

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Инженерно-технический институт
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:

И.о. директора института



Т. В. Пасько

«17» июня 2026 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.В.ДВ.06.04 Программирование Java

Направление подготовки/специальность: 03.03.02 - Физика

Профиль/направленность/специализация: Физические основы робототехнических систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2026

Автор программы:

Кандидат физико-математических наук, доцент Лопатин Дмитрий Валерьевич

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 03.03.02 - Физика (уровень бакалавриата) (приказ Министерства науки и высшего образования РФ от «07» августа 2020 г. № 891).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «16» июня 2026 г. Протокол № 11

Рассмотрена и одобрена на заседании Ученого совета Инженерно-технического института, Протокол от «17» июня 2026 г. № 10.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП бакалавриата.....	6
3. Объем и содержание дисциплины.....	6
4. Контроль знаний обучающихся и типовые оценочные средства.....	15
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	45
6. Учебно-методическое и информационное обеспечение дисциплины.....	46
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	47

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

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

- научно-исследовательский
- педагогический

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сферах: 01 Образование и наука (в сферах: реализации образовательных программ среднего общего образования, среднего профессионального образования, высшего образования и дополнительных профессиональных программ; научных исследований и научно-конструкторских разработок), 40 Сквозные виды деятельности в промышленности (в сферах: фундаментальных основ физики живых систем и физико-химической биологии, применения диагностического и лечебного оборудования, участия в инновационных и опытно-конструкторских разработках; эксплуатации электронных приборов и систем различного назначения; мониторинга параметров материалов; мониторинга состояния окружающей среды)

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
	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	Осуществляет поиск, критический анализ и структурирование информации, выбирает на этой основе оптимальные архитектурные и алгоритмические решения при разработке программного обеспечения

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения				
		Очная (семестр)				
		1	2	3	4	8
1	CAD-системы автоматического проектирования		+			
2	CAE-системы автоматического проектирования			+		
3	CAM-системы автоматического проектирования				+	

4	Алгоритмы машинного обучения			+		
5	Безопасность компьютерных сетей			+		
6	Бэкэнд - программирование			+		
7	Введение в высшую математику	+				
8	Введение в спортивное программирование		+			
9	Высшая математика		+			
10	Вычислительные среды обработки данных		+			
11	Графический дизайн			+		
12	Демонстрационный эксперимент в школе		+			
13	Инструменты визуализации данных				+	
14	Комбинаторный анализ		+			
15	Компьютерная графика				+	
16	Математическое и компьютерное моделирование			+		
17	Математическое моделирование и визуализация научных данных средствами языка Python				+	
18	Методы решения геометрических задач				+	
19	Организация школьного кабинета физики			+		
20	Программирование на PHP				+	
21	Программирование устройств телекоммуникаций на языках высокого уровня				+	
22	Программирование устройств телекоммуникаций на языках низкого уровня			+		
23	Проективная геометрия			+		
24	Решение олимпиадных физических задач				+	

25	Системы многоуровневой защиты информации				+	
26	Спортивное программирование: уровень 1			+		
27	Спортивное программирование: уровень 2				+	
28	Стандарты в области информационной безопасности		+			
29	Физика и химия твёрдого тела		+			
30	Философия					+
31	Цифровая культура	+				
32	Цифровая обработка изображений		+			
33	Экспертные системы		+			

2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Программирование Java» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 03.03.02 - Физика.

Дисциплина «Программирование Java» изучается в 2 семестре.

3. Объем и содержание дисциплины

3.1. Объем дисциплины: 2 з.е.

Очная: 2 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	144
Контактная работа	64
Лабораторные (Лаб. раб.)	64
Самостоятельная работа (СР)	80
Зачет	-

3.2. Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.		Формы текущего контроля
		Лаб	СР	
		раб.		
		О	О	
2 семестр				
1	Предмет и задачи программно-аппар атной защиты информации.	4	4	Доклад

2	Системы идентификации	5	6	Лабораторная работа
3	Доступ к данным со стороны процесса.	5	6	Лабораторная работа
4	Программно-аппаратные комплексы защиты информации.	5	6	Лабораторная работа
5	Методы и средства ограничения доступа к компонентам ЭВМ	4	6	Лабораторная работа
6	Понятие обратного проектирования.	5	6	Лабораторная работа
7	Защита программ от изучения.	4	6	Лабораторная работа

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

Лекция.

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

Лабораторные работы.

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

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

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 идентификации 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.

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.

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 шифрованного 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 «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 «Соболев»

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. Методы и средства ограничения доступа к компонентам ЭВМ

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 6. Понятие обратного проектирования.

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 дизассемблирования программ.
3. Покажите основные мониторы событий

Тема 7. Защита программ от изучения.

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 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 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.

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

2 семестр

- посещаемость – 10 баллов
- текущий контроль – 80 баллов
- контрольные срезы – 1 срез по 10 баллов каждый
- премиальные баллы – 20 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	10	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. Основные качества доклада подлежащего оценке: 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. 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. 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.
2.	Системы идентификации	Лабораторная работа	10	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 существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.
3.	Доступ к данным со стороны процесса.	Лабораторная работа	10	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 существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.

4.	Программно-аппаратные комплексы защиты информации.	Лабораторная работа(контрольный срез)	10	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 существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.
5.	Методы и средства ограничения доступа к компонентам ЭВМ	Лабораторная работа	10	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 существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.
6.	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
7.	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

8.	Посещаемость	10	10 баллов – стопроцентное посещение занятий студентом 7-9 баллов – посещаемость студента составляет не менее 80 % занятий 4-6 баллов – посещаемость студента составляет не менее 50 % занятий 1-3 балла – посещаемость студента составляет не менее 25 % занятий
9.	Премияльные баллы	20	- 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
10.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы	10	Решение кейса (10 баллов) Прохождение тестирования (30 вопросов) по всему курсу дисциплины (10 баллов)
11.	Итого за семестр	100	

Итоговая оценка по зачету 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
50 - 100 баллов	Зачтено
0 - 49 баллов	Не зачтено

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 удалённом 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 msixexec.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 я 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 «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.

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 назначения 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 Sneek.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. 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 "Закреть".

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 зашифрованных 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 "Заккрыть".

- Если не все ключевые носители были обработаны, то после нажатия кнопки "Заккрыть" (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, имеющихся 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 шифрованного 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 6. 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 7. 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, диассемблеры, 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 диассемблер).

С помощью Haker-VIEW можно посмотреть любой исполняемый файл по любому смещению. Можно выполнить какую-то часть программы. Это позволяет расшифровывать программы и обходить защиту от дизассемблирования. 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 Haker-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 дизассемблирования. 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?

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

Типовые вопросы зачета (УК-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 зачета (УК-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)
«зачтено» (50 - 100 баллов)	УК-1	
«не зачтено» (0 - 49 баллов)	УК-1	

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: <https://www.tsutmb.ru/biblio/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: официальный сайт. – URL: <https://www.rsl.ru>

5. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prlib.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.