Какие ключи используются в системах с открытым ключом
    а) открытый
    б) закрытый
    в) нет правильного ответа
19. Как связаны ключи друг с другом в системе с открытым ключом
    а) математически
    б) логически
    в) алгоритмически
20. Электронной подписью называется…
    а) присоединяемое к тексту его криптографическое преобразование
    б) текст
    в) зашифрованный текст
21. Криптостойкость – это…
    а) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа
    б) свойство гаммы
    в) все ответы верны
22. Показатели криптостойкости:
    а) количество всех возможных ключей
    б) среднее время, необходимое для криптоанализа
    в) количество символов в ключе
23. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
    а) знание алгоритма шифрования не должно влиять на надежность защиты
    б) структурные элементы алгоритма шифрования должны быть неизменными

в) не должно быть простых и легко устанавливаемых зависимостью между ключами последовательно используемыми в процессе шифрования

24. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
    а) длина шифрованного текста должна быть равной лине исходного текста
    б) зашифрованное сообщение должно поддаваться чтению только при наличии ключа
    в) нет правильного ответа
25. Основные современные методы шифрования:
    а) алгоритма гаммирования
    б) алгоритмы сложных математических преобразований
    в) алгоритм перестановки
26. Символы исходного текста складываются с символами некой случайной последовательности – это…
    а) алгоритм гаммирования
    б) алгоритм перестановки
    в) алгоритм аналитических преобразований
27. Символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом – это…
    а) алгоритм перестановки
    б) алгоритм подстановки
    в) алгоритм гаммрования
28. Самой простой разновидность подстановки является
    а) простая замена
    б) перестановка
    в) простая перестановка
29. Из скольки последовательностей состоит расшифровка текста по таблице Вижинера
    а) 3
    б) 4
    в) 5
30. Какие таблицы Вижинера можно использовать для повышения стойкости шифрования
    а) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке
    б) в качестве ключа используется случайность последовательных чисел
    в) нет правильного ответа
31. В чем суть метода перестановки
    а) символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов
    б) замена алфавита
    в) все правильные

32. Сколько существует способов гаммирования
    а) 2
    б) 5
    в) 3
33. Чем определяется стойкость шифрования методом гаммирования
    а) свойством гаммы
    б) длина ключа
    в) нет правильного ответа
34. Что может использоваться в качестве гаммы
    а) любая последовательность случайных символов
    б) число
    в) все ответы верны
35. Какой метод используется при шифровании с помощью аналитических преобразований
    а) алгебры матриц
    б) матрица
    в) факториал
36. Что используется в качестве ключа при шифровании с помощью аналитических преобразований
    а) матрица А
    б) вектор
    в) обратная матрица
37. Как осуществляется дешифрование текста при аналитических преобразованиях
    а) умножение матрицы на вектор
    б) деление матрицы на вектор
    в) перемножение матриц
38. Для чего использовался DES-алгоритм из-за небольшого размер ключа
    а) закрытия коммерческой информации
    б) шифрования секретной информации
    в) нет правильного ответа
39. Когда был введен в действие ГОСТ 28147-89
    а) 1990
    б) 1890
    в) 1995
40. Достоинства ГОСТа 28147-89
    а) высокая стойкость
    б) цена
    в) гибкость
41. Чем отличается блок-схема алгоритма ГОСТ от блок-схемы DES-алгоритма
    а) отсутствием начальной перестановки и числом циклов шифрования
    б) длиной ключа
    в) методом шифрования

42. Ключ алгоритма ГОСТ – это…
    а) массив, состоящий из 32-мерных векторов
    б) последовательность чисел
    в) алфавит
43. Какой ключ используется в шифре ГОСТ
    а) 256-битовый
    б) 246-битовый
    в) 356-битовый
44. Примеры программных шифраторов:
    а) PGP
    б) BestCrypt 6.04
    в) PTR
45. Плюсы программных шифраторов:
    а) цена
    б) гибкость
    в) быстродействие
46. УКЗД – это…
    а) устройство криптографической защиты данных
    б) устройство криптографической заданности данных
    в) нет правильного ответа

Основная литература:

1. *Запечников, С. В.* Криптографические методы защиты информации : учебник для сузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. - Москва : Издательство Юрайт, 2021. - 309 с. - (Профессиональное образование). - ISBN 978-5-534-02574-3. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/468902
2. *Васильева, И. Н.* Криптографические методы защиты информации : учебник и практикум для сузов / И. Н. Васильева. - Москва : Издательство Юрайт, 2020. - 349 с. - (Профессиональное образование). - ISBN 978-5-534-02883-6. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/450998
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. - Москва : Издательство Юрайт, 2021. - 312 с. - (Профессиональное образование). - ISBN 978-5-534-13221-2. - URL : https://urait.ru/bcode/476997

Дополнительная литература:

1. Коржик В.И. Основы криптографии [Электронный ресурс]: Учебное пособие/ Коржик В.И., Яковлев В.А.- Электронно - текстовые данные.- СПб.:Интермедия, 2017.- 312 с.- Режим доступа: http://www.bibliocomplectator.ru/book/?id=66798.-
2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд., испр. - Москва : Издательство Юрайт, 2021. - 424 с. - (Высшее образование). - ISBN 978-5-534-12474-3. - URL : https://urait.ru/bcode/469133
3. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. - Москва : Издательство Юрайт, 2022. - 209 с. - (Высшее образование). - ISBN 978-5-9916-7088-3. - URL : https://urait.ru/bcode/489745

Интернет-ресурсы:

1. Библиотека Альдебаран – компьютерная литература [Электронный ресурс]. – Режим доступа: http://www.aldebarans.ru/komp, свободный. – Загл. с экрана.
2. Википедия – Свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org, свободный. – Загл. с экрана.
3. Официальный сайт Министерства образования и науки Российской Федерации. – Режим доступа: http://www.mon.gov.ru, свободный. – Загл. с экрана.
4. Педагогика.ру – Справочный сайт [Электронный ресурс]. – Режим доступа: http://www.pedagogy.ru, свободный. – Загл. с экрана.
5. Портал нормативно-технической документации [Электронный ресурс]. – Режим доступа: http://www.pntdoc.ru, свободный. – Загл. с экрана.
6. Российское образование. Федеральный портал [Электронный ресурс].. – Режим доступа: http://www.edu.ru, свободный. – Загл. с экрана.
7. Техническая литература [Электронный ресурс]. – Режим доступа: http://www.tehlit.ru, свободный. – Загл. с экрана

КРИТЕРИИ ОЦЕНКИ

по дисциплине

МДК.02.03. КОРПОРАТИВНАЯ ЗАЩИТА ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Критерии оценки:

Оценка «отлично»: правильно выполнены все задания практической работы, правильно даны ответы на все контрольные вопросы, выполнены задания самостоятельной работы в полном объеме. Студент отвечает на вопросы, демонстрируя глубокие знания.

Оценка «хорошо»: выполнены все задания практической и контрольной работы с наличием несущественных ошибок, выполнены задания самостоятельной работы в неполном объеме, не противоречащих основным понятиям дисциплины. Студент уверенно отвечает на вопросы, демонстрируя достаточно высокий уровень знаний

Оценка «удовлетворительно»: выполнены все задания практической и контрольной работы с наличием грубых ошибок, выполнены задания самостоятельной работы в неполном объеме, противоречащих или искажающих основные понятия дисциплины. Студент демонстрирует достаточный уровень знаний, однако затрудняется отвечать на некоторые вопросы

Оценка «неудовлетворительно»: выполнены не все задания практической работы, даны не все ответы на контрольные вопросы, имеются грубые ошибки в выполнении практических заданий и/или ответах на контрольные вопросы, противоречащие или искажающие основные понятия дисциплины, самостоятельная работа не выполнена, либо выполнена на 50%. Студент затрудняется отвечать на вопросы.

Вопросы к дифференцированному зачету по дисциплине «Корпоративная защита внутренних угроз информационной безопасности»:

1. Конфигурация сетевой инфраструктуры: настройка хостмашины, сетевого окружения, виртуальных машин, и т.п.
2. Установка и настройка системы корпоративной защиты от внутренних угроз. Самостоятельный поиск и устранение неисправностей при развёртывании и настройке.
3. Установка и настройка агентского мониторинга.
4. Проведение синхронизации с LDAPсервером, разделе персоны.
5. Запуск системы корпоративной защиты от внутренних угроз.
6. Угрозы информационной безопасности.
7. Изучение структуры организации на основании полученных материалов («модели организации»), проведение обследования корпоративных информационных систем. Определение объекта защиты.
8. Перечень субъектов/персон сформулированных верно, роли пользователей, права доступа.
9. Политика безопасности.
10. Разработка новой и/или модифицирование существующей политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно конкурсного задания.
11. Использование различных технологий защиты: печатей, бланков, графических объектов, баз данных и т.п.
12. Модифицирование политики безопасности в системе IWTM в соответствие с получаемыми на практике данными перехвата.
13. Применение политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизировать число выявленных инцидентов безопасности.
14. Работа с интерфейсом управления системы корпоративной защиты информации.
15. Технология анализа и защиты сетевого трафика.
16. Развёртывание, настройка и проверка работоспособности VPN -сети на существующей и вычислительной инфраструктуре.
17. Развёртывание, настройка и проверка работоспособности IDS -системы на существующей и вычислительной.
18. Работа с узлами и пользователями. VPN. Компрометация узлов, ключей, пользователей. Восстановление связи.
19. Обновление ключевой информации. VPN. Межсетевое взаимодействие и туннелированные. VPN.
20. Централизованная политика безопасности.
21. Защита рабочих мест. IDS. Выявление большей части инцидентов безопасности за ограниченное время и/или с учётом неожиданно меняющихся условий.

22. Технологии агентского мониторинга.
23. Демонстрация знания механизмов работы агентского мониторинга.
24. Разработать и применить политику агентского мониторинга для работы с носителями и устройствами.
25. Разработка и применение политики агентского мониторинга для работы с файлами. Работа с исключениями из перехвата.
26. Анализ выявленных инцидентов. Подготовка отчётов о нарушениях.
27. Применение механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов.
28. Проведение классификацию уровня угроз инцидентов.
29. Оценка ущерба. Использование дополнительных модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса.
30. Выявление инцидентов и противодействие нарушителям с опорой на нормативную базу.

Кейс-задание по дисциплине «Корпоративная защита внутренних угроз информационной безопасности»

Задание

В следующем исходном коде показана стандартная структура теста Golang с использованием Terratest:

```
package test

import (
   "testing"

   "github.com/gruntwork-io/terratest/modules/terraform"
   test_structure "github.com/gruntwork-io/terratest/modules/test-structure"
)

func TestEndToEndDeploymentScenario(t *testing.T) {
   t.Parallel()

   fixtureFolder := "../"

   // User Terratest to deploy the infrastructure
   test_structure.RunTestStage(t, "setup", func() {
      terraformOptions := &terraform.Options{
         // Indicate the directory that contains the Terraform configuration to deploy
         TerraformDir: fixtureFolder,
      }

      // Save options for later test stages
```

```
        test_structure.SaveTerraformOptions(t, fixtureFolder, terraformOptions)

        // Triggers the terraform init and terraform apply command
        terraform.InitAndApply(t, terraformOptions)
    })

    test_structure.RunTestStage(t, "validate", func() {
        // run validation checks here
        terraformOptions := test_structure.LoadTerraformOptions(t, fixtureFolder)
            publicIpAddress := terraform.Output(t, terraformOptions,
"public_ip_address")
    })

    // When the test is completed, teardown the infrastructure by calling terraform
destroy
    test_structure.RunTestStage(t, "teardown", func() {
        terraformOptions := test_structure.LoadTerraformOptions(t, fixtureFolder)
        terraform.Destroy(t, terraformOptions)
    })
}
```

Как видно из предыдущего фрагмента кода, этот тест включает следующие этапы:

а) настройка (Terraform запускается для развертывания конфигурации);
б) проверка (Выполняются проверки и утверждения);
в) демонтаж (Инфраструктура очищается после выполнения теста);
г) все этапы.

Критерии оценки эссе (рефератов, докладов, сообщений)

Оценка «отлично»: выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка «хорошо»: основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются

упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

Оценка «удовлетворительно»: имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы.

Оценка «неудовлетворительно»: тема освоена лишь частично; допущены грубые ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Темы для эссе (рефератов, докладов, сообщений) по дисциплине «Корпоративная защита внутренних угроз информационной безопасности»:

1. Информация и информационные потоки.
2. Внутренние и внешние угрозы ИБ.
3. Модели угроз ИБ.
4. Классификация нарушителей корпоративной ИБ.
5. Особенности оценки ущерба.
6. Системы DLP и требования по информационной безопасности.
7. Категорирование информации в РФ.
8. Юридические вопросы использования DLP-систем: личная и семейная тайны; тайна связи; специальные технические средства.
9. Меры по обеспечению юридической значимости DLP (Pre-DLP).
10. Обзор практики право применения при расследовании инцидентов, связанных с нарушениями режима внутренней информационной безопасности (Post-DLP).
11. Формирование процессов и процедур аудита ИБ.
12. Обследование корпоративных информационных систем.
13. Состояние корпоративной информации.
14. Инструменты и технологии обеспечения корпоративной защиты от внутренних угроз.
15. Критерии эффективности проекта по обеспечению корпоративной защиты от внутренних угроз.
16. Препятствия реализации проектов по обеспечению корпоративной защиты от внутренних угроз.
17. Назначение системы IW Traffic monitor (IW TM).
18. Контролируемые каналы передачи данных.

19. Архитектура продукта IW TM.
20. Технологии анализа детектируемых объектов.
21. Задачи и принципы работы дополнительных модулей системы IW Device monitor (IW DM) и IW Crawler.

Структура итогового теста:

Тест содержит 20 вопросов случайным образом выбранных их списка. Тест проводиться на персональном компьютере в оболочке для тестирования MyTest. Результат выдается сразу после тестирования и формируется отчет протестированных студентов на сервере.

Время на подготовку и выполнение:

Выполнение – 20 минут. За правильный ответ выставляется по 1 баллу, затем результаты суммируются, и выставляется оценка. За неправильный ответ 0 баллов.

Критерии оценки промежуточной аттестации:

Оценка «отлично» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «отлично», средний балл по аттестациям не ниже 4,5.

Оценка «хорошо» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «хорошо», средний балл по аттестациям не ниже 3,5.

Оценка «удовлетворительно» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «удовлетворительно», средний балл по аттестациям не ниже 2,5.

Оценка «неудовлетворительно» выставляется, если имеются все конспекты лекции обучающимися выполнено менее 100% практических работ, оценка за итоговое тестирование – «неудовлетворительно», средний балл по аттестациям ниже 2,5.

Цель итогового тестирования:

Тестирование по учебной дисциплине **«Корпоративная защита внутренних угроз информационной безопасности»** предназначено для проверки теоретических знаний и понятийного аппарата, которые лежат в основе профессионального образования и найдут самое широкое применение в будущей профессиональной деятельности учащихся по специальности 10.02.05.Обеспечение информационной безопасности автоматизированных систем.

Критерии оценки знаний:

Процент правильных ответов, %	Оценка знаний
90-100	5 «отлично»
80-89	4 «хорошо»
70-79	3 «удовлетворительно»
Менее 70	2 «неудовлетворительно»

Список теоретических заданий для подготовки к итоговому тестированию (ТЗ) по дисциплине «Корпоративная защита внутренних угроз информационной безопасности»

1. Разделение информации на категории свободного и ограниченного доступа, причем информации ограниченного доступа подразделяются на:
    а) отнесенные к государственной тайне;
    б) отнесенные к служебной тайне (информации для служебного пользования),персональные данные (и другие виды тайн);
    в) отнесенные к информации о прогнозах погоды;
    г) все верны ответы.
2. К информации ограниченного доступа относятся:
    а) государственная тайна;
    б) конфиденциальная информация;
    в) персональные данные;
    г) все ответы верны.
3. К методам защиты корпоративной информационной среды относятся:
    а) система управления идентификацией и доступом пользователей (Identity and Access Management (IAM)); система управления событиями информационной безопасности (Security Information Event Management (SIEM)); средства предотвращения потери данных (Data Loss/Leak Prevention (DLP));
    б) система управления идентификацией и доступом пользователей (Identity and Access Management (IAM)); система управления событиями информационной безопасности (Security Information Event Management (SIEM)).
4. Средства предотвращения потери данных (Data Loss/Leak Prevention (DLP)) это:
    а) контроль рабочих станций сотрудников, контроль трафика корпоративной сети, контроль сетевых хранилищ информации;
    б) контроль рабочих станций сотрудников, контроль трафика корпоративной сети, контроль сетевых хранилищ информации, контроль посещения работы.

5. Установка, конфигурирование и устранение неисправностей в системах корпоративной защиты от внутренних угроз входит следующее:
    а) DLP – применение (IW Traffic Monitor);
    б) Linux, Windows администрирование DLP – установка, VPN установка/настройка, настройка политик домена;
    в) технологии агентского мониторинга.
6. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз включает:
    а) установка, конфигурирование и устранение неисправностей в системах корпоративной защиты от внутренних угроз;
    б) исследование (аудит) организации с целью защиты от внутренних угроз;
    в) DLP – применение (IW Traffic Monitor)
7. Основными источниками угроз информационной безопасности являются все указанное в списке?
    а) хищение жестких дисков, подключение к сети, инсайдерство;
    б) перехват данных, хищение данных, изменение архитектуры системы;
    в) хищение данных, подкуп системных администраторов, нарушение регламента работы.
8. Наиболее важным при реализации защитных мер политики безопасности является:
    а) аудит, анализ затрат на проведение защитных мер
    б) аудит, анализ безопасности
    в) аудит, анализ уязвимостей, риск-ситуаций
9. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
    а) снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования;
    б) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации;
    в) улучшить контроль за безопасностью этой информации;
    г) снизить уровень классификации этой информации.
10. Что самое главное должно продумать руководство при классификации данных?
    а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным;
    б) Необходимый уровень доступности, целостности и конфиденциальности
    в) Оценить уровень риска и отменить контрмеры
    г) Управление доступом, которое должно защищать данные
11. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
    а) поддержка высшего руководства

б) эффективные защитные меры и методы их внедрения
в) актуальные и адекватные политики и процедуры безопасности
г) ароведение тренингов по безопасности для всех сотруднико

12. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности
    а) список стандартов, процедур и политик для разработки программы безопасности;
    б) текущая версия iso 17799;
    в) структура, которая была разработана для снижения внутреннего мошенничества в компаниях;
    г) открытый стандарт, определяющий цели контроля.
13. К внутренним нарушителям информационной безопасности относится:
    а) клиенты;
    б) пользователи системы;
    в) посетители;
    г) любые лица, находящиеся внутри контролируемой территории;
    д) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
    е) персонал обслуживающий технические средства;
    ж) сотрудники отделов разработки и сопровождения ПО;
    з) технический персонал, обслуживающий здание.
14. Активный перехват информации это перехват, который: Варианты ответа:
    а) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
    б) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
    в) неправомерно использует технологические отходы информационного процесса; г) осуществляется путем использования оптической техники;
    г) осуществляется с помощью подключения телекоммуникационному оборудованию компьютера.
15. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?
    а) анализ связующего дерева;
    б) AS/NZS;
    в) NIST;
    г) анализ сбоев и дефектов.
16. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?
    а) NIST и OCTAVE являются корпоративными;
    б) NIST и OCTAVE ориентирован на ИТ;
    в) AS/NZS ориентирован на ИТ;
    г) NIST и AS/NZS являются корпоративными;

17. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?
    а) COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам;
    б) COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень;
    в) COSO учитывает корпоративную культуру и разработку политик;
    г) COSO – это система отказоустойчивости.
18. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
    а) чтобы убедиться, что проводится справедливая оценка;
    б) для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ;
    в) поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа;
    г) поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку.
20. WorldSkills - это:
    а) международное некоммерческое Движение, целью которого является повышение престижа рабочих профессий и развитие профессионального образования путем гармонизации лучших практик и профессиональных стандартов во всем мире посредством организации и проведения конкурсов по профессиональному мастерству, как в каждой из 80+ стран-членов Движения WSI, так в мире в целом;
    б) форма оценки соответствия уровня знаний, умений, навыков студентов и выпускников, осваивающих программы подготовки квалифицированных рабочих, служащих, специалистов среднего звена, позволяющих вести профессиональную деятельность в определенной сфере и (или) выполнять работу по конкретным профессии или специальности в соответствии со стандартами Ворлдсиллз Россия.

Основная литература:

1. Нестеров, С. А. Информационная безопасность: учебник и практикум для среднего профессионального образования / С. А. Нестеров. - Москва: Издательство Юрайт, 2018. - 321 с. - (Профессиональное образование). - ISBN 978-5-534-07979-1. - Текст: электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/424066.

2. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. - 3-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2020. - 161 с. - (Профессиональное образование). - ISBN 978-5-534-13948-8. - Текст: электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/467356 .
3. Моргунов А.В. Информационная безопасность: учебно-методическое пособие Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2019. – 83 с.: ил., табл. - 978-5- 7782-3918-0 https://biblioclub.ru/index.php?page=book&id=576726
4. Скляр В. В. Обеспечение безопасности АСУТП в соответствии с современными стандартами Москва, Вологда: Инфра-Инженерия, 2018. - 385 с. - 978-5-9729-0230-9 http://biblioclub.ru/index.php

Дополнительная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. - 3-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2022. - 161 с. - (Высшее образование). - ISBN 978-5-534-07248-8. - URL : https://urait.ru/bcode/490277
2. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. - 2-е изд., испр. и доп. - Москва : Издательство Юрайт, 2021. - 246 с. - (Высшее образование). - ISBN 978-5-534-01679-6. - URL : https://urait.ru/bcode/468273
3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. - Москва : Издательство Юрайт, 2022. - 309 с. - (Высшее образование). - ISBN 978-5-534-04732-5. - URL : https://urait.ru/bcode/490019

Интернет-ресурсы:

1. Библиотека Альдебаран – компьютерная литература [Электронный ресурс]. – Режим доступа: http://www.aldebarans.ru/komp, свободный. – Загл. с экрана.
2. Википедия – Свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org, свободный. – Загл. с экрана.
3. Официальный сайт Министерства образования и науки Российской Федерации. – Режим доступа: http://www.mon.gov.ru, свободный. – Загл. с экрана.
4. Педагогика.ру – Справочный сайт [Электронный ресурс]. – Режим доступа: http://www.pedagogy.ru, свободный. – Загл. с экрана.
5. Портал нормативно-технической документации [Электронный ресурс]. – Режим доступа: http://www.pntdoc.ru, свободный. – Загл. с экрана.
6. Российское образование. Федеральный портал [Электронный ресурс].. – Режим доступа: http://www.edu.ru, свободный. – Загл. с экрана.

7. Техническая литература [Электронный ресурс]. – Режим доступа: http://www.tehlit.ru, свободный. – Загл. с экрана