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
«30» 04 2022 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине

МДК.02.02. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Махачкала - 2022

Составитель/ составители:

Шахбанова М.И. - преподаватель кафедры естественнонаучных 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 дисциплины рассмотрен и рекомендован к утверждению кафедрой специальных дисциплин Колледжа ДГУ.

Протокол № 8 от « 30 » 04 2022г.

Зав.кафедрой специальных дисциплин _____Магомедова К.К.

Утверждена на заседании учебно-методического совета колледжа ДГУ

Ст. методист _____/Шамсутдинова У.А./

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

МДК.02.02. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

№	Контролируемые разделы, темы, модули	Код контролируемой компетенции	Наименование оценочного средства
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.

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:* а) 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; б) реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей; в) творческого уровня, позволяющие оценивать и диагностировать умения,	Комплект разно-уровневых задач и заданий

		интегрировать знания различных областей, аргументировать собственную точку зрения.	
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.02.02. 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 дифференцированному зачёту:

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□8)=y(33-2□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	X	У	А	М	.	Ы	А	О
4	Г	D	Ы	Y	М	В	Н	X	Э	В	П
5	Д	Е	Е	Z	К	Н	Х	Y	Ь	Н	Р
6	Е	F	Ь	про-бел	Х	I	Л	,	Ъ	I	С
7	Ё	G	З	.	Ч	J	И	!	Ш	J	Т
8	Ж	Н	Ш	,	И	Е	Й	S	Щ	Е	У
9	З	I	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	С	N	Б	М	Ю	О	О	М	Ы
18	Р	R	О	О	Ю	N	Я	Р	П	N	Э
19	С	S	У	Р	Г	U	Ы	L	М	U	Ю
20	Т	Т	М	Q		V	Э	М	Н	V	Я
21	У	U	Х	R	Е	W	Ь	N	К	W	про-бел
22	Ф	V	К	S	Ь	:	про-бел	О	Л	:	А
23	Х	W	Ч	Т	З	S	Ш	Р	про-	S	Б

									бел		
24	Ц	X	И	U	Ш	T	Щ	A	Й	T	B
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	E
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).

$$y_i = x_i \oplus g_i \tag{2.1}$$

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
  00110 00001 01000
  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 $f(t(1), ... t(n))$, 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):

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)

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, 2022. — 309 с. — (профессиональное образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489487
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