Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Система расширенного мандатного разграничения доступа в локальной сети

АВТОРЕФЕРАТ

дипломной работы

студентки 6 курса 632 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Дорошенковой Таисии Андреевны

Научный руководитель

доцент, к.ф.-м.н. _____ А. В. Жаркова

18.01.2018 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В. Н. Салий

18.01.2018 г.

Саратов 2018

ВВЕДЕНИЕ

Разграничение доступа является одним из базовых средств защиты информации от несанкционированного доступа, оно позволяет организовать обработку информации таким образом, чтобы доступ к каждому документу мог получить только тот сотрудник, который имеет на это право.

Доступ к информации (доступ) – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение. [1]

Защита информации от несанкционированного доступа – деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил. [2]

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа. [1]

Статистические исследования в области компьютерной безопасности [3] показывают, что постоянно выявляются ошибки, связанные с недостаточным разграничением доступа. Согласно [4] процент инцидентов в компьютерных системах, связанных со злоупотреблениями сотрудников, составляет 14%. Также сообщается, что внутренние угрозы (нарушение правил безопасности и злоупотребления сотрудников) часто оказываются более опасны, чем внешние атаки. Кроме того, данные статистические исследования проводились в крупных корпорациях, в которых вопросам безопасности уделяется повышенное внимание. Это означает, что менее крупные фирмы могут ощущать данные проблемы ещё острее.

Существует два основных класса моделей разграничения доступа – дискреционные и мандатные. Дискреционные модели являются наиболее распространёнными на практике в компьютерных системах. А мандатные модели были разработаны специалистами для секретного документооборота.

Первая мандатная модель была описана американскими специалистами Дэвидом Беллом и Леонардом ЛаПадулой и была названа моделью Белла – ЛаПадулы. Эта модель сыграла огромную роль в развитии теории компьютерной безопасности, и её положения были введены в качестве обязательных требований к системам, обрабатывающим информацию, содержащую государственную тайну, в стандартах защищенных компьютерных систем. [5]

В настоящей работе будут рассмотрены расширения мандатной модели Белла – ЛаПадулы – как более гибкая модификация данной модели, так и сочетание мандатной модели с дискреционной, и будет построена система, демонстрирующая особенности данных расширений.

Кроме того, следует учитывать, что чем крупнее система по составу пользователей и документов, тем сложнее она для администрирования и тем более вероятны ошибки в её организации и настройке, которые могут привести к серьёзным последствиям. Для решения данной проблемы необходимо осуществлять анализ системы разграничения доступа. Задачей анализа системы разграничения доступа является вычисление уровня избыточности назначенных в системе прав и определение того, как можно было бы оптимизировать систему, путём уменьшения дублированной информации, что особенно актуально для крупных систем.

Цель настоящей работы – рассмотреть принципы классической и расширенной мандатных моделей, их возможное сочетание с дискреционной моделью разграничения доступа, в результате чего требуется разработать и реализовать программный продукт, демонстрирующий работу данной системы, дополнив его возможностью применения методов анализа и оптимизации системы разграничения доступа, а также защитой хранимых данных средствами криптографии.

В процессе работы необходимо выполнить следующие задачи:

1) изучить основные положения классической мандатной модели разграничения доступа Белла – ЛаПадулы, а также её наиболее практически применимые расширения;

2) изучить выбранную модель дискреционного разграничения доступа;

3) изучить методы анализа систем разграничения доступа и привести необходимые формулы для численных оценок;

4) описать систему, демонстрирующую сочетание мандатных моделей с дискреционным разграничением доступа;

5) изучить криптографические протоколы, необходимые для защиты данных в разрабатываемой системе;

6) разработать и реализовать программный продукт, позволяющий организовывать систему, содержащую пользователей и документы, права доступа в которой регулируются с помощью расширенной мандатной модели, включающую в себя инструмент для анализа оптимальности заданного разграничения доступа, а также защиту хранимых и обрабатываемых данных средствами криптографии.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 6 приложений. Общий объем работы – 138 страниц, из них 61 страница – основное содержание, включая 50 рисунков и 2 таблицы, список использованных источников из 27 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В дипломной работе в разделе «Модели разграничения доступа» приводятся необходимые определения из области универсальной алгебры и теории компьютерной безопасности согласно [5–12], описывается классическая мандатная модель Белла – ЛаПадулы и её расширение (модель Low-Watermark) и описываются дискреционные модели на основе матрицы доступа в соответствии с [5] и [12].

Во 2 разделе работы «Анализ индивидуально-групповых систем разграничения доступа» обосновывается актуальность задачи анализа и оптимизации систем разграничения доступа, приводятся формулы для вычисления индивидуальных и групповых прав доступа, даётся определение коэффициента дублирования прав доступа, приводится формула для его вычисления, выводится формула для вычисления максимального коэффициента дублирования прав доступа, описывается способ вычисления близости рабочих групп, основываясь на [5].

В 3 разделе работы «Необходимые алгоритмы и протоколы» приводятся используемые математические обозначения согласно [9–10], описывается шифр RSA [13], протокол передачи секретного сеансового ключа по открытому каналу («цифровой конверт») [6], шифр Магма согласно [9] и [14], функция хэширования ГОСТ Р 34.11-2012 [10]. Данные алгоритмы и протоколы используются в построенной системе расширенного мандатного разграничения доступа в локальной сети для обеспечения её безопасности.

В 4 разделе работы «Построение защищённой системы с расширенной мандатной моделью Белла – ЛаПадулы» описывается система, содержащая пользователей и файлы, права доступа в которой регулируются с помощью расширенной мандатной модели Белла – ЛаПадулы, включающая в себя инструмент для анализа оптимальности заданного разграничения доступа, а также защиту хранимых и обрабатываемых данных средствами криптографии.

Также в 4 разделе описывается программный продукт, разработанный и реализованный в результате проделанной работы, состоящий из трёх программ: программы администратора, серверной части и приложения для клиентов. Программы написаны на языке Java (версия 1.8), скомпилированы и протестированы в среде IntelliJ IDEA Community Edition 2017.1.4, графический интерфейс написан с использованием библиотеки Swing. Вся информация о системе хранится в базе данных MySQL версии 5.5.23. Для написания программ использовались источники [15–24].

Программа администратора позволяет организовывать систему, содержащую пользователей, рабочие группы и файлы, осуществлять настройки и анализировать оптимальность созданных групп и назначаемых дискреционных прав. Серверное приложение служит для взаимодействия с базой данных, общения с клиентскими программами и осуществления разграничения доступа. Программа для клиентов позволяет пользователям получать доступ к файлам, хранящимся на сервере в соответствии с установленной в системе политикой разграничения доступа.

ЗАКЛЮЧЕНИЕ

Задача организации документооборота таким образом, чтобы конфиденциальная информация была надёжно защищена, является чрезвычайно важной. Политика разграничения доступа является тем самым средством, которое позволяет организовать обработку информации так, чтобы доступ к каждому документу мог получить только тот сотрудник, который имеет на это право. Существует две основные модели разграничения доступа – дискреционная и мандатная. Мандатная модель была разработана специально для секретного документооборота, а дискреционные модели являются наиболее гибкими и распространёнными на практике в компьютерных системах. При этом чем крупнее система по составу пользователей и документов, тем сложнее она для администрирования и тем более вероятны ошибки в её организации и настройке, которые могут повлечь серьёзные последствия. Для решения данной проблемы необходимо осуществлять анализ системы разграничения доступа, который позволяет получить более оптимально организованную систему.

В ходе данной работы были рассмотрены принципы классической и расширенной мандатных моделей Белла – ЛаПадулы, их возможное сочетание с дискреционной моделью разграничения доступа, приведены необходимые формулы для численной оценки оптимальности системы, была выведена формула для вычисления максимального коэффициента дублирования прав доступа, и в результате был разработан и реализован на языке программирования Java программный продукт, демонстрирующий работу данной системы, с защитой хранимых данных средствами криптографии (в том числе с использованием отечественных стандартов блочного шифрования ГОСТ Р 34.12-2015 и функции хэширования ГОСТ Р 34.11-2012, а также криптографической системы с открытым ключом RSA).

Таким образом, все поставленные задачи были полностью выполнены, а цель работы достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] // ФСТЭК России [Электронный ресурс] : Федеральная служба по техническому и экспортному контролю. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3 (дата обращения: 07.11.2017). Загл. с экрана. Яз. рус.

2 Защита информации. Основные термины и определения [Электронный ресурс] // Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс] : [сайт]. URL: http://protect.gost.ru/v.aspx?control=8&baseC=6&page=0&month=1&year=2008&search=%D0%93%D0%9E%D0%A1%D0%A2%20%D0%A0%2050922-2006&RegNum=1&DocOnPageCount=15&id=121129&pageK=E10BFA12-ED02-4212-8D58-3F1D91F314A0 (дата обращения: 08.11.2017). Загл. с экрана. Яз. рус.

3 Инциденты в информационной безопасности крупных российских компаний (2013 год) [Электронный ресурс] // Positive Technologies [Электронный ресурс] : [сайт]. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-Security-Incidents-2014-rus.pdf (дата обращения: 30.10.2017). Загл. с экрана. Яз. рус.

4 Positive Research : сб. исследований по практической безопасности [Электронный ресурс] // Positive Technologies [Электронный ресурс] : [сайт]. М., 2016. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2016-rus.pdf (дата обращения: 30.10.2017). Загл. с экрана. Яз. рус.

5 Гайдамакин, Н. А. Учебно-методический комплекс. Теоретические основы компьютерной безопасности [Электронный ресурс] / Н. А. Гайдамакин // Электронный научный архив УрФУ [Электронный ресурс] : [сайт]. URL: http://elar.urfu.ru/bitstream/10995/1778/5/1335332_schoolbook.pdf (дата обращения: 15.09.2017). Загл. с экрана. Яз. рус.

6 Мао, В. Современная криптография: теория и практика [Электронный ресурс] / В. Мао. М. : Издательский дом «Вильямс», 2005. 763 с. Загл. с экрана. Яз. рус.

7 Виноградов, И. М. Основы теории чисел [Электронный ресурс] / И. М. Виноградов. М. : Государственное издательство технико-теоретической литературы, 1952. 181 с. Загл. с экрана. Яз. рус.

8 Салий, В. Н. Криптографические методы и средства защиты информации [Электронный ресурс] : учеб. пособие / В. Н. Салий // Саратовский государственный университет имени Н. Г. Чернышевского [Электронный ресурс]. Саратов, 2017. 43 с. URL: https://www.sgu.ru/sites/default/files/textdocsfiles/2017/10/18/saliy_v.n._kriptograficheskie_metody_i_sredstva_zashchity_informacii.pdf (дата обращения: 09.11.2017). Загл. с экрана. Яз. рус.

9 ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры [Электронный ресурс] // Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс] : [сайт]. URL: http://protect.gost.ru/v.aspx?control=8&baseC=6&page=0&month=1&year=2012&search=Блочные%20шифры&RegNum=1&DocOnPageCount=15&id=193095&pageK=7E188721-BB9F-4CF5-96CB-80F3231C8D87 (дата обращения: 20.09.2017). Загл. с экрана. Яз. рус.

10 ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования [Электронный ресурс] // Федеральное агентство по техническому регулированию и метрологии

[Электронный ресурс] : [сайт]. URL: http://protect.gost.ru/document.aspx?control=7&id=180209 (дата обращения: 10.10.2017). Загл. с экрана. Яз. рус.

11 Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие [Электронный ресурс] / В. Ф. Шаньгин. М. : ИД «Форум»: ИНФРА-М, 2008. 416 с. Загл. с экрана. Яз. рус.

12 Грушо, А. А. Теоретические основы компьютерной безопасности: учеб. пособие [Электронный ресурс] / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. М. : Издательский центр «Академия», 2009. 272 с. Загл. с экрана. Яз. рус.

13 Rivest, R. L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems / R. L. Rivest, A. Shamir, L. Adleman [Электронный ресурс] // MIT CSAIL [Электронный ресурс] : MIT Computer Science and Artificial Intelligence Laboratory. 1977. URL: http://people.csail.mit.edu/rivest/Rsapaper.pdf (дата обращения: 12.11.2017). Загл. с экрана. Яз. англ.

14 ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров [Электронный ресурс] // Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс] : [сайт]. URL: http://protect.gost.ru/document1.aspx?control=31&baseC=6&page=0&month=12&year=2017&search=ГОСТ%20Р%2034.13-2015&id=200971 (дата обращения: 21.09.2017). Загл. с экрана. Яз. рус.

15 Java SE Application Design With MVC [Электронный ресурс] // Oracle Technology Network [Электронный ресурс] : [сайт]. URL: http://www.oracle.com/technetwork/articles/javase/index-142890.html (дата обращения: 30.07.2017). Загл. с экрана. Яз. англ.

16 Core J2EE Patterns – Data Access Object [Электронный ресурс] // Oracle Technology Network [Электронный ресурс] : [сайт]. URL:

http://www.oracle.com/technetwork/java/dataaccessobject-138824.html (дата обращения: 05.08.2017). Загл. с экрана. Яз. англ.

17 Trail: JDBC (TM) Database Access [Электронный ресурс] // The Java™ Tutorials [Электронный ресурс] : [сайт]. URL: https://docs.oracle.com/javase/tutorial/jdbc/index.html (дата обращения: 11.08.2017). Загл. с экрана. Яз. англ.

18 Lesson: All About Sockets [Электронный ресурс] // The Java™ Tutorials [Электронный ресурс] : [сайт]. URL: https://docs.oracle.com/javase/tutorial/networking/sockets/index.html (дата обращения: 29.10.2017). Загл. с экрана. Яз. англ.

19 Writing the Server Side of a Socket [Электронный ресурс] // The Java™ Tutorials [Электронный ресурс] : [сайт]. URL: https://docs.oracle.com/javase/tutorial/networking/sockets/clientServer.html (дата обращения: 30.10.2017). Загл. с экрана. Яз. англ.

20 Interface Serializable [Электронный ресурс] // The Java™ Tutorials [Электронный ресурс] : [сайт]. URL: https://docs.oracle.com/javase/7/docs/api/java/io/Serializable.html (дата обращения: 31.10.2017). Загл. с экрана. Яз. англ.

21 Object Streams [Электронный ресурс] // The Java™ Tutorials [Электронный ресурс] : [сайт]. URL: https://docs.oracle.com/javase/tutorial/essential/io/objectstreams.html (дата обращения: 31.10.2017). Загл. с экрана. Яз. англ.

22 Customize Your JList Display [Электронный ресурс] // Oracle Technology Network [Электронный ресурс] : [сайт]. URL: http://www.oracle.com/technetwork/articles/javase/oconner-customlist-gd-aurev-138792.html (дата обращения: 03.09.2017). Загл. с экрана. Яз. англ.

23 How to Use Tables [Электронный ресурс] // The Java™ Tutorials [Электронный ресурс] : [сайт]. URL:

https://docs.oracle.com/javase/tutorial/uiswing/components/table.html (дата обращения: 12.09.2017). Загл. с экрана. Яз. англ.

24 How to Use Buttons, Check Boxes, and Radio Buttons [Электронный ресурс] // The Java™ Tutorials [Электронный ресурс] : [сайт]. URL: https://docs.oracle.com/javase/tutorial/uiswing/components/button.html (дата обращения: 24.10.2017). Загл. с экрана. Яз. англ.