Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Н. Я. Великите

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие по изучению дисциплины
для студентов специальности
10.05.03 Информационная безопасность автоматизированных систем

Калининград
Издательство ФГБОУ ВО «КГТУ»
2023

УДК 004.056.57(075)

Рецензент:
доцент кафедры информационной безопасности
Института цифровых технологий ФГБОУ ВО
«Калининградский государственный технический университет»
А. Г. Жестовский

Великите, Н. Я.
Теоретические основы компьютерной безопасности: учеб.-метод. пособие по изучению дисциплины для студ. специальности 10.05.03 Информационная безопасность автоматизированных систем / Н. Я. Великите. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2023. – 23 с.

Учебно-методическое пособие является руководством к изучению дисциплины «Теоретические основы компьютерной безопасности» для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем. В нем представлен тематический план изучения дисциплины, содержание дисциплины по ее разделам и темам, темы практических занятий, указания к изучению каждой темы, рекомендации по выполнению практических заданий. Содержатся требования к текущей и промежуточной аттестации, определены условия получения положительной оценки.
Табл. 1, список лит. – 6 наименований

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала на заседании кафедры информационной безопасности ФГБОУ ВО «Калининградский государственный технический университет» 8 сентября 2022 г., протокол № 1

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в качестве локального электронного методического материала в учебном процессе методической комиссией Института цифровых технологий, протокол от 5 июля 2023 г., № 8

УДК 004.056.57(075)

Оглавление

1 Введение

В данном учебно-методическом пособии изложены основы теории компьютерной безопасности, объединяющие широкий спектр проблем защиты информации в процессе ее преобразования, хранения и передачи в автоматизированных системах обработки данных. Приводится описание основных моделей систем защиты и наиболее существенные результаты их анализа. Также уделено внимание важному понятию компьютерной безопасности – политике безопасности.

В результате освоения дисциплины ожидается, что студенты получат целостное представление о широкой сфере проблем обеспечения теоретических основ компьютерной безопасности в автоматизированных системах.

В учебно-методическом пособии по изучению дисциплины с практическими заданиями представлен тематический план, содержащий перечень изучаемых тем, обязательных практических работ, мероприятий текущей аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана на семестр следует оценивать рекомендуемое время на изучение дисциплины; возможно, вам потребуется больше времени на выполнение отдельных заданий или проработку отдельных тем.

В разделе «Содержание дисциплины» приведены подробные сведения об изучаемых вопросах, по которым вы можете ориентироваться в случае пропуска каких-либо занятий, а также методические рекомендации преподавателя для самостоятельной подготовки. Каждая тема имеет ссылки на литературу (или иные информационные ресурсы), а также контрольные вопросы для самопроверки.

Раздел «Текущая аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к промежуточной аттестации – экзамену.

Помимо данного пособия, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделе ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную учебную группу.

Перечень программного обеспечения:

- Microsoft Windows; - OpenOffice; - Kaspersky Endpoint Security 10 для Windows; - 7-Zip; - Google Chrome, программное обеспечение, по договору об образовательном сотрудничестве (лицензия компании Falcongaze на DLP SecureTower).

2 Тематический план

№ п.п.	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
		Лекции		
1	Раздел 1. Структура теории компьютерной безопасности	Тема 1 История развития теории и практики обеспечения компьютерной безопасности	2+2(РЭ)	-
2		Тема 2 Основные понятия компьютерной безопасности	2+2(РЭ	-
3		Тема 3 Анализ угроз компьютерной безопасности	4+2(РЭ	-
4	Раздел 2. Формальные политики безопасности	Тема 4 Понятие формальной политики, доступа и монитора безопасности	4+2(РЭ	-
5		Тема 5 Основные типы формальных политик безопасности	4+2(РЭ	-
6		Тема 6 Разработка и реализация формальных политик безопасности	4+2(РЭ	-
7	Раздел 3. Математические модели компьютерной безопасности	Тема 7 Модели безопасности на основе дискреционной политики	4+2(РЭ	-
8		Тема 8 Модели безопасности на основе мандатной политики	4+1(РЭ	-
9		Тема 9 Модели безопасности на основе тематической политики	4+1(РЭ	-
10		Тема 10 Модели безопасности на основе ролевой политики	2+1(РЭ	-
			34+17(РЭ)	-
		Лабораторные занятия		
1	Раздел 1. Структура теории компьютерной безопасности	Реализация политики информационной безопасности на примере дискреционной модели	3	-
2		Изучение уязвимости модели Харрисона – Руззо – Ульмана	2	-
3		Реализация распространения прав доступа по модели take-grant	2	-
4	Раздел 2. Формальные политики безопасности	Расширенная модель прав доступа take-grant	2	-
5		Нарушение дискреционной политики безопасности программой «Троянский конь»	2	-
6		Мандатные политики безопасности	2	-
7	Раздел 3. Математические модели компьютерной безопасности	Субъектно-объектная модель. Изолированная программная среда	2	-
8		Работа с матрицей доступов. Домены безопасности	2+2,25(КА)	-
			17+2,25(КА)	-

№ п.п.	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
		Практические занятия		
1	Раздел 2. Формальные политики безопасности	Установка и настройка серверных компонентов Falcongaze SecureTower	4	1
2		Мониторинг сетевой и компьютерной активности пользователей при помощи Консоли пользователя Falcongaze SecureTower. Ч1,Ч2	5	1
3		Практикум по назначению политик безопасности в Центре обеспечения безопасности Клиентской консоли Falcongaze SecureTower	5	1
4	Раздел 3. Математические модели компьютерной безопасности	Разработка политики безопасности Монитора безопасности объекта с использованием дискреционных моделей	10	1
5		Разработка политики безопасности Монитора безопасности объекта с использованием мандатных моделей	10	2
			34	**6**
		Рубежный (текущий) и итоговый контроль		
		Итоговый контроль (экзамен**)**		33,75
				33,75
		Всего	**85+17(РЭ)+2,25(КА)**	**39,75**

3 Содержание дисциплины и указания к изучению

3.1 Раздел 1. Структура теории компьютерной безопасности

3.1.1 Тема 1.1 История развития теории и практики обеспечения компьютерной безопасности

Перечень изучаемых вопросов:

1. Введение в предмет компьютерной безопасности (КБ).
2. Основные этапы теории и практики КБ.
3. Отечественная школа КБ.

Методические указания к изучению:

В данной теме мы рассмотрим предмет и задачи дисциплины. Рассмотрим специфику, задачи обеспечения безопасности компьютерной информации в автоматизированных системах. Ознакомимся с этапами развития теории КБ. Рассмотрим основополагающие работы зарубежных и отечественных авторов. Покажем, как сформировались три составляющих и, соответственно, три, хотя и взаимосвязанных, но различных направления защиты компьютерной информации: обеспечение конфиденциальности информации, обеспечение целостности данных, обеспечение сохранности и работоспособности данных.

1. Гайдамакин 6-8.
2. Щербаков 10-13.

3.1.2 Тема 1.2 Основные понятия компьютерной безопасности

Перечень изучаемых вопросов:

1. Иерархия понятий в области ИБ.
2. Современное содержание понятия компьютерной безопасности.
3. Методологическая база понятия ИБ.

Методические указания к изучению:

В рамках данной темы мы познакомимся со следующими понятиями:

- информационная безопасность – показывает, что ключевыми являются следующие аспекты: информационная сфера (объект), угрозы (внутренние и внешние) и состояние защищенности (предмет объекта).

В этой логике сфера понятия «компьютерная безопасность» сужается до объекта, именуемого компьютерной системой, под которой будем понимать человеко-машинную систему, представляющую совокупность электронно-программируемых технических средств обработки, хранения и представления данных, программного обеспечения (ПО), реализующего информационные технологии осуществления каких-либо функций, и информации (данных). В развитии этой логики, под компьютерной безопасностью понимается состояние защищенности (безопасность) информации (данных) в компьютерных системах и безотказность (надежность) функционирования компьютерных систем. В результате составляющими компьютерной безопасности выступают безопасность информации (данных), накапливаемых, обрабатываемых в компьютерной системе, и безопасность (безотказность, надежность) функций КС.

Содержательный анализ самого понятия «информация» (сведения (сообщения, данные) независимо от формы их представления), особенностей процессов и технологий ее сбора, обработки, хранения, представления и выдачи показывает, что безотносительно к функционально-содержательной стороне работы с информацией (данными) понятие «безопасность информации» включает три составляющих:

- обеспечение конфиденциальности;
- обеспечение целостности;
- обеспечение доступности.

1. Гайдамакин 9-11.
2. Щербаков 14-15.

3.1.3 Тема 1.3 Анализ угроз компьютерной безопасности

Перечень изучаемых вопросов:

1. Понятие и классификация угроз.
2. Идентификация и каталогизация угроз.

Методические указания к изучению:

Понятие угрозы безопасности является наряду с понятием безопасности информации краеугольным камнем в сфере компьютерной безопасности, поскольку выбор защитных механизмов определяется исходя из целей устранения, нейтрализации угроз, снижения последствий (ущерба) от их возможного проявления и воздействия.

Для того чтобы обеспечить эффективную защиту информации в компьютерной системе, необходимо в первую очередь рассмотреть и проанализировать все факторы, представляющие угрозу информационной безопасности. Рассмотрение понятий: «угроза», «атака», «уязвимость».

Рассмотрена классификация угроз информационной безопасности компьютерных систем по ряду базовых признаков. Понятия «классификация», «систематизация», «каталогизация».

Рекомендуется просмотреть соответствующие ресурсы по ссылкам в ЭИОС, которые обращаются к анализу угроз в компьютерной безопасности.

Контрольные вопросы к Разделу 1:

1. Назовите две составляющие в информационной системе.
2. Какие процессы называются информационными процессами?
3. Что понимается под понятием «Информационная среда»?
4. Что является объектом защиты информации?
5. Что является предметом защиты в КС?
6. Что понимается под информационной безопасностью?
7. Дайте определение уязвимости КС.
8. Назовите основные угрозы безопасности компьютерной системы.
9. Что представляет собой «защищенная компьютерная система»?
10. Дайте определение безопасности компьютерной системы.
11. Дайте определение угрозе.
12. Дайте определение атаке.
13. Дайте определение уязвимости КС.
14. Назовите основные угрозы безопасности компьютерной системы.
15. Что представляет собой «защищенная компьютерная система»?

Литература:

1. Гайдамакин 15-18.
2. Щербаков 25-27.
3. Девянин 5-7.

3.2. Раздел 2. Формальные политики безопасности

3.2.1 Тема 2.1 Понятие формальной политики, доступа и монитора безопасности

Перечень изучаемых вопросов:

1. Объект, субъект, доступ.
2. Монитор безопасности компьютерной системы.

Методические указания к изучению:

Фундаментальным понятием в сфере защиты информации компьютерных систем является политика безопасности. Под ней понимают интегральную совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает состояние защищенности информации в заданном пространстве угроз. Формальное выражение политики безопасности (математическое, схемотехническое, алгоритмическое и т. д.) называют моделью безопасности. Модели безопасности играют важную роль в процессах разработки и исследования защищенных компьютерных систем, так как обеспечивают системотехнический подход, включающий решение следующих важнейших задач:

- выбор и обоснование базовых принципов архитектуры защищенных компьютерных систем (КС), определяющих механизмы реализации средств и методов защиты информации;

- подтверждение свойств (защищенности) разрабатываемых систем путем формального доказательства соблюдения политики безопасности (требований, условий, критериев);

- составление формальной спецификации политики безопасности как важнейшей составной части организационного и документационного обеспечения разрабатываемых защищенных компьютерных систем.

По сути модели безопасности являются исходным связующим элементом в триаде «Заказчик (Потребитель) – Разработчик (Производитель) – Эксперт (Аудитор)». На основе моделей безопасности заказчики могут формулировать те требования к защищенным КС, которые соответствуют политике безопасности, технологическим процессам обработки информации, принятым в своих организациях и предприятиях. Разработчики на основе моделей безопасности формируют технико-технологические требования и программно-технические решения по разрабатываемым системам. В этой теме также рассматриваются понятия: субъект, объект, доступ, монитор безопасности, домен безопасности.

Литература:

1. Гайдамакин 22-27.
2. Щербаков 40-46.
3. Девянин 4-5.

1. Практическое занятие «Установка и настройка серверных компонентов Falcongaze SecureTower»

Цель практического занятия: научиться устанавливать компоненты программного комплекса на локальный компьютер, устанавливать агента на компьютер рабочей группы, настраивать перехват данных при помощи агента, настраивать работу ключевых сервисов Falcongaze SecureTower.

Оборудование: ПК, включенные в рабочую группу компьютеров.

Рекомендации по выполнению работы:

Изучите теоретическую часть лабораторного практикума, изложенную в разделе «Общие сведения», перед выполнением практических заданий.

Выполнять задания практикума следует строго в соответствии с пунктами, как указано в разделе «Порядок выполнения работы». Шаги и задания, помеченные «*», выполняются по указанию преподавателя.

После каждого шага или при возникновении вопросов о выполнении задания сравните результат на экране с соответствующим рисунком. Для быстрого получения помощи в работе с программой, а также получения дополнительной информации нажмите клавишу F1 либо обратитесь к преподавателю, либо к руководству пользователя, системного администратора, руководству по инсталляции (по настройке системы).

Чтобы проверить, насколько хорошо Вы усвоили материал, ответьте на контрольные вопросы в конце работы.

Литература в комплекте поставки с лицензией на использование DLP SecureTower:

1. Методические указания по выполнению практикума компании Фальконгейз.
2. Руководство системного администратора.
3. Руководство пользователя.
4. Руководство по инсталляции.
5. Краткое руководство по настройке системы. Быстрый старт.

Контрольные вопросы:

1. Для чего используется Консоль администратора?
2. В каких случаях при подключении к серверу указывается локальный компьютер?
3. Какие способы перехвата поддерживает система и в чем их отличие?
4. Для чего необходимо добавить правило записи при создании новой группы ротации/добавлении хранилища.
5. Какие способы установки агентов поддерживает система?
6. Возможно ли, используя настройки агента, запретить доступ к USB/сетевым ресурсам/принтерам?
7. Как, используя параметры профиля настроек, защитить агента от удаления?
8. Какой раздел Консоли администратора содержит информацию о работе агентов, установленных на компьютеры в сети организации?
9. Каким образом осуществляется привязка перехваченной информации к конкретным пользователям?
10. Как добавляется и обновляется информация о пользователях системы, если сеть организации построена на базе Active Directory/рабочей группы?

3.2.2 Тема 2.2 Основные типы формальных политик безопасности

Перечень изучаемых вопросов:

1. Гарантирование выполнения политики безопасности. Изолированная программная среда
2. Аксиомы защищённости компьютерных систем
3. Характеристика основных типов формальных политик безопасности

Методические указания к изучению:

Большинство моделей разграничения доступа основывается на представлении КС как совокупности субъектов и объектов доступа. Приводятся основные положения субъ-

ектно-объектной формализации компьютерных систем в аспекте безопасности информации.

Постулируя наличие в КС субъекта, реализующего политику безопасности, рассмотрены описания (на уровне моделей) некоторых известных политик безопасности. Для строгого и однозначного толкования норм и правил политики безопасности обычно дается ее формализованное описание в виде соответствующей модели. Основная цель такого описания – это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений. На практике это означает, что только соответствующим образом уполномоченные пользователи получат доступ к информации и смогут осуществить с ней только санкционированные действия.

Все существующие в настоящее время модели безопасности основаны на следующих базовых представлениях.

1. Компьютерная система является совокупностью взаимодействующих сущностей – субъектов и объектов. Объекты можно интуитивно представлять в виде контейнеров, содержащих информацию, а субъектами считать выполняющиеся программы, которые воздействуют на объекты различными способами. При таком представлении безопасность обработки информации обеспечивается путем решения задачи управления доступом субъектов к объектам в соответствии с тем набором правил и ограничений, которые образуют политику безопасности. Считается, что система безопасна, если субъекты не имеют возможности нарушать правила политики безопасности. Таким образом, общим кодом для всех моделей является именно разделение множества сущностей, образующих систему, на множества субъектов и объектов.

2. Все взаимодействия в системе моделируются установлением отношений определенного типа между субъектами и объектами. Множество типов таких отношений определяется в виде набора операций, которые субъекты могут производить над объектами.

3. Все операции между субъектами и объектами, контролируемые монитором взаимодействий, либо запрещаются, либо разрешаются в соответствии с правилами политики безопасности.

4. Политика безопасности задается в виде правил, определяющих все взаимодействия между субъектами и объектами. Взаимодействия, приводящие к нарушению этих правил, пресекаются средствами контроля доступа и не могут быть осуществлены.

5. Совокупность множеств субъектов, объектов и отношений между ними (установившихся взаимодействий) определяет состояние системы. В этом пространстве состояний каждое состояние системы является либо безопасным, либо небезопасным в соответствии с принятым в модели критерием безопасности.

6. Основной элемент модели безопасности – это доказательство того, что система, находящаяся в безопасном состоянии, не может перейти в небезопасное состояние при соблюдении всех установленных правил и ограничений.

Среди моделей политики безопасности можно выделить три основных типа: дискреционные (произвольные), мандатные (нормативные) и ролевые. В основе этих моделей лежат, соответственно, дискреционное управление доступом (Discretionary Access Control – DAC), мандатное управление доступом (Mandatory Access Control – MAC) и ролевое управление доступом (Role-Based Access Control – RAC) .

Литература:

1. Гайдамакин 28-34.
2. Щербаков 46-56.
3. Девянин 7-10.

2. Практическое задание «Мониторинг сетевой и компьютерной активности пользователей при помощи Консоли пользователя Falcongaze SecureTower. Ч1,Ч2»

Цель практического занятия: Научиться работе с Клиентской консолью Falcongaze SecureTower для проведения расследований и предупреждения инцидентов информационной безопасности организации, освоить различные виды поиска информации в объеме перехваченных данных. Научиться интерпретировать фотографию рабочего дня пользователя. (Ч1). Научиться работе с Клиентской консолью Falcongaze SecureTower для проведения расследований и предупреждения инцидентов информационной безопасности организации, освоить инструмент создания статистических отчетов о компьютерной и сетевой активности пользователей. Научиться использовать инструменты системы для наблюдения за активностью пользователей в режиме реального времени и для мониторинга файловых систем. (Ч2).

Оборудование и настройки: ПК с установленным комплексом Falcongaze SecureTower.

Рекомендации по выполнению работы

Изучите теоретическую часть лабораторного практикума, изложенную в разделе «Общие сведения», перед выполнением практических заданий.

Выполнять задания лабораторного практикума следует строго в соответствии с пунктами, как указано в разделе «Порядок выполнения работы». Шаги и задания, помеченные «*», выполняются по указанию преподавателя.

После каждого шага или при возникновении вопросов о выполнении задания сравните результат на экране с соответствующим рисунком. Для быстрого получения помощи в работе с программой, а также получения дополнительной информации используйте команды меню Помощь либо обратитесь к преподавателю, руководствам пользователя, администратора.

Чтобы проверить, насколько хорошо Вы усвоили материал, в конце работы ответьте на контрольные вопросы.

Литература в комплекте поставки с лицензией на использование DLP SecureTower:

1. Методические указания по выполнению практикума компании Фальконгейз.
2. Руководство системного администратора.
3. Руководство пользователя.
4. Руководство по инсталляции.
5. Краткое руководство по настройке системы. Быстрый старт.

Контрольные вопросы:

1. Чем вызваны различия результатов поиска по ключевой фразе «высылаю резюме» при выполнении заданий на шагах 2.2 – 2.5?
2. Какие логические операторы могут применяться для создания поискового запроса при комбинированном поиске?
3. Как отрегулировать интервал Данные, которые должны быть проверены на соответствие условиям поискового запроса?

4. Возможно ли создать карточку для нового пользователя через Консоль пользователя?

5. Как быстро проверить все взаимосвязи одного пользователя с другими пользователями сети?

6. Каковы возможности компонентов консоли по отслеживанию коммуникаций с внешними контактами и их идентификации?

7. Какие виды активности пользователя отображаются в отчете о дневной активности пользователя?

8. Какой инструмент Консоли пользователя позволяет провести комплексный (и качественный и количественный) анализ статистики по выбранному направлению активности пользователя в сети?

9. Перечислите виды активности, по которым доступно построение статистических отчетов для отдельного пользователя сети организации.

10. Как получить информацию о соблюдении режима рабочего дня пользователя?

11. Для чего выполняется индексирование файловых систем компьютеров?

12. Возможно ли выполнить поиск произвольного файла в файловой системе контролируемого компьютера? Например, файла, выбранного пользователем, или с указанным именем или расширением.

13. Возможно ли записать видео рабочего стола пользователя вручную?

14. Позволяет ли система производить автоматическую запись результатов мониторинга компьютеров пользователей?

3.2.3 Тема 2.3 Разработка и реализация формальных политик безопасности

Перечень изучаемых вопросов:

1. Механизм реализации политики безопасности в локальном сегменте компьютерной системы

2. Управление безопасностью компьютерной системой.

Методические указания к изучению:

Субъект, который активизируется при возникновении потока информации от любого субъекта (его ассоциированного объекта) к любому объекту, называется монитором обращений. В теории компьютерной безопасности различают два вида монитора обращений: индикаторный и содержательный.

Политику безопасности механизма авторизации реализует монитор безопасности объектов (МБО) – монитор обращений, который разрешает поток, принадлежащий только подмножеству легального доступа P1.

В мониторе безопасности объектов реализуется та или иная модель политики безопасности, с помощью которой осуществляется фильтрация потоков, относящихся к множеству потоков легального доступа.

Предполагается, что в локальном сегменте компьютерной системы существуют только попарно корректные субъекты, замкнутые в изолированной программной среде, с контролем целостности порождаемых субъектов. Другими словами, в составе локального сегмента компьютерной системы существует монитор безопасности субъектов (МБС). Кроме того, в локальном сегменте компьютерной системы действует монитор безопасности объектов (МБО), реализующий некоторую политику безопасности.

В защищенной компьютерной системе должна быть создана изолированная программная среда, в состав которой входят монитор безопасности объектов, гарантирующий порождение легальных потоков, и монитор безопасности субъектов, гарантирующий порождение субъектов только для определенных пар «субъект-объект».

Монитор безопасности субъектов и монитор безопасности объектов относятся к субъектам защищенной компьютерной системы и, следовательно, имеют ассоциированные с ними объекты-данные, которые содержат необходимые для функционирования субъектов данные.

Объекты – данные, ассоциированные с монитором безопасности субъектов (МБС) и монитором безопасности объектов (МБО), называют объектом управления (ОУ). Совокупность МБО, МБС и ОУ называют ядром безопасности.

Управление безопасностью изучает вопросы формирования и изменения объекта ОУ для субъектов, реализующих политику безопасности (МБО) и субъектов, гарантирующих её выполнение (МБС).

Компьютерная система называется управляемой, если в ней существует субъект, для ассоциированных объектов которого существует поток к объекту управления. Этот субъект называется субъектом администрирования или администрирующим субъектом. Пользователя, который управляет администрирующим субъектом, обычно называют администратором безопасности компьютерной системы.

Можно так же сказать, что только администратор безопасности должен иметь возможность порождения субъекта администрирования. Следовательно, только субъект администрирования должен иметь доступ на запись к объекту управления, а МБО и МБС должны иметь доступ на чтение к объекту управления.

Компьютерная система называется корректно управляемой, если поток к объекту управления существует только для субъекта управления (администрирующего субъекта).

Утверждение (о корректном управлении в ИПС): Если в компьютерной системе поддерживается изолированная программная среда с контролем неизменности объектов-источников и существует МБО, который разрешает доступ на запись к объекту управления только субъекту администрирования, то с момента активизации МБО управление в компьютерной системе корректно.

Литература:

1. Гайдамакин 35-42.
2. Щербаков 70-75.

Контрольные вопросы по Разделу 2:

1. Дайте определение политики безопасности.
2. Дайте определение понятия «Доступа».
3. Назовите основные характеристики системы.
4. Назовите основные типы политики безопасности.
5. Что значит «мандатное управление доступом»?
6. Что является основой мандатной политики безопасности?
7. Что значит «дискреционное управление доступом»?
8. Что является основой ролевой политики безопасности?
9. Что понимается под доменом безопасности?
10. Что называется монитором обращений?
11. Дайте определение монитора безопасности объектов.

12. Что называется методом расщепления прав пользователя?

13. Какая программная среда называется изолированной?

14. Какие два субъекта называются корректными относительно друг друга?

15. Какая программная среда называется замкнутой по порождению объектов?

16. Что называют объектом управления?

17. Что является ядром безопасности?

18. Какая компьютерная система называется корректно управляемой?

19. В чём состоит важность основной аксиомы теории защиты информации?

20. Какие основные виды политик безопасности рассматриваются в теории защиты информации?

3. Практическое задание «Практикум по назначению политик безопасности в Центре обеспечения безопасности Клиентской консоли Falcongaze SecureTower»

Цель практического занятия: научиться управлять работой Центра обеспечения безопасности Клиентской консоли Falcongaze SecureTower, получить опыт создания правил безопасности различных типов, освоить работу с уведомлениями об инцидентах безопасности.

Оборудование и настройки: ПК, включенный в рабочую группу компьютеров (локальный компьютер с установленным комплексом Falcongaze SecureTower).

Рекомендации по выполнению работы:

Изучите теоретическую часть практикума, изложенную в разделе «Общие сведения» перед выполнением практических заданий.

Выполнять задания практикума следует строго в соответствии с пунктами, как указано в разделе «Порядок выполнения работы». Шаги и задания, помеченные «*», выполняются по указанию преподавателя.

После каждого шага или при возникновении вопросов о выполнении задания сравните результат на экране с соответствующим рисунком. Для быстрого получения помощи в работе с программой, а также получения дополнительной информации используйте команды меню Помощь либо обратитесь к преподавателю.

Чтобы проверить, насколько хорошо Вы усвоили материал, в конце работы ответьте на контрольные вопросы.

Литература в комплекте поставки с лицензией на использование DLP SecureTower:

1. Методические указания по выполнению практикума компании Фальконгейз.

Контрольные вопросы:

1. Какие способы используются в системе SecureTower для оповещения о сетевых событиях, нарушающих политику безопасности?

2. Какие виды правил безопасности доступны в Центре обеспечения безопасности?

3. Для каких источников данных доступна возможность создания цифровых отпечатков?

4. В чем основные отличия контроля по тексту, по словарю от контроля за событиями безопасности по цифровым отпечаткам?

3.3. Раздел 3. Математические модели компьютерной безопасности

3.3.1 Тема 3.1 Модели безопасности на основе дискреционной политики

Перечень изучаемых вопросов:

1. Общая характеристика политики дискреционного доступа

2. Пятимерное пространство Хартсона.

3. Модели на основе матрицы доступа.

4. Модели распространения прав доступа.

Методические указания к изучению:

Модели безопасности, строящиеся на субъектно-объектной модели КС, еще называют моделями конечных состояний. В данных моделях инициализация информационных потоков трактуется как запросы субъектов на доступ к объектам, которые в зависимости от политики безопасности разрешаются или запрещаются. Осуществление субъектом разрешенного доступа к объекту переводит систему в следующий момент времени в другое состояние, рассматриваемое как совокупность состояний субъектов и объектов системы.

Проблема безопасности в КС рассматривается с точки зрения анализа и исследования условий, правил, порядка и т. п. разрешений запросов на доступ, при которых система, изначально находясь в безопасном состоянии, за конечное число переходов перейдет также в безопасное состояние.

Политика дискреционного доступа охватывает самую многочисленную совокупность моделей разграничения доступа, реализованных в большинстве защищенных КС, и исторически является первой проработанной в теоретическом и практическом плане. Специфика и значение моделей заключается в том, что исходя из способа представления (описания) области безопасного доступа и механизма разрешений на доступ анализируется и доказывается, что за конечное число переходов система останется в безопасном состоянии. В теоретическом и практическом плане наибольшее развитие и применение получили дискреционные модели, основанные на матрице доступа. В данных моделях область безопасного доступа строится как прямоугольная матрица (таблица), строки которой соответствуют субъектам доступа, столбцы объектам доступа, а в ячейках записываются разрешенные операции соответствующего субъекта над соответствующим объектом. В моделях распространения прав доступа проблема безопасности КС рассматривается с точки зрения анализа возможности или невозможности получения каким-либо субъектом определенных прав доступа к определенному объекту. Иначе говоря, анализируются прежде всего изменения прав доступа субъектов к объектам в результате некоторых обусловленных операций (переходов), а не сами процессы осуществления доступов субъектов к объектам.

Литература:

1. Гайдамакин 43-71.

2. Девянин 18-32.

4. Практическое занятие «Разработка политики безопасности Монитора безопасности объекта с использованием дискреционных моделей»

Цель: Моделирование политики безопасности МБО.

Задание:

При разработке политики безопасности МБО использовать формальную модель Харрисона – Руззо – Ульмана (например, добавление субъекта в матрицу прав доступа с учетом критерия безопасности). Проанализировать состояния компьютерной системы при выполнении следующих процессов:

- пользователь 1 разрабатывает на языке программирования С++ код приложения Структура и запускает его на выполнение, затем текст кода приложения Структура

записывает в файл, созданный текстовым процессором Word, и выводит текст на печатающее устройство;

- пользователь 2 запускает на выполнение код приложения Структура, разрабатывает на языке программирования С++ код приложения и записывает его в файл 5, выводит на печатающее устройство файлы 9 и А5 и с помощью субъекта 3 запускает на выполнение файл 4.

Права доступа:

1 read 1, код приложения Структура

write 1, 9

execute код приложения, 9, 1, А5, Visual C++, текстовый процессор Word

2 read 5, 9, код приложения,

write код приложения Структура, А5

execute код приложения Структура, 4, Vis-ual C++, текстовый процессор Word.

Индивидуальное задание по практической работе 4 и пример выполнения можно посмотреть в системе ЭИОС.

3.3.2 Тема 3.2 Модели безопасности на основе мандатной политики

Перечень изучаемых вопросов:

1. Общая характеристика моделей полномочного (мандатного) доступа.
2. Модель Белла – ЛаПадулы.
3. Расширения модели Белла – ЛаПадулы.

Методические указания к изучению:

Модели безопасности, строящиеся на Мандатное УД (Mandatory Access Control – MAC) – разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности. Оно основано на сопоставлении атрибутов безопасности субъекта (уровня допуска пользователя) и объекта (грифа секретности информации).

Мандатная модель управления доступом основана на правилах секретного документооборота, принятых в государственных и правительственных учреждениях многих стран. Основным положением данной ПБ, взятым из реальной жизни, является назначение всем участникам процесса обработки защищаемой информации и документам, в которых она содержится, специальной метки, получившей название уровень безопасности (метка безопасности). Метка субъекта описывает его благонадежность, а метка объекта – степень закрытости содержащейся в нем информации. Уровни секретности, поддерживаемые системой, образуют множество, упорядоченное с помощью отношения доминирования. Такое множество может выглядеть следующим образом: сов. секретно, секретно, конфиденциально, несекретно и т. д.

Система в мандатной модели представляется в виде множеств субъектов S, объектов O, решетки уровней безопасности L и матрицы доступа M.

Достоинства мандатного УД:

- экономия памяти, так как элементы матрицы доступа не хранятся, а динамически вычисляются при попытке доступа для конкретной пары «субъект-объект» на основе их меток;
- удобство корректировки базы данных защиты, то есть модификации меток;

• принудительное УД хорошо согласуется с работой государственных, правительственных и военных организаций, так как переносит общепринятые и хорошо отработанные принципы обращения с бумажными секретами на современную основу работы с документами.

Недостатки мандатного УД:

• затруднено задание прав доступа конкретного субъекта к конкретному объекту;

• каждый субъект и объект должен быть помечен и при любых операциях с данными метки должны оставаться правильными. В особенности это относится к экспорту и импорту данных. Например, печатный документ должен открываться заголовком, содержащим текстовое и/или графическое представление метки безопасности. Аналогично, при передаче файла по каналу связи должна передаваться и ассоциированная с ним метка, причем в таком виде, чтобы удаленная система могла ее правильно трактовать, несмотря на возможные различия в уровнях секретности и наборе категорий.

Наиболее известными мандатными моделями являются ММ Белла – Лападула (Дэвид Белл и Леонардо ЛаПадула), ММ Биба, решетчатая модель Д. Деннинга, ММ совместного доступа с уполномоченными субъектами и т. д.

Литература:

1. Гайдамакин 72-85.

5. Практическое занятие «Разработка политики безопасности Монитора безопасности объекта с использованием мандатных моделей»

Цель: Моделирование политики безопасности МБО.

Задание:

При разработке политики безопасности МБО использовать формальную модель Белла –ЛаПадулы (моделирование безопасной функции перехода Мак-Лина по чтению, алгоритм).

 Определение субъекта, имеющего наименьшее количество доступов типа write и read к объектам матрицы доступа.

 Составление списка пользователей, которые вошли в систему и ни разу не обратились к матрице прав доступа.

2. Проанализировать состояния компьютерной системы при выполнении следующих процессов:

 пользователь Н1 запускает на выполнение Excel и сохраняет созданный файл с именем Список1, затем читает файл Список2 и запускает его на выполнение;

 пользователь Н2 запускает на выполнение Access и создает две таблицы Таблица1 и Таблица2, затем с помощью объекта Формы заполняет таблицы конкретными данными и сохраняет их под теми же именами;

 пользователь Н3 запускает на выполнение файлы Поиск1.c и Поиск2.c.

Данные для отладки кодов приложений задать самостоятельно по следующей схеме в соответствии с выполняемыми процессами:

Объекты:

Пользователи: Н1, Н2, Н3

Права доступа:

Н1 read

write

execute

H2 read
write
execute
H3 read
write
execute.

3.3.3 Тема 3.3 Модели безопасности на основе тематической политики

Перечень изучаемых вопросов:

1. Общая характеристика тематического разграничения доступа.
2. Тематическая решетка мультирубрик иерархического рубрикатора.
3. Модели тематико-иерархического разграничения доступа.

Методические указания к изучению:

Важным аспектом, присутствующим в практике разграничения доступа к «бумажным» ресурсам, является тематическая «окрашенность» информационных ресурсов предприятий, учреждений по организационно-технологическим процессам и профилям деятельности. Организация доступа сотрудников к информационным ресурсам организации (в библиотеках, архивах, документальных хранилищах) осуществляется на основе тематических классификаторов. Все документы информационного хранилища тематически индексируются, т. е. соотносятся с теми или иными тематическими рубриками классификатора. Сотрудники предприятия согласно своим функциональным обязанностям или по другим основаниям получают права работы с документами определенной тематики. Данный подход, в сочетании с избирательным и мандатным доступом, обеспечивает более адекватную и гибкую настройку системы разграничения доступа на конкретные функционально-технологические процессы, предоставляет дополнительные средства контроля и управления доступом.

Анализ библиотечных и других автоматизированных систем документального поиска, основанных на тематическом индексировании содержания документов (текстов), показывает, что определяющее значение в таких системах имеет тематико-классификационная схема, в большинстве случаев именуемая тематическим рубрикатором. Применяются три основных способа тематической классификации:

• перечислительная классификация (дескрипторный подход);
• систематизированная классификация (иерархический подход);
• аналитико-синтетическая классификация (фасетный подход).

Литература:

1. Гайдамакин 86-111.

3.3.4 Тема 3.4 Модели безопасности на основе ролевой политики

Перечень изучаемых вопросов:

1. Модели ролевого доступа.
2. Модели индивидуально-группового доступа.
3. MMS-модель.

Методические указания к изучению:

Анализ различных организационно-управленческих и организационно-технологических схем показывает, что в реальной жизни сотрудники предприятий, учреждений выполняют определенные функциональные обязанности не от своего личного имени, а в рамках некоторой должности. Должность, которую можно трактовать как

определенную роль, представляет некоторую абстрактную, точнее, обобщенную сущность, выражающую определенный тип функций и тип положения работника (подчиненность, права и полномочия). Таким образом, в реальной жизни в большинстве организационно-технологических схем права и полномочия предоставляются конкретному сотруднику не лично (непосредственно), а через назначение его на определенную должность (роль), с которой он и получает некоторый типовой набор прав и полномочий.

Еще одним аспектом реальных организационно-технологических и управленческих схем является использование понятий прав и полномочий, как неких процедур над ресурсами системы, отражающих организационно-технологические процессы предметной области КС. Иначе говоря, права и полномочия сотрудникам по их должностям предоставляются не на уровне элементарных операций над ресурсами (читать, изменять, добавлять, удалять, создавать), а на уровне совокупностей элементарных операций, сгруппированных в отдельные логически обобщенные процедуры обработки информации (например, кредитные или дебетные операции над определенными бюджетами).

Таким образом, политика разграничения доступа в компьютерных системах, автоматизирующих те или иные организационно-технологические или организационно-управленческие процессы, должна строиться на основе функционально-ролевых отношений, складывающихся в предметной области КС.

Впервые подобный подход был рассмотрен в конце 70-х – начале 80-х гг. в исследованиях по процессам разграничения доступа корпорации IBM и получил название ролевого управления доступом. В начале 80-х гг. была представлена модель Лендвера – МакЛина, встречающаяся в литературе также под названием MMS-модели, сочетающая дискреционный и мандатный принципы разграничения доступа с использованием понятия и механизма ролей. Несколько позже появились и формальные выражения ролевых основ управления доступом (Role-Based Access Control –RBAC).

Ролевое УД (Role-Based Access Control – RAC) – универсальная надстройка (каркас), применяемая с дискреционным и мандатным УД и предназначенная для упрощения функций администрирования систем с большим количеством субъектов и объектов.

Суть ролевого УД состоит в том, что между пользователями и их правами доступа к объектам появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права доступа к объекту и, наоборот, несколько пользователей может выступать в одной роли по отношению к одному объекту. Между ролями могут быть установлены связи, аналогичные отношению наследования в ООП. Таким образом может быть построена иерархия ролей, используя которую можно существенно сократить количество контролируемых (администрируемых) связей.

Литература:

1. Гайдамакин 111-132.

Контрольные вопросы по Разделу 3:

1. Назовите дискреционные модели безопасности.
2. Назовите мандатные модели безопасности.
3. К какому типу моделей политики безопасности относится модель АДЕПТ – 50?
4. К какому типу моделей политики безопасности относится модель Харрисона – Руззо –Ульмана?
5. Что рассматривается в модели Харрисона – Руззо – Ульмана?

6. К какому типу моделей политики безопасности относится модель типизированной матрицы доступа?

7. Какая реализация модифицированной типизированной матрицей доступа называется ациклической?

8. Какая реализация модифицированной типизированной матрицей доступа называется циклической?

9. К какому типу моделей политики безопасности относится модель Белла – Лападулы?

10. Что называется уровнем безопасности в модели Белла – Лападулы?

11. Дайте определение решетки уровней безопасности в модели Белла – Лападулы.

12. На какие состояния делятся системы в классической мандатной модели Белла – Лападулы?

13. Назовите основную теорему безопасности (модель Белла – Лападулы).

14. Дайте понятия пользователя и роли в ролевой политики безопасности.

4 Примерные вопросы к экзамену по дисциплине

1. Методы реализации угроз нарушения конфиденциальности, целостности, отказа доступа, раскрытия параметров системы и методы защиты на уровнях: носителей информации; средств взаимодействия с носителем; представления информации; содержания данных.

2. Основные принципы обеспечения информационной безопасности в автоматизированных системах.

3. Структура понятия «компьютерная безопасность» и основные направления ее обеспечения.

4. Понятие защищенности (безопасности) компьютерной информации.

5. Конфиденциальность, целостность и доступность информации.

6. Понятие угроз безопасности компьютерной информации и их классификация.

7. Таксонометрия угроз безопасности и изъянов (брешей) систем защиты. ГОСТ Р 51275-99.

8. Человеческий фактор и модель нарушителя безопасности информации.

9. Субъектно-объектная модель компьютерной системы. Понятие потока, доступа и правил разграничения доступа. Основные типы политик разграничения доступа.

10. Монитор безопасности КС и гарантирование выполнение политики безопасности.

11. Изолированная программная среда.

12. Дискреционные модели безопасности компьютерных систем. Пятимерное пространство Хартсона.

13. Модели безопасности на основе матрицы доступа. Способы организации матрицы доступа и управления доступом в компьютерных системах.

14. Дискреционные модели распространения прав доступа.

15. Модель и теоремы безопасности Харрисона – Руззо – Ульмана.

16. Модель типизованной матрицы доступа.

17. Модель TAKE-GRANT.

18. Расширенная модель TAKE-GRANT.

19. Основы политики мандатного доступа. Решетка безопасности.

20. Модель Белла – ЛаПадулы и основная теорема безопасности.

21. Основные расширения модели Белла – ЛаПадулы.

22. Общая характеристика политики тематического разграничения доступа.

23. Решетки в моделях тематического разграничения доступа.

24. Решетка мультирубрик на иерархических рубрикаторах.

25. Скрытые каналы утечки информации и теоретико-информационные модели безопасности.

26. Технологии «представлений» и «разрешенных процедур».

27. Модели ролевого доступа. Иерархические системы ролей.

28. Принципы наделения ролей полномочиями.

29. Политика и зональная модель безопасности в распределенных КС.

30. Модели обеспечения целостности. Дискреционная модель Кларка – Вильсона.

31. Модели обеспечения целостности. Мандатная модель Кена Биба.

32. Объединение мандатных моделей Белла – ЛаПадулы и Кена Биба.

5 Список литературы

5.1 Основная литература:

1. Гайдамакин, Н. А. Теоретические основы компьютерной безопасности: учебное пособие / Н. А. Гайдамакин. - Екатеринбург, 2008, - 201 с.

2. Щербаков, А. Ю. Введение в теорию и практику компьютерной безопасности / А. Ю. Щербаков. - Москва: Издатель Молгачев С. В. – 2001 - 352 с.

3. Девянин, П. Н. Модели безопасности компьютерных систем: учебное пособие / П. Н. Девянин. - Москва: Academia, 2005. - 144 с.

5.2 Дополнительная литература:

4. Прокопьев, И. В. Введение в теоретические основы компьютерной безопасности: учебное пособие / И. В. Прокопьев, И. Г. Шрамков, А. Ю. Щербаков. - Москва, 1998. - 184 с.

5. Зегжда, Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. - Москва: Горячая линия - Телеком, 2000. - 452 с.

5.3 Учебно-методические пособия по дисциплине:

6. Теоретические основы компьютерной безопасности: учебное пособие для вузов / П. Н. Девянин, О. О.Михальский, Д. И. Правиков и др. - Москва: Радио и Связь, 2000. - 192 с.

6 Заключение

В результате изучения теоретических основ компьютерной безопасности студент должен составить представление о компьютерных системах и механизмах их защиты в терминах объектно-субъектных моделей, изучить формальные модели безопасности, политики безопасности, а также уметь использовать теоретические знания моделей механизмов защиты компьютерных систем и критериев, обеспечивающих их защиту.

Локальный электронный методический материал

Наталья Яронимо Великите

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Редактор М. А. Дмитриева

Уч.-изд. л. 1,1. Печ. л. 1,4.

Издательство федерального государственного бюджетного
образовательного учреждения высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1