

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт математики, физики и информационных технологий
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:
Директор института



Н. Л. Королева
«05» июля 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.О.18 Программно-аппаратные средства защиты информации

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2021

Автор программы:

Кандидат физико-математических наук, доцент Лопатин Дмитрий Валерьевич

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «17» ноября 2020 г. № 1427).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «18» мая 2021 г. Протокол № 9

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «05» июля 2021 г. № 5.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП бакалавра.....	4
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	20
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	93
6. Учебно-методическое и информационное обеспечение дисциплины.....	95
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	95

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-1 Способен администрировать подсистемы защиты информации в операционных системах

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- организационно-управленческий

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сфере: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ПК-1 Способен администрировать подсистемы защиты информации в операционных системах	Администрирует программно-аппаратные подсистемы защиты информации в операционных системах

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-1 Способен администрировать подсистемы защиты информации в операционных системах

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения		
		Очная (семестр)		
		3	6	7
1	Автоматизация деятельности предприятий	+		
2	Безопасные информационные технологии		+	+
3	Ознакомительная практика		+	
4	Основы программирования в корпоративных информационных системах	+		
5	Программирование 1С	+		
6	Программирование на Python	+		

2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Программно-аппаратные средства защиты информации» относится к обязательной части учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Программно-аппаратные средства защиты информации» изучается в 5, 6 семестрах.

3.Объем и содержание дисциплины

3.1.Объем дисциплины: 9 з.е.

Очная: 9 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	324
Контактная работа	184
Лекции (Лекции)	92
Лабораторные (Лаб. раб.)	92
Самостоятельная работа (СР)	68
Экзамен	72

3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
5 семестр					
1	Предмет и задачи программно-аппаратной защиты информации.	8	8	8	Доклад
2	Системы идентификации	8	8	8	Лабораторная работа
3	Доступ к данным со стороны процесса.	8	8	6	Лабораторная работа
4	Программно-аппаратные комплексы защиты информации.	8	8	6	Лабораторная работа
5	Электронный идентификатор ruToken.	8	8	6	Лабораторная работа
6	Система биометрической идентификации BioLink.	8	8	6	Лабораторная работа; Тестирование
7	Методы защиты программного обеспечения от несанкционированного использования.	8	8	6	Лабораторная работа

8	Методы и средства ограничения доступа к компонентам ЭВМ	8	8	6	Лабораторная работа
6 семестр					
9	Понятие обратного проектирования.	7	7	4	Лабораторная работа
10	Атаки на модули проверки корректности ключевой информации	7	7	4	Лабораторная работа
11	Защита программ от изучения.	7	7	4	Лабораторная работа
12	Защита от разрушающих программных воздействий.	7	Пп 7	4	Лабораторная работа; Практическое задание для практической подготовки

Тема 1. Предмет и задачи программно-аппаратной защиты информации. (ПК-1)

Лекция.

Предмет и задачи программно-аппаратной защиты информации. Классификация методов и средств программно-аппаратной защиты информации.

Лабораторные работы.

Не предусмотрено

Задания для самостоятельной работы.

1. Перечислите задачи программно-аппаратной защиты информации.
2. Произведите классификацию методов и средств программно-аппаратной защиты информации

Тема 2. Системы идентификации (ПК-1)

Лекция.

Программно-аппаратная идентификация субъекта. Понятие протокола идентификации. Организация хранения ключей.

Лабораторные работы.

Лабораторная работа. Защита компьютера и данных с помощью ruToken

Теоретическая часть

Задание 1. Установка программного продукта.

Задание 2. Вход в Windows с помощью ruToken

Задание 3. Использование ruToken и Rohos Logon Key в сети

Утилита для Управления USB ключами

Утилита - Rohos Remote Config

MSI пакет для установки в сети

Задание 4. Настройка ruToken в Rohos Logon Key

Задание 5. Настройка дополнительных опций

Задание 6. Настройка пользователей

Задание 7. Настройка электронного ключа.

Вопросы и практические задания

Список литературы

Задания для самостоятельной работы.

1. Перечислите виды идентификация субъекта на основе программно-аппаратных решений.
2. Что может служить в качестве аутентификатора. Проанализируйте сильные слабые стороны предложенных решений.
3. Перечислите достоинства и недостатки парольной аутентификации. Оцените стойкость предложенных паролей.

Тема 3. Доступ к данным со стороны процесса. (ПК-1)

Лекция.

Процессы и данные. Способы фиксации факта доступа. Надежность систем ограничения доступа. Защита файлов от модификации. Электронная подпись.

Лабораторные работы.

Лабораторная работа. Управление доступом к файловым ресурсам

Цель работы: Освоение навыков управления доступом пользователей к файлам и папкам с целью защиты информации от несанкционированного доступа

Теоретическая часть

Файловые системы современных операционных систем при соответствующей настройке эффективно обеспечивают безопасность и надежность хранения данных на дисковых накопителях. Для операционных систем Windows стандартной является файловая система NTFS.

Устанавливая для пользователей определенные разрешения для файлов и каталогов (папок), администраторы могут защитить информацию от несанкционированного доступа. Каждый пользователь должен иметь определенный набор разрешений на доступ к конкретному объекту файловой системы. Кроме того, он может быть владельцем файла или папки, если сам их создает. Администратор может назначить себя владельцем любого объекта файловой системы, но обратная передача владения от администратора к пользователю невозможна.

Назначение разрешений производится для пользователей или групп. Так как рекомендуется выполнять настройки безопасности для групп, то необходимо, чтобы пользователь был членом хотя бы одной группы на компьютере или в домене.

Разрешения могут быть установлены для различных объектов компьютерной системы, однако в этой работе будут рассмотрены разрешения для файлов и папок. Другие задачи, например разрешения для принтеров, решаются аналогичным образом.

Задания для самостоятельной работы.

1. Доступ к каким данным со стороны процесса может вызывать тревогу.
2. Способы фиксации факта доступа. Возможные варианты обхода регистрации доступа.
3. Реализуйте основные способы защиты файлов от модификации. Проанализируйте стойкость предложенных решений

Тема 4. Программно-аппаратные комплексы защиты информации. (ПК-1)

Лекция.

Программно-аппаратные комплексы. Цели. Классификация. Типы. Назначение. Сертификация. Установка ПО. Средства управления. Установка клиента. Способы аутентификации пользователя при входе в операционную систему. Временная блокировка компьютера. Создание зашифрованного каталога. Расшифровывание файла. Работа с конфиденциальными ресурсами. Смена аутентификатора администратора. Тестирование памяти. Корректировка шаблонов контроля целостности

Лабораторные работы.

Лабораторная работа. Электронный замок Соболев

Теоретическая часть

Задание 1. Установить программное обеспечение комплекса «Соболь».

Задание 2. Настроить общие параметры комплекса.

Задание 3. Зарегистрироваться в системе в качестве Администратора.

Задание 4. Зарегистрировать в списке пользователей нового пользователя

комплекса.

Задание 5. Сменить аутентификатор администратора

Задание 6. Провести тестирование памяти NVRAM

Задание 7. Корректировка шаблонов для контроля целостности.

Задание 8. Выполнить расчет эталонных значений контрольных сумм.

Задание 9. Просмотреть записи журнала.

Задание 10. Удалите ПО для комплекса «Соболь»

Вопросы и практические задания

Список использованных источников.

Задания для самостоятельной работы.

1. Перечислите возможности программно-аппаратных комплексов защиты информации.
2. Предложите решение для построения аппаратных или программных компонент защиты данных.
3. Реализуйте на основе ПАК подсистемы защиты, предусмотренные стандартами безопасности. Обоснуйте достижение необходимых показателей из стандарта безопасности.

Тема 5. Электронный идентификатор ruToken. (ПК-1)

Лекция.

Безопасность в ruToken и спектр его возможностей. Применение и обзор архитектуры ruToken. Как устроен ruToken. Разработка приложений для ruToken. Использование ruToken как персональное средство аутентификации и хранения сертификатов. Виды электронных ключей и принципы их работы. Вход в систему с использованием ruToken.

Лабораторные работы.

Лабораторная работа. Вход в систему с использованием ruToken

Теоретическая часть

Задание 1. Установка компонентов системы

Задание 2. Создание профиля.

Задание 3. Вход с помощью электронного идентификатора.

Задание 4. Вход в систему с использованием пароля.

Задание 5. Использование дополнительных библиотек аутентификации

Вопросы и практические задания.

Список литературы

Задания для самостоятельной работы.

1. Предложите процедуру использования ruToken как персонального средства аутентификации, шифрования и хранения сертификатов.
2. Осуществите вход в операционную систему с использованием ruToken.
3. Предложите как можно использовать ruToken как одно из средств сертификационного центра.

Тема 6. Система биометрической идентификации BioLink. (ПК-1)

Лекция.

Биометрические системы. Идентификация по дактилоскопическому узору, лицу, радужной оболочке глаза, строению руки или пальца, голосу, походке, клавиатурному подчерку и т.д. Комплект разработчика. Работа с SDK. Типовые задачи биометрических систем.

Лабораторные работы.

Лабораторная работа. BioLink U-Match 3.5

Теоретическая часть

Описание ПО BioLink Authentication Center

Задание 1. Установка BioLink Windows Logon

Задание 2. Первый вход в систему по отпечатку пальца или по паролю

Задание 3. Разблокирование рабочей станции

Задание 4. Создание новой персоны

Задание 5. Установка BioLink Password Vault

Задание 6. Написание сценария для DialUp – подключения.

Задание 7. Написание сценария для программы TrueCrypt

Задание 8. Написание сценария для почтового сервера.

Контрольные вопросы

Список использованных источников.

Задания для самостоятельной работы.

1. Разработайте систему идентификация по клавиатурному подчерку.

2. В чем недостатки идентификации (дактилоскопический узор, лицо, радужной оболочке глаза, строению руки или пальца, голосу, походке, клавиатурному подчерку и т.д.).

Тема 7. Методы защиты программного обеспечения от несанкционированного использования. (ПК-1)

Лекция.

Методы защиты программного обеспечения от несанкционированного использования для идентификации и аутентификации пользователей. Методы защиты программного обеспечения основных способов защиты распространения ПО. Условно-бесплатное программное обеспечение. Использование электронных ключей для защиты ПО. Угроза нарушения функциональности модуля защиты.

Лабораторные работы.

Лабораторная работа. Разработка программного продукта для работы с ЭЦП на основе электронных ключей ruToken

Теоретическая часть

Описание продукта.

Задание 1. Реализация процедуры создания в памяти ruToken нового контейнера.

Задание 2. Реализация процедуры удаления из памяти ruToken контейнера. 4 Задание 3. Реализация процедуры проверки существования контейнера ключей

Задание 4. Реализация процедуры генерации в контейнере заданного имени ключевой пары заданного размера. 6

Задание 5. Реализация процедуры экспорта открытого ключа из контейнера7 Задание 6. Реализация процедуры просмотра открытого ключа.

Задание 7. Реализация процедуры подписи документа.

Задание 8. Реализация процедуры верификации подписи документа.

Вопросы и практические задания.

Задания для самостоятельной работы.

1. Защита данных от несанкционированного доступа.

2. Основные подходы к защите данных от несанкционированного доступа.

3. Защита программ от несанкционированного копирования.

Тема 8. Методы и средства ограничения доступа к компонентам ЭВМ (ПК-1)

Лекция.

Ограничение доступа к компонентам ЭВМ. Классификация методов защиты информации от несанкционированного копирования. Основные подходы к защите данных от несанкционированного доступа. Шифрование. Контроль доступа и разграничение доступа. Иерархический доступ к информационным ресурсам. Защита сетевого ресурса. Протоколирование доступа к файлам.

Лабораторные работы.

Лабораторная работа. Система защиты информации от несанкционированного доступа Secret Net 5.0 автономный вариант

Теоретическая часть

Задание 1. Установка программы Secret Net 5.0

Задание 2. Варианты входа в систему

Задание 3. Смена пароля.

Задание 4. Временная блокировка компьютера.

Задание 5. Смена ключей

Задание 6. Работа с конфиденциальными ресурсами

Задание 7. Изменение категории конфиденциальности.

Задание 8. Работа с конфиденциальным документом в MS Word и MS Excel

Задание 9. Печать конфиденциального документа MS Word

Задание 10. Деинсталляция программы Secret Net 5.0 (автономный вариант)

Вопросы и практические задания.

Список использованных источников

Задания для самостоятельной работы.

1. Произведите защиту данных от несанкционированного доступа.
2. Основные подходы к защите данных от несанкционированного доступа

Тема 9. Понятие обратного проектирования. (ПК-1)

Лекция.

Основные методы обратного проектирования. Отладка программ, дизассемблирование программ. Мониторы событий. Классификация средств обратного проектирования ПО.

Лабораторные работы.

Лабораторная работа. Понятие обратного проектирования.

Теоретическая часть

Основными угрозами для программного продукта, защищенного от несанкционированного использования способом ввода ключевой информации пользователем являются:

угроза нарушения функциональности модуля защиты

угроза раскрытия ключевой информации.

Реализация угрозы нарушения функциональности модуля защиты может заключаться:

в обходе модуля защиты путем модификации кода программы

в полном отключении модуля защиты путем модификации кода программы.

Реализация угрозы раскрытия ключевой информации – в выяснении путем исследования программы ключевой информации, требуемой при регистрации.

Существует несколько задач, которые злоумышленник должен решить при реализации данных угроз.

1. Задача обнаружения в коде программы модуля защиты.
2. Задача исследования модуля защиты и понимания принципов его действия.

Следует отметить, что задачи в принципе не решаемы за приемлемое время.

Это обусловлено следующими обстоятельствами.

Задача обнаружения в коде программы модуля защиты.

1. Модуль защиты занимает достаточно малый объем в общей совокупности кода программы. Задача ручного поиска блока модуля защиты размером 100 – 200 байт в общем коде программы, занимающем сотни мегабайт, без использования специализированных средств в принципе не решается за приемлемое время.

Задача обнаружения в коде программы модуля защиты.

2. Анализ кода программы в значительной степени затрудняется тем, что производится анализ не исходного текста программы на языке высокого уровня, а анализ машинного кода, сформированного компилятором. На разборку и понимание такого кода уходит значительное время даже у специалистов высокого класса в данной области. Зачастую даже анализ исходных текстов программы, написанных другим человеком, является нетривиальной задачей. Анализ же машинного кода усложняет задачу уже в тысячи раз. Недостаточно провести анализ каждой машинной команды. Как правило, при анализе машинного кода приходится увязывать в единую последовательность действий как минимум 80 – 100 байт, чтобы понять, что действительно скрыто за данной последовательностью кодов. Как правило, это очень усложняет анализ программы

Задача исследования модуля защиты и понимания принципов его действия.

Злоумышленник должен понять, каким образом построена защита, где она хранит (если хранит) ключевую информацию, где сохраняет (если сохраняет) свои метки и ключи, на каком этапе принимается решение о регистрации программы либо об отклонении регистрации. При этом злоумышленник сталкивается с проблемой анализа машинного кода, что приводит к трудностям, перечисленным в первой задаче.

Трудности реализации угроз от угрозы нарушения функциональности модуля защиты и от угрозы раскрытия ключевой информации

Вывод: отсутствие необходимости защиты ПО!!!

Продукты фирм, пренебрегающих защитой от реализации данных угроз, оказываются взломанными в числе первых.

Большой объем взломанных программ на рынке ПО говорит об обратном, – что эти угрозы вполне реальны и осуществимы.

Трудности реализации угроз от угрозы нарушения функциональности модуля защиты и от угрозы раскрытия ключевой информации

Существует множество программных продуктов, облегчающих злоумышленнику решение задач 1 и 2!!! Их реализация, в отдельных случаях доводится до автоматизма

Алгоритм решения задач 1 и 2 показывает, что основная цель, решаемая злоумышленником при взломе ПО

о анализ работы программы

о поиск в ней участка кода, отвечающего за реализацию модуля защиты

о детальное исследование принципов и механизмов работы данного модуля.

Решение задач 1 и 2 показывает, что основная цель, решаемая злоумышленником при взломе ПО.

При этом ставится задача представления машинного кода на как можно более высоком уровне с целью упрощения его понимания.

Для злоумышленника наиболее оптимальный вариант – формирование по машинному коду модуля защиты, его текста на исходном языке высокого уровня.

Под обратным проектированием (reverse engineering) понимают процесс исследования и анализа машинного кода, нацеленный на понимание общих механизмов функционирования программы, а также на его перевод на более высокий уровень абстракции (более высокий уровень языка программирования) вплоть до восстановления текста программы на исходном языке программирования.

Основными методами обратного проектирования являются

- отладка программ
- дизассемблирование программ.

Средства (инструменты) обратного проектирования.

- Отладчики
- Дизассемблеры
- Мониторы событий
- Редакторы кода.

Отладчики

Программные средства, позволяющие выполнять программу в пошаговом режиме, контролировать ее выполнение, вносить изменения в ход выполнения. Данные средства позволяют проследить весь механизм работы программы на практике и являются средствами динамического исследования работы программ

Дизассемблеры

Программные средства, позволяющие получить листинг программы на языке ассемблера, с целью его дальнейшего статического изучения. Дизассемблеры являются средствами статического исследования.

Мониторы событий

Программные средства, позволяющие отслеживать определенные типы событий, происходящие в системе. Наиболее опасными для программного обеспечения с точки зрения их защиты являются мониторы операций с реестром и мониторы файловых операций, позволяющие проследить – какая программа куда и что записывала, считывала и т.д.

Редакторы кода

Занимают отдельное место среди средств обратного проектирования. Данные средства, как правило, включают функции дизассемблирования, но позволяют также вносить изменения в код программы.

Задания для самостоятельной работы.

1. Проанализируйте основные задачи, решаемы отладчиками.
2. Перечислите основные методы дизассемблирование программ.
3. Покажите основные мониторы событий

Тема 10. Атаки на модули проверки корректности ключевой информации (ПК-1)

Лекция.

Угроза раскрытия ключевой информации. Задача обнаружения в коде программы модуля защиты. Задача исследования модуля защиты, принципов его действия.

Лабораторные работы.

Лабораторная работа. Атаки на модули проверки корректности ключевой информации.

Теоретическая часть

Для вскрытия защиты модуля проверки корректности ключевой информации в первую очередь необходимо найти в коде программы мотивация

код модуля защиты

Процедуру проверки

В большинстве программных продуктов проверка корректности ключевой информации выполняется непосредственным образом. При этом исходный текст программы выглядит приблизительно следующим образом.

Object Pascal

```
If not ValidUser(Login, Password)
```

```
then
```

```
begin
```

```
ShowMessage(„Неверный пользователь“);
```

```
Halt(1);
```

```
end;
```

C++

```
If (!ValidUser())
```

```
{
```

```
Message (“Неверный пользователь”);
```

```
Abort;
```

```
}
```

Здесь, ValidUser() – базовая процедура проверки. Ключевая информация может вводиться пользователем как в данной процедуре, так и ранее.

Object Pascal

```
If not ValidUser(Login, Password)
Then
begin
ShowMessage(„Неверный пользователь“);
Halt(1);
end;
C++
```

```
If (!ValidUser())
{
Message (“Неверный пользователь”);
Abort;
}
```

Object Pascal

```
If not ValidUser(Login, Password)
Then
Begin
ShowMessage(„Неверный пользователь“);
Halt(1);
end;
C++
```

```
If (!ValidUser())
{ Message (“Неверный пользователь”);
Abort;
}
```

PUSH AX CALL IsValidUser; POP AX OR AX, AX JZ continue PUSH offset str_invalid_user CALL Message CALL Abort COUNTINUE If not ValidUser(Login, Password) Object Pascal then begin ShowMessage(„Неверный пользователь“); Halt(1); end; If (!ValidUser()) C++ { Message (“Неверный пользователь”); Abort; } Компилятор Delphi Компилятор C++ Builder Assembler `6 Assembler – КМБ
PUSHAX- занесение параметра в стек PUSH – offset str_invalid_user – занесение указателя в стек
CALL- вызов процедуры (IsValidUser; Message; Abort) POP AX - вызов из стека результата OR - оператор OR JZ – условный оператор (аналог IF) , Результат ... AX- регистры стека (AX, BX, CX..) COUNTINUE – метка

Assembler PUSH AX CALL IsValidUser; POP AX В данном коде команда CALL IsValidUser осуществляет вызов процедуры IsValidUser. Передача в данную процедуру параметров (например, ссылки на ключевую информацию) осуществляется через стек командами PUSH (занесение параметра в стек) до команды CALL и POP (вызов из стека результата, возвращенного процедурой IsValidUser) после команды CALL. В представленном примере результат выполнения процедуры IsValidUser заносится в регистр AX. Assembler OR AX, AX JZ continue PUSH offset str_invalid_user CALL Message CALL Abort COUNTINUE В дальнейшем производится проверка на равенство нулю возвращенного результата (команды OR AX,AX). Если AX=0, то ключевая информация верна, производится ее регистрация и дальнейшее продолжение работы (JZ continue). В ином случае выводится сообщение о невозможности продолжения работы (PUSH offset str_invalid_user; CALL Message) и завершение работы программы (CALL Abort).

- Hex: Asm: Means
- 75 or 0F85 jne jump if not equal
- 74 or 0F84 je jump if equal
- EB jmp jump directly to
- 90 nop no operation
- 77 or 0F87 ja jump if above

- 0F86 jna jump if not above
- 0F83 jae jump if above or equal
- 0F82 jnae jump if not above or equal
- 0F82 jb jump if below
- 0F83 jnb jump if not below
- 0F86 jbe jump if below or equal
- 0F87 jnbe jump if not below or equal
- 0F8F jg jump if greater
- 0F8E jng jump if not greater
- 0F8D jge jump if greater or equal
- 0F8C jnge jump if not greater or equal
- 0F8C jl jump if less
- 0F8D jnl jump if not less
- 0F8E jle jump if less or equal
- 0F8F jnle jump if not less or equal

Assembler В данной ситуации, после обнаружения представленного выше программного кода модуля защиты, взломщик может осуществить атаку следующим образом.

- Заменить команду условного перехода JE continue на команду безусловного перехода JNE continue. В данном случае, регистрация программы будет осуществляться в любом случае, вне зависимости от правильности ввода ключевой информации.
- Изменить в процессе работы программы содержимое регистра AX после команды POP AX, либо значение регистра флагов после команды OR AX,AX. В данном случае злоумышленник вынужденно заставляет модуль защиты работать по нужной ветке.
- Исследовать работу процедуры IsValidUser вручную с целью выяснения ключевой информации.

Реализация первых двух типов атак называется «жестким» взломом программного продукта, так как он требует модификации кода программы. Первые два типа взлома позволяют осуществить взлом программного продукта в достаточно короткие сроки, не прилагая к этому слишком больших усилий (можно привести примеры, когда такие защиты взламывались в течение 10 секунд).

Реализация третьего типа атак называется «мягким» взломом программного продукта и во многих случаях является более предпочтительным для злоумышленника, хотя и требует от него несколько больших временных затрат. Достоинством для злоумышленника третьего типа взлома является то, что иногда, исследовав логику работы процедуры IsValidUser, можно не только вычислить ключевую информацию, но и написать генератор ключевой информации для последующего использования другими пользователями. Это возможно сделать, если разработчик вложил в модуль защиты непосредственную связь между идентификатором пользователя и его аутентификатором (ключевой информацией).

Отслеживание обращений к этим адресам позволит локализовать код, отвечающий за проверку адекватности ключевой информации.

Довольно часто злоумышленником производится исследование содержимого ОЗУ на осмысленные последовательности символов, а также отслеживание обращений к адресам, по которым хранятся эти последовательности (например, “Invalid Registration”, “Password Fail”, “Error” т.д.). Как правило, эти сообщения находятся недалеко от модулей защиты, отвечающих за проверку корректности ключевой информации. По обращению к адресам, хранящим данные сообщения, также можно локализовать код проверки адекватности ключевой информации. Перечисленные элементы являются наиболее уязвимыми с точки зрения взлома в процедуре IsValidUser. Как правило, передача параметров в функции и их возврат осуществляется через 32-битные регистры EAX, EBX, а также используя регистры ESI и EDI для указания на используемые данные. Совершив “мягкий” взлом (получив ключевую информацию), злоумышленник снимает все проблемы «Жесткий» взлом иногда затруднителен: проверка корректности осуществляется в нескольких местах программы и различными способами.

- Hex: Asm: Means
- 75 or 0F85 jne jump if not equal

- 74 or 0F84 je jump if equal
- EB jmp jump directly to
- 90 nop no operation
- 77 or 0F87 ja jump if above
- 0F86 jna jump if not above
- 0F83 jae jump if above or equal
- 0F82 jnae jump if not above or equal
- 0F82 jb jump if below
- 0F83 jnb jump if not below
- 0F86 jbe jump if below or equal
- 0F87 jnbe jump if not below or equal
- 0F8F jg jump if greater
- 0F8E jng jump if not greater
- 0F8D jge jump if greater or equal
- 0F8C jnge jump if not greater or equal
- 0F8C jl jump if less
- 0F8D jnl jump if not less
- 0F8E jle jump if less or equal
- 0F8F jnle jump if not less or equal

Задания для самостоятельной работы.

1. Обнаружение в коде программы модуля защиты.
2. Исследования модуля защиты, принципов его действия.
3. Классификация средств обратного проектирования ПО.

Тема 11. Защита программ от изучения. (ПК-1)

Лекция.

Общие принципы защиты от изучения. Защита от отладки. Защита от дизассемблирования. Защита от трассировки по прерываниям

Лабораторные работы.

Лабораторная работа. Защита программ от дизассемблирования.

Цель: освоить технологию работы с дизассемблером и декомпилятором

Теоретическая часть

Дизассемблер — транслятор, преобразующий машинный код, объектный файл или библиотечные модули в текст программы на языке ассемблера.

По режиму работы с пользователем делятся на

- Автоматические
- Интерактивные

Примером автоматических дизассемблеров может служить Sourcer. Такие дизассемблеры генерируют готовый листинг, который можно затем править в текстовом редакторе. Пример интерактивного — IDA. Он позволяет изменять правила дизассемблирования и является весьма удобным инструментом для исследования программ.

Дизассемблеры бывают однопроходные и многопроходные. Основная трудность при работе дизассемблера — отличить данные от машинного кода, поэтому на первых проходах автоматически или интерактивно собирается информация о границах процедур и функций, а на последнем проходе формируется итоговый листинг. Интерактивность позволяет улучшить этот процесс, так как просматривая дампы дизассемблируемой области памяти, программист может сразу выделить строковые константы, дать содержательные имена известным точкам входа, прокомментировать разобранные им фрагменты программы.

Чаще всего дизассемблер используют для анализа программы (или ее части), исходный текст которой неизвестен — с целью модификации, копирования или взлома. Реже — для поиска ошибок (багов) в программах и компиляторах, а также для анализа оптимизации создаваемого компилятором машинного кода. Обычно однопроходный дизассемблер (как и построчный ассемблер) является составной частью отладчика.

Защита от дизассемблирования

Первое направление защиты, как правило, реализуется значительно легче, чем второе, поэтому будет приведен лишь краткий обзор данного направления. При реализации защиты программ от дизассемблирования можно применять различные приемы.

Среди них наиболее часто используемым и эффективным приемом является зашифровка и \ или запаковка отдельных участков исходного кода или всего кода целиком, при этом необходимо позаботиться о распаковке \ расшифровке программы на точке входа. Таким образом, при просмотре исполняемого машинного кода исполняемого файла вместо рабочего кода программы будет отображен лишь бессмысленный набор операций. При реализации защиты от дизассемблирования используется также множество приемов, которые реализуются с целью запутать потенциального взломщика. Можно привести несколько примеров такого вида приемов:

- увеличение исходного кода программы добавлением множества «бессмысленных» операций, а рабочий участок программы записать в определенное место этого множества;
- замена местами адресов обработчиков (векторов) прерываний, например, поменять местами вектор прерывания видео сервиса (INT 10h) с вектором прерывания сервиса DOS (INT 21h), после такой замены для вызова из программы какой-либо функции прерывания INT 21h необходимо пользоваться вызовом прерывания INT 10h.

Для достижения наиболее надежной и эффективной защиты используется комбинация нескольких приемов.

Защита от отладки Для защиты программы от трассировки отладчиком также существует несколько способов. Наиболее распространенными являются два из них.

Первый способ

Идея:

При трассировке программы команды выполняются по команде человека, поэтому длительность выполнения операций (время от начала одной операции до начала следующей) изменяется. Поэтому в программу можно включать точки для проверки времени выполнения одинаковых участков кода программы. Если время выполнения выполнения одинаковых участков различна, то это означает, что программа трассируется в данный момент, необходимо выйти из программы, иначе - продолжить выполнение.

Алгоритм реализации:

1. Запомнить текущее время;
2. Выполнить контрольный участок кода;
3. Запомнить текущее время и разность текущего и предыдущего запомненного времени;
4. Выполнить контрольный участок кода повторно;
5. Сравнить разность текущего времени и предыдущего запомненного текущего времени с предыдущей запомненной разностью;
6. Если разности совпадают, продолжить выполнение, иначе — выйти из программы.

- метаморфическое преобразование кода программы, позволяющее защитить программу от дизассемблирования и модификации;
- защита ключом отдельных участков кода программы (поддерживается только в зарегистрированной версии);
- полное разрушение логики защищенных фрагментов кода, не позволяющее анализировать программу с помощью дизассемблера или отладчика;
- обнаружение и противодействие отладчикам SoftIce, NtIce, TD и др.;
- защита точки входа;
- защита от модификации кода;

- защищенная работа с реестром, не позволяющая программам вроде RegMon определить, к какому ключу реестра обращается твоя программа;
- технология "динамического импорта", которая разрушает имена всех импортируемых функций, а также не использует функцию GetProcAddress;
- сжатие ресурсов и исполнимого кода приложения;
- поддержка коротких серийных номеров (12 символов);
- поддержка внешнего генератора серийных номеров с OLE/DLL-интерфейсом;
- технология OneTouch Trial (о ней читай ниже).

Самое главное, что нас интересует – это метаморфическое преобразование кода программы и поддержка серийных номеров. Метаморфическое кодирование позволяет изменить код программы до неузнаваемости и запутать отладчик и человека, который запустил этот отладчик.

Декомпилятор.

Он переводит двоичный код в символьный на языке команд какого-нибудь языка. Например, диасемблеры, деклиппер и многие другие. Эти средства появились раньше отладчиков, т.к. вначале не было архитектуры со встроенными средствами отлаживания программ. С помощью декомпиляторов можно изменять исходный код программы. Допустим необходимо внести крупные изменения в код программы. Прямая вставка двоичных кодов не помогает, т.к. нарушается расположение меток перехода и процедур. Программа – это линейка кода, по которой нужно перемещаться нелинейно, переходить с определенным смещением. Если линейка удлиняется из-за добавления чего-то в середине, все смещения будут показывать не туда куда нужно. Повторная перекомпиляция вписывает новые смещения.

Среди декомпиляторов можно выделить: Hacker-VIEW (HVIEW), IDA (интерактивный дизасемблер).

С помощью Hacker-VIEW можно посмотреть любой исполняемый файл по любому смещению. Можно выполнить какую-то часть программы. Это позволяет расшифровывать программы и обходить защиту от дизасемблирования. Этот декомпилятор «понимает» как старые форматы исполняемых файлов DOS-COM и DOS-EXE, так и форматы исполняемых файлов Windows.

IDA очень мощное средство работы с ассемблерными текстами программ. Обладает широким спектром возможностей, имеет более удобный интерфейс, чем Hacker-VIEW. Очень хорошо предусмотрена архитектура работы программ в Windows (такие вещи, как DLL, расширенный режим работы с памятью и т.д.).

Декомпиляторы программ занимают свое место в инструментарии взломщика. В основном это совместное использование с отладчиками.

Второе средство – отладчики.

Отладчики позволяют запускать отдельные части программы и следить за изменениями, которые она производит, за результатами ее работы.

Защите от отладки не стоит уделять много времени, т.к. все возможные хитрости и приемы уже известны и взломщикам и программистам. Так же и шифрование. Любой хакер, если получает заказ на взлом, имеет доступ к нормальной копии программы. То есть он ее либо может купить, либо попользоваться ею на компьютере покупателя.

Среди отладчиков выделим: SOFTICE и WINICE.

С появлением Windows отладка программ стала на порядок проще и намного удобнее дизасемблирования. Принципиально изменился стиль некоторых атак на защиту программ. Теперь не надо шаг за шагом смотреть на ассемблерный код, «продираться» сквозь дебри незначущих кодов и защит. Теперь надо отловить нужное событие и понять как на него реагирует программа. Это, конечно, не всегда бывает так просто, как выглядит на словах. Как и ранее, отладка требует знание архитектуры операционной системы.

Неважно насколько сложным был бы механизм защиты, все сводится к простейшей проверке или дешифровке. И взлом, в случае с проверкой, можно разбить на два этапа: установка «брейков» на «подозрительные» флаги, обнаруженные в процедуре защиты; анализ обращений к флагам. По реакции программы можно судить флаг это или просто переменная.

Практическая часть.

1. Изучить теоретическую часть. Сделать записи в тетради.
2. Провести сравнение декомпилятора и отладчика. По данным составить таблицу сравнений.
3. Ответить на контрольные вопросы

Контрольные вопросы:

1. Что такое дизассемблер?
2. Как происходит защита программ от дизассемблирования?
3. Как происходит защита программ от отладки?
4. Какие виды отладчиков вы знаете?
5. Что такое декомпилятор?
6. Какие он функции выполняет?
7. Что такое трассировка?
8. Какие виды дизассемблеров вам известны?
9. Какие приемы дизассемблирования вам известны?

Задания для самостоятельной работы.

1. Защита программ от изучения.
2. Защита данных от несанкционированного доступа.
3. Защита файлов от изменения.
4. Надежность систем ограничения доступа.

Тема 12. Защита от разрушающих программных воздействий. (ПК-1)

Лекция.

Деструктивные программы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия предупреждения разрушающего воздействия. Понятие изолированной программной среды.

Лабораторные работы.

Лабораторная работа. RuToken и PGP

Теоретическая часть

Установка

Настройка RuToken

Создание ключей в памяти RuToken

Использование ключей хранящихся в памяти RuToken

Вопросы и практические задания.

Источники литературы

Теоретическая часть

PGP – это криптографическая (шифровальная) программа с высокой степенью надежности, которая позволяет пользователям обмениваться информацией в электронном виде в режиме полной конфиденциальности.

Главное преимущество этой программы состоит в том, что для обмена зашифрованными сообщениями пользователям нет необходимости передавать друг другу тайные ключи т.к. эта программа построена на новом принципе работы – публичной криптографии или обмене открытыми (публичными) ключами, где пользователи могут открыто посылать друг другу свои публичные ключи с помощью сети «Интернет» и при этом не беспокоиться о возможности несанкционированного доступа каких-либо третьих лиц к их конфиденциальным сообщениям.

В PGP применяется принцип использования двух взаимосвязанных ключей: открытого и закрытого.

К закрытому ключу имеете доступ только вы, а свой открытый ключ вы распространяете среди своих корреспондентов.

Установка.

Для выполнения этого задания необходимо сделать следующее:

Зайдите на сайт разработчика www.pgpru.ru Скачайте новую версию продукта.

Следуйте инструкциям процесса установки.

Настройка RuToken

Запустите утилиту PGP Desktop:

В меню Tools выберите пункт PGP Options...

Перейдите на закладку Keys:

В выпадающем списке Synchronize with smart cards and tokens выберите пункт Other... :

И укажите путь к библиотеке PKCS#11 ! файл rtPKCS11.dll (по умолчанию библиотека находится в папке %SYSTEMROOT%\SYSTEM32), нажмите кнопку Открыть:

Закройте окно PGP Options, нажав на кнопку Ok. На этом настройка поддержки Rutoken завершена.

Создание ключей в памяти RuToken

Для создания ключевой пары и размещения ее в защищенной памяти токена в утилите PGP Desktop, в меню File выберите пункт New PGP Key....:

Откроется мастер генерации ключей:

Подключите Rutoken, в памяти которого будут записаны ключи шифрования. Дождитесь, пока светодиод перестанет мигать.

После этого станет доступной опция Generate Key on Token. Отметьте ее галочкой и нажмите кнопку Далее:

Заполните поля Full Name и Primary Email, при необходимости задайте дополнительные параметры для ключей шифрования, нажав кнопку Advanced. Нажмите кнопку Далее:

Вам предложат ввести PIN!код для доступа к памяти Rutoken. Введите текущий PIN!код

Пользователя Rutoken и нажмите кнопку Далее:

Начнется процесс создания ключей и записи их в защищенную память Rutoken. Процесс может занять 1 - 3 минуты.

8. По окончании процесса генерации и записи ключей нажмите кнопку Далее:

9. Появится окно публикации открытого ключа в PGP Global Directory. В случае необходимости публикации нажмите кнопку Далее и следуйте указаниям Мастера. Иначе нажмите кнопку Skip:

10. Вы вернетесь в основной экран утилиты PGP Desktop. В случае успешной генерации и записи ключевой пары в окне All Keys будет отображаться запись, соответствующая сгенерированной ключевой паре и индикатор Validity будет зеленым:

11. При отключении токена индикатор Validity становится серым, что указывает на отсутствие доступа к ключевой паре.

Использование ключей хранящихся в памяти RuToken

1. В дальнейшем, для использования ключей требуется предварительно подключить Rutoken.

2. При выборе типа ключа (там, где это требуется) выбирать Public Key User:

Из списка ключей шифрования выбрать требующийся:

Ввести PIN!код Пользователя* и нажать кнопку ОК:

* PIN_код Пользователя по умолчанию: 12345678

Вопросы и практические задания.

1. Создайте пару ключей на памяти RuToken'a
2. Закодируйте ряд файлов (на выбор преподавателя) с использованием RuToken'a
3. Протестируйте результат (зашифрованные файлы)
4. Создайте новый zip-контейнер с использованием RuToken'a
5. Настройте почтовый адрес для защищенного обмена информацией
6. Создайте защищенный виртуальный диск с использованием RuToken'a
7. Создайте log о использовании почтовых клиентов
8. Зашифруйте сетевую папку с использованием RuToken'a

9. Добавьте user'a, допущенного для пользования сетевой папкой

10. Удалите ключи с памяти RuToken'a

11. 10. Удалите PGP

Источники литературы

1. www.pgpru.ru

2. www.rutoken.ru

Задания для самостоятельной работы.

1. Защита от разрушающих программных воздействий.

2. Компьютерные вирусы как особый класс разрушающих программных воздействий.

3. Необходимые и достаточные условия недопущения разрушающего воздействия.

4. Изолирование программной среды

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

5 семестр

- посещаемость – 10 баллов
- текущий контроль – 46 баллов
- контрольные срезы – 2 среза: 8 баллов, 6 баллов
- премиальные баллы – 20 баллов
- ответ на экзамене: не более 30 баллов

Распределение баллов по заданиям:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки

1.	Предмет и задачи программно-аппаратной защиты информации.	Доклад	3	<p>Доклад студента предполагает организацию совместной дискуссии автора, преподавателя и студентов по вопросам, связанных с определенным разделом, проблеме или способе реализации т.п. После доклада все члены группы активно участвуют в обсуждении, добавляют информацию, задают вопросы и делают замечания докладчику.</p> <p>Основные качества доклада подлежащего оценке:</p> <p>3 балла – четко сформулированы проблемы, соответствующая теме доклада; полнота раскрытия материала темы доклада; в основной части логично, связно и полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; нет замечаний по презентационному материалу; правильно используются и приведены авторитетные источники информации; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>2 балла – четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; в основной части полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; есть замечания по презентационному материалу; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>1балл - четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; недостаточно полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; есть замечания по презентационному материалу; слабо выполнена задача заинтересованности слушателей в группе.</p>
2.	Системы идентификации	Лабораторная работа	8	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>5 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
3.	Доступ к данным со стороны процесса.	Лабораторная работа	8	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>5 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>

4.	Программно-аппаратные комплексы защиты информации.	Лабораторная работа(контрольный срез)	8	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 5 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы. 2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.
5.	Электронный идентификатор ruToken.	Лабораторная работа	8	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 5 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы. 2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.
6.	Система биометрической идентификации BioLink.	Лабораторная работа	3	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 3 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы. 1 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.
		Тестирование(контрольный срез)	6	Оценка теста по текущему разделу или теме дисциплины 6 балла – студент правильно отвечает на 50-100% вопросов в тесте. 2 балла - студент правильно отвечает на 25-50% вопросов в тесте.

7.	Методы защиты программного обеспечения от несанкционированного использования.	Лабораторная работа	8	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>5 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
8.	Методы и средства ограничения доступа к компонентам ЭВМ	Лабораторная работа	8	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>5 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
9.	Посещаемость		10	<p>10 баллов – стопроцентное посещение занятий студентом</p> <p>7-9 баллов – посещаемость студента составляет не менее 80 % занятий</p> <p>4-6 баллов – посещаемость студента составляет не менее 50 % занятий</p> <p>1-3 балла – посещаемость студента составляет не менее 25 % занятий</p>
10.	Премиальные баллы		20	<p>Дополнительные премиальные баллы могут быть начислены:</p> <ul style="list-style-type: none"> - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20

11.	Ответ на экзамене	30	<p>Оценка «удовлетворительно»- студент имеет достаточный минимальный объем знаний по дисциплине; студентом усвоена основная литература, рекомендованная учебной программой; студент умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; студент умеет делать выводы без существенных ошибок;</p> <p>Оценка «хорошо» – «достаточно полные и систематизированные знания по дисциплине;» умение ориентироваться в основном теориях, концепциях и направлениях дисциплины и давать им критическую оценку; использование научной терминологии, лингвистически и логически правильное изложение ответа на вопросы, умение делать обоснованные выводы; владение инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач; усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; средний уровень сформированности заявленных в рабочей программе компетенций.</p> <p>- Оценка «отлично» – систематизированные и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; точное использование научной терминологии систематически грамотное и логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; выраженная способность самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; умение ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин; творческая самостоятельная работа; активное участие в групповых обсуждениях.</p>
-----	-------------------	----	--

12.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы	10	<p>Доклад студента предполагает организацию совместной дискуссии автора, преподавателя и студентов по вопросам, связанных с определенным разделом, проблеме или способе реализации т.п. После доклада все члены группы активно участвуют в обсуждении, добавляют информацию, задают вопросы и делают замечания докладчику.</p> <p>Основные качества доклада подлежащего оценке:</p> <p>10 баллов – четко сформулированы проблемы, соответствующая теме доклада; полнота раскрытия материала темы доклада; в основной части логично, связно и полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; нет замечаний по презентационному материалу; правильно используются и приведены авторитетные источники информации; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>8 баллов – четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; в основной части полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; есть замечания по презентационному материалу; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>6 баллов - четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; недостаточно полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; есть замечания по презентационному материалу; слабо выполнена задача заинтересованности слушателей в группе.</p>
13.	Итого за семестр	100	

6 семестр

- посещаемость – 10 баллов
- текущий контроль – 42 балла
- контрольные срезы – 2 среза: 10 баллов, 8 баллов
- премиальные баллы – 20 баллов
- ответ на экзамене: не более 30 баллов

Распределение баллов по заданиям:

№ темы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мак. кол-во баллов	Методика проведения занятия и оценки
--------	------------------------------------	---------------------------------	--------------------	--------------------------------------

1.	Понятие обратного проектирования.	Лабораторная работа	20	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 20 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 14 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы. 7 баллов - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы
2.	Атаки на модули проверки корректности ключевой информации	Лабораторная работа(контрольный срез)	10	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 10 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 8 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы. 4 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы
3.	Защита программ от изучения.	Лабораторная работа	20	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 20 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 14 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы. 7 баллов - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы
4.	Защита от разрушающих программных воздействий.	Лабораторная работа(контрольный срез)	8	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 5 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы. 3 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы

		Практическое задание для практической подготовки	2	<p>Практические задания выполняются по тематике практических занятий.</p> <p>2 баллов – практическое задание выполнено в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>1 балла – практическое задание выполнено, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p>
5.	Посещаемость		10	<p>10 баллов – стопроцентное посещение занятий студентом</p> <p>7-9 баллов – посещаемость студента составляет не менее 80 % занятий</p> <p>4-6 баллов – посещаемость студента составляет не менее 50 % занятий</p> <p>1-3 балла – посещаемость студента составляет не менее 25 % занятий</p>
6.	Премияльные баллы		20	<p>Дополнительные премияльные баллы могут быть начислены:</p> <ul style="list-style-type: none"> - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20

7.	Ответ на экзамене	30	<p>Оценка «удовлетворительно»- студент имеет достаточный минимальный объем знаний по дисциплине; студентом усвоена основная литература, рекомендованная учебной программой; студент умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; студент умеет делать выводы без существенных ошибок;</p> <p>Оценка «хорошо» – «достаточно полные и систематизированные знания по дисциплине;» умение ориентироваться в основном теориях, концепциях и направлениях дисциплины и давать им критическую оценку; использование научной терминологии, лингвистически и логически правильное изложение ответа на вопросы, умение делать обоснованные выводы; владение инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач; усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; средний уровень сформированности заявленных в рабочей программе компетенций.</p> <p>- Оценка «отлично» – систематизированные и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; точное использование научной терминологии систематически грамотное и логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; выраженная способность самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; умение ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин; творческая самостоятельная работа; активное участие в групповых обсуждениях.</p>
----	-------------------	----	--

8.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы	10	<p>Доклад студента предполагает организацию совместной дискуссии автора, преподавателя и студентов по вопросам, связанных с определенным разделом, проблеме или способе реализации т.п. После доклада все члены группы активно участвуют в обсуждении, добавляют информацию, задают вопросы и делают замечания докладчику.</p> <p>Основные качества доклада подлежащего оценке:</p> <p>10 баллов – четко сформулированы проблемы, соответствующая теме доклада; полнота раскрытия материала темы доклада; в основной части логично, связно и полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; нет замечаний по презентационному материалу; правильно используются и приведены авторитетные источники информации; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>8 баллов – четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; в основной части полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; есть замечания по презентационному материалу; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>6 баллов - четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; недостаточно полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; есть замечания по презентационному материалу; слабо выполнена задача заинтересованности слушателей в группе.</p>
9.	Итого за семестр	100	

Итоговая оценка по экзамену выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
85 - 100 баллов	Отлично
70 - 84 баллов	Хорошо
50 - 69 баллов	Удовлетворительно
Менее 50	Неудовлетворительно

4.2 Типовые оценочные средства текущего контроля

Доклад

Тема 1. Предмет и задачи программно-аппаратной защиты информации.

Темы докладов.

1. Средства защиты информации

2. Аппаратные средства защиты информации

3. Задачи аппаратного обеспечения защиты информации
4. Виды аппаратных средств защиты информации
5. Программные средства защиты информации
6. Средства архивации информации
7. Антивирусные программы
8. Криптографические средства
9. Идентификация и аутентификация пользователя
10. Защита информации в КС от несанкционированного доступа
11. Другие программные средства защиты информации

Лабораторная работа

Тема 2. Системы идентификации

Лабораторная работа. Защита компьютера и данных с помощью ruToken

Теоретическая часть

Задание 1. Установка программного продукта.

Задание 2. Вход в Windows с помощью ruToken

Задание 3. Использование ruToken и Rohos Logon Key в сети

Утилита для Управления USB ключами

Утилита - Rohos Remote Config

MSI пакет для установки в сети

Задание 4. Настройка ruToken в Rohos Logon Key

Задание 5. Настройка дополнительных опций

Задание 6. Настройка пользователей

Задание 7. Настройка электронного ключа.

Вопросы и практические задания

Список литературы

Теоретическая часть.

Теперь популярный идентификатор ruToken можно использовать в программах Rohos Logon Key как единый Ключ для входа в Windows и защиты данных. Программа Rohos Logon Key полноценно работает в Windows Vista, а также поддерживает авторизацию на удаленный рабочий стол с помощью ruToken.

Rohos Logon Key – это программа, взаимодействующая с различными usb-токенами, флэш-картами, смарт-картами и usb-флешками. Основная

функция программы – настройка входа в систему путём идентификации пользователя по электронному ключу.

Разработчик: Tesline-Service

Сайт программы: www.rohos.ru

Категория программы: Условно бесплатная (испытательный срок) Интерфейс: Русский

Версия: 2.5

Размер файла: 1934.688 кб

Система: Windows 98/ME/2000/XP

Задание 1. Установка программного продукта.

При установки программный продукт даст о себе краткую информацию, потребует соглашение с лицензией и предоставит выбор пути установки.

После запуска программа откроет окно.

Задание 2. Вход в Windows с помощью ruToken.

Программа Rohos Logon Key устанавливает надежную двухфакторную аутентификацию, когда доступ в Windows можно получить, только обладая USB токеном, и зная некоторый пароль (PIN-код). Все что должен сделать пользователь - подключить ruToken к USB-порту и набрать PIN-код.

Rohos Logon Key единственная программа, которая полноценно работает в Windows Vista, а также поддерживает авторизацию на удаленный рабочий стол с помощью ruToken.

Преимущества использования ruToken в Rohos Logon:

- Полноценная поддержка Windows Vista включая: Доступ на удаленный рабочий стол, автоматическая смена пароля по требованию Администратора, работа в Windows Active Directory, поддержка UAC - получение пароля администратора с ruToken в диалоге запроса полномочий.

Узнать подробнее: Rohos Credential Provider.

- Аварийный вход - помогает войти в Windows при утере или поломке ruToken.

- PIN код по умолчанию - если установить PIN код 1111, тогда программа Rohos Logon Key не будет его запрашивать у пользователя.

- Возможность использования нескольких ruToken для входа на один компьютер, и наоборот одного брелка для нескольких компьютеров.

- Rohos Logon Key занимает 4кб на rutoken и совместим с другими программами, использующими ruToken.

Задание 3. Использование ruToken и Rohos Logon Key в сети

Rohos Logon Key поддерживает работу в рамках сети Windows Active Directory. Серверная версия Rohos Logon Key позволяет легко настраивать программу и USB ключ eToken на множестве компьютерах удаленно.

Серверная версия включает в себя две утилиты:

- Утилита управления token - используется для настройки всех token для аутентификации на рабочих станциях в сети (создание/удаление профайлов на token, создание резервной копии, установка PIN кода, настройка eToken на удаленный рабочий стол).

- Утилита Rohos Remote Admin - позволяет менять настройки Rohos Logon Key на удаленном компьютере, подключенном к Active Directory. Позволяет изменять следующие настройки: разрешение входа только по eToken, действие после извлечения token, блокировка token для пользователей и др.

- MSI пакет установки программы.

Утилита для Управления USB ключами

С помощью этой утилиты Администратор сети может на своем рабочем месте настроить новый USB ключ для авторизации на любой компьютер в сети и выдать его пользователю. Программа Rohos поддерживает авторизацию в Windows Domain, Active Directory и удаленный рабочий стол.

Функции:

- Настройка USB Ключа для аутентификации на заданном компьютере в сети;
- Редактирование logon профайлов;
- Создание универсальных профайлов для авторизации на любом компьютере в сети в качестве Администратора.
- Копирование профайлов между USB ключами;
- Установка ПИН кода ключа ;
- Создание резервной копии содержимого USB ключа (login профайлов) и восстановление профайлов из копии.
- Настройка USB flash drive для авторизации к удаленному рабочему столу . Это позволяет не устанавливать программу на каждый компьютер в сети.

Для правильной работы программы, необходимо настроить USB ключ в соответствии с настройками сетевого окружения. Это можно сделать с помощью диалога редактирования профайлов на USB ключе:

- Если авторизация пользователя производится в домен, непосредственно на клиентской машине или через терминальный сервер:

Поле Domain должно быть: "\\название домена";

- Если авторизация пользователя производится только на терминальный сервер:

Поле Domain должно быть: "имя компьютера терминального сервера";

- Если поле Domain пустое, это означает, что данный профайл применим на любом компьютере для любого типа авторизации.

Утилита - Rohos Remote Config

Позволяет Администратору изменять настройки "Rohos Logon Key" на удаленном компьютере подключенном к ActiveDirectory.

Преимущества:

- Список компьютеров на которых установлен Rohos Logon Key.
- Позволяет менять удаленно все настройки программы Rohos Logon на компьютере в Windows Active Directory;
- Позволяет удаленно настраивать USB ключ;
- Удаленная установка Rohos Logon Key на компьютер в сети с помощью MSI инсталлятора.

MSI пакет для установки в сети

Для быстрой установки программы в компьютерной сети предлагается использовать MSI пакет.

При запуске пакета с помощью msixec.exe можно задавать опции программы:

- LOGON_MODE=2 (автоматически выбирается, если не задано) Указать режим авторизации (logon): 1 - Окно Приветствия Rohos (GINA модуль, rohos_ui.dll) 2 - Окно Приветствия Windows XP + Rohos
- 3 - Окно авторизации Windows (msgina.dll)(Перед использованием этого параметра прочитайте описание режимов)

LOGON_CAPTION="Вход в Windows "

(default ="Вход в Windows")

заголовок окна авторизации (крупным шрифтом)

LOGON_TEXT=""

(default = "")

текст, который будет виден всем в окне авторизации.

DISABLE_LOG=1

(default =0)

Отключить запись LOG файлов в программе.

USB_KEY_LOGIN_ONLY=1

(default =0)

Запретить всем входить в систему по паролю, разрешается использовать только USB ключ!

(Администратор может использовать Safe mode для входа по паролю)

USB_REMOVAL=1

(default =0)

Заблокировать компьютер при отключении USB ключа . (эта опция переопределяет локальную настройку)

DISABLE_SHUTDOWNDLG=1

(default =0)

Не заменять стандартный диалог выключения компьютера.

DISABLE_CENTER=1

(default =0)

Запретить открывать Rohos и менять настройки.

REG_NUMBER=""

(default =0)

Задать регистрационный номер (лицензия)

LockUSBKey ="1"

Блокирование доступа к USB носителям.

"1" - блокировать только USB ключ, который используется в программе.

"All" - блокировать все USB носители.

"0" - отключить блокирование (по умолчанию).

Задание 4. Настройка ruToken в Rohos Logon Key.

В главном окне программы открыть окно "Опции"

В этом окне как тип устройства, которое будет использовано как ключ для входа, следует выбрать ruToken (эта опция может быть установлена по умолчанию в параметрах MSI пакета)

В этом окне можно установить различные опции для USB ключа.

Подробности можно узнать в справке.

Настраивать ruToken для входа в систему необходимо в окне "Настроить ключ"

Задание 5. Настройка дополнительных опций.

Программа предоставляет возможность настроить диалоговое окно входа в систему. Здесь доступна настройка картинок на электронный ключ, фоновый рисунок экрана, текстового приветствия и дополнительного сообщения.

Задание 6. Настройка пользователей.

Программа позволяет настроить не только тип учётной записи пользователя, но и его время пребывания в системе. Настройка точного времени доступа и времени на работу пользователя будет крайне полезна для организаций со строгим рабочим графиком.

Задание 7. Настройка электронного ключа.

Для того, что бы настроить выбранный ключ под пользователя (которого можно выбрать, нажав на строку «Изменить»), нужно выбрать usb- ключ из списка предлагаемых. Затем ввести пароль на вход в систему.

В этом же окне можно установить новый PIN код для ключа, снять блокировку с заблокированного ключа, и настроить аварийный вход. Для выбора того или иного действия следует нажимать на выделенные синим строки (Установить PIN код, снять блокировку, настроить аварийный вход). Блокировка ставится на ключ после неудачных попыток ввода пинкода.

Для того, что бы настройки ключа вступили в силу, нужно нажать на кнопку «Настроить USB Ключ»

Задание 8. Настройка аварийного входа в систему.

Во избежании потери доступа к компьютеру из-за потери ключа или его неисправности следует настроить аварийный вход в систему, который предложит пользователю заполнить ответы на несколько вопросов.

Задание 9. Смена пароля на вход в систему.

Программа так же позволяет сменить пароль на вход в систему. Стоит заметить, что при попытке смены пароля программа потребует ввода PIN кода ключа. Так же программа может создавать сложные пароли, состоящие из набора букв и цифр. Задача воспроизведения человеком такого пароля сильно усложняется, что даёт дополнительную защиту от нежелательного входа в систему злоумышленника.

Вопросы и практические задания

1. Можно ли сделать вход в систему только по usb-ключу?
2. Как настроить вход в систему для нескольких пользователей
3. Как ограничить время работы пользователя с 9 утра до 6 вечера?
4. Как настроить систему, что бы работать под конкретным пользователем можно было только при наличии включенного ключа?
5. Как создать сложный пароль на вход в систему?

Список литературы

1. Rohos Logon Key. Руководство пользователя (RohosWelcomeUserGuide.pdf)
2. Сайт разработчика [Электронный ресурс] // компания «Rohos»
3. режим доступа: www.rohos.ru

Тема 3. Доступ к данным со стороны процесса.

Лабораторная работа. Управление доступом к файловым ресурсам

Цель работы: Освоение навыков управления доступом пользователей к файлам и папкам с целью защиты информации от несанкционированного доступа

Теоретическая часть

Файловые системы современных операционных систем при соответствующей настройке эффективно обеспечивают безопасность и надежность хранения данных на дисковых накопителях. Для операционных систем Windows стандартной является файловая система NTFS.

Устанавливая для пользователей определенные разрешения для файлов и каталогов (папок), администраторы могут защитить информацию от несанкционированного доступа. Каждый пользователь должен иметь определенный набор разрешений на доступ к конкретному объекту файловой системы. Кроме того, он может быть владельцем файла или папки, если сам их создает. Администратор может назначить себя владельцем любого объекта файловой системы, но обратная передача владения от администратора к пользователю невозможна.

Назначение разрешений производится для пользователей или групп. Так как рекомендуется выполнять настройки безопасности для групп, то необходимо, чтобы пользователь был членом хотя бы одной группы на компьютере или в домене.

Разрешения могут быть установлены для различных объектов компьютерной системы, однако в этой работе будут рассмотрены разрешения для файлов и папок. Другие задачи, например разрешения для принтеров, решаются аналогичным образом.

Указания к проведению лабораторной работы

Для назначения разрешений для файла или папки администратор выбирает данный файл или папку и при нажатии правой кнопки мыши использует команду Свойства (Properties) и в появившемся окне переходит на вкладку Безопасность (Security).

В зоне Имя (Name) имеется список групп и пользователей, которым уже назначены разрешения для данного файла или папки.

Для добавления пользователя или группы нажмите кнопку Добавить (Add) или Удалить (Remove). При добавлении появится диалог Выбор: Пользователи, Компьютеры или Группы (SelectUsers,Computers,orGroups). Добавив пользователя или группу мы увидим этот объект в зоне Имя и выделив его, можем задать необходимые разрешения с помощью установки флажков Разрешить (Allow) или Запретить (Deny) в зоне Разрешения (Permissions).

Стандартные разрешения для файлов:

- Полный доступ (Full Control);
- Изменить (Modify);
- Чтение и выполнение (Read&Execute);
- Чтение (Read);
- Запись (Write).

Стандартные разрешения для папок:

- Полный доступ (Full Control);
- Изменить (Modify);
- Чтение и выполнение (Read&Execute);
- Список содержимого папки
- Чтение (Read);
- Запись (Write).

Разрешение Чтение позволяет просматривать файлы и папки и их атрибуты.

Разрешение Запись позволяет создавать новые файлы и папки внутри папок, изменять атрибуты и просматривать владельцев и разрешения.

Разрешение Список содержимого папки позволяет просматривать имена файлов и папок.

Разрешение Чтение и выполнение для папок позволяет перемещаться по структуре других папок и служит для того, чтобы разрешить пользователю открывать папку, даже если он не имеет прав доступа к ней, для поиска других файлов или вложенных папок. Разрешены все действия, право на которые дают разрешения Чтение и Список содержимого папки. Это же разрешение для файлов позволяет запускать файлы программ и выполнять действия, право на которые дает разрешение Чтение.

Разрешение Изменить позволяет удалять папки, файлы и выполнять все действия, право на которые дают разрешения Запись и Чтение и выполнение.

Разрешение Полный доступ позволяет изменять разрешения, менять владельца, удалять файлы и папки и выполнять все действия, на которые дают право все остальные разрешения NTFS.

Разрешения для папок распространяются на их содержимое: подпапки и файлы.

При назначении пользователю или группе разрешения на доступ к файлу или папке руководствуются тем уровнем доступа, который достаточен для данной группы или пользователя при выполнении им своих рабочих обязанностей.

Рассмотренные разрешения относятся к пользователям данного компьютера, совершившим вход локально непосредственно на данную машину. Такие разрешения называются разрешениями файловой системы.

Так как файловая система Windows называется NTFS, то разрешения файловой системы для Windows называют разрешениями NTFS.

Разрешения для пользователей, получившим доступ к папке или файлу через сеть, регулируются отдельно с помощью так называемых разрешений общего доступа. Эти разрешения распространяются только на папки, к которым предоставлен общий доступ через сеть и действуют только для пользователей, обращающихся к папке через сеть. Возможности пользователя задаются разрешениями, представленными ниже:

- Полный доступ (Full Control);
- Изменить (Change);
- Чтение (Read);

Доступ к средствам настройки разрешений общего доступа выполняется через свойства папки, предоставленной в общий доступ.

Разрешения общего доступа являются средством обеспечения безопасности данных при коллективной работе с документами и поэтому должны устанавливаться очень тщательно и обоснованно. При этом администратору рекомендуется действовать следующим образом.

- Для каждого ресурса общего доступа определить, каким группам пользователей необходим доступ к нему и какой требуется уровень доступа;
- Для упрощения администрирования назначайте разрешения группам, а не отдельным пользователям;
- Устанавливайте максимально строгие разрешения, которые, однако, должны позволять пользователям совершать необходимые действия;
- Организуйте ресурсы общего доступа таким образом, чтобы папки с одинаковым уровнем требований безопасности находились в одной папке. Затем установите общий доступ только к ней, все вложенные папки наследуют настройки безопасности;
- Для папок общего доступа применяйте интуитивно понятные пользователям имена, корректно отображаемые всеми клиентскими операционными системами, используемыми на предприятии.
- Если в общих папках предполагается хранить программы-приложения, то целесообразно поместить их в одну папку – единое место хранения и обновления приложений;

Несколько общих папок, доступных членам группы Администраторы, так называемые скрытые Административные общие папки, создаются операционной системой автоматически. Имена этих папок заканчиваются знаком \$. Это корневые каталоги каждого тома на жестком диске (C\$,D\$ и т.д.), папка Admin\$ для доступа к системному каталогу, папка Print\$ для доступа к файлам драйверов принтеров.

Кроме того, скрытую папку с общим доступом можно создать с целью доступа к ней только тех пользователей, которые будут знать имя скрытой папки.

Получить доступ к общим папкам других компьютеров можно используя компоненты Сетевое окружение, Мой компьютер, Мастер добавления в сетевое окружении и команду выполнить (Run).

Соединение с общей папкой через Сетевое окружение выполняется двойным щелчком по ресурсу, к которому необходимо получить доступ. Если общий ресурс отсутствует в списке доступных, выберите значок Добавить новый элемент в сетевое окружение и укажите адрес подключаемого ресурса.

Соединение с общей папкой через компонент Мой компьютер выполняется через меню Сервис этого компонента в пункте Подключить сетевой диск при указании пути к общему ресурсу. Если необходимо пользоваться этим соединением постоянно, нужно чтобы флажок Восстанавливать при входе в систему был установлен. Соединение будет доступно в разделе Сетевые диски окна Мой компьютер.

Для соединения с общей папкой с помощью команды Выполнить щелкните Пуск, затем Выполнить и введите путь к папке в формате UNC(\\имя_компьютера\имя_общей папки).

Рассмотрим, как пользоваться средствами установки разрешений файловой системы и общего доступа.

После выбора объекта, для которого будет выполняться настройка разрешений файловой системы, в диалоговом окне свойств файла или папки необходимо выбрать вкладку Безопасность, показанную на рисунке 4.3.

В данном случае показано, что для папки Авиатор для группы Администраторы установлены разрешения уровня Полный доступ, а для группы Все разрешения ограничены на уровне Чтение.

При установке разрешений в списке групп можно заметить имена так называемых встроенных системных групп, невидимых при использовании оснасток для управления группами и пользователями. Эти группы не имеют определенных членств, которые можно назначить или изменить, но в них система включает различных пользователей в различное время, в зависимости от того, каким образом пользователь получает доступ к системе или ресурсам.

Встроенные системные группы были рассмотрены выше в лабораторной работе №3. В данном случае имеется в виду группа Все, в которую во время своей работы входят все, кто получил доступ к компьютеру или домену.

Разрешения можно не только устанавливать, но запрещать. Запрет имеет больший приоритет, чем разрешение. Запрет разрешений как метод контроля ресурсов Microsoft применять не рекомендует, и он используется, в основном, для дополнительной настройки разрешений конкретным пользователям, в отличие от разрешений для других пользователей группы.

Рассмотренные разрешения называются стандартными и позволяют решить большинство задач, связанных с регулированием уровня доступа групп к ресурсам.

Кнопка Дополнительно служит для задания специальных разрешений. Каждое стандартное разрешение состоит из нескольких специальных, например стандартное разрешение Запись состоит из шести специальных разрешений: создание файлов/запись данных, Создание папок/дозапись данных, запись атрибутов, Запись дополнительных атрибутов, чтение разрешений, синхронизация. Специальные разрешения можно использовать для более тонкой настройки в нестандартных ситуациях.

В окне специальных разрешений имеются закладки Аудит, Владелец. и Эффективные разрешения. Аудит - это процесс, позволяющий фиксировать события, происходящие в системе и имеющие отношения к безопасности. На данной вкладке производится выбор пользователя или группы, для которых данная папка (или файл) будет объектом аудита. Аудит изучается в лабораторной работе № 6.

Закладка Владелец обеспечивает такое свойство безопасности, как право владения объектом файловой системы. Администратор всегда может стать владельцем любого объекта файловой системы, любой пользователь является владельцем созданных им объектов и, если локальные или доменные политики безопасности разрешат, пользователь может назначать себя владельцем других файлов и папок.

Подробное рассмотрение вопросов владения выходит за рамки данного пособия, однако отметим, что многие операции с файлами и папками, например смена разрешений, шифрование и дешифрование привязаны к факту владения данным объектом.

Список управления доступом (ACL) хранится на диске NTFS для каждого файла или папки. В нем перечислены пользователи и группы, для которых установлены разрешения для файла или папки, а также сами назначенные разрешения.

Каждому пользователю или группе могут быть установлены множественные разрешения через участие в нескольких группах с разным набором разрешений. В этом случае действуют эффективные разрешения – пользователь обладает всеми назначенными ему разрешениями.

Действует приоритет разрешений для файлов над разрешениями для папок и приоритет запрещения над разрешением.

Разрешения, назначенные родительской папке, по умолчанию наследуются всеми подпапками и файлами, содержащимися в папках. Однако есть возможность предотвратить наследование для любой вложенной папки и в этом случае эта папка сама становится родительской для вложенных в нее папок.

Если папка предоставлена для общего доступа, то на нее распространяются разрешения двух видов:

- разрешения файловой системы, установленные для пользователей данного компьютера;
- разрешения общего доступа, объявленные для пользователей, получивших доступ через сеть.

Обычно для папок общего доступа задают разрешения полного доступа, а ограничения вводят установкой разрешений NTFS[4,5].

В этом случае действует объединение разрешений NTFS и разрешений для общей папки, при котором наиболее строгое разрешение имеет приоритет над другими.

Задание к проведению лабораторной работы

1. Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe. Например, одну из стандартных программ Windows, такую как notepad.exe (Блокнот).
2. Установите для этой папки разрешения полного доступа для одного из пользователей группы администраторы, и ограниченные разрешения для пользователя с ограниченной учетной записью.
3. Выполните различные действия с папкой и файлами для обеих учетных записей и установите, как действуют ограничения, связанные с назначением уровня доступа ниже, чем полный доступ.
4. Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера.
5. Установите разрешения общего доступа так, чтобы администратор не имел ограничений, а пользователь имел ограниченный уровень доступа.
6. Экспериментально убедитесь в правилах объединения разрешений NTFS и разрешений общего доступа.
7. Составьте отчет о проведенных экспериментах.
8. Разработайте стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

Контрольные вопросы

1. Какое из следующих разрешений NTFS для папок позволяет вам удалять папку?
 - Чтение
 - Чтение и выполнение
 - Изменение
 - Администрирование
2. Какое разрешение NTFS для файлов следует установить для файла, если вы позволяете пользователям удалять файл, но не позволяете становиться владельцами файла?
3. Какие объекты по умолчанию наследуют разрешения, установленные для родительской папки?
4. Кто может устанавливать разрешения для отдельных пользователей и групп? (выберите все правильные ответы)
 - Члены группы Администраторы
 - Члены группы Опытные пользователи
 - Пользователи, обладающие разрешением Полный доступ
 - Владельцы файлов и папок
5. Какой из следующих вкладок диалогового окна свойств файла или папки следует воспользоваться для установки или изменений разрешений NTFS:
 - Дополнительно
 - Разрешения
 - Безопасность
 - Общие
6. Если вы хотите, чтобы пользователь или группа не имела доступа к определенной папке или файлу, следует ли запретить разрешения для этой папки или файла?

Тема 4. Программно-аппаратные комплексы защиты информации.

Лабораторная работа. Электронный замок Соболев

Теоретическая часть

Задание 1. Установить программное обеспечение комплекса «Соболев».

Задание 2. Настроить общие параметры комплекса.

Задание 3. Зарегистрироваться в системе в качестве Администратора.

Задание 4. Зарегистрировать в списке пользователей нового пользователя комплекса.

Задание 5. Сменить аутентификатор администратора

Задание 6. Провести тестирование памяти NVRAM

Задание 7. Корректировка шаблонов для контроля целостности.

Задание 8. Выполнить расчет эталонных значений контрольных сумм.

Задание 9. Просмотреть записи журнала.

Задание 10. Удалите ПО для комплекса «Соболь»

Вопросы и практические задания

Список использованных источников.

Теоретическая часть

Электронный замок «Соболь» разработан научно-инженерным предприятием «ИНФОРМЗАЩИТА» и предназначен для предотвращения несанкционированного доступа посторонних лиц к ресурсам защищаемого компьютера.

Электронный замок "Соболь" сертифицирован ФСБ (сертификат № СФ/027- 0792 от 18.05.2005). Это позволяет применять "Соболь" для защиты информации, составляющей коммерческую или государственную тайну.

Кроме того, электронный замок "Соболь" сертифицирован Гостехкомиссией России (сертификат № 907 от 18.05.2004г.), что подтверждает соответствие этого изделия требованиям руководящего документа Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите

информации" и позволяет использовать его при разработке средств защиты для автоматизированных систем с классом защищенности до 1В включительно.

Электронный замок «Соболь» сертифицирован Федеральным агентством правительственной связи и информации России. Сертификаты ФАПСи № СФ/122- 0305 и № СФ/022-0306 от 10.02.2000 позволяют применять данное средство для защиты информации, составляющую коммерческую или государственную тайну.

Действие комплекса «Соболь» состоит в проверке полномочий пользователя на вход в систему. При этом пользователь получает доступ к компьютеру только после регистрации его в списке пользователей комплекса. Регистрация пользователей осуществляется администратором и состоит в присвоении пользователю имени, персонального идентификатора и назначении пароля. Регистрация администратора осуществляется при инициализации комплекса.

Если предъявлены необходимые атрибуты – персональный идентификатор и пароль, пользователь получает право на вход. При их отсутствии вход в систему данного пользователя запрещается.

Системные требования.

Комплекс «Соболь» предназначен для использования на компьютерах, оснащенных процессорами семейства INTEL X86 (или совместимыми с ними), начиная с процессора i486 и выше.

Подсистемы контроля целостности и подсистемы запрета загрузки со съемных носителей функционируют под управлением следующих ОС:

MS DOS версий 5.0-6.22;

ОС семейства Windows'9x (FAT12, FAT16 или FAT32); Windows NT версий 3.51 и 4.0 с файловой системой NTFS; Windows 2000 с файловой системой NTFS;

ОС Windows XP и Windows 2003 с файловой системой NTFS и NTFS5;

Задание 1. Установить программное обеспечение комплекса «Соболь».

Программное обеспечение комплекса рекомендуется устанавливать до установки в компьютер его платы.

Для установки программного обеспечения следует:

1. Поместить установочный компакт-диск в привод CD-ROM и запустить на исполнение файл Setup.exe.

На экране появится сообщение о том, что в компьютере отсутствует плата комплекса. Для продолжения установки следует нажать клавишу <Enter>.

Программа установки выполнит подготовку к установке, после чего на экране появится стартовый диалог программы установки.

2. Далее следуйте инструкциям для продолжения установки.

Задание 2. Настроить общие параметры комплекса.

Перед тем, как начать работу с программно-аппаратным комплексом

«Соболь» следует выполнить его инициализацию. Первым шагом здесь будет настройка общих параметров.

1. Включите питание компьютера.

2. В появившемся окне Выберите клавишей или в меню команду «Инициализация платы» и нажмите клавишу <Enter>.

После выполнения этой процедуры на экране появится диалог.

3. Для параметра «Контроль целостности файлов и секторов» установите значение «Да». Это будет означать, что контроль целостности включен.

При присвоении параметру значения «Да» на экране появится окно для ввода пути к каталогу с файлами шаблонов контроля целостности. При обнаружении заданного каталога и находящихся в нем не поврежденных файлов шаблонов контроля целостности параметр примет значение «Да», иначе на экране появится сообщение об ошибке и значение параметра не изменится.

«2.0».

4. Для параметра «Версия криптографической схемы» установите значение

5. Для оставшихся параметров выбрать значения.

6. Нажмите клавишу <Esc> для сохранения установленных параметров.

Задание 3. Зарегистрироваться в системе в качестве Администратора.

После выполнения настройки общих параметров следующим шагом по инициализации комплекса является регистрация администратора. При регистрации администратора ему назначается пароль для входа в систему и присваивается персональный идентификатор.

Для регистрации администратора следует:

1. Выбрать в окне появившегося запроса вариант «Да» и нажать клавишу <Enter>.

2. Введите пароль администратора и нажмите <Enter>. После появления диалога для подтверждения введите тот же пароль и нажмите <Enter>.

Если оба значения пароля совпали и длина пароля не меньше заданной минимальной длины, на экране появится запрос.

3. Плотно приложите к считывателю персональный идентификатор, присваиваемый администратору комплекса «Соболь».

При присвоении персонального идентификатора в него записывается служебная информация.

4. По окончании инициализации выключите компьютер и переведите комплекс в режим эксплуатации.

Задание 4. Зарегистрировать в списке пользователей нового пользователя комплекса.

При регистрации нового пользователя в списке пользователей комплекса ему присваиваются следующие атрибуты: имя, аутентификатор и пароль для входа в систему, персональный идентификатор iButton

Служебная информация о пользователе сохраняется в энергозависимой памяти комплекса – создается учетная запись пользователя.

Для регистрации нового пользователя выполняются следующие действия:

1. Войти в систему, предъявив пароль и идентификатор администратора.

2. В меню администратора активировать команду «Список пользователей».

3. Находясь в списке пользователей, нажать клавишу <Insert>.

4. Ввести имя пользователя, содержащее не более 40 символов. Нажать клавишу <Enter>.

5. Введите и подтвердите пароль пользователя.

6. Плотно приложите к считывателю персональный идентификатор, присваиваемый пользователю.

После успешного присвоения пользователю персонального идентификатора и записи служебной информации о регистрации в энергозависимую память комплекса на экране появится сообщение об успешной регистрации пользователя.

Задание 5. Сменить аутентификатор администратора.

Администратор комплекса «Соболь» может сменить пароль для входа в систему и аутентификатор. Аутентификатор – структура данных, хранящаяся в персональном идентификаторе пользователя (аутентифицирующая информация пользователя), которая наравне с паролем пользователя участвует в процедуре аутентификации.

При смене пароля и аутентификатора изменяется содержимое персонального идентификатора администратора.

Для смены аутентификатора следует:

1. В меню администратора выберите команду «Смену аутентификатора» и нажмите клавишу <Enter>.
2. Введите текущий пароль администратора и нажмите <Enter>.
3. Плотно приложите к считывателю персональный идентификатор администратора.

Далее происходит сопоставление введенного пароля с информацией, хранящейся на идентификаторе. При первой смене аутентификатора новый аутентификатор записывается в персональный идентификатор администратора, при этом старый аутентификатор сохраняется в памяти персонального идентификатора.

По окончании процедуры записи аутентификатора на экране появится сообщение.

Задание 6. Провести тестирование памяти NVRAM.

Тест NVRAM памяти проверяет работоспособность энергонезависимой памяти комплекса «Соболь». В ходе проверки осуществляются попытки доступа на чтение и запись для каждого сегмента двух банков NVRAM памяти комплекса.

Для проверки NVRAM памяти:

1. Выбрать в меню администратора команду «Диагностика платы»
2. Выбрать команду «Тест NVRAM памяти» и нажать <Enter>

После выполнения этой команды начнется процедура проверки.

3. Просмотрите полученные результаты.

Задание 7. Корректировка шаблонов для контроля целостности.

Исходные шаблоны для контроля целостности создаются при установке ПО комплекса и содержат перечень файлов и секторов жестких дисков, по умолчанию включаемых в шаблоны.

Программа подготовки шаблонов Sneck.exe является компонентом, входящим в комплект поставки «Соболя». Данная программа позволяет определить списки файлов и секторов жестких дисков, целостность которых требуется контролировать.

Для выполнения корректировки шаблонов следует выполнить:

1. Нажмите кнопку «Пуск» и активируйте в главном меню Windows команду «Программы \ ПО для электронного замка «Соболь \ Программа подготовки шаблонов для КЦ»»
2. Выполните корректировку шаблонов для контроля целостности:

В диалоге файлы выберите «Файлы» подлежащие контролю

В диалоге «Секторы» выберите секторы жесткого диска, целостность которых требуется контролировать

3. Нажмите кнопку «Сохранить», чтобы внесенные изменения были сохранены.

Задание 8. Выполнить расчет эталонных значений контрольных сумм.

После корректировки шаблонов для контроля целостности необходимо заново рассчитать эталонные значения контрольных сумм.

1. Перезагрузите компьютер и войдите в систему с правами администратора комплекса
2. В меню администратора выберите команду «Расчет контрольных сумм».

Начнется расчет эталонных значений контрольных сумм объектов, заданных шаблонами для контроля целостности.

Задание 9. Просмотреть записи журнала.

Записи о событиях, регистрируемых комплексом «Соболь» во время своей работы, хранятся в журнале регистрации событий, который размещается в специальной энергонезависимой памяти комплекса.

Для просмотра журнала записей:

1. В меню администратора выберите команду «Журнал регистрации событий»
2. Ознакомьтесь с содержанием журнала регистрации событий
3. Нажмите для <Esc> возврата к меню администратора.

Задание 10. Удалите ПО для комплекса «Соболь».

1. Нажмите на кнопку Пуск и выберите Настройки | Панель управления.
2. Выберите «Установка и удаление программ».
3. В появившемся списке выберите «ПО для электронного замка «Соболь» и нажмите кнопку «Добавить/Удалить».
4. Подтвердите удаление.

Вопросы и практические задания

1. Создать учетную запись пользователя, которому будет разрешен доступ к компьютеру на неделю, после чего учетная запись будет заблокирована.
2. Поставить пользователю пароль, сгенерированный комплексом, заблокировать учетную запись при втором неудачном входе.
3. Запретить ранее созданному пользователю смотреть свою статистику.
4. Произвести смену пароля администратора.
5. Выполнить тест считывателя iButton.
6. Скорректировать списки контролируемых файлов.
7. Очистить журнал регистрации событий.
8. Просмотреть информацию о программе подготовки шаблонов контроля целостности.
9. Выполнить диагностику платы ПАК «Соболь».
10. Установить число попыток тестирования ДСЧ на значение «2».

Список использованных источников.

1. Электронный ресурс \ Информзащита – режим доступа: <http://www.infosec.ru>. – Загл. с экрана;
2. Руководство по эксплуатации Программно-аппаратного комплекса «Соболь»: Москва, 2006;
3. ЭЛЕКТРОННЫЙ ЗАМОК СОБОЛЬ - РАЗРАБОТКА НИП ИНФОРМЗАЩИТА - Новые технологии - Деловая пресса_ Электронные газеты [Электронный ресурс]- Режим доступа: <http://www.buisnesspress.ru/newspaper/>
4. Электронный ресурс // Защита информации – режим доступа: <http://www.zinfo.ru>. – Загл. с экрана;
5. Электронный ресурс // More PC – режим доступа: <http://www.morepc.ru>. – Загл. с экрана.

Тема 5. Электронный идентификатор ruToken.

Лабораторная работа. Вход в систему с использованием ruToken

Теоретическая часть

Задание 1. Установка компонентов системы

Задание 2. Создание профиля.

Задание 3. Вход с помощью электронного идентификатора.

Задание 4. Вход в систему с использованием пароля.

Задание 5. Использование дополнительных библиотек аутентификации

Вопросы и практические задания.

Список литературы

Теоретическая часть

Система Zlogin предназначена для двухфакторной аутентификации пользователей сети с использованием электронных ключей или смарт-карт. Вместо пароля пользователь должен предъявить смарт-карту или электронный USB-ключ и ввести PIN-код.

Характеристики:

Многофакторная аутентификация с помощью электронного ключа и PIN-кода;

Использование в качестве электронных идентификаторов смарт-карт и USB-ключей;

Минимизация «человеческого фактора». Система освобождает пользователей от необходимости запоминать длинные пароли и периодически придумывать новые пароли при их смене;

Централизованное управление системой через службу каталога — Microsoft Active Directory или Novell NDS/eDiracory;

Возможность использования совместно с Novell Modular Authentication Service (NMAS), интеграция с Novell Certificate Server и инфраструктурой открытых ключей PKI;

Возможность использования одного электронного ключа для доступа к разным сетям и приложениям.

Задание 1. Установка компонентов системы.

Установка Администратора

Для начала установки необходимо запустить файл установки администрирования. Мастер установки InstallShield проведет необходимые предварительные операции и отобразит приглашающее окно.

Нажмите кнопку —Далее > и ознакомьтесь с Лицензионным соглашением. Нажмите —Дал.

На следующем этапе предлагается указать каталог для установки файлов, нажав кнопку "Обзор", или воспользоваться папкой по умолчанию. Нажмите "Далее >" для начала установки.

Дождитесь окончания процесса копирования и перезагрузите компьютер, выбрав пункт "Да, перезагрузить компьютер сейчас" и нажав "Готово".

Установка Клиента

Для начала установки необходимо запустить файл установки клиента. Мастер установки InstallShield проведет необходимые предварительные операции и отобразит приглашающее окно. Нажмите кнопку —Далее > и ознакомьтесь с Лицензионным соглашением. Если Вы согласны с предлагаемыми условиями, нажмите —Дал. Нажмите "Далее >".

Если установочная программа обнаружит ПО для работы с терминальными серверами, Вам будет предложено выбрать необходимые компоненты для установки.

Выберите все компоненты установки и нажмите "Далее".

Дождитесь окончания процесса копирования и перезагрузите компьютер, выбрав пункт "Да, перезагрузить компьютер сейчас" и нажав "Готово".

Задание 2. Создание профиля.

Вставьте USB-ключ Rutoken в свободный интерфейс.

Откройте модуль администрирования: "Управление компьютером" из папки "Администрирование" ("Administrative Tools") в панели управления. Затем нужно раскрыть узлы "Служебные программы" ("System Tools"), "Администрирование продуктов SecurIT", "Zlogin" и выберите ключ Rutoken.

Для создания профиля необходимо выбрать пункт "Новый профиль" в меню "Действие" ("Action").

На первом этапе мастера по выдаче электронного идентификатора ознакомьтесь с предстоящими действиями и нажмите "Далее >". На втором шаге потребуется выбрать нужные учетные записи для последующего включения авторизационной информации о них в электронный идентификатор.

Поставьте флажок напротив пункта "Локальная учетная запись" и выберите свою учетную запись.

На следующем шаге мастера необходимо ввести имя профиля – любое понятное для пользователя название профиля. Если в одном электронном идентификаторе будет находиться два или более профилей, то перед входом в сеть пользователю будет выведен список имен профилей и будет предложено выбрать один из них для входа в сеть.

В данном окне можно поставить дополнительные опции:

"Данный профиль будет использоваться в Windows 9x" – если планируется использование профиля для входа в сеть на рабочих станциях Windows 98/Me, отметьте эту опцию. Если в профиль также включена учетная запись NDS, то имена пользователей в NDS и домене (локально) должны совпадать. При этом система Zlogin будет производить автоматическую синхронизацию паролей. "Защитить профиль ПИН-кодом" – применяется для входа в сеть без ввода PIN-кода. Достаточно подключить электронный идентификатор, и Zlogin Клиент сразу произведет аутентификацию в сети с использованием данного профиля.

На следующем шаге мастер задайте политику смены паролей. Выберите "Пароль генерируется системой Zlogin" (означает использовать «сильные» пароли 14-значной длины, генерируемые автоматически. Система Zlogin при первой попытке входа в систему запросит пароль у пользователя и, если пароль окажется правильным, произведет его смену).

Поставьте флажок "Сменить пароль при создании профиля" – сразу по завершении мастера выдачи электронного идентификатора система произведет генерацию пароля и смену его в домене (NDS) методом «сброса» (reset password). Таким образом, запрос пароля у пользователя при первой попытке входа производиться не будет.

На последнем шаге мастера убедитесь в правильности выбора учетных записей и политик смены паролей, после чего нажмите "Готово" (при создании первого защищенного PIN-кодом профиля потребуются ввести PIN- код данного электронного идентификатора).

Задание 3. Вход с помощью электронного идентификатора.

Подсоедините электронный идентификатор и введите PIN-код в появившемся окне.

Нажмите кнопку ОК. Zlogin произведет аутентификацию пользователя с использованием учетных записей, находящихся в профиле.

Выберите свой профиль для входа в систему.

Задание 4. Вход в систему с использованием пароля.

Включите ПК при загрузке системы появится окно приветствия. Введите имя учетной записи, пароль.

После установки Zlogin Клиента рабочая станция конфигурируется таким образом, что при входе с электронным идентификатором и последующем его отсоединении происходит блокировка консоли. Рабочую станцию также можно заблокировать стандартными способами.

Для разблокировки консоли пользователю следует подключить электронный идентификатор и ввести PIN-код.

Задание 5. Использование дополнительных библиотек аутентификации.

Zlogin предоставляет возможность подключать дополнительные библиотеки входа в сеть (GINA) без использования электронного идентификатора. Например, в их качестве могут выступать стандартная

MSGINA из состава MS Windows или NWGINA от клиента для сетей Novell NetWare.

Для настройки данной возможности нажмите Alt + Z в окне "Вас приветствует операционная система Windows".

Выбранная библиотека загрузится после нажатия кнопки "Выбор". Теперь, при нажатии комбинации клавиш Ctrl+Alt+Del появится окно выбранной библиотеки. Если необходимо каждый раз загружать определенную библиотеку, необходимо предварительно нажать кнопку —Сохранить выбор».

Вопросы и практические задания.

1. Какие функции выполняет модуль GINA.DLL?
2. Какой алгоритм шифрования используется в сертификатах Zlogin?
3. Создать новый профиль с использованием учетной записи NDS
4. Установите периодичность смены паролей в Domain Security Policy

Список литературы.

1. Руководство администратора Zlogin
2. <http://www.securit.ru/> - сайт разработчика (Компания SecurIT)

Лабораторная работа. Работа с утилитой администрирования ruToken

Теоретическая часть

Задание 1. Выбрать ридер с подключенным к нему ruToken

Задание 2. Установка прав доступа Администратора.

Задание 3. Установка прав доступа Пользователя.

Задание 4. Разблокирование PIN-кода Пользователя.

Задание 5. Смена PIN-кода.

Задание 6. Изменение символьного имени ruToken

Задание 7. Инициализация памяти ruToken

Задание 8. Получение информации о программе и о ruToken

Вопросы и практические задания.

Список литературы

Теоретическая часть.

Утилита администрирования предназначена, в первую очередь, для использования администраторами систем безопасности или, иначе говоря, офицерами безопасности.

Утилита администрирования позволяет выполнять следующие операции:

Получение информации о подключенных токенах Разблокирование PIN-кода Пользователя

Установка новых PIN-кодов Пользователя и Администратора Изменение символьного имени токена

Инициализация памяти токена

Для того чтобы начать работу с утилитой администрирования, нужно запустить приложение rtAdmin.exe.

Задание 1. Выбрать ридер с подключенным к нему ruToken.

Перед запуском rtAdmin.exe убедитесь в том, что в системе установлен драйвер ruToken. Если токен не подключен, подсоедините его к свободному USB-порту.

Выбор ридера осуществляется из выпадающего списка, содержащего имена ридеров. Ридеры, к которым подключены токены, отмечены в списке пиктограммой. Для выбора ридера нажмите на соответствующий элемент списка.

Задание 2. Установка прав доступа Администратора.

Для выполнения операций разблокирования токена, изменения PIN- кода и инициализации памяти нужно иметь права доступа Администратора. Для установки прав доступа Администратора выполняется операция Login. После нажатия в главном окне утилиты на кнопку [Login] на экране отображается диалог для ввода PIN-кода.

В диалоге требуется выбрать уровень прав доступа из развертывающегося списка (по умолчанию - Администратор) и ввести

соответствующий PIN-код - 87654321. Набираемый PIN-код отображается в виде символов '*'. Всего может быть предпринято до 15 попыток ввода PIN- кода.

Если набран PIN-код Администратора, то доступны для выполнения все операции с ruToken, кроме изменения его символьного имени.

Задание 3. Установка прав доступа Пользователя.

После предъявления прав доступа Пользователя становятся доступны только функции изменения PIN-кода Пользователя и символьного имени токена. Для установки прав доступа Пользователя выполняется операция Login. После нажатия в главном окне утилиты на кнопку [Login] на экране отображается диалог для ввода PIN-кода.

В диалоге требуется выбрать уровень прав доступа Пользователя из разворачивающегося списка и ввести соответствующий PIN-код - 12345678. Набираемый PIN-код отображается в виде символов '*'. Всего может быть предпринято до 15 попыток ввода PIN-кода.

Если набран PIN-код Пользователя, то недоступны операции разблокирования PIN-кода Пользователя и инициализации памяти токена.

После завершения операций с токеном следует выполнить сброс текущих прав доступа (Logout), для чего нужно нажать на соответствующую кнопку. Если Logout не выполнен, по завершении работы утилиты текущими остаются назначенные права доступа.

Задание 4. Разблокирование PIN-кода Пользователя.

Разблокирование PIN-кода Пользователя guToken выполняется в тех случаях, когда он был заблокирован после определенного числа последовательных неудачных попыток ввода. Для его разблокирования нужно нажать на кнопку [Лечить] в главном окне утилиты.

При выполнении этой операции счетчик попыток доступа к соответствующему GCHV-объекту восстанавливается в свое исходное значение, заданное при инициализации токена.

Для выполнения этой операции необходимо, чтобы текущими были права доступа Администратора.

Задание 5. Смена PIN-кода.

По умолчанию для PIN-кода Пользователя и PIN-кода Администратора установлены значения '12345678' и '87654321' соответственно.

При работе с guToken значения PIN-кода по умолчанию необходимо изменить на собственные в целях обеспечения безопасности.

Установка новых значений PIN-кодов производится после нажатия на кнопку [PIN-код] в главном окне утилиты.

Если стоят права доступа Администратора, то доступны все группы установки PIN-кодов.

Если стоят права доступа Пользователя, то доступна только группа установки PIN-кода Пользователя.

Установка PIN-кода Пользователя и Администратора производится по отдельности. Для установки каждого из них необходимо нажать кнопку [Установить] в соответствующей группе. Максимальная длина PIN-кода – 16 символов, регистр учитывается.

Для смены PIN-кода Администратора необходимо, чтобы текущими были права доступа Администратора.

Владелец токена, которому разрешено менять PIN-код Пользователя, определяется политикой смены PIN-кода Пользователя, определяемой при инициализации памяти токена.

Задание 6. Изменение символьного имени guToken.

Символьное имя токена служит для облегчения его идентификации. Для изменения символьного имени токена требуются права доступа Пользователя. После установки текущих прав доступа и нажатия на кнопку [Имя] появится диалог, в котором следует указать новое имя токена.

Максимальная длина символьного имени токена - 255 байт.

Допустимыми являются все отображаемые символы, регистр учитывается.

Задание 7. Инициализация памяти guToken.

Инициализация памяти предназначена в основном для того, чтобы удалить содержимое памяти токена – например, при передаче другому владельцу. После выполнения инициализации в памяти токена содержится только дерево предопределенных папок со служебными файлами, а также GCHV-объекты с PIN-кодами Пользователя и Администратора.

Для запуска инициализации нужно нажать на кнопку [Формат].

После нажатия на кнопку [Пуск] выводится предупреждение о том, что запрещается производить инициализацию памяти ruToken в виртуальных машинах типа VMware. После подтверждения запускается прерыватель

который нельзя. Для выполнения этой операции необходимо, чтобы текущими были права доступа Администратора.

Если при пакетном форматировании в поле «Авто-Login с PIN-кодом:» введен неверный PIN-код Администратора, то при подсоединении следующего токена будет предложено набрать PIN-код еще раз и подтвердить его использование.

Если пакетное форматирование не используется, то при присоединении нового токена каждый раз будет запрашиваться PIN-код Администратора

Задание 8. Получение информации о программе и о ruToken.

Для получения информации о токене нужно нажать на кнопку [Свойства] в главном окне утилиты.

В нем отображается следующая информация:

Символьное имя токена (Имя)

Тип токена (Тип), включая об в килобайтах

ID токена в виде шестнадцатиричного числа (ID) Версия ruToken (Версия)

Номер протокола обмена с драйвером ruToken (Протокол)

Номер микропрограммы, прошитой в токен (Микропрограмма) Номер заказа (Заказ)

Доступная память токена в байтах (Свободная память)

Кнопка [>] в главном окне утилиты позволяет выбирать язык (английский / русский), вызывать файл справки, а также выводить информацию о программе.

После выбора пункта «О программе» появляется окно, в котором показывается версия утилиты rtAdmin.exe, а также список модулей ПО

ruToken (драйверы, провайдеры, библиотека PKCS#11, библиотека ядра и т.п.), установленных в системе:

Вопросы и практические задания.

1. Для чего предназначена утилита администрирования?
2. Назначьте количество ридеров ruToken - 4.
3. В чем отличие прав доступа Администратора от прав доступа Пользователя?
4. Смените PIN-код Пользователя на polsovat.
5. Можно ли разблокировать PIN-код Пользователя с правами доступа Пользователя?
6. Заблокируйте PIN-код Пользователя и разблокируйте его.
7. Измените символьное имя токена на ruToken1.
8. Как можно просмотреть список модулей ПО ruToken (драйверы, провайдеры, библиотека PKCS#11, библиотека ядра и т.п.), установленных в системе?
9. Выполните сброс текущих прав доступа.

Список литературы.

1. www.rutoken.ru - официальный сайт разработчика

2. Руководство Пользователя ruToken

Лабораторная работа. Работа с редактором памяти ruToken

Теоретическая часть

Задание 1. Изучение главного окна rtEditor.

Задание 2. Установка прав доступа Администратора.

Задание 3. Установка прав доступа Пользователя.

Задание 4. Смена PIN-кода Пользователя.

Задание 5. Создание файла в ruToken

Задание 6. Создание папки в ruToken

Задание 7. Создание GOST-объектов (ключей шифрования ГОСТ).

Задание 8. Создание SE-объектов (окружений безопасности).

Задание 9. Просмотр и редактирование файлов.

Задание 10. Зашифрование и расшифрование данных по ГОСТ 28147-89

Вопросы и практические задания.

Список литературы

Теоретическая часть.

Утилиту rtEditor могут использовать как Администратор, так и Пользователь ruToken. Она позволяет просматривать содержимое памяти токена, создавать и редактировать объекты файловой системы, определять их свойства, создавать символьное имя токена, производить шифрование данных по алгоритму ГОСТ 28147-89, выполнять другие сервисные действия.

Задание 1. Изучение главного окна rtEditor.

Для того чтобы начать работу с редактором памяти токена, нужно запустить приложение rtEditor.exe. Перед запуском rtEditor.exe убедитесь в том, что в системе установлен драйвер ruToken и, по крайней мере, один токен подключен к одному из

доступных портов USB. Подключение можно будет выполнить также после запуска утилиты.

При успешном запуске редактора появится главное окно rtEditor.

В главном окне отображаются следующие элементы управления: Меню

Панель инструментов Окно просмотра

Панель состояния

Окно просмотра разделено на два фрейма:

В левом фрейме отображается список доступных токенов и структура папок каждого из них.

Каждый доступный токен обозначается в списке пиктограммой, символьным именем (если оно отсутствует, токен маркируется как) и именем ридера. Структура папок отображается в виде дерева

В правом фрейме отображается содержимое текущей папки: вложенные папки, файлы и объекты данных с указанием ID, типа и размера объекта файловой системы.

В панели состояния отображается следующая информация: Текущие права доступа: Гость, Пользователь, Администратор ID токена в 16-ном формате (ID (hex))

Доступный объем памяти токена в байтах (Свободно байт)

Список доступных токенов отображается в левом фрейме окна просмотра. Для утановки текущего токена нужно выбрать его в списке и щелкнуть левой кнопкой мыши на его имени.

Задание 2. Установка прав доступа Администратора.

После выбора текущего токена текущие права доступа установлены в нем на уровне «Гость». Для выполнения операций и доступа к файлам и объектам, требующим прав доступа Пользователя или Администратора, нужно выполнить аутентификацию владельца токена с соответствующими правами. Для этого служит команда меню Действия|Login или кнопка в панели инструментов.

В диалоге требуется выбрать уровень прав доступа из развертывающегося списка (по умолчанию - Администратор) и ввести соответствующий PIN-код - 87654321. Набираемый PIN-код отображается в виде символов '*'. Всего может быть предпринято до 15 попыток ввода PIN- кода.

По исчерпанию числа попыток доступа PIN-код Администратора блокируется без возможности его разблокирования и становится невозможным выполнять любые действия, требующие прав Администратора.

Такой токен подлежит возврату поставщику для восстановления его полной работоспособности (в процессе восстановления токена все данные на нем будут уничтожены).

Задание 3. Установка прав доступа Пользователя.

Для выполнения операций и доступа к файлам и объектам, требующим прав доступа Пользователя служит команда меню Действия|Login или кнопка в панели инструментов.

В диалоге требуется выбрать уровень прав доступа Пользователя из разворачивающегося списка и ввести соответствующий PIN-код - 12345678. Набираемый PIN-код отображается в виде символов '*'. Всего может быть предпринято до 15 попыток ввода PIN-кода. По исчерпании числа попыток доступа PIN-код Пользователя блокируется и может быть разблокирован только Администратором при помощи утилиты администрирования токена rtAdmin.

После завершения операций с токеном следует выполнить сброс текущих прав доступа (Logout), для чего нужно нажать на Действие/Logout. Если Logout не выполнен, по завершении работы утилиты текущими остаются назначенные права доступа.

Задание 4. Смена PIN-кода Пользователя.

PIN-код Пользователя может быть изменен, если это позволяет политика смены PIN-кодов, определенная на этапе инициализации токена.

Для смены PIN-кода Пользователя служит одноименная команда меню или кнопка в панели инструментов

В диалоге нужно ввести новый PIN-код и подтвердить его. При успешном выполнении операции появится соответствующее сообщение, в противном случае будет возвращена ошибка «Права доступа неудовлетворительны для выполнения команды».

Задание 5. Создание файла в ruToken.

Файлы могут быть созданы как в Корневой папке (Master File, MF), так и в других папках. Для создания нового файла нужно сделать текущей папку, в которой он будет создан. Затем, после выбора команды меню Файл|Создать|Файл (либо аналогичной команды контекстного меню или кнопки в панели инструментов), появится диалог создания файла.

Для создания файлов требуются права доступа, определенные атрибутом безопасности 'Создать файл' той папки, в которой будет создаваться новый файл.

В этом диалоге необходимо ввести имя создаваемого файла, его размер, установить его тип и атрибуты безопасности.

ID (идентификатор файла, используемый в качестве его имени) - двухбайтовое числовое значение, вводимое в виде шестнадцатичного числа.

Размер (байт) - размер файла. Указывается в байтах и не может быть изменен в дальнейшем.

Тип - тип файла. Выбирается в соответствии с предустановленными наборами атрибутов безопасности.

Для удаления файла требуются права доступа, определенные атрибутом безопасности 'Удалить файл' данного файла. Если для операции Удалить (Delete file) установлен атрибут 'Никогда', файл не может быть удален ни Пользователем, ни Администратором - его удаление возможно только при инициализации токена.

Чтобы удалить файл, нужно сделать его текущим, а затем выбрать команду меню Файл|Удалить (либо аналогичную команду контекстного меню или кнопку в панели инструментов).

Задание 6. Создание папки в ruToken.

Папки могут быть созданы как в Корневой папке, так и в других папках. Для создания новой папки необходимо сделать текущей папку, в которой она будет создана. Затем, после выбора команды меню Файл|Создать|Папку (либо аналогичной команды контекстного меню или кнопки в панели инструментов), появится диалог создания папки.

Для создания папки требуются права доступа, определенные атрибутом безопасности 'Создать файл' той папки, в которой будет создаваться новая.

В этом диалоге необходимо ввести имя создаваемой папки, установить ее тип и атрибуты безопасности.

ID (идентификатор папки, использующийся в качестве ее имени) – двухбайтовое числовое значение, вводимое в виде шестнадцатичного числа.

Тип – тип папки. Выбирается в соответствии с предустановленными наборами атрибутов безопасности.

Для удаления папки требуются права доступа, определенные атрибутом безопасности 'Удалить' этой папки. Если установлен атрибут 'Никогда', папка не может быть удалена ни Пользователем, ни Администратором – ее удаление возможно только при инициализации памяти токена.

Чтобы удалить папку, нужно сделать ее текущей, а затем выбрать команду меню Файл|Удалить (либо аналогичную команду контекстного меню или кнопку в панели инструментов).

Задание 7. Создание GOST-объектов (ключей шифрования ГОСТ).

Ключи шифрования по ГОСТ 28147-89 могут создаваться в папке по умолчанию (3F00\0000\0001\), либо в текущей папке. Местоположение объекта данных определяется значением старшего бита его ID. Если старший бит ID содержит 0, объект будет создан в папке по умолчанию, если 1 – в текущей папке. Если предполагается, что объект данных будет создан не в папке по умолчанию, нужно сделать папку, в которой он будет создан, текущей. Затем, вне зависимости от предполагаемого местоположения объекта, нужно выбрать команду меню Файл|Создать|Ключ (либо аналогичной команду контекстного меню или кнопки в панели инструментов). После этого появится диалог создания ключа.

Для создания объектов данных требуются права доступа, определенные атрибутом безопасности 'Создать объект' той папки, в которой будет создаваться объект данных.

В этом диалоге необходимо ввести идентификатор создаваемого объекта, установить способ получения ключа шифрования (будет ли он сгенерирован самим токеном или импортирован в токен из файла), установить требуемые свойства ключа, флаги и атрибуты безопасности.

ID - идентификатор объекта данных. Представляет собой однобайтовое числовое значение, вводимое в виде шестнадцатиричного числа.

Создать как - определяет метод создания: генерацию ключа токеном, либо импорт ключа из внешнего двоичного файла длиной 32 байта (256 бит).

Флаги определяют, будет ли доступна для чтения длина ключа или он будет закрытым объектом.

Опции задают режим шифрования ГОСТ, который будет использовать данный GOST-объект: простая замена, гаммирование или гаммирование с обратной связью.

Атрибуты безопасности назначают различным операциям с данным объектом, предваряющие их security-ориентированные действия, успешное

выполнение которых является необходимым условием выполнения самой операции.

Задание 8. Создание SE-объектов (окружений безопасности).

Объекты окружения безопасности (SE-объект) могут создаваться в папке по умолчанию (3F00\0000\), либо в текущей папке. Место положение объекта данных, содержащего окружение безопасности, определяется значением старшего бита его ID. Если старший бит ID содержит 0, объект будет создан в папке по умолчанию, если 1 – в текущей папке. Если предполагается, что объект данных будет создан не в папке по умолчанию, нужно сделать папку, в которой он будет создан, текущей. Затем, вне зависимости от предполагаемого местоположения объекта, нужно выбрать команду меню Файл|Создать|SE (либо аналогичную команду контекстного меню или кнопки в панели инструментов). После этого появится диалог создания SE-объекта.

В этом диалоге необходимо ввести идентификатор создаваемого объекта, задать значения требуемым компонентам окружения безопасности, установить флаги и атрибуты безопасности.

ID - идентификатор объекта данных: однобайтовое числовое значение, вводимое в виде шестнадцатиричного числа.

Флаги – определяют уровень открытости SE-объекта. Если установлен флаг 'Закрытый', то ни длина, ни содержимое объекта не будут доступны для чтения. Установленный флаг 'Открытая длина' означает, что для чтения будет доступна только информация о длине тела, но не само тело объекта. Установка флага 'Открытый' делает доступным для чтения и длину тела, и само тело объекта.

Компоненты – содержат ID объектов данных, которые будут использованы токеном для выполнения security-ориентированных операций после того, как окружение безопасности из этого SE-объекта будет загружено как текущее.

Компоненты Значение
Комментарий

A-

компонента ID GCHV-

объекта ID объекта, используемого для аутентификации. Компоненте могут быть присвоены значения 0x01 (Администратор) и 0x02 (Пользователь).

C-

компонента ID GOST-

объекта ID объекта, используемого для шифрования данных по ГОСТ 28147-89

H-

компонента ID GOST-

объекта ID объекта, используемого для хеширования данных (выработки имитовставки по ГОСТ 28147-89)

Таблица 1. Компоненты создания SE-объектов

Атрибуты безопасности (Security attributes) назначают различным операциям с данным объектом, предваряющие их security-ориентированные действия, успешное выполнение которых является необходимым условием самой операции.

Задание 9. Просмотр и редактирование файлов.

Для чтения файла требуются права доступа, определенные атрибутом безопасности 'Читать', для записи отредактированного файла – права доступа, определенные атрибутом безопасности 'Обновить' данного файла.

После установки соответствующих прав доступа файл можно открыть для просмотра и (или) редактирования двойным щелчком левой кнопки мыши на его ID, либо при помощи команды [Открыть] контекстного меню.

При этом откроется окно редактора, который позволяет просматривать и редактировать файлы в шестнадцатичном или символьном режиме.

Отредактированный файл можно сохранить в памяти токена командой Файл|Сохранить или оставить неизменным, закрыв окно редактора и отказавшись от сохранения.

Команда меню Правка|Заполнить символом... позволяет заполнить выделенную область файла символом с выбранным шестнадцатичным значением. Для выделения области надо переместить по ней указатель мыши, удерживая нажатой ее левую кнопку. Команда меню Правка|Выделить все используется для выделения всего содержимого файла.

Команды Правка|Копировать и Правка|Вставить позволяют скопировать выделенный фрагмент файла в буфер обмена и вставить содержимое буфера обмена в текущую позицию курсора.

Команда меню Правка|Удалить заполняет выделенную область файла шестнадцатичным значением «0».

Задание 10. Зашифрование и расшифрование данных по ГОСТ 28147-89.

Для выполнения операций зашифрования и расшифрования данных по ГОСТ 28147-89 требуются права доступа, определенные атрибутом безопасности 'Использовать' GOST-объекта с нужным ключом шифрования.

Чтобы зашифровать данные, нужно сделать выбранный GOST-объект текущим и при помощи команды меню Действия|Зашифровать (либо аналогичной команды контекстного меню или кнопки в панели инструментов) инициировать процедуру зашифрования.

В диалоге указывается файл с данными для зашифрования (Исходный файл), имя файла, в котором будут сохранены зашифрованные данные (Сохранить как) и способ генерации синхропосылки. Последняя может быть сгенерирована токеном (Сгенерировать) или введена вручную (Использовать). Если выбранный GOST-объект реализует шифрование в

режиме простой замены, группа «Синхропосылка» будет недоступна, т.к. в этом режиме шифрования синхропосылка не используется.

После того как все необходимые параметры введены, процесс зашифрования запускается нажатием на кнопку [Ok]. По окончании процесса зашифрованные данные помещаются в указанный файл; если применялся режим шифрования, использующий синхропосылку, она будет записана в первые 8 байт файла.

Процедура расшифрования выполняется аналогичным способом командой меню Действия|Расшифровать (либо аналогичной команды контекстного меню или кнопки в панели инструментов).

В качестве параметров в диалоге указываются имена файла с зашифрованными данными (Зашифрованный файл) и файла для сохранения расшифрованных данных (Сохранить как).

Если выбранный GOST-объект реализует шифрование в режиме гаммирования или гаммирования с обратной связью, в первых 8 байтах зашифрованного файла должна находиться синхропосылка. По окончании процесса расшифрованные данные помещаются в указанный файл; синхропосылка теряется.

Вопросы и практические задания.

1. Для чего предназначен редактор памяти ruToken?
2. Получите информацию об объекте файловой системы.
3. Измените символьное имя токена.
4. Создайте на рабочем столе файл 1.txt и зашифруйте его.
5. Где могут быть созданы SE-объекты и GOST-объекты?
6. Создайте папку с ID - 3003, типом - специальная и атрибутом безопасности - Администратор. Сбросьте текущие права доступа, затем удалите данную папку.
7. Создайте файл любого размера и типом - общий.
8. Смените PIN-код пользователя на 11223344.
9. Какие объекты можно создавать в редакторе памяти rtEditor?

Список литературы.

1. www.rutoken.ru - официальный сайт разработчика
2. Руководство Пользователя ruToken

Лабораторная работа. Работа с браузером сертификатов ruToken

Теоретическая часть

Задание 1. Выбор объектов и просмотр их свойств.

Задание 2. Аутентификация пользователя.

Задание 3. Добавление сертификата в хранилище сертификатов.

Задание 4. Импорт сертификата из файла.

Задание 5. Импорт сертификата из CER-файла.

Задание 6. Импорт сертификата из PFX-файла.

Задание 7. Экспорт сертификата в файл

Задание 8. Экспорт сертификата в CER-файл и PFX-файл

Задание 9. Назначение контейнера по умолчанию

Задание 10. Отмена контейнера по умолчанию и удаление контейнера.

Вопросы и практические задания.

Список литературы

Теоретическая часть.

Утилиту rtCert могут использовать все пользователи ruToken. Она предназначена для работы с контейнерами MS CAPi и сертификатами X.509, сохраненными в памяти токена и поддерживает следующие операции:

Просмотр записанных контейнеров MS CAPi и хранящихся в них сертификатов X.509

Регистрация сертификатов в Личном хранилище сертификатов

Удаление зарегистрированных сертификатов из Личного хранилища Импорт сертификатов из PFX- и CER-файлов в память ruToken Экспорт сертификатов из памяти токена в PFX- и CER-файлы

Назначение и отмена контейнера по умолчанию

Удаление контейнеров MS CAPi вместе с их содержимым из памяти ruToken

Задание 1. Выбор объектов и просмотр их свойств.

Для начала работы с браузером сертификатов ruToken необходимо запустить приложение rtCert.exe.

Перед этим следует убедиться, что в системе установлен драйвер ruToken и, по крайней мере, один ruToken подключен к порту USB. Подсоединить токен можно и после запуска утилиты.

При успешном запуске редактора появится главное окно rtCert.

Для выбора нужного объекта надо щелкнуть левой кнопкой мыши на соответствующей строке списка в левом фрейме окна просмотра. После этого в правом фрейме будут показаны свойства объекта.

Задание 2. Аутентификация пользователя.

Аутентификация Пользователя необходима для выполнения следующих операций:

Импорт сертификата из файла в память токена

Экспорт сертификата из памяти токена в PFX-файл Назначение и отмена контейнера по умолчанию

Удаление контейнера с сертификатами из памяти токена

Для выполнения аутентификации нужно выбрать пункт меню Действия|Login (либо аналогичную команду в контекстном меню, либо кнопку в панели инструментов). При этом появляется диалог, в котором нужно ввести PIN-код и нажать [OK].

При успешном вводе PIN-кода на токене будут установлены права доступа Пользователя.

После завершения операций с токеном следует выполнить сброс текущих прав доступа, для чего нужно выбрать пункт меню Действия|Logout (либо аналогичную команду в контекстном меню, либо кнопку в панели инструментов).

Задание 3. Добавление сертификата в хранилище сертификатов.

Эта операция позволяет зарегистрировать выбранный сертификат в Личном хранилище сертификатов данного компьютера. Для выполнения операции достаточно прав доступа Гостя.

Для выполнения операции надо отметить нужный незарегистрированный сертификат и выбрать пункт меню Действия|Добавить сертификат в хранилище сертификатов (либо аналогичную команду в контекстном меню, либо кнопку в панели инструментов). При этом выбранный сертификат будет занесен в память компьютера и зарегистрирован в Личном хранилище.

Зарегистрированный сертификат можно использовать в соответствующем ПО, даже если токен отсоединен от компьютера.

По завершении операции сертификат в списке помечается как зарегистрированный.

В списке сертификатов в левом фрейме сертификаты, зарегистрированные в Личном хранилище, помечены соответствующей иконкой. Для того чтобы удалить выбранный зарегистрированный сертификат, надо выбрать пункт меню Действия|Удалить сертификат из хранилища сертификатов, (либо аналогичную команду в контекстном меню, либо кнопку в панели инструментов).

Выбранный сертификат будет удален из Личного хранилища данного компьютера, однако останется в памяти токена.

Задание 4. Импорт сертификата из файла.

Для выполнения операции импорта необходимо установить права доступа Пользователя.

При выборе пункта меню Действия|Импорт сертификата из файла (либо аналогичной команды в контекстном меню, либо кнопк панели инструментов) появляется диалоговое окно.

Задание 5. Импорт сертификата из CER-файла.

При импорте из CER-файла следует учитывать, что в таком файле может храниться только сам сертификат без соответствующей ему ключевой пары RSA. В данной версии rtCert импорт из CER-файла возможен при выполнении двух условий:

Импорт производится в контейнер MS CAPI, уже существующий в памяти токена

В этом контейнере уже хранится, как минимум, ключевая пара RSA, соответствующая импортируемому сертификату (либо сам сертификат с ключевой парой)

Таким образом, на сегодняшний день импорт из CER-файла практически применим только для обновления или восстановления содержимого контейнера, по каким либо причинам испорченного в процессе работы.

Для импорта из CER-файла надо выбрать контейнер, а в нем - ключевую пару или сертификат, куда будет производиться импорт. Затем в диалоге Импорт сертификата из файла надо выбрать нужный тип файла. Кодировка CER-файла распознается утилитой автоматически.

После того как файл выбран, rtCert проверит, соответствует ли ключевая пара в памяти токена сертификату, хранящемуся в выбранном CER-файле. Если соответствует, то кнопка [Выбрать] становится активной, и можно нажать на нее для завершения операции.

По завершении операции сертификат из CER-файла будет импортирован в контейнер и дополнит хранящуюся в нем ключевую пару RSA (либо заместит аналогичный сертификат, уже записанный в контейнере). В будущих версиях rtCert функциональность при работе с CER - файлами будет разрешена.

Задание 6. Импорт сертификата из PFX-файла.

В PFX-файле хранится сертификат вместе с соответствующей ему ключевой парой RSA, т. е. такой файл содержит все данные, необходимые для последующей работы с сертификатом.

Импорт из PFX-файла сопряжен с созданием в памяти токена нового контейнера MS CAPI, в который и будет импортирован сертификат вместе с ключевой парой.

Для импорта сертификата в память токена нужно выбрать любой объект на токене, а в диалоге Импорт сертификата из файла выбрать соответствующий тип файла, выделить нужный PFX-файл и нажать кнопку [Выбрать].

После выбора PFX-файла появится диалоговое окно, в котором нужно ввести пароль для закрытого ключа и нажать кнопку [Далее].

В следующем диалоге нужно задать имя контейнера MS CAPI, в который будет импортирован сертификат, а также указать, будет ли закрытый ключ для этого сертификата экспортабельным.

Имя контейнера можно задать вручную, либо сгенерировать, нажав кнопку [Уникальное имя].

Установка флага Разрешить экспорт тому, что закрытый ключ из ключевой пары для этого сертификата при импортировании на токен получит свойство «экспортабельный». Это позволит в будущем экспортировать данный сертификат вместе с его ключевой парой обратно в PFX-файл.

Если такая операция не планируется, то рекомендуется не устанавливать этот флаг, т. к. степень защищенности экспортабельного ключа в памяти токена ниже.

По нажатию кнопки [Далее>] сертификат вместе со своей ключевой парой RSA будет импортирован в созданный на токене контейнер MS CAPI. В текущей версии rtCert имеются следующие ограничения на импорт сертификатов из PFX-файлов:

Импорт из PFX-файлов поддерживается только в ОС Windows 2000 и старше

Из PFX-файла импортируется только сертификат нижнего уровня (т. е. личный сертификат)

В будущих версиях rtCert функциональность при работе с PFX- файлами будет расширена.

Задание 7. Экспорт сертификата в файл.

Браузер сертификатов rtCert поддерживает возможность экспорта сертификата из памяти токена в файл.

Экспорт возможен в файлы тех же типов, из которых возможен импорт. При выборе пункта меню Действия | Экспорт сертификата в файл (либо аналогичной команды в контекстном меню, либо кнопки в панели инструментов) появится диалоговое окно.

Задание 8. Экспорт сертификата в CER-файл и PFX-файл.

Для экспорта в CER-файлы достаточно прав доступа Гостя. Процесс экспорта в CER-файл состоит из выбора нужного сертификата на токене и выбора пункта меню Действия | Экспорт сертификата в файл (либо аналогичной команды в контекстном меню, либо кнопки в панели инструментов).

В появившемся диалоге следует задать имя CER-файла, а в списке Файлы типа - выбрать нужную кодировку. Поддерживается 2 типа кодировки: DER и Base64.

По нажатию кнопки [Выбрать] сертификат (без соответствующей ему ключевой пары) будет экспортирован из памяти токена в указанный файл.

Экспорт сертификатов в PFX-файлы выполняется с правами доступа Пользователя. Для корректного экспорта ключевой пары сертификата необходимо, чтобы соответствующий закрытый ключ был экспортным.

Для экспорта в PFX-файл нужно отметить нужный сертификат в окне просмотра rtCert и выбрать пункт меню Действия|Экспорт сертификата в файл (либо аналогичную команду в контекстном меню, либо кнопку в панели инструментов).

В появившемся диалоге надо задать имя PFX-файла, а в списке Файлы типа выбрать «Файлы обмена личной информацией (*.PFX)» .

В нем нужно задать пароль для защиты закрытого ключа. По нажатию кнопки [Далее>] сертификат вместе с ключевой парой будет экспортирован из памяти токена в указанный файл.

Задание 9. Назначение контейнера по умолчанию.

Понятие контейнера по умолчанию весьма часто используется в ОС Windows. Так, для осуществления Logon в домене Windows используется сертификат, хранящийся в контейнере по умолчанию. Утилита rtCert позволяет назначить любой из контейнеров, записанных в памяти ruToken, контейнером по умолчанию. Если сертификат, хранящийся в этом контейнере, имеет признак Smartcard Logon или Smartcard User, такой сертификат будет использован Windows при выполнении входа в домен с использованием данного ruToken.

Для того чтобы назначить контейнер по умолчанию, нужно отметить контейнер в окне просмотра rtCert и выбрать пункт меню Действия|Сделать контейнером по умолчанию (либо аналогичную команду в контекстном

меню, либо кнопку в панели инструментов). По окончании операции контейнер получит признак «по умолчанию» и будет помечен в списке жирным шрифтом.

Если в памяти токена уже существовал контейнер по умолчанию, новый контейнер станет контейнером по умолчанию вместо него (т. е. может существовать только один контейнер по умолчанию). Для выполнения данной операции требуются права доступа Пользователя.

Задание 10. Отмена контейнера по умолчанию и удаление контейнера.

Выписанный сертификационным центром сертификат с признаком Smartcard Logon или Smartcard User чаще всего записывается в контейнер по умолчанию. Если же в памяти токена уже существует контейнер по умолчанию, он может быть физически уничтожен (т. е. перезаписан новым контейнером). Чтобы избежать этого и сохранить сертификат из контейнера по умолчанию, утилита rtCert предоставляет возможность отменить регистрацию этого контейнера как контейнера по умолчанию.

Для выполнения операции нужно отметить контейнер по умолчанию в окне просмотра rtCert (контейнер по умолчанию выделен в списке жирным шрифтом) и выбрать пункт меню Действия|Убрать состояние «по умолчанию» (либо аналогичную команду в контекстном меню, либо кнопку в панели инструментов). По окончании операции в памяти токена не будет контейнера по умолчанию, и теперь можно безопасно выписывать новый сертификат. Для выполнения операции требуются права доступа Пользователя.

Операция Удаление позволяет удалить из памяти токена контейнер MS CAPI вместе со всем его содержимым. Для выполнения операции требуются права доступа Пользователя. Кроме того, должен быть отмечен пункт меню Вид|Показывать контейнеры. Для удаления контейнера нужно в левом фрейме окна просмотра отметить контейнер для удаления и выбрать пункт меню Действия|Удалить контейнер (либо аналогичную команду в контекстном меню, либо кнопку в панели инструментов). После соответствующего предупреждения контейнер со всем содержимым будет физически удален из памяти токена.

Вопросы и практические задания.

1. Для чего предназначен браузер сертификатов ruToken?
2. Какие элементы управления отображаются в главном окне браузера сертификатов?
3. Зачем необходима аутентификация Пользователя?
4. Добавьте любой сертификат в хранилище сертификатов, а затем удалите его.
5. Из файлов каких типов можно импортировать сертификаты?
6. Импортируйте любой сертификат из CER-файла.
7. Какие имеются в текущей версии ограничения на импорт сертификатов из PFX-файлов?
8. Экпортируйте сертификат из любого файла.
9. Назначьте контейнер по умолчанию.

Список литературы.

1. www.rutoken.ru - официальный сайт разработчика
2. Руководство Пользователя ruToken

Тема 6. Система биометрической идентификации BioLink.

Лабораторная работа. BioLink U-Match 3.5

Теоретическая часть

Описание ПО BioLink Authentication Center

Задание 1. Установка BioLink Windows Logon

Задание 2. Первый вход в систему по отпечатку пальца или по паролю

Задание 3. Разблокирование рабочей станции

Задание 4. Создание новой персоны

Задание 5. Установка BioLink Password Vault

Задание 6. Написание сценария для DialUp – подключения.

Задание 7. Написание сценария для программы TrueCrypt

Задание 8. Написание сценария для почтового сервера.

Контрольные вопросы

Список использованных источников.

Теоретическая часть

BioLink U-Match 3.5 - офисный оптический USB-сканер отпечатков пальцев. Сканеры отпечатков пальцев BioLink U-Match 3.5 пользуются особой популярностью у заказчиков. Количество выпущенных сканеров данной модели уже составляет десятки тысяч штук, эти сканеры применяются сотрудниками сотен коммерческих компаний и государственных структур более чем в 50 странах мира.

Системные требования:

- процессор Pentium 200 MHz, 32 Мб RAM и более (рекомендуется 64 Мб RAM)
- Microsoft Windows 98/ME/NT/2000/XP/2003/Vista

- свободный USB-порт

- наличие какого-либо из программных продуктов BioLink: IDenium, BioTime, Authentication Center 5.x, SDK 5.x и выше, другого ПО, разработанного на основе BioLink SDK

Технические характеристики BioLink U-Match 3.5:

Способ сканирования оптический

Окно сканирования отпечатков 25,5 * 18 мм

Разрешение 508 dpi

Скорость сканирования 1/15 с

False Acceptance Rate (FAR — вероятность допуска «чужого») (1 случай из 1 000 000 000)

Размеры (длина * ширина * высота) 45 * 63 * 26 мм

Вес 120 г

Интерфейс USB 2.0/1.1, plug&play, кабель

2 м в комплекте поставки

Рабочая температура от -10°C до +55°C

Влажность (без конденсата) от 30% до 90%

Энергопотребление (по USB) 350 мВт (режим сканирования) 100 мВт (режим Standby) 40 мВт («спящий» режим)

Исполнение настольное корпусное устройство

Описание ПО BioLink Authentication Center

Программное обеспечение биометрической идентификации BioLink Authentication Center (BioLink AC) применяется для идентификации

пользователей локальных компьютеров (в т.ч. ноутбуков). В корпоративных сетях для идентификации пользователей и управления их доступом к информационным ресурсам применяется сервис BioLink IDenium.

ПО BioLink AC функционирует под управлением операционных систем Microsoft Windows 9x/Me/NT4/2000/XP/2003. Для биометрической идентификации пользователей операционных систем Microsoft Windows более поздних версий применяется сервис BioLink IDenium.

Используя ПО BioLink Authentication Center, можно заменять отпечатком пальца многочисленные пароли для доступа в сеть и к документам, обрабатываемым прикладными программами.

Изображение отпечатка пальца преобразуется в цифровую модель (шаблон), обратное преобразование шаблона в изображение реального биометрического идентификатора невозможно.

При идентификации пользователя формируется цифровая модель вновь предъявленного идентификатора, которая сравнивается с моделью ранее зарегистрированного отпечатка пальца. При совпадении моделей разрешается доступ в операционную систему (или документу, созданному с помощью прикладной программы).

В состав ПО BioLink Authentication Center входят модули BioLink Windows Logon и BioLink Password Vault.

Первым на компьютер следует устанавливать компонент BioLink Windows Logon. Он отвечает за биометрическую аутентификацию пользователя при входе в операционную систему, домен или обращении к ресурсам компьютера.

Затем, по желанию пользователя, можно установить BioLink Password Vault, который позволяет автоматизировать и упростить выполнение повседневных задач.

Задание 1. Установка BioLink Windows Logon.

Чтобы установить BioLink Windows Logon:

Шаг 1. Подключите к компьютеру устройство серии BioLink U-Match, следуя инструкциям по установке устройства. При необходимости перезагрузите компьютер.

Шаг 2. Вставьте компакт-диск с программным обеспечением BioLink Authentication Center в устройство чтения компакт-дисков (CD-ROM).

Примечание. На компьютере под управлением Windows NT 4.0/2000/XP необходимо зарегистрироваться под учетной записью локального администратора.

Шаг 3. Если устройство чтения компакт-дисков (CD-ROM) установлено в режим

автоматического запуска Autorun, программа автозапуска Autorun запустится автоматически. В противном случае Вы можете запустить ее вручную.

Для этого в меню

Пуск выберите команду Выполнить и нажмите кнопку Обзор, выберите сначала устройство CD-ROM вашего компьютера, затем файл Autorun.exe. В окне Запуск программы нажмите кнопку ОК.

Шаг 4. В меню установки АС выберите команду Установка BioLink Windows Logon.

В окне подготовки будет отображаться индикатор процесса, что позволит Вам наблюдать за ходом подготовки к установке BioLink Windows Logon на Ваш компьютер.

Шаг 5. Дождитесь появления на экране окна приветствия программы установки BioLink Windows Logon и нажмите Далее.

Шаг 6. В окне Сведения ознакомьтесь с последними обновлениями и изменениями в программе и нажмите кнопку Далее.

Шаг 7. В окне Лицензионное соглашение прочитайте текст лицензионного соглашения до конца. Для просмотра полного текста лицензионного соглашения используйте клавиши клавиатуры Стрелка Вниз, Page Down либо мышь. Затем выберите Да и нажмите кнопку Далее.

Шаг 8. В окне Выбор папки назначения нажмите Обзор, чтобы выбрать папку для установки BioLink Windows Logon. Для продолжения нажмите Далее.

Шаг 9. Если вы устанавливаете BioLink Windows Logon на компьютер, на котором уже есть база данных АС, на экране появится окно Выбор варианта. Вы можете удалить ранее созданную базу данных, выбрав настройку Удалить базу данных. Если вы хотите сохранить существующую базу данных, выберите настройку Сохранить имеющуюся базу данных.

Шаг 10. Если база данных АС пуста (это возможно в том случае, если вы устанавливаете АС на компьютер впервые, или если вы удалили старую

базу данных), вы должны ввести имя и пароль локального администратора АС в окне Администратор локальной базы данных.

Шаг 11. В окне Выбор компонентов выберите компоненты, которые следует установить. После того, как компоненты выбраны, нажмите кнопку Далее.

Шаг 12. В окне Язык интерфейса выберите язык интерфейса (названия команд, окон, текст сообщений и т.д.) приложения BioLink Windows Logon.

Шаг 13. В окне Начало копирования файлов представлена информация о тех файлах, которые вы устанавливаете на ваш компьютер. Чтобы вернуться к предыдущему окну, воспользуйтесь кнопкой Назад. Для продолжения нажмите кнопку Далее.

Примечание. В ходе установки драйвера устройства BioLink U-Match на экране появится окно Цифровая подпись не найдена. Нажмите Да для продолжения установки.

Шаг 14. В окне завершения установки нажмите кнопку Готово.

Шаг 15. После нажатия кнопки Готово компьютер перезагрузится автоматически.

Задание 2. Первый вход в систему по отпечатку пальца или по паролю.

Чтобы войти в систему по отпечатку пальца, выполнить следующие действия:

Шаг 1. Запустите компьютер

Шаг 2. После того, как компьютер запустится, на экране появится окно Вход в систему с приглашением приложить палец к окну сканера для отпечатков пальцев.

Шаг 3. Приложите палец к окну сканера.

Шаг 4. После успешного распознавания Вас по отпечатку Вашего пальца загрузится операционная система.

Или

Чтобы войти в систему по паролю:

Шаг 1. Включите компьютер

Шаг 2. После загрузки на экране появится окно Вход в систему Шаг 3. Выберите вкладку Вход по паролю

Далее:

Введите следующие данные:

- Имя пользователя в поле имя

- Пароль пользователя для входа на сервер АС в поле пароль Нажмите кнопку ОК или клавишу ввода Enter

Задание 3. Разблокирование рабочей станции.

Использование блокировки компьютера является одним из первостепенных условий надежной защиты ресурсов пользователя от несанкционированного доступа. Authentication Center позволяет использовать биометрическую идентификацию пользователя вместо парольной при разблокировании компьютера.

Для снятия блокировки используется описанная ниже процедура. Независимо от того, каким способом Вы заблокировали компьютер - вручную, нажатием на клавиши CTRL+ALT+DEL, или посредством защищенной паролем экранной заставки - при попытке получить доступ к компьютеру на экране появляется окно Снятие блокировки.

Чтобы разблокировать компьютер, выполните следующие действия: На компьютере под управлением Windows NT/2000/XP

Приложите палец к окну сканера отпечатков пальцев, следуя инструкциям в окне Снятие блокировки.

или

Воспользуйтесь вкладкой Вход по паролю для ввода имени и пароля персоны в АС.

На компьютере под управлением Windows 9x/Me

Нажмите любую клавишу для вывода на экран окна Снятие блокировки и затем приложите палец к окну сканера отпечатков пальцев.

Или

Воспользуйтесь вкладкой Вход по паролю для ввода имени и пароля персоны Authenticon, а затем нажмите кнопку ОК.

Если на компьютере, работающем под управлением Windows 95/98/Me, установлена не защищенная паролем экранная заставка, то после установки АС автоматически активизируется опция Защита паролем в свойствах экранной заставки, а на экране появится предупреждение.

Задание 4. Создание новой персоны.

Персона в АС должна создаваться для каждого пользователя, получающего доступ к системным и/или сетевым ресурсам. Персона АС имеет личные идентификаторы, которые служат для распознавания или проверки пользователя и включают в себя имя и пароль пользователя, а также эталон его отпечатка пальца. Если база данных АС не содержит никаких идентификационных сведений, пользователь не сможет получить доступ к ресурсам, защищенным центром аутентификации АС.

Примечание. Только пользователи с привилегиями администратора АС имеют право добавлять новые персоны.

Чтобы зарегистрировать новую персону, используя приложение BioLink Logon Manager:

Шаг 1. Запустите Мастер BioLink одним из следующих способов:

-В меню Персона выберите Создать.

-Нажмите INSERT.

-На панели инструментов нажмите кнопку Создание новой персоны

-Правой кнопкой мыши щелкните по имени любой персоны в левой области окна BioLink Logon Manager и выберите команду Создать в контекстном меню.

Шаг 2. Для продолжения в окне Мастер BioLink - Добро пожаловать нажмите кнопку Далее.

Примечание. В любой момент можно прервать процедуру создания новой персоны нажатием кнопки Отмена либо клавиши ESC.

Шаг 3. В окне Мастер BioLink - Создание новой персоны введите имя персоны, полное имя персоны (не обязательно) и описание (не обязательно). Укажите, если необходимо, следующие политики для персоны:

- Установите флажок Запретить использовать пароль для аутентификации, чтобы запретить пользователю применять пароль его персоны при входе в систему, разблокировке компьютера, выполнении Password Vault сценариев и т.д.
- Установите флажок Запретить персоне менять свои идентификаторы, чтобы запретить пользователю изменять его идентификаторы (эталон отпечатка и пароль персоны).
- Введите минимальную длину пароля персоны (возможные значения от 1 до 15).

Для продолжения нажмите Далее.

Шаг 4. Окно Обучение позволяет зарегистрировать идентификаторы для новой персоны. Выберите нужный тип идентификатора из списка Установленные устройства и нажмите кнопку Обучить.

Шаг 5. Чтобы создать эталон отпечатка пальца с использованием устройства серии BioLink U-Match:

- Выберите Сканер BioLink U-Match из списка Установленные устройства.
- Нажмите кнопку Обучить. Откроется окно Процесс обучения.
- Новый пользователь должен приложить свой палец к окну сканера устройства BioLink U-Match, и следовать инструкциям мастера. Если пользователь проходит процедуру обучения успешно, окно закрывается автоматически.

Обратите внимание, что для корректного обучения необходимо каждый раз немного изменять положение пальца при сканировании. Каждый раз при сканировании палец нужно приподнимать и вновь прикладывать с небольшим смещением и поворотом

Шаг 6. Чтобы ввести имя и пароль новой персоны:

- Выделите Пароль в списке Установленные устройства.
- Нажмите кнопку Обучить.

-Введите дважды пароль персоны в полях Пароль и Подтверждение пароля. Нажмите кнопку ОК.

Примечание. Пароль, указанный в данном окне, представляет собой пароль персоны в АС.

Пользователь может применять этот пароль для входа в систему вместо прохождения процедуры распознавания по отпечатку пальца в том случае, если это разрешено администратором системы.

Шаг 7. Чтобы завершить процедуру регистрации новой персоны, снимите флажок Да, я хочу установить связь сейчас. Для продолжения нажмите кнопку Далее.

Если флажок Да, я хочу установить связь сейчас установлен, Мастер BioLink предложит создать новую учетную запись в АС, либо выбрать уже существующую учетную запись и связать ее с новой персоной.

Шаг 8. Информация о новой персоне будет представлена в окне Мастер BioLink - Завершение.

Нажмите кнопку Готово для завершения процесса регистрации персоны.

Задание 5. Установка BioLink Password Vault

Шаг 1. Вставьте компакт-диск с программным обеспечением BioLink Authentication Center в устройство чтения компакт-дисков (CD-ROM).

Примечание. На компьютере под управлением Windows NT 4.0/2000/XP необходимо зарегистрироваться под учетной записью локального администратора.

Шаг 2. Если дисковод установлен в режим автоматического запуска Autorun, программа автозапуска Autorun запустится автоматически. В противном случае вы можете запустить ее вручную. Для этого в меню Пуск выберите команду Выполнить и нажмите кнопку Обзор, выберите ваш CD- ROM дисковод и затем файл Autorun.exe. В окне Запуск программы нажмите кнопку ОК.

Шаг 3. В меню установки Authentication Center выберите Установка BioLink Password Vault.

Шаг 4. Запустится программа установки BioLink Password Vault.

Шаг 5. В окне приветствия программы установки нажмите кнопку Далее.

Шаг 6. В окне Сведения ознакомьтесь с последними обновлениями и изменениями в программе и нажмите Далее .

Шаг 7. В окне Лицензионное соглашение прочитайте текст лицензионного соглашения до конца. Для просмотра полного текста лицензионного соглашения используйте клавиши клавиатуры Стрелка вниз, Page Down либо мышь. Затем выберите Да и нажмите Далее.

Шаг 8. В окне Выбор папки назначения нажмите Обзор, чтобы выбрать папку для установки BioLink Password Vault. Для продолжения нажмите Далее.

Шаг 9. В окне Выбор компонентов выберите компоненты для установки. По завершении нажмите Далее.

Шаг 11. В окне Начало копирования файлов просмотрите настройки установки. Чтобы вернуться назад и изменить параметры, воспользуйтесь кнопкой Назад. Для продолжения нажмите Далее.

Шаг 12. В окне завершения установки нажмите кнопку Готово. После нажатия Готово компьютер автоматически перезапустится.

После перезапуска системы на панели задач Windows появится значок программы Password Vault Agent: .

Написание сценариев.

Задание 6. Написание сценария для DialUp – подключения.

Шаг 1. Для начала нужно выбрать подключение. Для этого ПУСК – Сетевые подключения – DialUp.

Шаг 2. Далее нажимаем CTRL+ALT+F10. Появится окно с предложением записать сценарий.

Шаг 3. Заполните все необходимые поля и нажмите на кнопку вызов.

Шаг 4. Нажмите CTRL+ALT+F11 для завершения процедуры записи сценария. На экране появится окно, информирующее пользователя об окончании записи сценария.

Шаг 5. Введите необходимую информацию о только что записанном сценарии и нажмите Сохранить для его сохранения в базе данных.

Шаг 6. В свойствах сценария, перейдите на вкладку Параметры и отметьте следующие параметры Проверка правильности работы сценария.

Шаг 7. Закройте приложение или окно, для которого был создан сценарий, а затем откройте его вновь.

Шаг 8. На экране появится приглашение пройти верификацию по отпечатку пальца. Следуя указаниям программы, приложите палец к окну сканера.

Шаг 9. После того, как права пользователя подтверждены, программа Password Vault выполнит записанный сценарий. Результатом успешного выполнения сценария будет запуск интернет – соединения.

Задание 7. Написание сценария для программы TrueCrypt.

Шаг 1. Запустите программу TrueCrypt.

Шаг 2. Далее нажимаем CTRL+ALT+F10. Появится окно с предложением записать сценарий.

Шаг 3. Выберите файл – контейнер и нажмите кнопку Mount.

Шаг 4. Введите пароль и нажмите кнопку ОК.

Шаг 5. Нажмите CTRL+ALT+F11 для завершения процедуры записи сценария. На экране появится окно, информирующее пользователя об окончании записи сценария.

Шаг 6. Введите необходимую информацию о только что записанном сценарии и нажмите Сохранить для его сохранения в базе данных.

Шаг 7. В свойствах сценария, перейдите на вкладку Параметры и отметьте необходимые параметры Проверка правильности работы сценария.

Шаг 7. Закройте TrueCrypt, а затем откройте его вновь.

Шаг 8. На экране появится приглашение пройти верификацию по отпечатку пальца. Следуя указаниям программы, приложите палец к окну сканера.

Шаг 9. После того, как права пользователя подтверждены, программа Password Vault выполнит записанный сценарий. Результатом успешного выполнения сценария будет запуск программы TrueCrypt, и монтирование контейнера.

Задание 8. Написание сценария для почтового сервера.

Шаг 1. Перейдите на сайт <http://www.mail.ru>.

Шаг 2. Далее нажимаем CTRL+ALT+F10. Появится окно с предложением записать сценарий.

Шаг 3. Заполните поля Имя и пароль.

Шаг 4. Нажмите кнопку Войти.

Шаг 5. Нажмите CTRL+ALT+F11 для завершения процедуры записи сценария. На экране появится окно, информирующее пользователя об окончании записи сценария.

Шаг 6. Введите необходимую информацию о только что записанном сценарии и нажмите Сохранить для его сохранения в базе данных.

Шаг 7. В свойствах сценария, перейдите на вкладку Параметры и отметьте необходимые параметры

Проверка правильности работы сценария.

Шаг 7. Закройте браузер, а затем откройте его вновь и перейдите по ссылке <http://www.mail.ru>.

Шаг 8. На экране появится приглашение пройти верификацию по отпечатку пальца. Следуя указаниям программы, приложите палец к окну сканера.

Шаг 9. После того, как права пользователя подтверждены, программа Password Vault выполнит записанный сценарий. Результатом успешного выполнения сценария будет автоматический вход в почтовую систему.

Контрольные вопросы.

1. Подключите к компьютеру устройство BioLink U-Match 3.5.
2. Установите программное обеспечение Authentication Center.
3. Создайте нового администратора в Windows Logon.
4. Создайте ограниченную учетную запись в Windows Logon, создайте новую персону и свяжите их.
5. Напишите сценарий для программы Microsoft Outlook.
6. Напишите еще один сценарий для данной программы.
7. Напишите сценарий для любой Web-страницы, содержащей поля для ввода имени пользователя и пароля.
8. Удалите программный комплекс АС.

Список использованных источников.

1. Руководство пользователя Autentication Center
2. <http://www.biolink.ru>

Лабораторная работа. Настройка системы идентификации и учета рабочего времени

Теоретическая часть

Задание №1 Настройка подключения компонента BioTime Agent

Задание №2 Добавление события

Задание №3 Отмечание отсутствия

Задание №4 Отмечание отсутствия с помощью области «События за выбранный день»

Задание №5 Удаление события

Задание №6 Удаление отсутствия

Задание №7 Просмотр событий за выбранный день

Задание №8 Добавление нового отчета

Задание №9 Просмотр отчетов

Задание №10 Экспорт данных отчетов

Задание №11 Удаление отчетов

Вопросы и практические задания

Теоретическая часть

Приложение BioTime Agent является «мгновенным информатором» позволяет быстро и удобно наблюдать за всеми событиями, регистрируемыми системой. Интерфейс приложения BioTime Agent представлен на рисунке ниже.

Цифрами на рисунке обозначены:

- 1) Диалоговое окно Настройки приложения BioTime Agent. Позволяет настраивать подключение к BioTime Server и внешний вид окна приложения BioTime Agent.
- 2) Окно приложения BioTime Agent.
- 3) Список всех сотрудников, зарегистрированных в BioTime. Отображается в окне BioTime Agent.
- 4) Всплывающие сообщения BioTime Agent, информирующие пользователя обо всех событиях, зарегистрированных системой.
- 5) Контекстное меню BioTime Agent.
- 6) Значок приложения BioTime Agent в области пиктограмм панели задач Windows.

Применение BioTime Agent оправдано в следующих случаях:

Службе персонала или руководителям организации требуется постоянный контроль над сотрудниками. В таком случае на компьютер(ы) устанавливается BioTime Agent, позволяющий в режиме реального времени анализировать приходы и уходы зарегистрированных сотрудников.

Сотрудникам организации необходимо знать присутствуют ли их коллеги на рабочем месте. В крупных организациях, чьи офисы могут занимать несколько этажей или вообще находиться на некотором расстоянии друг от друга, проблема связи между сотрудниками остается почти всегда неразрешенной. С помощью BioTime Agent теперь не надо будет долго звонить коллеге, подниматься на другой этаж или отправлять письма по электронной почте, чтобы узнать находится ли он(а) на рабочем месте.

Конечно, указанными двумя ситуациями возможности по использованию BioTime Agent не ограничиваются. Все зависит от конкретных задач, стоящих перед службами управления персоналом в различных организациях.

Чтобы наблюдать за всеми событиями, регистрируемыми сотрудниками, достаточно запустить приложение BioTime Agent. Как только какое-либо событие будет зарегистрировано кем-либо из сотрудников, появится всплывающее сообщение, сообщающее ФИО сотрудника, зарегистрировавшего событие, дату, время и тип события.

Отчеты – неотъемлемая часть любой системы учета рабочего времени, особенно биометрической. Без них все усилия персонала компании, сбор данных, регистрация событий, ввод причин отсутствия и т.д. были бы полностью бесполезны. Можно сказать, что отчеты – это визуальное представление данных, содержащихся в базе данных системы. Чем более гибкими, удобными, понятными пользователям являются отчеты, тем проще и эффективнее работать с системой сотрудникам отделов персонала и HR.

Отчеты BioTime

служат для наглядного представления, сортировки и анализа всех зарегистрированных в BioTime событий в форме и виде, соответствующим

стандартам Российской Федерации в области учета рабочего времени и управления человеческими ресурсами предприятия;

оперативно и наглядно иллюстрируют события прихода/ухода сотрудников, их присутствие на рабочих местах;

позволяют выявить прогулы, недоработки и переработки, понять, сколько часов отработал тот или иной сотрудник и весь отдел в целом;

позволяют мгновенно оценить сложившуюся ситуацию в компании, принять быстрые, своевременные, и, самое главное, правильные решения в области

учета рабочего времени и контроля доступа.

Виды отчетов

В BioTime по умолчанию уже созданы следующие виды отчетов:

Табель Т13 (стандартный табель учета рабочего времени, созданный в соответствии с требованиями и нормами РФ в области учета и управления кадрами);

Журнал рабочего времени (отчет, показывающий статистику посещения офиса сотрудниками компании. Содержит следующие поля: Время прихода, Время ухода, Отработано, Норма, Недоработка, Переработка, Опоздание, Ранний уход);

Табель прихода (отчет, показывающий время прихода сотрудников на работу);

Табель ухода (отчет, показывающий время ухода сотрудников с работы)

Статистика посещений (отчет, показывающий общую статистику посещения офиса сотрудниками организации).

Журнал автоуходов (отчет, выделяющий сотрудников, забывающих отметить свой уход с работы).

Журнал причин отсутствия (отчет, показывающий в наглядной форме, кто и по какой причине отсутствовал в офисе).

Дни рождения сотрудников (отчет, отображающий дни рождения сотрудников в отсортированном по месяцам порядке).

Журнал опозданий (отчет, показывающий опаздывающих сотрудников, а также дату и время опоздания).

Табель рабочего времени (отчет, показывающий время, отработанное сотрудниками).

Расписание рабочих смен (отчет, позволяющий получить информацию о графиках выходов сотрудников на работу).

Расчет заработной платы (отчет, позволяющий получать информацию о количестве начисленных сотрудникам денежных средств в зависимости от фактически отработанного времени).

Ход работы:

Задание №1 Настройка подключения компонента BioTime Agent.

Настроить приложение BioTime Agent в соответствии с потребностями и предпочтениями пользователя можно с помощью диалогового окна Настройки.

Настройка BioTime Agent включает в себя следующие задачи:

настройка подключения к серверу BioTime;

настройка отображения списка сотрудников (кроме шрифта отображения и интервала обновления списка сотрудников, можно создать

свой собственный список сотрудников, чьи события будут отображаться BioTime Agent).

настройка прозрачности окна приложения BioTime Agent; включение или выключение всплывающего сообщения;

включение или выключение показа времени зарегистрированных событий.

Задание №2 Добавление события.

Добавление нового события происходит с помощью одноименного Мастера. Но гораздо удобнее использовать область События за выбранный день, так как в этом случае ФИО сотрудника и примерный временной интервал, в котором будет зарегистрировано событие, автоматически добавляются воответствующие поля Мастера.

Чтобы добавить событие с помощью раздела События за выбранный день, выполните следующие действия:

- 1) В Панели списков выберите сотрудника, для которого требуется добавить событие.
- 2) В разделе Календарь выберите день, когда требуется добавить новое событие.
- 3) В разделе События за выбранный день выберите нужный промежуток времени, щелкнув по строке таблицы мышкой.
- 4) Нажмите правую кнопку мыши, чтобы открыть контекстное меню.
- 5) В контекстном меню выберите пункт Добавить событие.
- 6) Откроется Мастер добавления нового события, где можно будет указать точное время события, тип события и, если требуется, изменить сотрудника, для которого это событие следует добавить.

Задание №3 Отмечание отсутствия.

Чтобы отметить отсутствие сотрудника на рабочем месте вы можете использовать:

Область Календарь функциональной страницы Журнал;

Область События за выбранный день функциональной страницы Журнал;

Мастер добавления отсутствия (запускаемый с функциональных страниц Журнал и Общая информация).

Отмечание отсутствия с помощью области Календарь

Чтобы отметить отсутствие с помощью календаря, выполните следующие действия:

- 1) В области Календарь щелчком левой кнопки мыши выделите первый день отсутствия.
- 2) Не отпуская кнопку мыши подведите курсор к последнему дню отсутствия.
- 3) Отмеченный интервал окрасится в синий цвет.
- 4) Щелкните правой кнопкой мыши на выделенном интервале.
- 5) Из появившегося контекстного меню выберите Отметить отсутствие.
- 6) Откроется Мастер добавления отсутствия. Далее следуйте инструкциям на экране.

Задание №4 Отмечание отсутствия с помощью области «События за выбранный день».

Чтобы отметить отсутствие с помощью раздела События за выбранный день, выполните следующие действия:

- 1) В Панели списков выберите сотрудника, для которого требуется отметить отсутствие.
- 2) В разделе Календарь выберите день, когда сотрудник отсутствовал на работе.
- 3) Выберите начало интервала, щелкнув мышкой по нужной строке таблицы.
- 4) Не отпуская кнопку мыши, выделите все строки ниже вплоть до того времени, когда сотрудник пришел на работу.
- 5) Нажмите правую кнопку мыши, чтобы открыть контекстное меню.
- 6) В контекстном меню выберите пункт Отметить отсутствие.
- 7) Откроется Мастер добавления отсутствия, где можно будет указать точное время начала и окончания отсутствия, причину отсутствия и, если требуется, изменить сотрудника, для которого это отсутствие следует отметить.

Задание №5 Удаление события.

Для удаления события выполните следующие действия:

- 1) В Панели списков выберите сотрудника, чье событие необходимо удалить.
- 2) В Панели информации в разделе Календарь выберите день, когда удаляемое событие было зарегистрировано.
- 3) В области События за выбранный день щелкните мышью по строке таблицы, содержащей информацию о событии.

- 4) Щелкните правой кнопкой мыши, чтобы открыть контекстное меню.
- 5) В контекстном меню выберите пункт Удалить событие. 6) Выбранное событие будет удалено.

Задание №6 Удаление отсутствия.

Для удаления отсутствия выполните следующие действия:

- 1) В Панели списков выберите сотрудника, чье отсутствие необходимо отменить.
- 2) В Панели информации в разделе Календарь щелкните правой кнопкой мыши на любом дне, входящим в удаляемый интервал отсутствия.

- 3) В открывшемся контекстном меню выберите пункт Удалить отсутствие.

Задание №7 Просмотр событий за выбранный день.

Чтобы просмотреть события за выбранный день, выполните следующие действия:

- 1) В Панели списков щелчком мыши выберите сотрудника, чьи события необходимо просмотреть.
- 2) В Панели информации в разделе Календарь выберите день, за который требуется просмотреть события.
- 3) В таблице в разделе События за выбранный день появится список всех зарегистрированных в этот день событий для выбранного сотрудника.

Обратите внимание на список. Приход и уход отображаются разными цветами. Также при ручном добавлении событий в скобках после типа события указывается сотрудник, добавивший это событие.

Задание №8 Добавление нового отчета.

Чтобы добавить в BioTime новый тип отчета, запустите Мастер добавления нового отчета и следуйте инструкциям Мастера. Вам будет предложено указать путь к файлу отчета (.rpt).

Для добавления нового события выполните следующие действия:

1. В Панели задач выберите элемент Отчеты.
2. В разделе Действия выберите пункт Добавить новый отчет.

– или – нажмите Действия – Добавить новый отчет.

– или – щелкните левой кнопкой мыши по соответствующей кнопке на панели инструментов

3. Откроется Мастер добавления нового отчета.

4. Следуйте указаниям мастера. Переключение между закладками мастера осуществляется с помощью кнопки Далее и Назад. Для сохранения сделанных изменений на последнем этапе нажмите Сохранить. Для выхода из мастера нажмите Отмена.

Задание №9 Просмотр отчетов.

Чтобы просмотреть результаты отчета, выполните следующие действия:

- 1) В разделе Выбор типа отчета функциональной страницы Отчеты выберите тот отчет, результаты которого необходимо просмотреть и проанализировать.
- 2) Настройте Фильтр Панели Информации.

Для этого:

1. В поле Отдел из раскрывающегося списка выберите отдел (подразделение) компании, по которому будет построен отчет.
2. Из раскрывающегося списка в поле Сотрудник выберите сотрудника, по которому будет построен отчет. Обратите внимание, что используя это поле, также можно выбрать категорию сотрудников, для которых будет построен отчет. Это удобно, если необходимо построить отчет по всем сотрудникам, относящимся к, например, категории Внештатные. 3. Установите промежуток времени, за который требуется построить отчет (область За период).
4. Далее выберите вид сортировки. Доступны следующие значения: Сотрудник
Позиция

5. Установите Порядок сортировки, выбрав одно из двух значений: По убыванию или По возрастанию.

6. В области Помещения выберите помещение. В отчете будут отражены данные, относящиеся только к выбранному помещению.

7. Настройте дополнительные режимы фильтрации данных в отчетах, если таковые присутствуют.

Задание №10 Экспорт данных отчетов.

Экспорт отчетов по внешние форматы может быть удобен для:

обмена данными с внешними корпоративными системами (если экспорт данных напрямую в эти системы не поддерживается BioTime;

печати данных отчетов в составе других документов;

структурирования и хранения отчетов, если того требует общая концепция документооборота компании;

отправки отчета по электронной почте;

Чтобы сохранить отчет в файл, выполните следующие действия:

1) Создайте отчет.

2) Щелкните по ссылке Сохранить результат.

3) Откроется стандартное Windows окно Сохранить как. В поле Тип файла из раскрывающегося списка выберите требуемый формат экспорта отчета.

Доступные форматы экспорта отчетов:

Документ Excel; Документ HTML; Документ XML.

4) Нажмите кнопку Сохранить. Отчет будет сохранен в файл.

Задание №11 Удаление отчетов.

Чтобы удалить отчет, выполните следующие действия:

1. В Панели задач выберите тот отдел, который необходимо удалить.

2. В разделе Действия нажмите Удалить отдел.

– или – нажмите Действия – Удалить отдел

– или – щелкните левой кнопкой мыши по соответствующей кнопке на панели инструментов

Вопросы и практические задания.

1. Каковы основные функции и возможности BioTime Agent.

2. Каково применение BioTime Agent.

3. Назовите основные функции и виды отчетов.

4. Настройте подключение компонента BioTime Agent.

5. Добавьте событие с помощью раздела «События за выбранный день».

6. Отметьте отсутствие с помощью области «Календарь».

7. Отметьте отсутствие с помощью раздела «События за выбранный день».

8. Удалите добавленное Вами событие/отсутствие.

9. С помощью чего инспектор и оператор могут просматривать информацию о времени работы сотрудников компании (организации).

10. Добавьте новый отчет.

11. Экспортируйте данные отчета в документ HTML.

12. Удалите отчет.

Список использованной литературы.

1. Biolink - [Электронный ресурс]. Режим доступа: <http://biolink.ru/>

2. Biotime - [Электронный ресурс]. Режим доступа: <http://biotime.ru/>

Тема 7. Методы защиты программного обеспечения от несанкционированного использования.

Лабораторная работа. Разработка программного продукта для работы с ЭЦП на основе электронных ключей ruToken

Теоретическая часть

Описание продукта.

Задание 1. Реализация процедуры создания в памяти ruToken нового контейнера.

Задание 2. Реализация процедуры удаления из памяти ruToken контейнера. 4 Задание 3. Реализация процедуры проверки существования контейнера ключей

Задание 4. Реализация процедуры генерации в контейнере заданного имени ключевой пары заданного размера. 6

Задание 5. Реализация процедуры экспорта открытого ключа из контейнера 7 Задание 6. Реализация процедуры просмотра открытого ключа.

Задание 7. Реализация процедуры подписи документа.

Задание 8. Реализация процедуры верификации подписи документа.

Вопросы и практические задания.

Теоретическая часть.

Электронная цифровая подпись - последовательность символов, полученная в результате криптографического преобразования электронных данных. ЭЦП добавляется к блоку данных и позволяет получателю блока проверить источник и целостность данных и защититься от подделки. ЭЦП используется в качестве аналога собственноручной подписи для организации юридически значимого электронного документооборота.

В реализации ЭЦП используются ассиметричные системы шифрования, генерирующие два разных ключа: один из ключей держится в

строжайшем секрете (он называется "закрытый"), другой - публикуется ("открытый"). Передаваемое сообщение (документ) отправитель шифрует своим закрытым ключом. Расшифровка происходит с помощью открытого ключа. То есть, расшифровать может кто угодно, а зашифровать - только отправитель. Таким образом, получатель, расшифровывая сообщение открытым ключом отправителя, производит его аутентификацию.

CryptoAPI

Для разработки в среде Delphi приложений, работающих с электронно- цифровой подписью (ЭЦП), используются криптографические возможности ОС Windows, а именно криптографический интерфейс прикладных программ (CryptoAPI).

Код функций криптографической подсистемы CryptoAPI содержится в нескольких динамически загружаемых библиотеках Windows (advapi32.dll, crypt32.dll). Для обращения к этим функциям из прикладной программы на Object Pascal можно объявить их как внешние, но проще использовать специально разработанный программистами Microsoft для этой цели модуль wcrypt2.pas., подключаемый к проекту.

Для использования возможностей CryptoAPI в работе Рутокена используется криптопровайдер «Aktiv ruToken CSP v1.0» (устанавливается в операционную систему вместе с драйверами Рутокена). Данный криптопровайдер, как и другие, представляет собой dll-файл. В нем описано 25 функций CryptoAPI, применимых к Рутокену. (Описание функций Aktiv ruToken CSP v1.0 смотрите в Руководстве пользователю Rutoken).

Описание продукта.

ruTokenEDS (от англ. EDS – electronic digital signature – электронно- цифровая подпись) - программный продукт, разработанный в среде Delphi и реализующий ЭЦП документов с помощью ruToken.

ЭЦП производится встроенными возможностями Windows с помощью криптопровайдера ruToken по следующему алгоритму:

1. в памяти ruToken создается криптографический контейнер для хранения ключевой пары (открытого и закрытого ключа);
2. для конкретного контейнера генерируется пара ключей заданного размера;
3. документ (выбранный файл в памяти Windows) подписывается: с помощью закрытого ключа шифруется хэш файла, результат сохраняется в виде двоичного файла в памяти Windows;

4. проверка подписи документа (выбранный файл в памяти Windows): с помощью открытого ключа, который должен был быть предварительно экспортирован получателю (сохранен в виде двоичного файла с выбранной директории Windows), происходит расшифровка файла, то есть верификация подписи .

Функции Rutoken EDS:

1. Работа с контейнерами ключей:

- Создание контейнера
- Удаление контейнера
- Проверка контейнера на существование

2. Работа с ключами подписи:

- Генерирование пары ассиметричных ключей в контейнере
- Экспорт открытого ключа из контейнера
- Просмотр экспортированного открытого ключа

3. Работа с подписями документов:

- Подпись электронного документа
- Верификация подписи документа

Задание 1. Реализация процедуры создания в памяти ruToken нового контейнера.

В программе за создание контейнера в памяти ruToken отвечает процедура CreateButtonClick (Листинг 1):

Листинг 1:

```
procedure TContainersForm.CreateButtonClick(Sender: TObject); var cont: PChar; err: string; hProv:
HCRYPTPROV; begin err := ContainerEdit.Text; cont
:= StrAlloc(length(err) + 1); StrPCopy(cont, err); if not CryptAcquireContext(@hProv, cont, 'Aktiv ruToken
CSP v1.0', PROV_RSA_FULL, CRYPT_NEWKEYSET) then begin //обработка ошибок
MessageDlg('Ошибка создания контейнера: ' + err, mtError, [mbOK], 0); exit; end else
MessageDlg('Создан контейнер с именем ' + err, mtInformation, [mbOK], 0); if not
CryptReleaseContext(hProv, 0) then begin //обработка ошибок MessageDlg('Не удалось освободить
контекст: ' + err, mtError, [mbOK], 0); end; end;
```

Создания в памяти ruToken нового контейнера происходит по заданному пользователем имени ContainerEdit.Text.

Для подключения к криптопровайдеру с заданным типом и именем и возвращения его дескриптора (контекста) используется функция CryptAcquireContext (дескриптор криптопровайдера, контейнер, криптопровайдер, тип провайдера, флаги). Для создания нового контейнера функции передается флаг CRYPT_NEWKEYSET.

Для освобождения дескриптора криптопровайдера используется функция CryptReleaseContext (провайдер, флаги).

Задание 2. Реализация процедуры удаления из памяти ruToken контейнера.

В программе за удаление контейнера из памяти ruToken отвечает процедура DeleteButtonClick (Листинг 2):

Листинг 2:

```
procedure TContainersForm.DeleteButtonClick(Sender: TObject); var cont:
PChar; err: string; hProv: HCRYPTPROV; begin err := ContainerEdit.Text; cont
:= StrAlloc(length(err) + 1); StrPCopy(cont, err); if not
CryptAcquireContext(@hProv, cont, 'Aktiv ruToken CSP v1.0', PROV_RSA_FULL,
CRYPT_DELETEKEYSET) then begin case int64(GetLastError) of
ERROR_INVALID_PARAMETER: err := 'ERROR_INVALID_PARAMETER';
ERROR_NOT_ENOUGH_MEMORY: err := 'ERROR_NOT_ENOUGH_MEMORY';
NTE_BAD_FLAGS: err
:= 'NTE_BAD_FLAGS'; NTE_BAD_KEYSET: err := 'NTE_BAD_KEYSET';
NTE_BAD_KEYSET_PARAM: err := 'NTE_BAD_KEYSET_PARAM'; NTE_BAD_PROV_TYPE: err
```

```

:= 'NTE_BAD_PROV_TYPE'; NTE_BAD_SIGNATURE: err := 'NTE_BAD_SIGNATURE';
NTE_EXISTS: err := 'NTE_EXISTS'; NTE_KEYSET_ENTRY_BAD: err :=
'NTE_KEYSET_ENTRY_BAD'; NTE_KEYSET_NOT_DEF: err := 'NTE_KEYSET_NOT_DEF';
NTE_NO_MEMORY: err := 'NTE_NO_MEMORY'; NTE_PROV_DLL_NOT_FOUND: err :=
'NTE_PROV_DLL_NOT_FOUND'; NTE_PROV_TYPE_ENTRY_BAD: err :=
'NTE_PROV_TYPE_ENTRY_BAD'; NTE_PROV_TYPE_NO_MATCH: err :=
'NTE_PROV_TYPE_NO_MATCH'; NTE_PROV_TYPE_NOT_DEF: err :=
'NTE_PROV_TYPE_NOT_DEF'; NTE_PROVIDER_DLL_FAIL: err :=
'NTE_PROVIDER_DLL_FAIL'; NTE_SIGNATURE_FILE_BAD: err :=
'NTE_SIGNATURE_FILE_BAD'; else err := 'Unknown error'; end;
MessageBox('Ошибка удаления контейнера: ' + err, mtError, [mbOK], 0); end
else MessageBox('Удален контейнер с именем ' + err, mtInformation, [mbOK],
0); end;

```

Для подключения к криптопровайдеру с заданным типом и именем и удаления из него контейнера заданного имени используется функция CryptAcquireContext (дескриптор криптопровайдера, контейнер, криптопровайдер, тип провайдера, флаги) с флагом CRYPT_DELETEKEYSET.

Для получения кода последней ошибки используется функция

GetLastError.

Задание 3. Реализация процедуры проверки существования контейнера ключей.

Если значение имени контейнера ключей пользователем не введено, проверять контейнер с именем текущего пользователя ОС.

За реализацию в программе проверки существования в памяти ruToken контейнера ключей с заданным именем отвечает процедура VerifyButtonClick (Листинг 3):

Листинг 3:

```

procedure TContainersForm.VerifyButtonClick(Sender: TObject); var cont:
PChar; err: string; hProv: HCRYPTPROV; begin if length(ContainerEdit.Text) =
0 then begin cont := nil; err := 'по умолчанию'; end else begin err :=
ContainerEdit.Text; cont := StrAlloc(length(err) + 1); StrPCopy(cont, err);
end; if not CryptAcquireContext(@hProv, cont, 'Aktiv ruToken CSP v1.0',
PROV_RSA_FULL, 0) then begin //обработка ошибок MessageBox('Ошибка
открытия контейнера: ' + err, mtError, [mbOK], 0); exit; end
else MessageBox('Контейнер с именем ' + err + ' успешно открыт',
mtInformation, [mbOK], 0); if not CryptReleaseContext(hProv, 0) then
//обработка ошибок end;

```

Процедура аналогична процедуре создания контейнера, только функции CryptAcquireContext не передается никакой флаг (0).

Если поле ContainerEdit.Text пусто, то имени контейнера присваивается значение по умолчанию - nil, что означает имя текущего пользователя системы.

Задание 4. Реализация процедуры генерации в контейнере заданного имени ключевой пары заданного размера.

За реализацию в программе генерации в контейнере заданного имени ключевой пары заданного размера отвечает процедура OkButtonClick (Листинг 4):

Листинг 4:

```

procedure TGenerateForm.OkButtonClick(Sender: TObject); var cont: PChar;
err: string; hProv: HCRYPTPROV; KeyExchKey, SignKey: HCRYPTKEY; flag, keyLen:
DWORD; begin err := ContainerEdit.Text; cont := StrAlloc(length(err) + 1);
StrPCopy(cont, err); if not CryptAcquireContext(@hProv, cont, 'Aktiv ruToken
CSP v1.0', PROV_RSA_FULL, 0) then begin //обработка ошибок MessageBox('Ошибка
открытия контейнера: ' + err, mtError, [mbOK], 0); exit; end; keyLen :=

```

```
strtoint(SignKeyLenEdit.text); flag := keyLen shl 16; if not
CryptGenKey(hProv, AT_SIGNATURE, flag, @SignKey) then begin //обработка
ошибок MessageDlg('Ошибка создания ключа подписи: ' + err, mtError, [mbOK],
0); end else MessageDlg('Ключи успешно сгенерированы ', mtInformation,
[mbOK], 0); if not CryptReleaseContext(hProv, 0) then begin //обработка
ошибок MessageDlg('Не удалось освободить контекст: ' + err, mtError, [mbOK],
0); end; end;
```

Для генерации в контейнере ключевой пары заданного размера используется функция CryptGenKey (провайдер, алгоритм, флаги, ключ): размер передается во флаге из поля SignKeyLenEdit.text.

Задание 5. Реализация процедуры экспорта открытого ключа из контейнера.

За реализацию в программе экспорта открытого ключа из контейнера отвечает процедура OkButtonClick (Листинг 5):

Листинг 5:

```
procedure TExportForm.OkButtonClick(Sender: TObject); var cont: PChar;
err: string; hProv: HCRYPTPROV; key, expKey: HCRYPTKEY; pbuf: PBYTE; buflen:
DWORD; f: file; hash: HCRYPTHASH; begin //инициализация криптопровайдера и
открытие контейнера заданного имени с обработкой ошибок repeat if not
CryptGetUserKey(hProv, AT_SIGNATURE, @key) then //обработка ошибок {$B-} if
not (CryptExportKey(key, 0, PUBLICKEYBLOB, 0, nil, @buflen)) then begin
//обработка ошибок MessageDlg('Ошибка открытия контейнера: ' + err, mtError,
[mbOK], 0); exit; end; GetMem(pbuf, buflen); if not (CryptExportKey(key, 0,
PUBLICKEYBLOB, 0, pbuf, @buflen)) then begin //обработка ошибок
MessageDlg('Ошибка получения ключа подписи: ' + err, mtError, [mbOK], 0);
break; end; if not CryptDestroyKey(key) then begin //обработка ошибок
MessageDlg('Ошибка освобождения дескриптора ключа подписи: ' + err, mtError,
[mbOK], 0); end; //сохранение содержимого буфера pbuf в файл until true;
//освобождение дескриптора контейнера с обработкой ошибок end;
```

Чтобы запросить у криптопровайдера дескриптор самого экспортируемого ключа используется функция CryptGetUserKey (провайдер, описание ключа, дескриптор ключа). Описание ключа - это либо AT_KEYEXCHANGE (ключи обмена), либо AT_SIGNATURE (ключ подписи).

Название функции CryptExportKey(дескриптор ключа, шифрование, тип ключа, флаги, буфер, длина буфера) говорит само за себя. Заметим, что параметры шифрование и флаги для криптопровайдера ruToken всегда должны быть равны 0.

В первый раз CryptExportKey вызывается со значение буфера равным nil, так как не известна его длина buflen. Затем определяется длина в функции GetMem(буфер, длина буфера). Затем в функции CryptExportKey уже с указанным буфером pbuf происходит экспорт в него ключа. Затем идет сохранение ключа из буфера в файл.

Задание 6. Реализация процедуры просмотра открытого ключа.

За реализацию в программе просмотра заданного открытого ключа, предварительно экспортированного в память ОС Windows в виде двоичного файла, отвечает процедура ViewClick (Листинг 6):

Листинг 6:

```
procedure TMainForm.ViewClick(Sender: TObject); var f: file of byte; b,
i: byte; s: string; begin OpenFileDialog1.Title := 'Выберите файл с открытой
частью ключа'; if OpenFileDialog1.Execute then begin AssignFile(f,
OpenFileDialog1.FileName); reset(f); s := ''; read(f, b); s := s + ByteToHex(b);
i := 1; while not eof(f) do begin read(f, b); s := s + '-' + ByteToHex(b);
inc(i); if i = 20 then begin ViewMemo.Lines.Add(s); i := 0; s := ''; end;
end; if i > 0 then ViewMemo.Lines.Add(s); CloseFile(f); end; end;
```

В данной процедуре происходит выбор и открытие файла с ключом на считывание(функции OpenFileDialog.Execute, AssignFile, reset)

Затем посимвольное считывание перевод из битового типа в символьный и запись в мемо(функции read, ByteToHex, ViewMemo.Lines.Add)

Задание 7. Реализация процедуры подписи документа.

За реализацию в программе подписи документа с помощью закрытого ключа указанного именем контейнера отвечает процедура SignButtonClick (Листинг 7):

Листинг 7:

```
procedure TSigningForm.SignButtonClick(Sender: TObject); var cont:
PChar; err: string; hProv: HCRYPTPROV; key: HCRYPTKEY; alg: ALG_ID; hash:
HCRYPTHASH; infile, outfile: file; size: DWORD; buf: array [0..511] of byte;
signature: PBYTE; begin // проверка на существование файла с именем
DataNameEdit.Text AssignFile(infile, DataNameEdit.Text); //присваивание имени
контейнеру cont, инициализация криптопровайдера alg:=CALG_SHA; if not
CryptCreateHash(hProv, alg, 0, 0, @hash) then begin //обработка ошибок
MessageDlg('Ошибка создания хеш-объекта: ' + err, mtError, [mbOK], 0); exit;
end; SaveDialog1.Title := 'Задайте имя файла для хранения подписанных
данных'; if SaveDialog1.Execute then begin AssignFile(outfile,
SaveDialog1.FileName); rewrite(outfile, 1); BlockWrite(outfile, alg, 4);
reset(infile, 1); size := FileSize(infile); BlockWrite(outfile, size, 4);
while not eof(infile) do begin BlockRead(infile, buf, 512, size);
BlockWrite(outFile, buf, size); if not CryptHashData(hash, @buf, size, 0)
then begin //обработка ошибок MessageDlg('Ошибка при хешировании: ' + err,
mtError, [mbOK], 0); break; end; end; CloseFile(infile); if not
CryptSignHash(hash, AT_SIGNATURE, nil, 0, nil, @size) then //обработка ошибок
MessageDlg('Ошибка при определении размера подписи: ' + err, mtError, [mbOK],
0); CloseFile(outfile); exit; end; GetMem(signature, size); if not
CryptSignHash(hash, AT_SIGNATURE, nil, 0, signature, @size) then //обработка
ошибок CloseFile(outfile); exit; end else MessageDlg('Файл подписан ',
mtInformation, [mbOK], 0); BlockWrite(outfile, size, 4); BlockWrite(outfile,
signature^, size); CloseFile(outfile); end; if not CryptDestroyHash(hash)
then //обработка ошибок //освобождение дескриптора криптопровайдера с
обработкой ошибок end;
```

При помощи функции CryptCreateHash(провайдер, алгоритм, опции, флаги, хэш, инициализируется объект хэш. Затем выбирается файл в который будет сохранена ЭЦП документа.

Затем вычисляется хэш документа. Для вычисления значения хэша файла и записи его в буфер используется функция CryptHashData(хэш, буфер, длина буфера, флаги) Для подписи вычисленного хэша файла используется функция CryptSignHash (хэш, описание ключа, комментарий, флаги, подпись, длина подписи). Первый раз она вызывается чтобы прежде вычислить размер буфера под ЭЦП - GetMem(signature, size). Затем уже для собственно вычисления подписи и записи ее в буфер а затем и в файл.

Задание 8. Реализация процедуры верификации подписи документа.

За реализацию в программе верификации подписи документа с помощью открытого ключа, предварительно экспортированного в память ОС Windows, отвечает процедура VerifyClick (Листинг 8):

Листинг 8:


```

Procedure TMainForm.VerifyClick(Sender: TObject); var err: string; hProv: HCRYPTPROV; key:
HCRYPTKEY; alg: ALG_ID; hash: HCRYPTHASH; infile: file; size, test, textsize: DWORD; buf:
PBYTE; signature, signkey: PBYTE; begin if not CryptAcquireContext(@hProv, nil, 'Aktiv ruToken CSP
v1.0', PROV_RSA_FULL, CRYPT_VERIFYCONTEXT) then begin //обработка ошибок
MessageDlg('Ошибка открытия контейнера: ' + err, mtError, [mbOK], 0); exit; end; //открытие файла с
подписанными данными infile в буфер buf и
//определение его размера в textsize if not CryptCreateHash(hProv, alg, 0, 0, @hash) then begin
//обработка ошибок MessageDlg('Ошибка создания хеш-объекта: ' + err, mtError, [mbOK], 0); exit; end;
if not CryptHashData(hash, buf, textsize, 0) then begin //обработка ошибок MessageDlg('Ошибка при
хешировании: ' + err, mtError, [mbOK], 0); exit; end; //выбор файла с открытым ключом и загрузка его
в буфер signkey if not CryptImportKey(hProv, signkey, size, 0, 0, @key) then //обработка ошибок
MessageDlg('Ошибка импорта ключа: ' + err, mtError, [mbOK], 0); exit; end; FreeMem(signkey, size); if
CryptVerifySignature(hash, signature, test, key, nil, 0) then begin MessageDlg('Подпись верна.',
mtInformation, [mbOK], 0); //сохранение документа без подписи из буфера buf в файл infile end else
begin //обработка ошибок MessageDlg(err, mtError, [mbOK], 0); end; end;

```

Для инициализации криптопровайдера в режиме сверки подписи функция CryptAcquireContext используется с флагом CRYPT_VERIFYCONTEXT. Для импорта открытого ключа из буфера signkey в ключ key криптопровайдера используется функция CryptImportKey. Для проверки ЭЦП документа используется функция CryptVerifySignature (хэш, буфер с подписью, размер буфера, дескриптор открытого ключа, описание, флаги).

Вопросы и практические задания.

1. Что такое ЭЦП и как она реализуется в среде Delphi?
2. Каковы функции и алгоритм работы RutokenEDS?
3. Реализуйте процедуру создания в памяти ruToken нового контейнера ключей по заданному имени (с обработкой ошибок).
4. Реализуйте процедуру удаления из памяти ruToken контейнера по заданному имени (с обработкой ошибок). Если значение имени контейнера ключей пользователем не введено, удаляется контейнер с именем текущего пользователя ОС.
5. Реализуйте процедуру экспорта открытого ключа из контейнера заданного имени в память ОС Windows (с обработкой ошибок).
6. Реализуйте процедуру перевода ключа из байтового типа в символьный. Используя ее, реализуйте процедуру экспорта открытого ключа из контейнера заданного имени в память ОС Windows (с обработки ошибок).
7. Реализуйте процедуру подписи документа с помощью закрытого ключа указанного именем контейнера с выбором алгоритма хеширования файла (с обработки ошибок).
8. Реализуйте процедуру верификации подписи документа с помощью открытого ключа, предварительно экспортированного в память ОС Windows (с обработкой ошибок).

Тема 8. Методы и средства ограничения доступа к компонентам ЭВМ

Лабораторная работа. Система защиты информации от несанкционированного доступа Secret Net 5.0 автономный вариант

Теоретическая часть

Задание 1. Установка программы Secret Net 5.0

Задание 2. Варианты входа в систему

Задание 3. Смена пароля.

Задание 4. Временная блокировка компьютера.

Задание 5. Смена ключей

Задание 6. Работа с конфиденциальными ресурсами

Задание 7. Изменение категории конфиденциальности.

Задание 8. Работа с конфиденциальным документом в MS Word и MS Excel

Задание 9. Печать конфиденциального документа MS Word

Задание 10. Деинсталляция программы Secret Net 5.0 (автономный вариант)

Вопросы и практические задания.

Список использованных источников

Теоретическая часть

Secret Net 5.0 автономный вариант - система защиты информации от несанкционированного доступа нового поколения, которая реализует требования руководящих документов и ГОСТ по защите информации, не ограничивая возможности ОС и прикладного программного обеспечения.

Secret Net 5.0 - это программно-аппаратный комплекс, который обеспечивает защиту серверов, рабочих станций и мобильных ПК, работающих под управлением операционных систем Windows 2000, Windows XP и Windows 2003.

Ключевую роль сыграло то, что в начале июня Secret Net 5.0 получил сертификат ФСТЭК о соответствии требованиям по защите конфиденциальной информации от несанкционированного доступа. Данный сертификат важен для

работы с коммерческими организациями, а результаты новых испытаний дают

«зеленый свет» на использование системы компании «Информзащита» учреждениями, чья работа связана с государственной тайной.

Согласно полученному заключению сетевой вариант Secret Net 5.0 соответствует 4-му классу защищенности от несанкционированного доступа и 3-му уровню контроля отсутствия недекларированных возможностей (в соответствии с требованиями РД Гостехкомиссии России). Автономный вариант Secret Net 5.0 соответствует 3-му классу защищенности и 2-му уровню контроля.

На практике соответствие этим классам защищенности и уровням контроля означает, что, если в сети компьютеров организации установлен Secret Net 5.0, данная организация может оперировать информацией, составляющей государственную тайну вплоть до грифов «С» и «СС».

Задание 1. Установка программы Secret Net 5.0.

Прежде чем приступить к установке, убедитесь в том, что на данной машине установлена одна из перечисленных ниже операционных систем (Windows 2000, Windows XP и Windows 2003).

Внимание: Система Secret Net 5.0 несовместима с ОС Windows XP Home Edition.

Рассмотрим процесс установки СЗИ Secret Net 5.0 (автономный вариант) на примере компьютера работающего под управлением ОС Windows 2000

1. Для установки СЗИ Secret Net 5.0 (автономный вариант) на компьютер, работающий под управлением ОС Windows 2000, требуется наличие установленного пакета обновлений SP4. Так же должны быть установлены более поздние обновления (Hotfix), распространяемые компанией Microsoft.

Рекомендации: Компакт-диск комплекта поставки содержит необходимое для установки обновление "Windows2000-KB891861-x86..." в каталоге \Tools\Microsoft\2000 SP4 Update Rollup 1\.. Перед установкой системы защиты проверьте наличие на компьютере данного обновления и при необходимости установите его.

2. Перед установкой на компьютер, работающий под управлением ОС Windows 2003, необходимо включить режим разрешения установки неподписанных драйверов.

3. Если программа установки аварийно завершает работу с сообщением "Внутренняя ошибка: 2738", необходимо установить компонент Windows Scripting Host 5.6. Файл для установки компонента содержится на компакт-диске в каталоге \Tools\Microsoft\Windows Script 5.6 for 2000 and XP\.

4. При попытке установки во время максимальной загрузки системы (например, во время сканирования диска антивирусным программным обеспечением) может произойти аварийное завершение работы программы установки.

Рекомендации: Дождитесь снижения загрузки системы и заново запустите программу установки.

5. При установке осуществляется трассировка работы программы установки (после завершения установки трассировка отключается). Если в процессе установки возникли проблемы, причины которых выяснить не удалось, обратитесь за помощью в службу технической поддержки компании "Информзащита". Чтобы получить консультации специалистов, вам необходимо предоставить файл трассировки, который находится в каталоге c:\logs.
6. При первой перезагрузке после установки или обновления выполняется автоматическое утверждение аппаратной конфигурации компьютера. В связи с этим администратор безопасности должен контролировать первую загрузку компьютера после установки, чтобы не допустить регистрацию нежелательных устройств (которые могут быть подключены к компьютеру до загрузки).
7. Установка должна осуществляться только локально или с использованием процедуры автоматической установки СЗИ Secret Net 5.0 (автономный вариант) на компьютерах домена. Возможность установки из терминальных сессий не поддерживается.
8. Если региональные настройки "Язык программ, не поддерживающих Unicode" установлены не для русского языка, возникает ошибка при попытке установки путем запуска файла setup.exe. Рекомендации: Установите региональные настройки для русского языка.
9. Для совместной работы с Novell Netware Client выполните его установку до установки СЗИ Secret Net 5.0 (автономный вариант).
10. Для совместной работы с системой Citrix необходимо использовать особый порядок установки и специальный набор Reg-файлов. Дополнительные разъяснения и необходимые файлы предоставляются по требованию.
11. После установки или обновления СЗИ Secret Net 5.0 (автономный вариант) расчет контрольных сумм для подсистемы контроля целостности осуществляется при первой перезагрузке компьютера (а не во время работы программы установки).
12. После обновления СЗИ Secret Net 5.0 (автономный вариант) расчет контрольных сумм в программно-аппаратном комплексе "Соболь" выполняется при второй перезагрузке компьютера.
13. При обновлении СЗИ Secret Net 5.0 (автономный вариант) возможна регистрация ряда ошибок в журнале приложений. Как правило такие ошибки не являются критическими и никак не влияют на дальнейшую работу системы.
14. Если установочный скрипт формируется с помощью программы установки, в полученном файле скрипта будут неверно указаны параметры: SNETPERMISSIONS и REBOOTPROMPT. В этом случае необходимо вручную указать правильные параметры в соответствии с описанием в документации.

Задание 2. Варианты входа в систему

Существует несколько способов входа в систему:

А. Вход при стандартной аутентификации.

Стандартная аутентификация выполняется по паролю пользователя. При стандартном режиме входа порядок действий совпадает с принятым в ОС

Windows. После включения питания компьютера на экране появится приглашение на вход в систему. Для входа в стандартном режиме:

1. Нажмите комбинацию клавиш <Ctrl>+<Alt>+. На экране появится запрос на ввод имени и пароля:

Укажите ваши учётные данные в системе:

1. Введите своё имя в поле «Пользователь»;
2. В поле «Пароль» введите свой пароль или оставьте это поле пустым, если вам разрешено входить в систему без пароля

На экране каждый символ пароля отображается как "*" (звездочка). Помните, что при вводе пароля различаются строчные и заглавные буквы, кириллица и латиница. Если при вводе имени или пароля была неправильно нажата какая-либо клавиша, удалите ошибочно набранные символы в строке ввода с помощью клавиши <BackSpace> или <Delete> и заново повторите ввод символов.

Выберите в поле "Вход в" ("Домен" в Windows 2000) имя домена, в котором вы зарегистрированы.

3. Нажмите кнопку "ОК" для продолжения работы.

Если введенный вами пароль правильный, выполняется загрузка ОС. В процессе загрузки на экран будут выводиться сообщения о выполняемых действиях.

В. Если вы входите в систему, используя персональный идентификатор, то выполните следующие действия

1. После появления приглашения на вход в систему предъявите свой персональный идентификатор. Если идентификатор eToken защищен нестандартным для Secret Net 5.0 PIN- кодом (паролем), на экране появится запрос. Введите PIN-код и нажмите кнопку "ОК".

Не прерывая контакт идентификатора со считывателем, дождитесь окончания процесса загрузки данных. Во время выполнения загрузки данных из идентификатора iButton на экране отображаются соответствующие сообщения. После того, как сообщения будут закрыты, идентификатор можно изъять из считывателя.

2. Реакция системы защиты зависит от информации о пароле, содержащейся в персональном идентификаторе. Возможны следующие варианты:

Ситуация 1. Если в идентификаторе содержится актуальный пароль, то после успешной проверки прав пользователя на вход в систему выполняется загрузка ОС. В процессе загрузки на экран будут выводиться сообщения о выполняемых действиях.

Ситуация 2. Если в идентификаторе нет пароля или содержится другой пароль, на экране появится сообщение о невозможности входа в систему. Нажмите кнопку "ОК". На экране появится диалог "Вход в Windows":

Имя пользователя, которому принадлежит предъявленный идентификатор При вводе пароля обратите внимание на состояние индикатора EN/RU

- Введите актуальный пароль в поле "Пароль" и нажмите кнопку "ОК".

Если введенный вами пароль правильный и хранение пароля в идентификаторе не предусмотрено, выполняется загрузка ОС. В процессе загрузки на экран будут выводиться сообщения о выполняемых действиях.

Если введенный вами пароль правильный и актуальный пароль нужно записать в идентификатор, на экране появится соответствующий запрос.

- Нажмите кнопку "Да" в окне запроса.

На экране появится диалог, содержащий список идентификаторов, в которые система предлагает записать новый пароль.

- Для записи пароля последовательно предъявите идентификаторы.

В результате успешной записи нового пароля в идентификаторе то статус в списке сменится на "Обработан". После этого идентификатор можно изъять из считывателя.

- По окончании обработки всех идентификаторов нажмите в диалоге кнопку "Закрыть".

После закрытия диалога выполняется загрузка операционной системы. В процессе загрузки на экран будут выводиться сообщения о выполняемых действиях.

С. Основные особенности входа при усиленной аутентификации выражаются в том, что

1. Если при входе в систему в режиме усиленной аутентификации имя пользователя было введено неверно, сообщение об ошибке выдается после запроса на предъявление электронного идентификатора.

2. При терминальном входе в режиме усиленной аутентификации на сервере в журнале приложений регистрируются ошибка WinLogon "Неверная функция".

Если в системе включен режим усиленной аутентификации, то при любом режиме входа в систему (стандартном, смешанном или по идентификатору) после диалога для ввода имени и пароля на экране появится диалог для выбора и предъявления ключевого носителя, из которого будет считан закрытый ключ пользователя (см. ниже).

D. Вход в режиме контроля потоков

Если в подсистеме полномочного разграничения доступа включен режим контроля потоков конфиденциальной информации, то при любом режиме входа в систему (стандартном, смешанном или по идентификатору) после успешной проверки прав пользователя на вход в систему на экране появится диалог для выбора уровня конфиденциальности сеанса. Указывая уровень конфиденциальности, вы тем самым указываете системе категорию конфиденциальности документов, с которыми собираетесь работать в текущем сеансе.

Задание 3. Смена пароля.

Если вам разрешено менять пароль, то на экране появится диалог:

1. в поле "Старый пароль" введите ваш текущий пароль в системе, на экране каждый символ пароля отображается как "*" (звездочка);
2. в поле "Новый пароль" введите новый пароль;
3. повторите ввод нового пароля в поле "Подтверждение".
4. нажмите кнопку "ОК" для запуска процедуры смены пароля.

Если требования, предъявляемые в системе к паролям, нарушены или старый пароль указан неправильно, на экране появится сообщение об ошибке. Нажмите кнопку "ОК" в окне сообщения и повторите ввод паролей, указав их правильно.

Если поля диалога смены пароля были заполнены правильно, на экране появится сообщение об успешном изменении пароля.

5. Нажмите кнопку "ОК". Если ваш старый пароль хранится в персональном идентификаторе или вы используете этот идентификатор для входа в комплекс "Соболь" (только для идентификаторов iButton), на экране появится диалог, содержащий список ваших персональных идентификаторов. Пояснение. В случае отказа от записи информации в персональный идентификатор iButton, который используется для входа в комплекс "Соболь", вход в комплекс "Соболь" будет возможен только по старому паролю.

6. Для смены пароля или записи новой служебной информации, необходимой при входе в комплекс "Соболь", последовательно предъявите каждый идентификатор.

Если предъявлен идентификатор eToken, который защищен нестандартным для Secret Net 5.0 PIN-кодом (паролем), на экране появится запрос. Введите PIN-код и нажмите кнопку "ОК".

В результате успешной записи нового пароля в идентификатор его статус сменится на "Обработан". После этого идентификатор можно изъять из считывателя.

7. По окончании обработки всех идентификаторов закройте диалог нажатием кнопки "Заккрыть".

Если же установленная политика паролей запрещает вам менять пароль, на экране появится сообщение об ошибке и процедура смены пароля будет прервана. В этом случае для смены пароля обратитесь за помощью к администратору.

Задание 4. Временная блокировка компьютера.

Если вам необходимо временно прервать работу на компьютере, то для защиты от несанкционированного использования совсем не обязательно его выключать. Можно воспользоваться функцией временной блокировки компьютера, при которой блокируется клавиатура и экран монитора. Разблокировать компьютер может только работающий на нем пользователь или администратор. Разблокирование компьютера администратором сопровождается завершением текущего сеанса работы пользователя и потерей всех несохраненных данных. Заблокировать компьютер можно с помощью стандартных средств ОС Windows вручную (см. ниже) или автоматически.

Автоматическая блокировка компьютера включается в том случае, если в течение определенного времени не использовались клавиатура и мышь. Такое время называется интервалом неактивности. Для активации механизма

автоматической блокировки его необходимо предварительно настроить.

Для временной блокировки компьютера вручную:

Нажмите комбинацию клавиш <Ctrl>+<Alt>+.

Нажмите кнопку "Блокировка" в появившемся на экране диалоге.

Клавиатура и экран монитора будут заблокированы, на экране появится сообщение

Если предварительно вами был настроен механизм автоматической блокировки (см. ниже), то по истечении времени, равного заданному интервалу неактивности, на экране заблокированного компьютера появится выбранная заставка.

Для настройки механизма автоматической блокировки:

1. Откройте окно настройки свойств экрана и перейдите к диалогу "Заставка".

Если окно настройки свойств экрана недоступно или в нем отсутствует нужная закладка, это означает, что администратор запретил вам доступ к этим элементам интерфейса. Для разрешения вопроса обратитесь к администратору

2. Выберите заставку из раскрывающегося списка, отличную от "Нет" ("None").
3. Установите значение параметра "Интервал" не равным "0".
4. Нажмите кнопку "ОК".

Разблокировать компьютер может только работающий на нем пользователь или администратор безопасности. Если разблокировку компьютера проводит администратор, то сеанс работы пользователя будет принудительно завершен с потерей несохраненных данных.

Для разблокирования компьютера выполните одну из следующих последовательностей действий:

- Если используется устройство аппаратной идентификации, предъявите персональный идентификатор.

Не прерывайте контакт идентификатора со считывателем до окончания процесса загрузки данных. Во время выполнения загрузки данных из идентификатора iButton на экране отображаются соответствующие сообщения. После того как сообщения будут закрыты, идентификатор можно изъять из считывателя.

Компьютер будет разблокирован, если в идентификаторе есть пароль. Если в персональном идентификаторе отсутствует пароль, введите его с клавиатуры в появившемся на экране диалоге и нажмите кнопку "ОК".

- Нажмите комбинацию клавиш <Ctrl>+<Alt>+, введите пароль с клавиатуры в появившемся на экране диалоге и нажмите кнопку "ОК".

Задание 5. Смена ключей.

Смена ключевой информации проводится в 2 этапа.

На первом выполняется смена ключевой информации, хранящейся на ключевом носителе.

На втором этапе осуществляется перевод шифрованных ресурсов на шифрование новыми ключами.

Смена ключевой информации на ключевом носителе возможна только по окончании минимального срока действия личной ключевой информации.

Для смены ключевой информации на ключевом носителе:

1. Вызовите контекстное меню пиктограммы Secret Net 5.0, находящейся в системной области панели задач Windows, и активируйте команду "Сменить ключ".

На экране появится диалог:

2. Предъявите один из ключевых носителей, в котором содержится текущая ключевая информация. В зависимости от вида ключевого носителя (персональный идентификатор или съемный диск) выполните соответствующее действие:

если вы используете персональный идентификатор, предъявите его;

если вы используете в качестве ключевого носителя съемный диск, вставьте дискету в дисковод, а съемный диск в разъем USB-порта, и нажмите кнопку "Диск".

Совет. Если подключено несколько съемных дисков одновременно, то для продолжения процедуры выберите в списке идентификаторов строку с наименованием нужного съемного диска и нажмите кнопку "ОК".

Не прерывайте контакт ключевого носителя со считывателем, до окончания загрузки ключевой информации. По окончании загрузки на экране появится диалог

Диалог содержит список ваших ключевых носителей, в которые система предлагает записать новую ключевую информацию.

3. Последовательно предъявите все ключевые носители. Если вы используете в качестве ключевого носителя дискету (или другой сменный диск)

— вставьте дискету в дисковод (подключите сменный диск) и нажмите кнопку "Диск".

Если предъявлен идентификатор eToken, который защищен нестандартным для Secret Net 5.0 PIN-кодом (паролем), на экране появится запрос. Введите PIN-код и нажмите кнопку "ОК".

В результате успешной записи ключевой информации на носитель его статус в списке сменится на "Обработан". После этого ключевой носитель можно изъять из считывателя.

4. По окончании обработки всех носителей нажмите кнопку "Закрыть".

• Если не все ключевые носители были обработаны, то после нажатия кнопки "Закрыть" (или "Отмена") на экране появится запрос

Для записи актуальной ключевой информации на необработанные ключевые носители нажмите кнопку "Да" и повторите действие. Чтобы прервать обработку ключевых носителей, нажмите кнопку "Нет".

Задание 6. Работа с конфиденциальными ресурсами.

Для изменения категории конфиденциальности каталога или файла в режиме полномочного разграничения доступа вы должны обладать привилегией "Управление категориями конфиденциальности". Если у вас нет такой привилегии, вы можете только повысить категорию конфиденциальности файла, но не выше своего уровня допуска или уровня конфиденциальности сеанса.

Внимание! Следуйте следующим рекомендациям:

не присваивайте категории "конфиденциально" и "строго конфиденциально" системным каталогам, каталогам, в которых размещается прикладное программное обеспечение, а также каталогу "Мои документы" и всем подобным ему;

во избежание непроизвольного повышения категорий конфиденциальности файлов храните файлы в каталогах с категорией конфиденциальности, равной категории конфиденциальности файлов.

Процедура выполняется с использованием программы "Проводник" ОС Windows.

Задание 7. Изменение категории конфиденциальности.

Для изменения категории конфиденциальности каталога:

1. В программе "Проводник" вызовите контекстное меню каталога .

Активируйте команду «Свойства». В появившемся на экране окне "Свойства" перейдите к диалогу "Secret Net".

2. Укажите необходимые значения параметров:

Выберите в раскрывающемся списке поля "Категория" нужную категорию конфиденциальности для каталога.

Выберите режим автоматического присвоения категории конфиденциальности файлам каталога, установив параметр "Автоматически присваивать новым файлам" в положение "Включено" или "Выключено".

3. Нажмите кнопку "ОК".

Для изменения категории конфиденциальности файла

Вызовите программу "Проводник".

Вызовите контекстное меню файла и активируйте в нем команду "Свойства".

В появившемся на экране окне "Свойства" перейдите к диалогу "Secret Net".

4. Выберите в раскрывшемся списке поля «Категория» нужную категорию конфиденциальности файла.

5. Нажмите кнопку «ОК»

Задание 8. Работа с конфиденциальным документом в MS Word и MS

Excel

Прежде чем начать работу с конфиденциальными документами в MS Word или MS Excel, рекомендуется сохранить и закрыть все ранее открытые неконфиденциальные документы

Для открытия конфиденциального документа:

1. 2.

Запустите MS Word или MS Excel.

Активируйте в главном меню команду "Файл Открыть" и в диалоге "Открытие документа" выберите конфиденциальный документ.

Если контроль потоков конфиденциальной информации отключен, на экране появится сообщение

Такое сообщение отображается всякий раз, когда открывается документ, категория конфиденциальности которого выше уровня конфиденциальности приложения.

3. Нажмите кнопку "Да" для открытия документа.

При сохранении конфиденциального документа под тем же или под другим именем необходимо учитывать, что категория конфиденциальности файла документа всегда остается прежней, если документ сохраняется в каталоге, категория конфиденциальности которого не ниже категории документа, и для каталога включен режим "Автоматически присваивать новым файлам".

Важно. Для сохранения категории конфиденциальности документа рекомендуется сохранять его в каталоги не ниже категории конфиденциальности документа. Иначе возможны следующие ситуации: если документ сохраняется в каталог с более низкой категорией конфиденциальности и для каталога включен режим "Автоматически присваивать новым файлам", то категория конфиденциальности документа понижается до категории конфиденциальности каталога;

если документ сохраняется в неконфиденциальный каталог или в конфиденциальный каталог, для которого отключен режим "Автоматически присваивать новым файлам", то файлу документа присваивается категория конфиденциальности "неконфиденциально".

Задание 9. Печать конфиденциального документа MS Word.

Для печати конфиденциального документа:

1. Откройте в MS Word конфиденциальный документ.

Список грифов конфиденциальности, имеющих в системе, отображается на панели инструментов "Гриффы Secret Net" в основном окне MS Word.

Если панель грифов не видна, выберите в основном меню "Вид | Панели инструментов | Грифы Secret Net".

2. Выберите нужный гриф конфиденциальности из раскрывающегося списка панели. Выберите нужный гриф конфиденциальности из раскрывающегося списка панели "Гриффы Secret Net", если грифов несколько

3. Активируйте команду "Файл | Печать" в главном меню.

На экране появится диалог для настройки полей грифа конфиденциальности. Нажмите кнопку "Печать". На экране появится стандартный диалог для определения параметров печати.

Укажите параметры печати и, если необходимо, настройте свойства принтера.

7. Нажмите кнопку "ОК" в диалоге параметров печати. В итоге документ будет распечатан вместе с грифом конфиденциальности.

Задание 10. Деинсталляция программы Secret Net 5.0 (автономный вариант) .

Чтобы удалить программу Secret Net 5.0 Express из вашего PC:

1. Откройте Установка/Удаление программ в Панели управления (Пуск ->

Настроить -> Панель управления).

2. Найдите запись Secret Net 5.0 в списке и выберите ее.

3. Нажмите кнопку Заменить/Удалить, чтобы начать удалять приложение и следуйте командам.

Вопросы и практические задания.

1. Включите режим контроля потоков конфиденциальной информации.

2. Осуществите вход в систему в режиме контроля потоков конфиденциальной информации.

3. Осуществите загрузку ключей.

4. Создайте зашифрованный каталог.

5. Создайте список пользователей, имеющих доступ к зашифрованному каталогу.

6. Зашифруйте файл.

7. Осуществите удаление зашифрованного каталога или файла.

8. Распечатайте документ в MS Excel.

9. Настройте механизм автоматической блокировки.

10. Выполните выгрузку ключевой информации после окончания работы.

Список использованных источников.

1. Электронный ресурс \ Информзащита – режим доступа: <http://www.infosec.ru>. – Загл. с экрана;

2. Руководство по эксплуатации устройства криптографической защиты данных Secret Net: Москва, 2006;

3. Сайт разработчика [Электронный ресурс] // АНКАД на защите информации – режим доступа: <http://www.ancud.ru>. – Загл. с экрана;

4. Электронный ресурс // Защита информации – режим доступа: <http://www.zinfo.ru>. – Загл. с экрана;

5. Электронный ресурс // More PC – режим доступа: <http://www.morepc.ru>. – Загл. с экрана.

Тема 9. Понятие обратного проектирования.

Лабораторная работа. Понятие обратного проектирования.

Теоретическая часть

Основными угрозами для программного продукта, защищенного от несанкционированного использования способом ввода ключевой информации пользователем являются:

угроза нарушения функциональности модуля защиты

угроза раскрытия ключевой информации.

Реализация угрозы нарушения функциональности модуля защиты может заключаться:

в обходе модуля защиты путем модификации кода программы

в полном отключении модуля защиты путем модификации кода программы.

Реализация угрозы раскрытия ключевой информации – в выяснении путем исследования программы ключевой информации, требуемой при регистрации.

Существует несколько задач, которые злоумышленник должен решить при реализации данных угроз.

1. Задача обнаружения в коде программы модуля защиты.

2. Задача исследования модуля защиты и понимания принципов его действия.

Следует отметить, что задачи в принципе не решаемы за приемлемое время.

Это обусловлено следующими обстоятельствами.

Задача обнаружения в коде программы модуля защиты.

1. Модуль защиты занимает достаточно малый объем в общей совокупности кода программы. Задача ручного поиска блока модуля защиты размером 100 – 200 байт в общем коде программы, занимающем сотни мегабайт, без использования специализированных средств в принципе не решается за приемлемое время.

Задача обнаружения в коде программы модуля защиты.

2. Анализ кода программы в значительной степени затрудняется тем, что производится анализ не исходного текста программы на языке высокого уровня, а анализ машинного кода, сформированного компилятором. На разборку и понимание такого кода уходит значительное время даже у специалистов высокого класса в данной области. Зачастую даже анализ исходных текстов программы, написанных другим человеком, является нетривиальной задачей. Анализ же машинного кода усложняет задачу уже в тысячи раз. Недостаточно провести анализ каждой машинной команды. Как правило, при анализе машинного кода приходится увязывать в единую последовательность действий как минимум 80 – 100 байт, чтобы понять, что действительно скрыто за данной последовательностью кодов. Как правило, это очень усложняет анализ программы

Задача исследования модуля защиты и понимания принципов его действия.

Злоумышленник должен понять, каким образом построена защита, где она хранит (если хранит) ключевую информацию, где сохраняет (если сохраняет) свои метки и ключи, на каком этапе принимается решение о регистрации программы либо об отклонении регистрации. При этом злоумышленник сталкивается с проблемой анализа машинного кода, что приводит к трудностям, перечисленным в первой задаче.

Трудности реализации угроз от угрозы нарушения функциональности модуля защиты и от угрозы раскрытия ключевой информации

Вывод: отсутствие необходимости защиты ПО!!!

Продукты фирм, пренебрегающих защитой от реализации данных угроз, оказываются взломанными в числе первых.

Большой объем взломанных программ на рынке ПО говорит об обратном, – что эти угрозы вполне реальны и осуществимы.

Трудности реализации угроз от угрозы нарушения функциональности модуля защиты и от угрозы раскрытия ключевой информации

Существует множество программных продуктов, облегчающих злоумышленнику решение задач 1 и 2!!! Их реализация, в отдельных случаях доводится до автоматизма

Алгоритм решения задач 1 и 2 показывает, что основная цель, решаемая злоумышленником при взломе ПО

о анализ работы программы

о поиск в ней участка кода, отвечающего за реализацию модуля защиты

о детальное исследование принципов и механизмов работы данного модуля.

Решение задач 1 и 2 показывает, что основная цель, решаемая злоумышленником при взломе ПО.

При этом ставится задача представления машинного кода на как можно более высоком уровне с целью упрощения его понимания.

Для злоумышленника наиболее оптимальный вариант – формирование по машинному коду модуля защиты, его текста на исходном языке высокого уровня.

Под обратным проектированием (reverse engineering) понимают процесс исследования и анализа машинного кода, нацеленный на понимание общих механизмов функционирования программы, а также на его перевод на более высокий уровень абстракции (более высокий уровень языка программирования) вплоть до восстановления текста программы на исходном языке программирования.

Основными методами обратного проектирования являются

- отладка программ
- дизассемблирование программ.

Средства (инструменты) обратного проектирования.

- Отладчики
- Дизассемблеры
- Мониторы событий
- Редакторы кода.

Отладчики

Программные средства, позволяющие выполнять программу в пошаговом режиме, контролировать ее выполнение, вносить изменения в ход выполнения. Данные средства позволяют проследить весь механизм работы программы на практике и являются средствами динамического исследования работы программ

Дизассемблеры

Программные средства, позволяющие получить листинг программы на языке ассемблера, с целью его дальнейшего статического изучения. Дизассемблеры являются средствами статического исследования.

Мониторы событий

Программные средства, позволяющие отслеживать определенные типы событий, происходящие в системе. Наиболее опасными для программного обеспечения с точки зрения их защиты являются мониторы операций с реестром и мониторы файловых операций, позволяющие проследить – какая программа куда и что записывала, считывала и т.д.

Редакторы кода

Занимают отдельное место среди средств обратного проектирования. Данные средства, как правило, включают функции дизассемблирования, но позволяют также вносить изменения в код программы.

Тема 10. Атаки на модули проверки корректности ключевой информации

Лабораторная работа. Атаки на модули проверки корректности ключевой информации.

Теоретическая часть

Для вскрытия защиты модуля проверки корректности ключевой информации в первую очередь необходимо найти в коде программы мотивация

код модуля защиты

Процедуру проверки

В большинстве программных продуктов проверка корректности ключевой информации выполняется непосредственным образом. При этом исходный текст программы выглядит приблизительно следующим образом.

Object Pascal

If not ValidUser(Login, Password)

then

begin

ShowMessage(„Неверный пользователь“);

Halt(1);

end;

C++

If (!ValidUser())

{

Message (“Неверный пользователь”);

Abort;

}

Здесь, ValidUser() – базовая процедура проверки. Ключевая информация может вводиться пользователем как в данной процедуре, так и ранее.

Object Pascal

If not ValidUser(Login, Password)

Then

begin

ShowMessage(„Неверный пользователь“);

Halt(1);

end;

C++

```
If (!ValidUser())
```

```
{
Message (“Неверный пользователь”);
Abort;
}
```

Object Pascal

```
If not ValidUser(Login, Password)
```

```
Then
Begin
ShowMessage(„Неверный пользователь”);
Halt(1);
end;
```

C++

```
If (!ValidUser())
{ Message (“Неверный пользователь”);
Abort;
}
```

PUSH AX CALL IsValidUser; POP AX OR AX, AX JZ continue PUSH offset str_invalid_user CALL Message CALL Abort COUNTINUE If not ValidUser(Login, Password) Object Pascal then begin ShowMessage(„Неверный пользователь”); Halt(1); end; If (!ValidUser()) C++ { Message (“Неверный пользователь”); Abort; } Компилятор Delphi Компилятор C++ Builder Assembler `6 Assembler – КМБ

PUSHAX- занесение параметра в стек PUSH – offset str_invalid_user – занесение указателя в стек CALL- вызов процедуры (IsValidUser; Message; Abort) POP AX - вызов из стека результата OR - оператор OR JZ – условный оператор (аналог IF) , Результат ... AX- регистры стека (AX, BX, CX..) COUNTINUE – метка

Assembler PUSH AX CALL IsValidUser; POP AX В данном коде команда CALL IsValidUser осуществляет вызов процедуры IsValidUser. Передача в данную процедуру параметров (например, ссылки на ключевую информацию) осуществляется через стек командами PUSH (занесение параметра в стек) до команды CALL и POP (вызов из стека результата, возвращенного процедурой IsValidUser) после команды CALL. В представленном примере результат выполнения процедуры IsValidUser заносится в регистр AX. Assembler OR AX, AX JZ continue PUSH offset str_invalid_user CALL Message CALL Abort COUNTINUE В дальнейшем производится проверка на равенство нулю возвращенного результата (команды OR AX,AX). Если AX=0, то ключевая информация верна, производится ее регистрация и дальнейшее продолжение работы (JZ continue). В ином случае выводится сообщение о невозможности продолжения работы (PUSH offset str_invalid_user; CALL Message) и завершение работы программы (CALL Abort).

- Hex: Asm: Means
- 75 or 0F85 jne jump if not equal
- 74 or 0F84 je jump if equal
- EB jmp jump directly to
- 90 nop no operation
- 77 or 0F87 ja jump if above
- 0F86 jna jump if not above
- 0F83 jae jump if above or equal
- 0F82 jnae jump if not above or equal
- 0F82 jb jump if below
- 0F83 jnb jump if not below
- 0F86 jbe jump if below or equal
- 0F87 jnbe jump if not below or equal
- 0F8F jg jump if greater

- 0F8E jng jump if not greater
- 0F8D jge jump if greater or equal
- 0F8C jnge jump if not greater or equal
- 0F8C jl jump if less
- 0F8D jnl jump if not less
- 0F8E jle jump if less or equal
- 0F8F jnle jump if not less or equal

Assembler В данной ситуации, после обнаружения представленного выше программного кода модуля защиты, взломщик может осуществить атаку следующим образом.

- Заменить команду условного перехода JE continue на команду безусловного перехода JNE continue. В данном случае, регистрация программы будет осуществляться в любом случае, вне зависимости от правильности ввода ключевой информации.
- Изменить в процессе работы программы содержимое регистра AX после команды POP AX, либо значение регистра флагов после команды OR AX,AX. В данном случае злоумышленник вынужденно заставляет модуль защиты работать по нужной ветке.
- Исследовать работу процедуры IsValidUser вручную с целью выяснения ключевой информации.

Реализация первых двух типов атак называется «жестким» взломом программного продукта, так как он требует модификации кода программы. Первые два типа взлома позволяют осуществить взлом программного продукта в достаточно короткие сроки, не прилагая к этому слишком больших усилий (можно привести примеры, когда такие защиты взламывались в течение 10 секунд).

Реализация третьего типа атак называется «мягким» взломом программного продукта и во многих случаях является более предпочтительным для злоумышленника, хотя и требует от него несколько больших временных затрат. Достоинством для злоумышленника третьего типа взлома является то, что иногда, исследовав логику работы процедуры IsValidUser, можно не только вычислить ключевую информацию, но и написать генератор ключевой информации для последующего использования другими пользователями. Это возможно сделать, если разработчик вложил в модуль защиты непосредственную связь между идентификатором пользователя и его аутентификатором (ключевой информацией).

Отслеживание обращений к этим адресам позволит локализовать код, отвечающий за проверку адекватности ключевой информации.

Довольно часто злоумышленником производится исследование содержимого ОЗУ на осмысленные последовательности символов, а также отслеживание обращений к адресам, по которым хранятся эти последовательности (например, “Invalid Registration”, “Password Fail”, “Error” т.д.). Как правило, эти сообщения находятся недалеко от модулей защиты, отвечающих за проверку корректности ключевой информации. По обращению к адресам, хранящим данные сообщения, также можно локализовать код проверки адекватности ключевой информации. Перечисленные элементы являются наиболее уязвимыми с точки зрения взлома в процедуре IsValidUser. Как правило, передача параметров в функции и их возврат осуществляется через 32-битные регистры EAX, EBX, а также используя регистры ESI и EDI для указания на используемые данные. Совершив “мягкий” взлом (получив ключевую информацию), злоумышленник снимает все проблемы «Жесткий» взлом иногда затруднителен: проверка корректности осуществляется в нескольких местах программы и различными способами.

- Hex: Asm: Means
- 75 or 0F85 jne jump if not equal
- 74 or 0F84 je jump if equal
- EB jmp jump directly to
- 90 nop no operation
- 77 or 0F87 ja jump if above
- 0F86 jna jump if not above
- 0F83 jae jump if above or equal
- 0F82 jnae jump if not above or equal
- 0F82 jb jump if below

- 0F83 jnb jump if not below
- 0F86 jbe jump if below or equal
- 0F87 jnbe jump if not below or equal
- 0F8F jg jump if greater
- 0F8E jng jump if not greater
- 0F8D jge jump if greater or equal
- 0F8C jnge jump if not greater or equal
- 0F8C jl jump if less
- 0F8D jnl jump if not less
- 0F8E jle jump if less or equal
- 0F8F jnle jump if not less or equal

Тема 11. Защита программ от изучения.

Лабораторная работа. Защита программ от дизассемблирования.

Цель: освоить технологию работы с дизассемблером и декомпилятором

Теоретическая часть

Дизассемблер — транслятор, преобразующий машинный код, объектный файл или библиотечные модули в текст программы на языке ассемблера.

По режиму работы с пользователем делятся на

- Автоматические
- Интерактивные

Примером автоматических дизассемблеров может служить Sourcer. Такие дизассемблеры генерируют готовый листинг, который можно затем править в текстовом редакторе. Пример интерактивного — IDA. Он позволяет изменять правила дизассемблирования и является весьма удобным инструментом для исследования программ.

Дизассемблеры бывают однопроходные и многопроходные. Основная трудность при работе дизассемблера — отличить данные от машинного кода, поэтому на первых проходах автоматически или интерактивно собирается информация о границах процедур и функций, а на последнем проходе формируется итоговый листинг. Интерактивность позволяет улучшить этот процесс, так как просматривая дампы дизассемблируемой области памяти, программист может сразу выделить строковые константы, дать содержательные имена известным точкам входа, прокомментировать разобранные им фрагменты программы.

Чаще всего дизассемблер используют для анализа программы (или ее части), исходный текст которой неизвестен — с целью модификации, копирования или взлома. Реже — для поиска ошибок (багов) в программах и компиляторах, а также для анализа оптимизации создаваемого компилятором машинного кода. Обычно однопроходный дизассемблер (как и построчный ассемблер) является составной частью отладчика.

Защита от дизассемблирования

Первое направление защиты, как правило, реализуется значительно легче, чем второе, поэтому будет приведен лишь краткий обзор данного направления. При реализации защиты программ от дизассемблирования можно применять различные приемы.

Среди них наиболее часто используемым и эффективным приемом является зашифровка и \ или запакковка отдельных участков исходного кода или всего кода целиком, при этом необходимо позаботиться о распаковке \ расшифровке программы на точке входа. Таким образом, при просмотре исполняемого машинного кода исполняемого файла вместо рабочего кода программы будет отображен лишь бессмысленный набор операций. При реализации защиты от дизассемблирования используется также множество приемов, которые реализуются с целью запутать потенциального взломщика. Можно привести несколько примеров такого вида приемов:

- увеличение исходного кода программы добавлением множества «бессмысленных» операций, а рабочий участок программы записать в определенное место этого множества;

- замена местами адресов обработчиков (векторов) прерываний, например, поменять местами вектор прерывания видео сервиса (INT 10h) с вектором прерывания сервиса DOS (INT 21h), после такой замены для вызова из программы какой-либо функции прерывания INT 21h необходимо пользоваться вызовом прерывания INT 10h.

Для достижения наиболее надежной и эффективной защиты используется комбинация нескольких приемов.

Защита от отладки Для защиты программы от трассировки отладчиком также существует несколько способов. Наиболее распространенными являются два из них.

Первый способ

Идея:

При трассировке программы команды выполняются по команде человека, поэтому длительность выполнения операций (время от начала одной операции до начала следующей) изменяется. Поэтому в программу можно включать точки для проверки времени выполнения одинаковых участков кода программы. Если время выполнения выполнения одинаковых участков различна, то это означает, что программа трассируется в данный момент, необходимо выйти из программы, иначе - продолжить выполнение.

Алгоритм реализации:

1. Запомнить текущее время;
2. Выполнить контрольный участок кода;
3. Запомнить текущее время и разность текущего и предыдущего запомненного времени;
4. Выполнить контрольный участок кода повторно;
5. Сравнить разность текущего времени и предыдущего запомненного текущего времени с предыдущей запомненной разностью;
6. Если разности совпадают, продолжить выполнение, иначе – выйти из программы.

- метаморфическое преобразование кода программы, позволяющее защитить программу от дизассемблирования и модификации;

- защита ключом отдельных участков кода программы (поддерживается только в зарегистрированной версии);

- полное разрушение логики защищенных фрагментов кода, не позволяющее анализировать программу с помощью дизассемблера или отладчика;

- обнаружение и противодействие отладчикам SoftIce, NtIce, TD и др.;

- защита точки входа;

- защита от модификации кода;

- защищенная работа с реестром, не позволяющая программам вроде RegMon определить, к какому ключу реестра обращается ваша программа;

- технология "динамического импорта", которая разрушает имена всех импортируемых функций, а также не использует функцию GetProcAddress;

- сжатие ресурсов и исполнимого кода приложения;

- поддержка коротких серийных номеров (12 символов);

- поддержка внешнего генератора серийных номеров с OLE/DLL-интерфейсом;

- технология OneTouch Trial (о ней читай ниже).

Самое главное, что нас интересует – это метаморфическое преобразование кода программы и поддержка серийных номеров. Метаморфическое кодирование позволяет изменить код программы до неузнаваемости и запутать отладчик и человека, который запустил этот отладчик.

Декомпилятор.

Он переводит двоичный код в символьный на языке команд какого-нибудь языка. Например, диасемблеры, деклиппер и многие другие. Эти средства появились раньше отладчиков, т.к. вначале не было архитектуры со встроенными средствами отлаживания программ. С помощью декомпиляторов можно изменять исходный код программы. Допустим необходимо внести крупные изменения в код программы. Прямая вставка двоичных кодов не помогает, т.к. нарушается расположение меток перехода и процедур. Программа – это линейка кода, по которой нужно перемещаться нелинейно, переходить с определенным смещением. Если линейка удлиняется из-за добавления чего-то в середине, все смещения будут показывать не туда куда нужно. Повторная перекомпиляция вписывает новые смещения.

Среди декомпиляторов можно выделить: Hacker-VIEW (HVIEW), IDA (интерактивный дизасемблер).

С помощью Hacker-VIEW можно посмотреть любой исполняемый файл по любому смещению. Можно выполнить какую-то часть программы. Это позволяет расшифровывать программы и обходить защиту от дизасемблирования. Этот декомпилятор «понимает» как старые форматы исполняемых файлов DOS-COM и DOS-EXE, так и форматы исполняемых файлов Windows.

IDA очень мощное средство работы с ассемблерными текстами программ. Обладает широким спектром возможностей, имеет более удобный интерфейс, чем Hacker-VIEW. Очень хорошо предусмотрена архитектура работы программ в Windows (такие вещи, как DLL, расширенный режим работы с памятью и т.д.).

Декомпиляторы программ занимают свое место в инструментарии взломщика. В основном это совместное использование с отладчиками.

Второе средство – отладчики.

Отладчики позволяют запускать отдельные части программы и следить за изменениями, которые она производит, за результатами ее работы.

Защите от отладки не стоит уделять много времени, т.к. все возможные хитрости и приемы уже известны и взломщикам и программистам. Так же и шифрование. Любой хакер, если получает заказ на взлом, имеет доступ к нормальной копии программы. То есть он ее либо может купить, либо попользоваться ею на компьютере покупателя.

Среди отладчиков выделим: SOFTICE и WINICE.

С появлением Windows отладка программ стала на порядок проще и намного удобнее дизасемблирования. Принципиально изменился стиль некоторых атак на защиту программ. Теперь не надо шаг за шагом смотреть на ассемблерный код, «продираться» сквозь дебри незначущих кодов и защит. Теперь надо отловить нужное событие и понять как на него реагирует программа. Это, конечно, не всегда бывает так просто, как выглядит на словах. Как и ранее, отладка требует знание архитектуры операционной системы.

Неважно насколько сложным был бы механизм защиты, все сводится к простейшей проверке или дешифровке. И взлом, в случае с проверкой, можно разбить на два этапа: установка «брейков» на «подозрительные» флаги, обнаруженные в процедуре защиты; анализ обращений к флагам. По реакции программы можно судить флаг это или просто переменная.

Практическая часть.

1. Изучить теоретическую часть. Сделать записи в тетради.
2. Провести сравнение декомпилятора и отладчика. По данным составить таблицу сравнений.
3. Ответить на контрольные вопросы

Контрольные вопросы:

1. Что такое дизасемблер?
2. Как происходит защита программ от дизасемблирования?
3. Как происходит защита программ от отладки?
4. Какие виды отладчиков вы знаете?
5. Что такое декомпилятор?
6. Какие он функции выполняет?
7. Что такое трассировка?
8. Какие виды дизасемблеров вам известны?

9. Какие приемы дизассемблирования вам известны?

Тема 12. Защита от разрушающих программных воздействий.

Лабораторная работа. RuToken и PGP

Теоретическая часть

Установка

Настройка RuToken

Создание ключей в памяти RuToken

Использование ключей хранящихся в памяти RuToken

Вопросы и практические задания.

Источники литературы

Теоретическая часть

PGP – это криптографическая (шифровальная) программа с высокой степенью надежности, которая позволяет пользователям обмениваться информацией в электронном виде в режиме полной конфиденциальности.

Главное преимущество этой программы состоит в том, что для обмена зашифрованными сообщениями пользователям нет необходимости передавать друг другу тайные ключи т.к. эта программа построена на новом принципе работы – публичной криптографии или обмене открытыми (публичными) ключами, где пользователи могут открыто посылать друг другу свои публичные ключи с помощью сети «Интернет» и при этом не беспокоиться о возможности несанкционированного доступа каких-либо третьих лиц к их конфиденциальным сообщениям.

В PGP применяется принцип использования двух взаимосвязанных ключей: открытого и закрытого. К закрытому ключу имеете доступ только вы, а свой открытый ключ вы распространяете среди своих корреспондентов.

Установка.

Для выполнения этого задания необходимо сделать следующее:

Зайдите на сайт разработчика www.pgpru.ru Скачайте новую версию продукта.

Следуйте инструкциям процесса установки.

Настройка RuToken

Запустите утилиту PGP Desktop:

В меню Tools выберите пункт PGP Options...

Перейдите на закладку Keys:

В выпадающем списке Synchronize with smart cards and tokens выберите пункт Other... :

И укажите путь к библиотеке PKCS#11 ! файл rtPKCS11.dll (по умолчанию библиотека находится в папке %SYSTEMROOT%\SYSTEM32), нажмите кнопку Открыть:

Закройте окно PGP Options, нажав на кнопку Ok. На этом настройка поддержки Rutoken завершена.

Создание ключей в памяти RuToken

Для создания ключевой пары и размещения ее в защищенной памяти токена в утилите PGP Desktop, в меню File выберите пункт New PGP Key....:

Откроется мастер генерации ключей:

Подключите Rutoken, в памяти которого будут записаны ключи шифрования. Дождитесь, пока светодиод перестанет мигать.

После этого станет доступной опция Generate Key on Token. Отметьте ее галочкой и нажмите кнопку Далее:

Заполните поля Full Name и Primary Email, при необходимости задайте дополнительные параметры для ключей шифрования, нажав кнопку Advanced. Нажмите кнопку Далее:

Вам предложат ввести PIN!код для доступа к памяти Rutoken. Введите текущий PIN!код Пользователя Rutoken и нажмите кнопку Далее:

Начнется процесс создания ключей и записи их в защищенную память Rutoken. Процесс может занять 1 - 3 минуты.

8. По окончании процесса генерации и записи ключей нажмите кнопку Далее:

9. Появится окно публикации открытого ключа в PGP Global Directory. В случае необходимости публикации нажмите кнопку Далее и следуйте указаниям Мастера. Иначе нажмите кнопку Skip:

10. Вы вернетесь в основной экран утилиты PGP Desktop. В случае успешной генерации и записи ключе!вой пары в окне All Keys будет отображаться запись, соответствующая сгенерированной ключевой паре и индикатор Validity будет зеленым:

11. При отключении токена индикатор Validity становится серым, что указывает на отсутствие доступа к ключевой паре.

Использование ключей хранящихся в памяти RuToken

1. В дальнейшем, для использования ключей требуется предварительно подключить Rutoken.

2. При выборе типа ключа (там, где это требуется) выбирать Public Key User:

Из списка ключей шифрования выбрать требующийся:

Ввести PIN!код Пользователя* и нажать кнопку ОК:

* PIN_код Пользователя по умолчанию: 12345678

Вопросы и практические задания.

1. Создайте пару ключей на памяти RuToken'a
2. Закодируйте ряд файлов (на выбор преподавателя) с использованием RuToken'a
3. Протестируйте результат (зашифрованные файлы)
4. Создайте новый zip-контейнер с использованием RuToken'a
5. Настройте почтовый адрес для защищенного обмена информацией
6. Создайте защищенный виртуальный диск с использованием RuToken'a
7. Создайте log о использовании почтовых клиентов
8. Зашифруйте сетевую папку с использованием RuToken'a
9. Добавьте user'a, допущенного для пользования сетевой папкой
10. Удалите ключи с памяти RuToken'a
11. 10. Удалите PGP

Источники литературы

1. www.pgpru.ru
2. www.rutoken.ru

Практическое задание для практической подготовки

Тема 12. Защита от разрушающих программных воздействий.

1. Деструктивные программы как особый класс разрушающих программных воздействий.
2. Необходимые и достаточные условия предупреждения разрушающего воздействия.
3. Понятие изолированной программной среды.
4. Контроль доступа и разграничение доступа.
5. Защита сетевого файлового ресурса.

Тестирование

Тема 6. Система биометрической идентификации BioLink.

Типовые вопросы для тестирования. Система биометрической идентификации BioLink.

1. С помощью каких встроенных средств BioLink (BioTime Agent) возможно осуществление удаленного мониторинга приходов и уходов сотрудников?

- a) BioTime Web Reports
- b) BioTime Clock
- c) BioTime WebClock
- d) Мобильное приложение BioTime

2. Энергопотребление (по USB) BioLink U-Match 3.5 в режиме сканирования:

- a) 100 мВт
- b) 350 мВт
- c) 600 мВт
- d) 220 мВт

3. Первый вход в систему BioLink U-Match 3.5 можно осуществить:

- a) по паролю
- b) по отпечатку пальца
- c) по паролю или отпечатку пальца
- d) без пароля

4. Одна из главных задач, которую решает программа BioLinkPasswordVault:

- a) упростить работу пользователя с защищенными приложениями за счет замены подтверждения пользователя по буквенно-цифровому паролю биометрической верификацией.
- b) упростить работу пользователя с защищенными приложениями за счет замены подтверждения пользователя по биометрической верификации буквенно-цифровым паролем

4.3 Промежуточная аттестация по дисциплине проводится в форме экзамена

Типовые вопросы экзамена (ПК-1)

- 1 Предмет и задачи программно-аппаратной защиты информации.
- 2 Предмет и задачи программно-аппаратной защиты информации.
- 3 Классификация методов и средств программно-аппаратной защиты информации.
- 4 Идентификация.
- 5 Идентификация субъекта.
- 6 Понятие протокола идентификации.
- 7 Идентифицирующая информация.
- 8 Защита данных от несанкционированного доступа.
- 9 Основные подходы к защите данных от несанкционированного доступа.
- 10 Шифрование.
- 11 Контроль доступа и разграничение доступа.
- 12 Иерархический доступ к файлу.
- 13 Защита сетевого файлового ресурса.
- 14 Фиксация доступа к файлам.
- 15 Доступ к данным со стороны процесса.
- 16 Процессы и данные.
- 17 Способы фиксации факта доступа.
- 18 Надежность систем ограничения доступа.
- 19 Защита файлов от изменения.
- 20 Электронная цифровая подпись.
- 21 Программно-аппаратные средства шифрования.
- 22 Построение аппаратных компонент криптозащиты данных.
- 23 Защита алгоритма шифрования.
- 24 Принцип чувствительной области и принцип главного ключа.

- 25 Необходимые и достаточные функции аппаратного средства криптозащиты.
- 26 Методы и средства ограничения доступа к компонентам ЭВМ Ограничение доступа к компонентам ЭВМ.
- 27 Защита программ от несанкционированного копирования.
- 28 Пароли и ключи.
- 29 Организация хранения ключей.
- 30 Защита программ от изучения.
- 31 Общие принципы защиты от изучения.
- 32 Защита от отладки.
- 33 Защита от дизассемблирования.
- 34 Защита от трассировки по прерываниям.
- 35 Защита от разрушающих программных воздействий.
- 36 Компьютерные вирусы как особый класс разрушающих программных воздействий.
- 37 Необходимые и достаточные условия недопущения разрушающего воздействия.
- 38 Понятие изолированной программной среды.

Типовые задания для экзамена (ПК-1)

- 1 Проект корпоративной сети для комплекса зданий. Проектирование иерархической сети. Требования к сети. Принципы структурированного проектирования.
- 2 Иерархия сети. Уровень доступа. Уровень распределения. Уровень ядра.
- 3 Корпоративная архитектура Cisco. Модуль комплекса зданий предприятия. Модуль границы предприятия. Граница сети оператора связи. Удалённая функциональная область.
- 4 Развивающиеся сетевые архитектуры. Сети без границ. Архитектура совместной работы. Центры обработки данных и виртуализация. Расширение сети.
- 5 Подключение к глобальной сети. Сети филиалов. Распределённая сеть. Устройства глобальной сети. Коммутация каналов и коммутация пакетов.
- 6 Сервисы глобальной сети. Инфраструктура сети оператора. Инфраструктуры частных глобальных сетей. Арендованные линии. Коммутируемый доступ. ISDN. FrameRelay. ATM. WAN на основе Ethernet. MPLS. VSAT.
- 7 Инфраструктура общедоступной глобальной сети. DSL. Кабель. Беспроводные технологии. Сотовая связь. Технология VPN. Выбор способа подключения к глобальной сети.
- 8 Последовательное соединение "точка-точка". Последовательные и параллельные порты. Связь по последовательному каналу. Мультиплексирование с разделением по времени. Устройства DTE и DCE. Последовательные кабели.
- 9 Инкапсуляция HDLC. Типы кадров. Настройка и отладка последовательного интерфейса. Принцип работы протокола PPP. LCP и NCP. Структура кадра PPP. Сеансы PPP.
- 10 Настройка протокола PPP. Команды базовой настройки. Сжатие данных. Мониторинг качества канала PPP. Проверка настроек.

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«отлично» (85 - 100 баллов)	ПК-1	Демонстрирует высокий уровень теоретических знаний в области программно-аппаратной защиты информации. Может провести анализ основных приемов злоумышленников при атаках на защищаемую информацию. Владеет основными методами защиты программного обеспечения от изучения и взлома. Способен администрировать программно-аппаратные средства защиты информации в операционных системах.

«хорошо» (70 - 84 баллов)	ПК-1	Демонстрирует хороший уровень теоретических знаний в области программно-аппаратной защиты информации. Может провести анализ основных приемов злоумышленников при атаках на защищаемую информацию. Владеет основным методами защиты программного обеспечения от изучения и взлома. Способен администрировать программно-аппаратные средства защиты информации в операционных системах.
«удовлетворительно» (50 - 69 баллов)	ПК-1	Демонстрирует достаточный уровень теоретических знаний в области программно-аппаратной защиты информации. Затрудняется провести анализ основных приемов злоумышленников при атаках на защищаемую информацию. Не до конца владеет основным методами защиты программного обеспечения от изучения и взлома. Не в полной мере способен администрировать программно-аппаратные средства защиты информации в операционных системах.
«неудовлетворительно» (менее 50 баллов)	ПК-1	Не демонстрирует знания в области программно-аппаратной защиты информации. Не может провести анализ основных приемов злоумышленников при атаках на защищаемую информацию. Не владеет основным методами защиты программного обеспечения от изучения и взлома. Не способен администрировать программно-аппаратные средства защиты информации в операционных системах.

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;

- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Шаньгин, В. Ф. Информационная безопасность и защита информации. - 2024-09-24; Информационная безопасность и защита информации. - Саратов: Профобразование, 2019. - 702 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/87995.html>
2. Лопатин Д. В. Программно-аппаратная защита информации : электрон. учеб. пособие. - Тамбов: [Б. и.], 2014. - 1 электрон. опт. диск (CD-ROM)
3. Иванова, Н. Ю., Маняхина, В. Г. Системное и прикладное программное обеспечение : учебное пособие. - Весь срок охраны авторского права; Системное и прикладное программное обеспечение. - Москва: Прометей, 2011. - 202 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/58201.html>
4. Башлы П. Н., Баранова Е. К., Бабаш А. В. Информационная безопасность : учебно-практическое пособие. - Москва: Евразийский открытый институт, 2011. - 375 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=90539>

6.2 Дополнительная литература:

1. Программно-аппаратная защита информации : учеб.-метод. комплекс, Блок 5: Защита программ от изучения: Теоретические и технические аспекты выявления работы защищенного приложения в аномальных и искусственных средах. - [Тамбов]: Изд-во ТГУ, [200. - 1 электрон. опт. диск (CD-ROM)].
2. Волосатова Т.М., Денисов А.В., Чичварин Н.В. Комбинированные методы защиты данных в САПР. - [М.]: Новые технологии, Информационные технологии, 2012. - 32 с.
3. Специальное и прикладное программное обеспечение : учеб.-метод. комплекс, Блок 1: Шпионское программное обеспечение. Руткиты. Программные закладки: обнаружение и нейтрализация. - [Тамбов]: Изд-во ТГУ, [200. - 1 электрон. опт. диск (CD-ROM)].
4. Специальное и прикладное программное обеспечение : учеб.-метод. комплекс, Блок 2: Брандмауэры: межсетевые экраны. Персональные межсетевые экраны. Определение надёжности межсетевых экранов. - [Тамбов]: Изд-во ТГУ, [200. - 1 электрон. опт. диск (CD-ROM)].
5. Специальное и прикладное программное обеспечение : учеб.-метод. комплекс, Блок 3: Восстановление утерянной информации. Безвозвратное удаление информации. Анонимная работа на компьютере. - [Тамбов]: Изд-во ТГУ, [200. - 1 электрон. опт. диск (CD-ROM)].
6. Специальное и прикладное программное обеспечение : учеб.-метод. комплекс, Блок 4: Сканеры уязвимостей. - [Тамбов]: Изд-во ТГУ, [200. - 1 электрон. опт. диск (CD-ROM)].

6.3 Иные источники:

1. Федеральный портал «Российское образование» - <http://www.edu.ru/>
2. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» - <http://school-collection.edu.ru/>
3. Федеральная служба по надзору в сфере образования и науки - <http://obrnadzor.gov.ru>
4. Вопросы образования - <http://www.ecsocman.edu.ru/vo>

7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

Microsoft Windows 10

Фикс 3.0 (программа фиксации и контроля исходного состояния)

Crypton IP Mobile

CryptonLock

Crypton Дозор

CryptonFastDisk

CryptonEmulato

CryptonDisk

Crypton LITE

CryptonArcMail

CryptonOffice

CryptonWipe

Библиотека CryptonArcMail

Библиотека Crypton DK

Crypton Шифрование

Драйвер шифрования RuToken

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>

2. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>

3. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>

4. Российская государственная библиотека. – URL: <https://www.rsl.ru>

5. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prilib.ru>

Электронная информационно-образовательная среда

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.