СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет ***Математики и информационных технологий***
Кафедра ***Математического моделирования***

Оценочные материалы по дисциплине (модулю)

дисциплина ***Программно-аппаратные средства защиты информации***

Блок Б1, обязательная часть, Б1.О.22
цикл дисциплины и его часть (обязательная часть или часть, формируемая участниками образовательных отношений)

Направление

10.03.01 ***Информационная безопасность***
код наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очно-заочная

Для поступивших на обучение в
2023 г.

Разработчик (составитель)
кандидат физико-математических наук, доцент
Беляева М. Б.
ученая степень, должность, ФИО

Стерлитамак 2023

1. Перечень компетенций, индикаторов достижения компетенций и описание показателей и критериев оценивания результатов обучения по дисциплине (модулю) 3

2. Оценочные средства, необходимые для оценки результатов обучения по дисциплине (модулю).....6

Практическая работа № 1. .....Простые алгоритмы шифрования данных 6

Оформите отчет 7

Практическая работа № 5. 15

Реализация и исследование политик информационной безопасности.....15

2. Мандатная модель политики безопасности 25

3. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю), описание шкал оценивания 32

1. Перечень компетенций, индикаторов достижения компетенций и описание показателей и критериев оценивания результатов обучения по дисциплине (модулю)

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)	Показатели и критерии оценивания результатов обучения по дисциплине (модулю)				Вид оценочного средства
1	2	3	4				5
			неуд.	удовл.	хорошо	отлично	
ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.1. Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.	Обучающийся должен: уметь оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	Отсутствие знаний	Неполные представления об оценке уровня безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	Сформированные, но содержащие отдельные пробелы представления об оценке уровня безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	Сформированные систематические представления об оценке уровня безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	Тесты
	ОПК-2.2. Умеет выбирать современные информационные технологии и	Обучающийся должен: уметь выбирать современные информационные технологии и	Отсутствие умений	В целом успешное, но не систематическое умение выбирать современные информационные	В целом успешное, но содержащее отдельные пробелы в умении	Сформированное умение выбирать современные информационные технологии и	Тесты

	программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.		технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	
	ОПК-2.3. Обладает навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Обучающийся должен: владеть навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Отсутствие навыков	В целом успешное, но непоследовательное владение навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	В целом успешное, но содержащее отдельные пробелы владения навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональн	Успешное и последовательное владение навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	Тесты

					ой деятельности		

2. Оценочные средства, необходимые для оценки результатов обучения по дисциплине (модулю)

Практическая работа № 1.
Простые алгоритмы шифрования данных

1. Используется программа **caesar.exe**. Работа в парах.
   а) Зашифруйте строчку какого-нибудь стихотворения с помощью шифра Цезаря и сохраните зашифрованное сообщение в виде текстового файла **C-NN.txt**, где вместо **NN** нужно подставить номер вашего компьютера.
   б) Скопируйте аналогичный файл вашего напарника на свой компьютер и расшифруйте его, подобрав ключ шифра.

   Сообщение:

2. Используется программа **vigenere.exe**.
   а) Зашифруйте имя и фамилию своего любимого писателя с помощью шифра Виженера, используя ключ, состоящий из четырех букв и запишите зашифрованное сообщение в файл **V-NN.txt**. Там же укажите начальную букву ключа. Формат файла:

   ЩЦЫ ЖВЩЖЬФР
   П***

б) Разместите созданный файл в общей папке
(Создайте папку с ФИО на ресурсе https://drive.google.com/drive/folders/1iLfbUs6bGyJ_C33EyyuK3FTZbODAYsim?usp=sharing).
   в) Скопируйте аналогичный файл вашего напарника на свой компьютер и расшифруйте его, подобрав ключ шифра. Если ключ подобрать не удается, попросите напарника назвать вторую букву ключа и т.д.

   Сообщение:

   Ключ:

3. Используется программа **vigenere.exe**. *Взлом шифра Виженера*. Работа в парах.
   а) Зашифруйте с помощью шифра Виженера с одним и тем же ключом названия двух последних книг, которые вам понравились.
   б) Создайте файл **VX-NN.txt**, который содержит открытое и зашифрованное название первой книги, а также зашифрованное название второй книги. Формат файла:

   А ЗОРИ ЗДЕСЬ ТИХИЕ
   В ЗЮЪШ ЗШЧУЬ ВТЕИЩ
   ВЛШЫР В ЕДТАЭП ЗУШЧУ

   в) Скопируйте аналогичный файл вашего напарника на свой компьютер и расшифруйте его, подобрав ключ шифра.

   Название второй книги:

   Ключ:

Оформите отчет

Практическая работа № 2.

Современные алгоритмы шифрования и хэширования

1. Используется программа **md5.exe**. Работа в парах.
   1) Создайте два текстовых файла с именами **NN-1.txt** и **NN-2.txt**, содержащих интересные новости (например, с сайта www.lenta.ru).
   2) Найдите хэш-коды этих файлов и запишите их в файл **hash-NN.txt** в следующем формате (вместо **NN** нужно подставить номер вашего компьютера):

      1.txt 051108949B293E5F5968875EEF7F8A39
      2.txt 22EF83B72E61FAEDA358CFC93CEB61B1

   3) Запишите файл **hash-NN.txt** в общую папку (Создайте папку с ФИО на ресурсе https://drive.google.com/drive/folders/1iLfbUs6bGyJ_C33EyyuK3FTZbODAYsim?usp=sharing).
   4) Измените один из файлов, например, добавив лишний пробел, а затем запишите файлы **NN-1.txt** и **NN-2.txt** в общую папку.
   5) Скопируйте на свой компьютер аналогичные файлы вашего напарника и определите, какой файл «исказился при передаче»:

   Искаженный файл:

   После скачивания и проверки файлов, хэш-код изменился у второго файла(**2.txt**):

   Исходный: **22EF83B72E61FAEDA358CFC93CEB61B1**

   Тот который получился: EF67F3386E6171E071E7E403FE1A81CA

2. Используется программа **rsa.exe**. Работа в парах.
   1) Сгенерируйте открытый и секретный ключи RSA, сохраните их на диске.

1) Открытый ключ разместите в общей папке (Создайте папку с ФИО на ресурсе https://drive.google.com/drive/folders/1iLfbUs6bGyJ_C33EyyuK3FTZbODAYsim?usp=sharing).
   2) Найдите в Интернете картинку, которую вы хотели бы передать своему напарнику.
   3) Скопируйте на свой компьютер файл, содержащий открытый ключ вашего напарника.
   4) Зашифруйте картинку с помощью этого ключа и разместите в общей папке.
   5) Используя свой закрытый ключ, расшифруйте файл, который прислал вам напарник таким же способом. Просмотрите рисунок на экране.

3. Используется программа **rsa.exe**. Работа в парах.
   1) Создайте два текстовых файла с именами **RSA-NN-1.txt** и **RSA-NN-2.txt**, содержащих интересные новости.
   2) Подпишите их с помощью своей электронной цифровой подписи, используя свой секретный ключ: с помощью программы **rsa.exe** постройте новые файлы (с расширением **.sig**), содержащие цифровые подписи к файлам **RSA-NN-1.txt** и **RSA-NN-2.txt**.
   3) Измените один из файлов, например, добавив лишний пробел, а затем запишите файлы **RSA-NN-1.txt** и **RSA-NN-2.txt** и файлы с электронными цифровыми подписями (**RSA-NN-1.sig** и **RSA-NN-2.sig**) в общую папку.
   4) Скопируйте на свой компьютер аналогичные файлы вашего напарника и определите с помощью программы **rsa.exe**, какой файл был искажен в пути или подделан:

   Искаженный файл:

   5) Чем отличается проверка подлинности сообщения с помощью электронной цифровой подписи и проверка с помощью хэш-суммы, например, MD5:

   Ответ:

Оформите отчет

Практическая работа № 3.
Использование стеганографии

Используется программа **stegano.exe**.

1. Извлеките текстовую информацию из файла **baloon.bmp**. Число измененных бит на пиксель определите подбором.
   Скрытый текст:

2. Работа в парах.
   1) Найдите в Интернете небольшой рисунок и текст, который вы хотели бы передать своему напарнику.
   2) Закодируйте текст внутри рисунка. Выберите количество изменяемых бит на пиксель так, чтобы искажение рисунка было почти незаметным.
   3) Передайте рисунок своему напарнику (например, через разделяемую сетевую папку).
   4) Расшифруйте текст, который был скрыт в рисунке, который передал вам напарник:

   Скрытый текст:

Практическая работа № 4.

Биометрическая аутентификация пользователя по

клавиатурному почерку

Цель занятия – познакомиться с биометрическими системами идентификации и аутентификации пользователей на примере биометрической системы аутентификации по клавиатурному почерку.

Теоретическая часть

Одними из перспективных в настоящее время методами аутентификации пользователей являются методы биометрической аутентификации.

Под *биометрической аутентификацией* понимают аутентификацию, основанную на использовании индивидуальных физиологических характеристиках человека, таких как отпечаток пальца, геометрия руки, сетчатка и радужная оболочка глаза, голос, клавиатурный почерк и т.д.

Среди характеристик, используемых для биометрической аутентификации пользователя, наиболее дешевым является использование характеристики, отражающей динамику работы пользователя на клавиатуре (индивидуальные особенности работы пользователя с клавиатурой) - скорость нажатия клавиш, временные задержки между нажатиями, использование функциональных клавиш, временные задержки между комбинациями клавиш и т.д.

Достоинством этой биометрической характеристики является отсутствие необходимости привлечения дорогих аппаратных устройств (необходимых, например, при сканировании отпечатков пальцев, сетчатки глаза и др.), а также возможность незаметного постоянного контроля пользователя.

Одним из главных отличий методов биометрической аутентификации от других методов аутентификации пользователя является то, что результат аутентификации в данных методах имеет вероятностный характер. Возможна ситуация, когда легальный пользователь, предъявивший свою биометрическую характеристику, не допускается в систему (из-за наличия побочных шумовых эффектов), либо наоборот, нелегальный пользователь допускается в систему, если его биометрическая характеристика похожа на биометрическую характеристику легального пользователя. Таким образом, методы биометрической аутентификации характеризуются коэффициентом ошибочных отказов (false rejection rate FRR) и коэффициентом ошибочных подтверждений (false acceptance rate FAR).

Под *коэффициентом ошибочных отказов (FRR)* понимают отношение количества отказов в аутентификации легальным пользователям к общему количеству попыток легальной аутентификации.

Пусть N – количество попыток аутентификации легальных пользователей в биометрической системе за достаточно большой промежуток времени, M – количество раз, когда легальным пользователям было отказано в прохождении аутентификации. Тогда, коэффициент ошибочных отказов оценивается по формуле

$$FRR = \frac{M}{N} \qquad (1)$$

Под *коэффициентом ошибочных подтверждений (FAR)* понимают отношение количества подтверждений аутентификации нелегальных пользователей к общему количеству попыток нелегальной аутентификации.

Пусть K – количество попыток аутентификации нелегальных пользователей в биометрической системе за достаточно большой промежуток времени, L – количество раз, когда нелегальные пользователи получили подтверждение аутентификации. Тогда, коэффициент ошибочных подтверждений оценивается по формуле

$$FAR = \frac{L}{K} \qquad (2)$$

Между коэффициентами FAR и FRR существует функциональная связь. Чем больше FAR, тем меньше FRR и наоборот, чем меньше FAR, тем больше FRR.

Вторым отличием биометрических систем от других систем аутентификации является наличие этапа обучения биометрической системы, на котором формируются эталонные шаблоны биометрических характеристик пользователя.

Принятие решения о прохождении биометрической аутентификации

При биометрической аутентификации пользователя, принятие решения о прохождении либо не прохождении аутентификации в общем случае выполняется неоднозначно и имеет вероятностный характер. Во многом это связано с тем, что биометрические характеристики любого пользователя не являются точными и изменяются со временем. На изменение биометрических характеристик влияет множество показателей, таких как освещенность (при аутентификации по геометрии лица), время суток, усталость, настроение (при аутентификации по клавиатурному почерку, по голосу) и т.д.

Сравнение биометрических характеристик пользователя выполняют, как правило, сравнивая не биометрические образы, а *векторы биометрических признаков*, между которыми вычисляют расстояние в векторном пространстве. Поэтому, при принятии решения о прохождении либо не прохождении биометрической аутентификации пользователем, как правило, поступают следующим образом.

1. На этапе обучения формируют *эталонный шаблон пользователя* в виде вектора биометрических признаков, наиболее соответствующих пользователю.
2. Вычисляют значения биометрических признаков реального пользователя, проходящего аутентификацию в настоящий момент, и формируют вектор биометрических признаков.
3. Сравнивают эталонный шаблон пользователя с вычисленным на втором шаге вектором биометрических признаков, вычисляя при этом достоверность совпадения.
4. Если достоверность совпадения превышает некоторый порог ε (например, 90%), то принимается решение о прохождении биометрической аутентификации пользователем. Если достоверность совпадения меньше порога ε то принимается решение о не прохождении аутентификации.

Достоверность совпадения биометрических характеристик находится в обратной зависимости от расстояния между полученным на втором шаге вектором биометрических характеристик и эталонным (чем больше данное расстояние, тем меньше достоверность совпадения).

Пример

Будем использовать биометрическую аутентификацию пользователя по клавиатурному подчерку и следующие 2 биометрических признака.

1. Математическое ожидание временного промежутка нажатия между клавишами.

2. Дисперсия (разброс от математического ожидания) временного промежутка нажатия между клавишами.

Допустим, что пользователю ИВАН соответствует эталонный вектор биометрических признаков (0.5, 0.2). То есть математическое ожидание временного промежутка нажатия между клавишами равен 0.5 секунд, а дисперсия = 0.2 секунды.

Пусть положительное решение о прохождении аутентификации формируется в том случае, *если расстояние по Евклиду до этого эталонного вектора меньше 0.2*.

Пусть для реального пользователя был получен вектор биометрических признаков (0.6; 0.3). Расстояние по Евклиду между данным вектором и эталонным вектором пользователя ИВАН вычисляется следующим образом $\sqrt{(0.6-0.5)^2+(0.3-0.2)^2}=\sqrt{0.02}$ =0.14.

Так как 0.14 < 0.2, то формируется решение, что пользователь с вектором биометрических признаков (0.6; 0.3) является ИВАНом. Если бы расстояние было больше или равно 0.2, то сформировалось бы решение, что пользователь с предъявленными биометрическими признаками - НЕ ИВАН.

В общем случае, когда эталонный вектор биометрических характеристик пользователя имеет вид *n*-мерного вектора $X=(x_1,...,x_n)$, а вектор признаков реального пользователя имеет вид *n*-мерного вектора $Y=(y_1,...,y_n)$ то расстояние по Евклиду между эталонным и реальным векторами вычисляется по формуле (3).

$$\rho(x,y)=\sqrt{\sum_{i=1}^{n}(x_i-y_i)^2} \quad (3)$$

Если расстояние, вычисленное по формуле (3) меньше, чем заданный порог, то формируется решение о том, что пользователь проходит аутентификацию и является легальным.

Порядок выполнения работы

Задание 1. Работа с комплексом биометрической аутентификации.

1. Ознакомьтесь с содержимым сайта http://www.secuteck.ru/ – журнал «Системы безопасности».

2. Выберите одну из современных систем биометрической аутентификации и опишите ее функционал

Задание 2.

Из таблицы 1 взять эталонный шаблон пользователя, вектор биометрических характеристик реального пользователя и граничный порог принятия решения. По формуле (3) вычислить расстояние между эталонным вектором биометрических характеристик и вектором биометрических характеристик реального пользователя, после чего по граничному порогу определить, проходит ли реальный пользователь аутентификацию в Вашем случае либо нет.

Сформируйте отчет по работе.

Контрольные вопросы

1. Что понимается под биометрической аутентификацией пользователя? Приведите примеры биометрических характеристик.
2. Перечислите основные отличия методов биометрической аутентификации пользователя от других (например, парольных).
3. Что понимают под коэффициентом ошибочных отказов и коэффициентом ошибочных подтверждений биометрической системы?
4. Как в биометрических системах принимается решение о прохождении или непрохождении пользователем аутентификации?

Табл. 1. Варианты

Номер варианта	Шаблон эталонного пользователя	Вектор реального пользователя	Граничный порог принятия решения
1	(1,7,3,6)	(2,3,6,6)	4
2	(1,7,3,6)	(2,7,4,6)	4
3	(9,23,1,3)	(8,20,7,5)	10
4	(2,45,6,1)	(3,45,3,1)	10
5	(3,3,6)	(7,6,4)	15
6	(0,2,2,1)	(3,2,3,5)	2
7	(87,2,9)	(80,10,34)	7
8	(10,2,5,7)	(7,6,5,3)	6
9	(2,4,56,23)	(3,4,61,20)	10
10	(2,6,1,8)	(1,7,4,8)	8
11	(25,7,9,5)	(27,8,10,3)	4
12	(6,7,2,90)	(6,7,10,50)	5
13	(8,4,3,3)	(4,5,6,8)	5
14	(8,5,2,3)	(5,4,2,2)	8
15	(6,4,8,4)	(8,3,4,6)	5
16	(7,5,3,4)	(7,4,3,1)	10
17	(4,7,5,2)	(9,3,5,2)	1
18	(4,23,5,6)	(5,21,2,4)	6

19	(7,5,3,6)	(8,5,3,2)	4
20	(6,4,2,4)	(7,4,6,3)	5
21	(6,7,8,6)	(6,8,4,5)	5
22	(4,3,5,6)	(9,3,35,6)	10
23	(76,6,5,4)	(74,3,3,6)	1
24	(2,4,7,9)	(4,5,7,3)	3
25	(3,5,2,4)	(5,2,4,5)	3
26	(9,7,5,3)	(4,6,3,4)	4
27	(5,6,8,3)	(6,3,4,3)	2
28	(8,4,3,7)	(7,5,4,1)	3
29	(5,8,4,6)	(5,4,3,1)	9
30	(4,8,4,5)	(5,4,1,1)	9

Практическая работа № 5.

Реализация и исследование политик информационной безопасности.

Цель занятия – изучение проблем реализации политик информационной безопасности в компьютерных системах на примере дискреционной модели.

Теоретический материал

Политики безопасности

Под политикой безопасности понимается набор норм, правил и практических рекомендаций, которые регулируют управление, защиту и распределение ценной информации. Политика безопасности задает механизмы управления доступа к объекту, определяет как разрешенные, так и запрещенные типы доступов, регламентирует поведение СЗИ в различных ситуациях.

При выборе и реализации политики безопасности в компьютерной системе, как правило, работают следующие шаги:

1. В информационную структуру вносится структура ценностей (определяется ценность информации) и проводится анализ угроз и рисков для информации и информационного обмена.
2. Определяются правила использования для любого информационного процесса, права доступа к элементам информации с учетом данной оценки ценностей.

Реализация политики безопасности должна быть четко продумана. Результатом ошибочного или бездумного определения правил политики безопасности, как правило, является разрушение ценности информации без нарушения политики.

Существует ряд моделей политик безопасности, отличающихся по возможностям защиты, по качеству защиты, по особенностям реализации. Одной из самых простых и распространенных моделей политик безопасности является дискреционная политика.

Дискреционная политика безопасности

Пусть O – множество объектов компьютерной системы, над которыми могут производиться различные операции, U – множество пользователей (субъектов) компьютерной системы, которые могут производить операции над объектами, S – множество всевозможных действий субъектов над объектами.

В соответствии с дискреционной политикой безопасности, каждой паре субъект-объект (O_j, U_k), $O_j \in O$, $U_k \in U$, ставится в соответствие определенное множество действий $S_i \subset S$, которое может выполнять субъект U_k над объектом O_j. В множество действий S_i может входить несколько элементарных действий (чтение, запись, модификация, право передачи своих прав другому пользователю и т.д.).

Указанные права доступа пользователей-субъектов к объектам компьютерной системы записываются в виде так называемой МАТРИЦЫ ДОСТУПОВ. На пересечении i-ой строки и j-ого столбца данной матрицы располагается элемент S_{ij} – множество разрешенных действий i-ого субъекта над j-ым объектом.

Пример

Пусть имеем множество из 3 пользователей-субъектов U={Администратор, Гость, Пользователь_1} и множество из 4 объектов O={Файл_1, Файл_2, CD-RW, Флоппи-Дисковод}.

Пусть множество возможных действий S включает в себя следующие: S={Чтение, Запись, Передача прав}. Кроме этого, существует два дополнительных множества операций - «Полные права», «Полный запрет». Действие «Полные права» разрешает выполнение всех из перечисленных 3 действий, «Полный запрет» запрещает выполнение всех из выше перечисленных действий. Право «Передача прав» позволяет передавать субъекту свои права на объект другому субъекту (кроме права передачи прав).

В рассматриваемом примере, матрица доступов, описывающая дискреционную политику безопасности, может выглядеть, например, следующим образом.

Табл. 1. Дискреционная матрица доступов

Объект / Субъект	**Файл_1**	**Файл_2**	**CD-RW**	**Флоппи-дисковод**
Администратор	Полные права	Полные права	Полные права	Полные права
Гость	Запрет	Чтение	Чтение	Запрет
Пользователь_1	Чтение, передача прав	Чтение, запись	Полные права	Полный запрет

Здесь, Пользователь_1 имеет права на чтение и запись в Файл_2.

Пользователь_1 может передать свое право на чтение из Файла_1 другому пользователю. Если Пользователь_1 передает право на чтение к Файлу_1 пользователю Гость, то у пользователя Гость появляется право чтения из Файла_1, соответственно модифицируется матрица доступов.

Порядок выполнения работы

Пусть множество *S* возможных операций субъектов над объектами компьютерной системы задано в виде: *S* = {«Доступ на чтение», «Доступ на запись», «Передача прав»}.

1.Получите из таблицы 2 информацию о количестве субъектов и объектов компьютерной системы, соответственно Вашему варианту.

2.Реализуйте программный модуль, формирующий матрицу доступов субъектов к объектам компьютерной системы в виде, аналогичном таблице 1. Реализация данного модуля подразумевает реализацию следующих шагов:

2.1. Выбрать идентификаторы пользователей, которые будут использоваться при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей задано для Вашего варианта). Например, множество из 3 идентификаторов пользователей {Ivan, Sergey, Boris}. Один из данных идентификаторов должен соответствовать администратору компьютерной системы (пользователю, обладающему полными правами ко всем объектам).

2.2. Создать и случайным образом заполнить матрицу доступа субъектов к объектам в виде, аналогичном таблице 1. Выдать матрицу на экран При заполнении матрицы учесть следующее:

2.2.1. Один из пользователей-субъектов должен являться администратором системы. Для него права доступа ко всем объектам системы должны быть установлены как полные.

2.2.2. Пользователь может иметь несколько прав доступа к некоторому объекту компьютерной системы, иметь полные права, либо совсем не иметь прав.

Замечание по реализации

Для реализации программной модели матрицы доступов можно использовать массив размерности M x N, где M – количество субъектов, N – количество объектов.

Права доступов в ячейках матрицы доступов можно кодировать трехбитовыми числами от 0 до 7, например, в следующем виде:

Бит доступа по чтению	Бит доступа по записи	Бит передачи прав

Тогда, соответствие множеств типов доступов и соответствующих значений в матрице доступов будет следующее:

Десятичное число	**Двоичное число**	**Разрешенные типы доступов**
0	000	Полный запрет
1	001	Передача прав
2	010	Запись
3	011	Запись, Передача прав
4	100	Чтение
5	101	Чтение, Передача прав
6	110	Чтение, Запись
7	111	Полный доступ

3. Реализовать программный модуль, демонстрирующий работу пользователя в дискреционной модели политики безопасности. Данный модуль должен выполнять следующие функции.

3.1. При запуске модуля должен запрашиваться идентификатор пользователя (должна проводиться его идентификация). В случае успешной идентификации пользователя должен осуществляться вход в систему, в случае неуспешной – выводиться соответствующее сообщение.

3.2. При входе в систему после успешной идентификации пользователя, на экране должен распечатываться список всех объектов системы с указанием перечня всех доступных прав доступа идентифицированного пользователя к данным объектам. Вывод можно осуществить, например, следующим образом:

User: Boris

Идентификация прошла успешно, добро пожаловать в систему

Перечень Ваших прав:

Объект1: Чтение

Объект2: Запрет

Объект3: Чтение, Запись

Объект4: Полные права

Жду ваших указаний >

3.3. После вывода на экран перечня прав доступа пользователя к объектам компьютерной системы, программа должна ждать указаний пользователя на осуществление действий над объектами в компьютерной системе. После получения команды от пользователя, на экран должно выводиться сообщение об успешности либо не успешности операции. При выполнении операции передачи прав (grant), должна модифицироваться матрица доступов. Должна поддерживаться операция выхода из системы (quit), после которой должен запрашиваться другой идентификатор пользователя. Диалог можно организовать, например, следующим образом:

Жду ваших указаний > read

Над каким объектом производится операция? 1

Операция прошла успешно

Жду ваших указаний > write

Над каким объектом производится операция? 2

Отказ в выполнении операции. У Вас нет прав для ее осуществления

Жду ваших указаний > grant

Право на какой объект передается? 3

Отказ в выполнении операции. У Вас нет прав для ее осуществления

Жду ваших указаний > grant

Право на какой объект передается? 4

Какое право передается? read

Какому пользователю передается право? Ivan

Операция прошла успешно

Жду ваших указаний > quit

Работа пользователя Boris завершена. До свидания.

User:

Замечание по реализации

Для контроля возможности доступа заданного типа в рамках предложенной выше программной модели необходимо проверить равенство единице соответствующего бита числа в ячейке матрицы доступов. Для этого можно воспользоваться свойствами операций целочисленного деления и взятия остатка от деления на 2.

Для того, чтобы проверить равенство n-го бита некоторого числа на равенство единице необходимо целочисленно поделить это число на 2^{n-1} и проверить на нечетность получившееся число. Если после деления получили нечетное число, то n-ый бит исходного числа равен единице, иначе – равен нулю.

Пример

Проверить возможность доступа по записи Пользователя_2 к Файлу_3.

1. Берем элемент матрицы доступов, находящийся на пересечении второй строки и третьего столбца. Пусть этот элемент равен 3.

2. Для контроля возможности доступа по чтению, необходимо проверить равенство второго бита числа на единицу. Для этого целочисленно поделим число 3 на $2^{2-1}=2$.

3. $\left\lfloor \frac{3}{2} \right\rfloor = 1$ - число нечетное, то есть второй бит числа 3 равен единице, то есть доступ по записи Пользователя_2 к Файлу_3 разрешен.

4. Протестировать реализованную программу, продемонстрировав реализованную модель дискреционной политики безопасности преподавателю.

5. Оформить в тетради отчет по работе согласно примеру, приведенному на последней странице. В прогонку программы, включаемую в отчет должны входить как примеры разрешенных операций, так и примеры неразрешенных операций, примеры выполнения операций по передаче прав.

Табл. 2. Варианты

Вариант	Количество субъектов доступа (пользователей)	Количество объектов доступа
1	3	3
2	4	4
3	5	4
4	6	5
5	7	6
6	8	3
7	9	4
8	10	4

9	3	5
10	4	6
11	5	3
12	6	4
13	7	4
14	8	5
15	9	6
16	10	3
17	3	4
18	4	4
19	5	5
20	6	6
21	7	3
22	8	4
23	9	4
24	10	5
25	3	6
26	4	3
27	5	4
28	6	4
29	6	5
30	8	6

Контрольные вопросы

1. Что понимается под политикой безопасности в компьютерной системе?

2. В чем заключается модель дискреционной политики безопасности?
3. Что понимается под матрицей доступов? Что хранится в данной матрице?
4. Какие действия производятся над матрицей доступа в том случае, когда один субъект передает другому субъекту свои права доступа к объекту компьютерной системы?

Пример оформления отчета

Практика № 5

НАЗВАНИЕ ЗАНЯТИЯ

ВЫПОЛНИЛ: ст. гр. ….. ФИО

ВАРИАНТ № …

ЦЕЛЬ ЗАНЯТИЯ

КОЛИЧЕСТВО СУБЪЕКТОВ ДОСТУПА = ……

КОЛИЧЕСТВО ОБЪЕКТОВ ДОСТУПА = …..

ТЕКСТ ПРОГРАММЫ

……..

МАТРИЦА ДОСТУПА СУБЪЕКТОВ К ОБЪЕКТАМ В ВИДЕ, АНАЛОГИЧНОМ ПРЕДСТАВЛЕННОМУ В ТАБЛИЦЕ 1, СФОРМИРОВАННАЯ СЛУЧАЙНЫМ ОБРАЗОМ ВАШЕЙ ПРОГРАММОЙ

……

ПРИМЕР ПРОГОНКИ ПРОГРАММЫ

User: Sergey

Идентификация прошла успешно, добро пожаловать в систему

Перечень Ваших прав:

Объект1: Полные права

Объект2: Полные права

Объект3: Полные права

Объект4: Полные права

Жду ваших указаний > quit

Работа пользователя Sergey завершена. До свидания.

2. Мандатная модель политики безопасности

Цель занятия – познакомиться с проблемами реализации политик безопасности в компьютерных системах на примере мандатной модели.

Теоретический материал

Мандатная модель политики безопасности предполагает нормативное управление доступом субъектов к объектам с использованием меток безопасности.

Мандатную модель можно определить следующей группой аксиом.

1. Вводится множество атрибутов безопасности *A*, элементы которого упорядочены с помощью установленного отношения доминирования. Например, для России характерно использование следующего множества уровней безопасности *A*={открыто (О), конфиденциально (К), секретно (С), совершенно секретно (СС), особая важность (ОВ)}.

2. Каждому объекту $O_j \in O$ компьютерной системы ставится в соответствие атрибут безопасности $x_{O_j} \in A$, который соответствует ценности объекта O_j и называется его *уровнем (грифом) конфиденциальности*.

3. Каждому субъекту $S_i \in S$ компьютерной системы ставится в соответствие атрибут безопасности $x_{S_i} \in A$, который называется *уровнем допуска* субъекта и равен максимальному из уровней конфиденциальности объектов, к которому субъект S_i будет иметь допуск.

4. Если субъект S_i имеет уровень допуска x_{S_i}, а объект O_j имеет уровень конфиденциальности x_{O_j}, то S_i будет иметь допуск к O_j тогда и только тогда, когда $x_{S_i} \geq x_{O_j}$.

При реализации мандатной модели политики безопасности вводят два вектора.

1. Вектор $OV = (ov_1, ..., ov_n)$, задающий уровни конфиденциальности для всех объектов компьютерной системы (*n* – количество объектов).

2. Вектор $UV = (uv_1, ..., uv_m)$, задающий уровни допуска для всех субъектов в компьютерной системе (m – число субъектов).

Система разграничения доступа при осуществлении доступа субъекта к объекту сравнивает уровень допуска субъекта с уровнем конфиденциальности объекта и по результатам этого сравнения разрешает либо запрещает данный доступ. Доступ разрешается, если уровень допуска субъекта больше либо равен уровню конфиденциальности объекта. В ином случае, доступ запрещается.

Порядок выполнения работы

Пусть задано множество атрибутов безопасности *A*={«Совершенно секретно», «Секретно», «Открытые данные»}.

1. Получить информацию о количестве объектов и субъектов компьютерной системы из таблицы 1, соответственно Вашему варианту.

2. Реализовать программный модуль, создающий мандатную модель политики безопасности. Реализация данного модуля подразумевает следующее.

2.1. Выбрать идентификаторы пользователей-субъектов, которые будут использоваться при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей-субъектов задано для Вашего варианта). Например, множество из 3 идентификаторов пользователей {Ivan, Sergey, Boris}.

2.2. Заполнить вектор *OV*, задающий уровни конфиденциальности объектов, случайным образом. Множество атрибутов безопасности *A* указано выше.

2.3. Заполнить вектор *UV*, задающий уровни допуска пользователей, случайным образом. Множество атрибутов безопасности *A* указано выше.

2.4. Распечатать на экране вектора *OV* и *UV*, определяющие уровни конфиденциальности объектов и уровни допуска пользователей. Вывод можно осуществить, например, следующим образом:

Уровни конфиденциальности объектов (*OV*):

Объект_1: Открытые данные

Объект_2: Секретно

Объект_3: Совершенно секретно

Объект_4: Открытые данные

Уровни допуска пользователей (*UV*)

Ivan: Совершенно секретно

Sergey: Секретно

Boris: Открытые данные

3. Реализовать программный модуль, демонстрирующий работу системы в мандатной модели политики безопасности. Данный модуль должен выполнять следующие функции:

3.1. Выполнять идентификацию пользователя при входе в систему. При успешной идентификации пользователя должен осуществляться вход в систему, при неуспешной – вывод соответствующего сообщение.

3.2. При входе в систему после успешной идентификации пользователя, на экране должен распечатываться список тех объектов системы, к которым у вошедшего пользователя есть доступ. Вывод можно осуществить, например, следующим образом:

User: Boris

Идентификация прошла успешно, добро пожаловать в систему

Перечень доступных объектов: Объект_1, Объект_4.

Жду ваших указаний >

3.3. После вывода на экран перечня доступных объектов, программа должна ждать указаний пользователя на осуществление действий над объектами в компьютерной системе (команда request). После получения команды request от пользователя, на экран должно выводиться сообщение об успешности либо не успешности операции. Должна поддерживаться операция выхода из системы (quit), после ввода которой должен запрашиваться другой идентификатор пользователя. Диалог можно организовать, например, следующим образом:

Жду ваших указаний > request

К какому объекту хотите осуществить доступ? 1

Операция прошла успешно

Жду ваших указаний > request

К какому объекту хотите осуществить доступ? 2

Отказ в выполнении операции. Недостаточно прав.

Жду ваших указаний > quit

Работа пользователя Boris завершена. До свидания.

User:

4. Исследовать работу реализованной программы, продемонстрировав реализованную модель мандатной политики безопасности преподавателю.

5. Оформить в тетради отчет по работе согласно примеру, приведенному на последней странице. В прогонку программы включить примеры как разрешенных, так и запрещенных операций.

ЗАМЕЧАНИЕ

Грифы конфиденциальности объектов и уровни доступа субъектов могут быть закодированы цифрами для удобства их хранения и сравнения. Для хранения в программной модели атрибутов безопасности множества A, можно закодировать их числами от 0 до 2 (от низших к высшим уровням безопасности), например, «Открытые данные»=0, «Секретно»=1, «Совершенно секретно»=2. В этом случае более легко можно реализовать контроль допуска субъектов к объектам.

Табл. 1. Варианты

Вариант	Количество субъектов доступа	Количество объектов доступа
1	3	3

2	4	4
3	5	4
4	6	5
5	7	6
6	8	3
7	9	4
8	10	4
9	3	5
10	4	6
11	5	3
12	6	4
13	7	4
14	8	5
15	9	6
16	10	3
17	3	4
18	4	4
19	5	5
20	6	6
21	7	3
22	8	4
23	9	4
24	10	5
25	3	6

26	4	3
27	5	4
28	6	4
29	6	5
30	8	6

Контрольные вопросы

1. В чем заключается модель мандатной политики безопасности в компьютерной системе?
2. Перечислить группу аксиом, определяющих мандатную модель политики безопасности.
3. К объектам какого уровня конфиденциальности будет иметь субъект с уровнем допуска «Открытые данные»?
4. Какой уровень допуска должен иметь администратор компьютерной системы?

Пример оформления отчета

ЗАНЯТИЕ №

НАЗВАНИЕ ЗАНЯТИЯ

ВЫПОЛНИЛ: ст. гр. ….. ФИО

ВАРИАНТ № …

ЦЕЛЬ ЗАНЯТИЯ

КОЛИЧЕСТВО СУБЪЕКТОВ ДОСТУПА = ……

КОЛИЧЕСТВО ОБЪЕКТОВ ДОСТУПА = …..

ТЕКСТ ПРОГРАММЫ

……..

ПРОГОНКА ПРОГРАММЫ

УРОВНИ КОНФИДЕНЦИАЛЬНОСТ И ОБЪЕКТОВ_____

УРОВНИ ДОПУСКА СУБЪЕКТОВ_____

1. Пользователь_1

Список доступных объектов для пользователя_1……..

2. Пользователь_2

Список доступных объектов для пользователя_2 ……..

3. Пользователь_3

Список доступных объектов для пользователя_3 ……..

4. Пользователь_4

Список доступных объектов для пользователя_4 ……..

……

ПРИМЕР РАБОТЫ С ПРОГРАММНОЙ МОДЕЛЬЮ МАНДАТНОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ

Уровни конфиденциальности объектов (*OV*):

Объект_1: Открытые данные

Объект_2: Секретно

Объект_3: Совершенно секретно

Объект_4: Открытые данные

Уровни допуска пользователей (*UV*)

Ivan: Совершенно секретно

Sergey: Секретно

Boris: Открытые данные

3. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю), описание шкал оценивания

Критериями оценивания при модульно-рейтинговой системе являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10; для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

(для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов)

Рейтинг-план дисциплины

№ п/п	Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
				Минимальный	Максимальный
Модуль 1					
Текущий контроль, в том числе				**0**	**25**
1.	Работа на практических занятиях	1	5	0	5
2.	Практическая работа	5	2	0	10
3.	Тест	10	1	0	10
Рубежный контроль, в том числе				**0**	**25**
1.	Тестирование	25	1	0	25
			Итого	**0**	**50**
Модуль 2					
Текущий контроль, в том числе					**25**
1.	Работа на практических занятиях	1	5	0	5
2.	Тест	20	1	0	20
Рубежный контроль, в том числе				**0**	**25**
1.	Тестирование	25	1	0	25
			Итого	**0**	**50**
Поощрительные баллы					**10**
1.	Выступление на семинаре кафедры	5	1	0	5
2.	Публикация статей	5	1	0	5
Посещаемость (баллы вычитаются из общей суммы набранных баллов)					
1.	Посещение лекционных занятий			0	-6
2.	Посещение практических			0	-10

	занятий				
Итоговый контроль					
	Зачет	0	0	**0**	**0**
			Итого	**0**	**110**

Результаты обучения по дисциплине (модулю) у обучающихся оцениваются по итогам текущего контроля количественной оценкой, выраженной в рейтинговых баллах. Оценке подлежит каждое контрольное мероприятие.

При оценивании сформированности компетенций применяется четырехуровневая шкала «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

Максимальный балл по каждому виду оценочного средства определяется в рейтинг-плане и выражает полное (100%) освоение компетенции.

Уровень сформированности компетенции «хорошо» устанавливается в случае, когда объем выполненных заданий соответствующего оценочного средства составляет 80-100%; «удовлетворительно» – выполнено 40-80%; «неудовлетворительно» – выполнено 0-40%

Рейтинговый балл за выполнение части или полного объема заданий соответствующего оценочного средства выставляется по формуле:

Рейтинговый балл = k × Максимальный балл,

где k = 0,2 при уровне освоения «неудовлетворительно», k = 0,4 при уровне освоения «удовлетворительно», k = 0,8 при уровне освоения «хорошо» и k = 1 при уровне освоения «отлично».

Оценка на этапе промежуточной аттестации выставляется согласно Положению о модульно-рейтинговой системе обучения и оценки успеваемости студентов УУНиТ:
На дифференцированном зачете выставляется оценка:

• отлично - при накоплении от 80 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
• хорошо - при накоплении от 60 до 79 рейтинговых баллов,
• удовлетворительно - при накоплении от 45 до 59 рейтинговых баллов,
• неудовлетворительно - при накоплении менее 45 рейтинговых баллов.

При получении на экзамене оценок «отлично», «хорошо», «удовлетворительно», на зачёте оценки «зачтено» считается, что результаты обучения по дисциплине (модулю) достигнуты и компетенции на этапе изучения дисциплины (модуля) сформированы.