Министерство образования и науки Республики Казахстан

Карагандинский государственный технический университет

«Утверждаю»
Председатель Ученого совета,
ректор, академик НАН РК
Газалиев А.М.

_____

«____» _____2014г

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ СТУДЕНТА (SYLLABUS)

Дисциплина **OTZI 4220** Организация и технология защиты информации
(код и наименование дисциплины)

Модуль **OTZI 27** Организация и технология защиты информации
(код и наименование модуля)

Специальность 5В070300 – Информационные системы
(шифр и наименование специальности)

Институт компьютерных технологий и системотехники

Кафедра «Информационные системы»

2014

Предисловие

Программа обучения по дисциплине для студента (syllabus) разработана: старшими преподавателями Кудышевой Г.О. и Клюевой Е.Г.
(ученая степень, ученое звание Ф. И. О.)

Обсуждена на заседании кафедры информационных систем
Протокол № _____ от «____»_____2014 г.
Зав. кафедрой _____ «____»_____2014 г.
(подпись)

Одобрена учебно-методическим советом института компьютерных технологий и системотехники
Протокол № _____ от «_____»_____2014г.
Председатель _____ «____»_____ 2014 г.

Сведения о преподавателе и контактная информация

Кудышева Гульзада Онайбековна, старший преподаватель, Клюева Елена Георгиевна, старший преподаватель
(фамилия, имя, отчество преподавателя, ученая степень, ученое звание, должность)

Кафедра ИС находится в главном корпусе КарГТУ (Караганда, б.Мира, 56), аудитория 408а , контактный телефон 56-59-35 (1094) , факс _-_, электронный адрес gulzada52@mail.ru, lenchik_t_k@mail.ru

Трудоемкость дисциплины

Семестр	Количество кредитов	Количество кредитов ECTS	Вид занятий					Количество часов СРС	Общее количество часов	Форма контроля
			количество контактных часов			количество часов СРСП	всего часов			
			лекции	практические занятия	лабораторные занятия					
Форма обучения – очная										
7	3	5	15	-	30	45	90	45	135	Экзамен
Форма обучения – очная, сокращенная										
5	3	5	15	-	30	45	90	45	135	Экзамен

Характеристика дисциплины

Дисциплина «Организация и технология защиты информации» входит в цикл профилирующих дисциплин рабочего учебного плана государственного общеобязательного стандарта образования по специальности.

Цель дисциплины

Дисциплина «Организация и технология защиты информации» ставит целью формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Задачи дисциплины

Задачи дисциплины следующие: изучение теоретических основ построения и практического использования систем защиты информации в информационных системах, обучение студентов систематизированным представлениям о принципах, методах и средствах реализации защиты данных, приобретению практических навыков по защите информации в информационных системах, необходимых для их проектирования и эксплуатации.

В результате изучения данной дисциплины студенты должны:

иметь представление:

- о методах и средствах защиты информации при реализации информационных процессов ввода, вывода, передачи, обработки и хранения информации;
- о целях, задачах и принципах инженерно-технической защиты информации;

знать:

- особенности объектов защиты информации;
- классификацию объектов защиты информации;
- ПЭВМ как объект защиты

уметь:

– ставить и решать конкретные задачи по применению средств защиты информации для оптимизации функционирования информационных систем;
– оценивать уровень безопасности в ИС;

приобрести практические навыки:

– применения полученных знаний на практике.

Пререквизиты

Для изучения данной дисциплины необходимо усвоение следующих дисциплин (с указанием разделов (тем)):

Дисциплина	Наименование разделов (тем)
Алгоритмы, структуры данных и программирование	Конструкции, операторы, типы данных языка программирования высокого уровня
2 Информатика	Понятие информации
3 Теория вероятностей и математическая статистика	Вероятностно-автоматное моделирование

Постреквизиты

Знания, полученные при изучении дисциплины «Организация и технология защиты информации», используются при освоении следующих смежных дисциплин:

1 Компьютерные сети.

Тематический план дисциплины

Наименование раздела, (темы)	**Трудоемкость по видам занятий, ч.**				
	лекции	**практи-ческие**	**лабора-торные**	**СРСП**	**СРС**
1. Введение в дисциплину: цели и задачи курса, обоснование проблемы защиты информации в ИС, классификация средств защиты информации, принципы и методы оценки эффективности средств защиты информации	1				2
2 Защита информации при реализации информационных процессов ввода, вывода, передачи, обработки и хранения информации: Классификация объектов защиты. Классификация элементов защиты технических устройств. Определение характеристик для объектов и элементов защиты, необходимых для решения задач защиты информации	2				2
3 Методы и средства защиты информации					
3.1 Теоретические методы защиты информации: Классификация и общий	1				2

анализ методов моделирования систем защиты информации. Основные положения теории нечетких множеств. Основные положения вероятностно-автоматного моделирования. Основные положения неформальной теории систем					
3.2 Практические методы защиты информации: Управление, препятствие, маскировка, регламентация, побуждение, принуждение	1				2
3.3 Программные средства защиты информации в компьютерных сетях	1				2
3.3.1 Защита от вирусов: классификация компьютерных вирусов, способы заражения среды обитания. Способы активизации вируса. Деструктивные действия вирусов. Способы маскировки. Способы выбора жертвы для инфицирования. Симптомы наличия вирусов. Другие опасные программы. Классификация антивирусных средств. Низкоуровневые редакторы. Доработка программных продуктов при отсутствии исходных текстов. Перспективные направления борьбы с вирусами.	1				2
3.3.2 Защита программного обеспечения от несанкцио-нированного доступа: Идентификация и аутентификация пользователя. Идентифика-ция ПЭВМ. Идентификация исполняемого модуля. Использование скрытых частей программы и особенностей физических носителей информации при защите от несанкциониро-ванного копирования	1				2
3.3.3 Организация защиты программного обеспечения от	1				2

исследования: Использование специфичес- ких особенностей работы отладчиков. Изощренное программирование. Язык программирования защищенных программ					
3.3.4 Защита информации в открытых сетях: обеспечение информационной безопасности при подключении к Интернет. Защита архитектуры клиент-сервер. Защита СУБД	1				2
3.4 Криптографические средства защиты информации				21	
3.4.1 Симметричные криптосистемы: Обзор симметричных криптосистем. Перестановки. Системы подстановок. Гаммирование. Датчики псевдослучайных чисел. Ознакомление со стандартами блочного шифрования.	2				2
3.4.2 Системы с открытым ключом: Теоретические основы систем с открытым ключом. Использование алгоритмов криптосистемы с открытым ключом для защиты передаваемых и хранимых данных. Применение криптосистемы с открытым ключом для распределения ключей. Электронная подпись	2				2
3.5 Организационные и технические средства защиты информации в компьютерных сетях: Методы оценки уровня безопасности в ИС. Организационные меры по управлению контролем и защитой информации. Законодательные меры по защите информации. Технические средства защиты информации.	1			24	3
4 Лабораторный практикум					

4.1 Защита информации на основе механизмов индентификации и аутентификации			3		2
4.2 Защита программного обеспечения от несанкционированного доступа			3		2
4.3 Методы и алгоритмы шифрования			3		2
4.4 Частотный криптоанализ			3		2
4.5 Методы криптографической защиты в системах с открытым ключом			3		2
4.6 Программная реализация датчиков псевдослучайных чисел			3		2
4.7 Обеспечение информационной безопасности средствами ОС Windows 7			3		2
4.8 Защита документов MS Office			3		2
4.9 Исследование признаков присутствия на компьютере вредоносных программ			3		2
4.10 Технология защиты сетевых компьютеров. Брандмауэр			3		2
ИТОГО:	**15**	**-**	**30**	**45**	**45**

Перечень лабораторных занятий

1 Защита информации на основе механизмов индентификации и аутентификации
2 Защита программного обеспечения от несанкционированного доступа
3 Методы и алгоритмы шифрования
4 Частотный криптоанализ
5 Методы криптографической защиты в системах с открытым ключом
6 Программная реализация датчиков псевдослучайных чисел
7 Обеспечение информационной безопасности средствами ОС Windows 7
8 Защита документов MS Office
9 Исследование признаков присутствия на компьютере вредоносных программ
10 Технология защиты сетевых компьютеров. Брандмауэр

Тематический план самостоятельной работы студента с преподавателем

Наименование темы СРСП	Цель занятия	Форма проведения занятия	Содержа-ние задания	Рекомендуе-мая литература
Криптографические средства защиты информации	Освоение материала по данной теме	Консультации и собеседование	Выполнение практического задания к	[2,8,9]

			аттестации 1	
Организационные и технические средства защиты информации в компьютерных сетях: Методы оценки уровня безопасности в ИС. Организационные меры по управлению контролем и защитой информации. Законодательные меры по защите информации. Технические средства защиты информации.	Освоение материала по данной теме	Консультации и собеседование	Выполнение практического задания к аттестации 2	[14,17, http://www.securitypolicy.ru]

Темы контрольных заданий для СРС

1. Проведение тематического исследования:

1. Классификация средств защиты информации, принципы и методы оценки эффективности средств защиты информации

2. Защита информации при реализации информационных процессов ввода, вывода, передачи, обработки и хранения информации: Классификация объектов защиты. Классификация элементов защиты технических устройств. Определение характеристик для объектов и элементов защиты, необходимых для решения задач защиты информации

3. Теоретические методы защиты информации: Классификация и общий анализ методов моделирования систем защиты информации. Основные положения теории нечетких множеств. Основные положения вероятностно-автоматного моделирования. Основные положения неформальной теории систем

4. Практические методы защиты информации: Управление, препятствие, маскировка, регламентация, побуждение, принуждение

5. Защита от вирусов: классификация компьютерных вирусов, способы заражения среды обитания. Способы активизации вируса. Деструктивные действия вирусов. Способы маскировки. Способы выбора жертвы для инфицирования. Симптомы наличия вирусов. Другие опасные программы. Классификация антивирусных средств. Низкоуровневые редакторы. Доработка программных продуктов при отсутствии исходных текстов. Перспективные направления борьбы с вирусами.

6 Защита программного обеспечения от несанкционированного доступа: Идентификация и аутентификация пользователя. Идентификация ПЭВМ. Идентификация исполняемого модуля. Использование скрытых частей программы и особенностей физических носителей информации при защите от несанкционированного копирования

7 Организация защиты программного обеспечения от исследования: Использование специфических особенностей работы отладчиков. Изощренное программирование. Язык программирования защищенных программ

8 Защита информации в открытых сетях: обеспечение информационной безопасности при подключении к Интернет. Защита архитектуры клиент-сервер. Защита СУБД

9 Симметричные криптосистемы: Обзор симметричных криптосистем. Перестановки. Системы подстановок. Гаммирование. Датчики псевдослучайных чисел. Ознакомление со стандартами блочного шифрования.

10 Системы с открытым ключом: Теоретические основы систем с открытым ключом. Использование алгоритмов криптосистемы с открытым ключом для защиты передаваемых и хранимых данных. Применение криптосистемы с открытым ключом для распределения ключей. Электронная подпись

11 Организационные и технические средства защиты информации в компьютерных сетях: Методы оценки уровня безопасности в ИС. Организационные меры по управлению контролем и защитой информации. Законодательные меры по защите информации. Технические средства защиты информации.

2. Подготовка к теоретическим модулям (изучение конспекта лекций и рекомендуемой литературы)

3. Изучение теоретических сведений по теме лабораторных работ, выполнение заданий и оформление отчета по лабораторным работам

Критерии оценки знаний студентов

Экзаменационная оценка по дисциплине определяется как сумма максимальных показателей успеваемости по рубежным контролям (60%) и итоговой аттестации (экзамен) (40%) и составляет значение 100% в соответствии с таблицей.

Оценка по буквенной системе	**Цифровые эквиваленты буквенной оценки**	**Процентное содержание усвоенных знаний**	**Оценка по традиционной системе**
A A-	4,0 3,67	95-100 90-94	Отлично
B+ B B-	3,33 3,0 2,67	85-89 80-84 75-79	Хорошо
C+ C C- D+ D-	2,33 2,0 1,67 1,33 1,0	70-74 65-69 60-64 55-59 50-54	Удовлетворительно
F	0	0-49	Неудовлетворительно

Оценка «А» (отлично) выставляется в том случае, если студент в течение семестра показал отличные знания по всем программным вопросам дисциплины, а также по темам самостоятельной работы, регулярно сдавал рубежные задания, проявлял самостоятельность в изучении теоретических и прикладных вопросов по основной программе изучаемой дисциплины, а также по внепрограммным вопросам.

Оценка «А-» (отлично) предполагает отличное знание основных законов и процессов, понятий, способность к обобщению теоретических вопросов дисциплины, регулярную сдачу рубежных заданий по аудиторной и самостоятельной работе.

Оценка «В+» (хорошо) выставляется в том случае, если студент показал хорошие и отличные знания по вопросам дисциплины, регулярно сдавал семестровые задания в основном на «отлично» и некоторые на «хорошо».

Оценка «В» (хорошо) выставляется в том случае, если студент показал хорошие знания по вопросам, раскрывающим основное содержание конкретной темы дисциплины, а также темы самостоятельной работы, регулярно сдавал семестровые задания на «хорошо» и «отлично».

Оценка «В-»(хорошо) выставляется студенту в том случае, если он хорошо ориентируется в теоретических и прикладных вопросах дисциплины как по аудиторным,

так и по темам СРС, но нерегулярно сдавал в семестре рубежные задания и имел случаи пересдачи семестровых заданий по дисциплине.

Оценка «C+» (удовлетворительно) выставляется студенту в том случае, если он владеет вопросами понятийного характера по всем видам аудиторных занятий и СРС, может раскрыть содержание отдельных модулей дисциплины, сдает на «хорошо» и «удовлетворительно» семестровые задания.

Оценка «C» (удовлетворительно) выставляется студенту в том случае, если он владеет вопросами понятийного характера по всем видам аудиторных занятий и СРС, может раскрыть содержание отдельных модулей дисциплины, сдает на «удовлетворительно» семестровые задания.

Оценка «C-» (удовлетворительно) выставляется студенту в том случае, если студент в течение семестра регулярно сдавал семестровые задания, но по вопросам аудиторных занятий и СРС владеет только общими понятиями и может объяснить только отдельные закономерности и их понимание в рамках конкретной темы.

Оценка «D+» (удовлетворительно) выставляется студенту в том случае, если он нерегулярно сдавал семестровые задания, по вопросам аудиторных занятий и СРС владеет только общими понятиями и может объяснить только отдельные закономерности и их понимание в рамках конкретной темы.

Оценка «D» (удовлетворительно) выставляется студенту в том случае, если он нерегулярно сдавал семестровые задания, по вопросам аудиторных занятий и СРС владеет минимальным объемом знаний, а также допускал пропуски занятий.

Оценка «F» (неудовлетворительно) выставляется тогда, когда студент практически не владеет минимальным теоретическим и практическим материалом аудиторных занятий и СРС по дисциплине, нерегулярно посещает занятия и не сдает вовремя семестровые задания.

Рубежный контроль проводится на 7, 14-й неделях обучения и складывается исходя из следующих видов контроля:

Вид контроля	%-ое содержание	Академический период обучения, неделя															Итого, %
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Посещаемость лекций	1	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	15
Лаб.работы	2,1		*	*		*	*		*	*		*	*		*	*	21
Практические задания	5							*							*		10
Теоретический модуль	7							*							*		14
Экзамен	40																40
Всего по аттестации								30							30		60
Итого																	100

Политика и процедуры

При изучении дисциплины ««Организация и технология защиты информации» » прошу соблюдать следующие правила:

1 Не опаздывать на занятия.

2 Не пропускать занятия без уважительной причины, в случае болезни прошу представить справку, в других случаях – объяснительную записку.

3 В обязанности студента входит посещение всех видов занятий.

4 Согласно календарному графику учебного процесса сдавать все виды контроля.

5 Пропущенные лабораторные занятия отрабатывать в указанное преподавателем время.

Учебно-методическая обеспеченность дисциплины

Ф.И.О автора	Наименование учебно-методической литературы	Издательство, год издания	Количество экземпляров	
			В библиотеке	на кафедре
Основная литература				
1 Б. Ю.Анин	Защита компьютерной информации: научное издание	СПб.: - Санкт-Петербург, 2000. - 368с.	4	-
2 А.А. Молдовян, Н.А. Молдовян	Криптография: скоростные шифры: научное издание.	СПб. : БХВ – Петербург, 2002. - 493 с.	10	-
3 В. И. Ярочкин	Информационная безопасность: Учебник	М.: Фонд "Мир", 2003. - 640 с.	3	-
4. А. В. Соколов	Методы информационной защиты объектов и компьютерных сетей научное издание	СПб. : Полигон ; М. : АСТ, 2000. - 272 с.	5	-
Дополнительная литература				
5 И. Конеев	Информационная безопасность предприятия: научное издание	СПб. : БХВ – Петербург, 2003. - 733 с.	1	-
6 А. А. Садердинов	Информационная безопасность предприятия : учеб. пособие	М. :Изд.-торговая корпорация Дашков и К*, 2004. - 335 с. : ил.	6	
7 В. М. Зима	Безопасность глобальных сетевых технологий - 2-е изд.	СПб. : БХВ – Петербург, 2003. - 362 с.	1	-
8 Пособие А. В. Асосков [и др.].	Поточные шифры (кн. 3).	М. : Кудиц-Образ, 2003. - 334 с.	5	-
9 О. С.Зензин	Стандарт криптографической защиты - AES. Конечные поля	М. : Кудиц-Образ, 2002. - 174 с. :	5	-
10 А. В. Петраков	Охрана и защита современного предприятия:	М. : ЭНЕРГОАТОМ ИЗДАТ, 1999. - 568 с.	5	-
11 Ю. Н. Максимов [и др.]	Технические методы и средства защиты информации:	СПб. : Полигон, 2000. - 320 с. : ил.	3	-
12 Л. К.Бабенко	Защита информации с использованием смарт-карт и электронных брелоков	М. : Гелиос АРВ, 2003. - 352 с.	1	-
13 В. А. Галатенко	Основы информационной безопасности : курс лекций	М.: Интернет-Унивеситет ИТ, 2004. - 277 с.	4	-
14 Скотт Бармен	Разработка правил информационной безопасности : пер. с англ.	М. ; СПб. ; Киев : ИД Вильямс, 2002. - 207с.	5	-
15 Норберт Польман	Архитектура брандмауэров для сетей предприятия : пер. с англ	М ; СПб.; ИД Вильямс, 2003. -420 с.	6	-

16 Г.Д. Когай	Проектирование и защита корпоративных информационных систем: монография	КарГТУ, Караганда : 2009. - 177 с.	96	
17 В.Ю. Скиба	Руководство по защите от внутренних угроз информационной безопасности:	М. ; СПб. ; Нижний Новгород : Питер, 2008. - 318 с. : ил.	3	
18 С.В. Гордейчик	Безопасность беспроводных сетей: научное издание	М. : Горячая линия - Телеком, 2008. - 288 с	5	-
19 В. В. Платонов	Программно-аппаратные средства обеспечения информационной безопаснос-ти выч. сетей	М. : Академия, 2006. - 239 с.	7	-
20 Д.Донцов	Как защитить компьютер от ошибок, вирусов, хакеров: научное издание	М. ; СПб. ; Нижний Новгород : Питер, 2006. - 143 с. :	3	-

График выполнения и сроки сдачи заданий по дисциплине

Вид контроля	Цель и содержание задания	Рекомендуемая литература	Продолжительность выполнения	Форма контроля	Срок сдачи
Посещаемость лекций и СРСП	Соблюдение процедур		15 контактных часов	Текущий	На каждом занятии
Лабораторные работы №№ 1-10	Усвоение материала по дисциплине	МУ к выполнению лабораторных работ	15 контактных часов	Текущий	На 2,3,5,6,8, 9,11,12, 14,15 неделях
Практическое задание к аттестации 1	Получение практических навыков	МУ к выполнению практического задания	6 контактных часов	Рубежный	7-я неделя
Теоретический модуль к аттестации 1	Проверка усвоения материала дисциплины	Конспект лекций	0,5 контактных часа	Рубежный	7-я неделя
Практическое задание к аттестации 2	Получение практических навыков	МУ к выполнению практического задания	6 контактных часов	Рубежный	14-я неделя
Теоретический модуль к аттестации 2	Проверка усвоения материала дисциплины	Конспект лекций	0,5 контактных часа	Рубежный	14-я неделя
Экзамен	Проверка усвоения материала дисциплины	[1…35]	1 контактный час	Итоговый	В период сессии

Вопросы (тестовые задания) для самоконтроля

1. Сформулируйте понятие идентификации
2. Сформулируйте понятие идентификатора
3. Сформулируйте понятие аутентификации
4. Сформулируйте понятие аутентификатора
5. Приведите примеры идентификаторов и аутентификаторов
6. Назовите возможные объекты идентификации
7. Перечислите виды средств, используемых для аутентификации
8. Сформулируйте различия между электронными устройствами типа «Электронный ключ» и «TouchMemory»
9. Назовите цели, для которых используются электронные ключи
10. Назовите цели, для которых используются устройства типа «TouchMemory»
11. Сформулируйте понятие биометрических технологий
12. Назовите области применения биометрических технологий
13. Перечислите биометрические методы идентификации
14. Перечислите критерии оценки методов биометрической идентификации
15. Назовите режимы работы систем биометрической идентификации
16. Перечислите функциональные модули систем биометрической идентификации
17. Назовите две методики использования паролей
18. Назовите достоинства и недостатки паролей, представляющих собой фиксированные последовательности символов
19. Перечислите правила выбора паролей
20. Перечислите правила, которые надо соблюдать при работе с паролями
21. Назовите достоинства и недостатки паролей, представляющих собой определенное правило (процедуру)
22. Перечислите возможности системы Windows по защите информации с помощью паролей
23. Что такое информационная безопасность?
24. В чем заключается утечка информации?
25. Какова цель создания системы компьютерной безопасности?
26. Назовите виды компьютерных атак.
27. Откуда следует ожидать компьютерной атаки?
28. Приведите примеры взломов сетей и Web-узлов через Internet.
29. Перечислите и охарактеризуйте основных пользователей Internet.
30. Как классифицируются злоумышленники в Internet?
31. Какие факторы уязвимости Internet?
32. Какими основными свойствами обладают "компьютерные вирусы"?
33. По каким классам разделяются "компьютерные вирусы"?
34. Как классифицируются "компьютерные вирусы"?
35. Какие "компьютерные вирусы" относятся к файловым?
36. Как разделяются файловые "компьютерные вирусы" по способу размножения?
37. Объясните алгоритм работы файлового вируса.
38. Какие "компьютерные вирусы" относятся к загрузочным?
39. Объясните алгоритм работы загрузочного вируса.
40. Какие "компьютерные вирусы" относятся к макровирусам?
41. Объясните алгоритм работы макровируса.
42. Какие "компьютерные вирусы" относятся к сетевым?
43. Какие программы являются вредными и почему?
44. В чем заключается ограничение доступа к компьютерным системам?
45. Как классифицируются системы тревожной сигнализации?
46. В чем заключается контроль доступа к аппаратуре?

47. От каких действий защищает контроль доступа к аппаратуре?
48. В чем заключается контроль доступа к информации?
49. В чем заключается разделение привилегий на доступ?
50. В чем заключается идентификация и установление подлинности объекта (субъекта)?
51. Что может быть объектом идентификации?
52. В чем заключается криптографическое преобразование информации?
53. Перечислите и объясните методы криптографического преобразования информации.
54. В чем заключается защита информации от утечки за счет побочного электромагнитного излучения и наводок?
55. В чем заключаются методы защиты информации от случайных воздействий?
56. Какие задачи имеет функциональный контроль компьютерной системы?
57. В чем заключаются методы защиты информации от аварийных ситуаций?
58. В чем заключаются организационные мероприятия по защите информации?
59. В чем заключаются законодательные меры по защите информации?
60. Объясните правила выбора паролей и требования к ним.

Верны ли следующие утверждения?

- Идентификация – это процесс сообщения своего имени
- Идентификация – это проверка подлинности
- Аутентификация – это проверка подлинности
- Имя, под которым пользователь входит в систему, является его аутентификатором
- Объектом идентификации может быть только пользователь системы
- Объектом идентификации может быть человек, программа или техническое устройство
- Аутентификация программ используется только для подтверждения их легальности
- Технические устройства могут использоваться, в частности, в качестве аутентификатора пользователя
- Технические устройства могут использоваться, в частности, для защиты программ от нелегального использования
- Электронные ключи программируются таким образом, чтобы хранить информацию о пользователях
- Электронные ключи и электронные замки – одно и то же
- Электронные замки используются в основном для защиты программ от нелегального использования
- Устройства типа «TouchMemory» могут использоваться для аутентификации пользователей
- Толчок развитию биометрии дал теракт в Нью-Йорке
- Критерий универсальности при сравнении биометрических систем идентификации предполагает, что характеристика не должна быть одинаковой у разных людей
- Критерий социальной приемлемости при сравнении биометрических систем идентификации означает, что применение метода биометрической идентификации должно быть максимально комфортно для человека
- Критерий перманентности при сравнении биометрических систем идентификации означает, что биометрическая характеристика не должна изменяться со временем

- В режиме верификации пользователь предварительно сообщает биометрической системе свое имя
- Занесение шаблона в базу данных реализовано в модуле идентификации биометрической системы
- Принцип действия прибора TouchLock основан на идентификации по кисти руки
- Принцип действия прибора Eyedentify основан на идентификации по сетчатке глаза
- В качестве паролей рекомендуется использовать слова одного из языков
- В паролях рекомендуется использовать буквы разных регистров и цифры
- Пароли, представляющие собой фиксированную последовательность символов, называются «одноразовыми»
- Пароли, представляющие собой некоторое правило (процедуру), называются «одноразовыми»

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ СТУДЕНТА (SYLLABUS)

Дисциплина **OTZI 4220** Организация и технология защиты информации
(код и наименование дисциплины)

Модуль **OTZI 27** Организация и технология защиты информации
(код и наименование модуля)

Специальность 5В070300 – Информационные системы
(шифр и наименование специальности)

Институт компьютерных технологий и системотехники

Кафедра «Информационные системы»

Гос.изд.лиц. № 50 от 31.03.2004. Подписано в печать ___.___.09г. Формат 60х90/16 Усл.печ.л. 1 Тираж Цена договорная

Издательство Карагандинского государственного технического университета
100027, Караганда, б.Мира, 56