

Аутентификация

Теория и практика

обеспечения безопасного доступа к информационным ресурсам

Рекомендовано Учебно-методическим объединением
по образованию в области информационной безопасности
и одобрено ФСТЭК России
в качестве учебного пособия для студентов высших
учебных заведений, обучающихся по специальностям
«Компьютерная безопасность»,
«Комплексное обеспечение информационной
безопасности автоматизированных систем»

Под редакцией

А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева

Москва
Горячая линия - Телеком
2012

УДК 004.732.056(075.8)
ББК 32.973.2-018.2я73
А93

А в т о р ы : А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов, Э. Р. Газизова, А. Л. Додохов, А. В. Крячков, О. Ю. Полянская, А. Г. Сабанов, М. А. Скида, С. Н. Халяпин, А. А. Шелупанов

А93 Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. – 2-е изд., стереотип. – М.: Горячая линия–Телеком, 2012. – 550 с.: ил.

ISBN 978-5-9912-0257-2.

Книга посвящена одному из аспектов проблемы управления доступом к информации в компьютерных системах – аутентификации.

Фактически защита информации начинается с аутентификации пользователей. Каждый пользователь современных компьютерных систем сталкивается с процедурами аутентификации неоднократно в течение рабочего дня. Книга описывает достоинства и недостатки практически всех существующих и используемых на настоящий момент способов аутентификации и ориентирована на широкий круг читателей.

Книга адресована студентам вузов и аспирантам, обучающимся по специальностям, связанным с защитой информации, ИТ-специалистам и специалистам по информационной безопасности; специалистам, получающим второе высшее образование в области защиты информации, и слушателям курсов переподготовки.

ББК 32.973.2-018.2я73

Адрес издательства в Интернет www.techbook.ru

Учебное издание

Аутентификация

Теория и практика обеспечения безопасного доступа
к информационным ресурсам

Учебное пособие для вузов

2-е издание, стереотипное

Редактор *И. Н. Андреева*

Компьютерная верстка *Н. В. Дмитриева*

Обложка художника *В. Г. Ситникова*

Подписано в печать 14.03.12. Формат 70×100/16. Усл. печ. л. 45,75. Тираж 100 экз. (1-й завод 50 экз.)
ООО «Научно-техническое издательство «Горячая линия–Телеком»

ISBN 978-5-9912-0257-2

© ЗАО «Аладдин Р.Д.», 2009, 2012

© Издательство «Горячая линия–Телеком», 2012

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ	7
ЧАСТЬ I. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ	9
Глава 1. ОБЩИЕ СВЕДЕНИЯ	10
1.1. Основные понятия и определения	10
1.2. Роль и задачи аутентификации. Место аутентификации в структуре основных направлений защиты информации	10
1.3. Факторы аутентификации	13
Контрольные вопросы	15
Глава 2. ПАРОЛЬНАЯ АУТЕНТИФИКАЦИЯ	16
2.1. Аутентификация с помощью запоминаемого пароля	16
2.2. Методы парольной аутентификации	16
2.3. Парольные политики	19
2.4. Недостатки методов аутентификации с запоминаемым паролем	19
Контрольные вопросы	22
Глава 3. АУТЕНТИФИКАЦИЯ С ПОМОЩЬЮ БИОМЕТРИЧЕСКИХ ХАРАКТЕРИСТИК	23
3.1. Биометрические характеристики	23
3.2. Как работают биометрические системы	24
3.3. Аутентификация и биометрическое распознавание	26
3.4. Реализация биометрических систем	27
3.5. Недостатки аутентификации с помощью биометрических характеристик. Возможные атаки	28
Контрольные вопросы	29
Глава 4. АУТЕНТИФИКАЦИЯ С ПОМОЩЬЮ ОДНОРАЗОВЫХ ПАРОЛЕЙ	30
4.1. Аппаратно-программные ОТР-токены	32
4.2. Как работают ОТР-токены	32
4.3. Методы аутентификации с помощью ОТР-токенов	32
4.4. Сравнение методов ОТР-аутентификации	36
4.5. Системы одноразовых паролей	37
4.6. Недостатки методов аутентификации с помощью ОТР. Возможные атаки	41
Контрольные вопросы	42
Глава 5. КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ	43
5.1. Общие сведения о криптографии с открытым ключом	43

5.2. Авторизация и обеспечение юридической значимости электронных документов	47
5.3. Конфиденциальность и контроль целостности передаваемой информации	48
5.4. Аутентификация связывающихся сторон	48
5.5. Установление аутентичного защищенного соединения.	48
5.6. Инфраструктура открытых ключей (PKI).	49
5.7. Аутентификация с помощью открытого ключа на основе сертификатов . . .	49
5.8. Организация хранения закрытого ключа	50
5.9. Интеллектуальные устройства и аутентификация с помощью открытого ключа	52
5.10. Недостатки аутентификации с помощью открытых ключей. Возможные атаки.	54
Контрольные вопросы	56
Глава 6. ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ В ЛОКАЛЬНОЙ СЕТИ.	57
6.1. Протоколы LAN Manager и NT LAN Manager	57
6.2. Протокол Kerberos	62
6.3. Протокол Kerberos + PKINIT	73
Контрольные вопросы	76
Глава 7. МЕХАНИЗМЫ АУТЕНТИФИКАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПОДКЛЮЧЕНИЙ	77
7.1. Протокол PPP PAP	77
7.2. Протокол PPP CHAP.	78
7.3. Протокол PPP EAP	79
7.4. Протокол TACACS+	81
7.5. Протокол RADIUS	84
7.6. Стандарт IEEE 802.1x и протокол EAPOL	86
7.7. Протокол EAP-TLS с использованием российской криптографии	89
7.8. Стандарт IEEE 802.1x в операционных системах Microsoft	93
7.9. Cisco NAC	94
Контрольные вопросы	97
Глава 8. АУТЕНТИФИКАЦИЯ В ЗАЩИЩЕННЫХ СОЕДИНЕНИЯХ	98
8.1. Протоколы SSL, TLS	98
8.2. Протокол SSH	100
8.3. Протокол S-HTTP	101
8.4. Протокол SOCKS	102
8.5. Семейство протоколов IPSec	103
8.6. Протоколы защищенного взаимодействия и аутентификации для корпоративных беспроводных локальных сетей	116
Контрольные вопросы	124

Глава 9. ПРИМЕНЕНИЕ АППАРАТНЫХ СРЕДСТВ АУТЕНТИФИКАЦИИ И ХРАНЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ	125
9.1. Аппаратные средства защиты в современных PKI-решениях	125
9.2. Необходимость применения аппаратных средств аутентификации и хранения ключевой информации	126
9.3. Типовые требования к средствам аутентификации и хранения ключевой информации.	135
9.4. Особенности корпоративного использования персональных средств аутентификации и хранения ключевой информации	139
9.5. Централизованная система управления средствами аутентификации и хранения ключевой информации пользователей	142
9.6. Типовые требования к системе управления токенами	145
9.7. Token Management System (TMS) компании Aladdin.	146
9.8. Практика: комплексная система на базе единого персонального средства аутентификации и хранения ключевой информации	149
Контрольные вопросы	153
Список использованной литературы	153

ЧАСТЬ II. ПРАКТИКА 155

Введение 156

Глава 1. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДОСТУПА К ДАННЫМ И ПРИЛОЖЕНИЯМ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ НА ОСНОВЕ РЕКОМЕНДАЦИЙ И ПРОДУКТОВ MICROSOFT. ТИПОВЫЕ РЕШЕНИЯ	157
--	-----

1.1. Основные сервисы для обеспечения надежной аутентификации и управления доступом	157
1.2. Авторизация при доступе к объекту	169
1.3. Система аудита Active Directory	170
1.4. Назначение и решаемые задачи инфраструктуры открытых ключей	172
1.5. Управление идентификацией (ILM)	173
1.6. Microsoft Identity Integration Server (MIIS)	173
1.7. Системы обеспечения	175

Глава 2. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДОСТУПА К ДАННЫМ И ПРИЛОЖЕНИЯМ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ НА ОСНОВЕ РЕКОМЕНДАЦИЙ И ПРОДУКТОВ ORACLE И ALADDIN. ТИПОВЫЕ РЕШЕНИЯ	177
---	-----

2.1. Управление доступом в СУБД Oracle с помощью встроенных механизмов безопасности и криптографических средств защиты	177
--	-----

**Глава 3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДОСТУПА К ДАННЫМ
И ПРИЛОЖЕНИЯМ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ
НА ОСНОВЕ ПРОДУКТОВ КОМПАНИИ CITRIX SYSTEMS 226**

- 3.1. Описание продуктов компании Citrix Systems 226
- 3.2. Компоненты систем, построенных с использованием XenApp 228

Список использованной литературы 244

Источники 245

ЧАСТЬ III. ЛАБОРАТОРНЫЕ РАБОТЫ 247

- Лабораторная работа № 1.** Подготовка стенда, установка и настройка ПО, подготовка электронных ключей eToken 248
- Лабораторная работа № 2.** Установка и настройка Центра сертификации, использование ключей eToken в домене Windows Server 2003 282
- Лабораторная работа № 3.** Использование eToken для безопасного доступа к информационным ресурсам, для шифрования и для ЭЦП 326
- Лабораторная работа № 4.** Сопровождение функционирования Центра сертификации, повышение защищенности систем на основе Windows Server 2003 399
- Лабораторная работа № 5.** Доступ в СУБД Oracle с аутентификацией по имени пользователя и паролю в LDAP-каталоге. 428
- Лабораторная работа № 6.** Доступ в СУБД Oracle с аутентификацией на основе сертификатов 458
- Лабораторная работа № 7.** Режимы работы протокола IPSec на модуле NME-RVPN при использовании программного обеспечения CSP VPN Gate для аутентификации и защиты данных 491
- Лабораторная работа № 8.** Настройка Web Interface 4.x для использования смарт-карт 509
- Лабораторная работа № 9.** Настройка Secure Gateway для безопасного подключения к опубликованным приложениям из недоверенных сред передачи данных. 530

ПРЕДИСЛОВИЕ

Судьба данного учебного пособия весьма необычна. На партнерской конференции по информационной безопасности компании Aladdin у нас появилась идея создать книгу по теоретическим и практическим вопросам аутентификации. Эту книгу можно было бы использовать не только при обучении студентов и аспирантов ВУЗов и СУЗов по учебным дисциплинам «Безопасность баз данных», «Программно-аппаратные средства обеспечения информационной безопасности», «Безопасность операционных систем», «Компьютерная безопасность» и т. д., но и в практической деятельности ИТ-специалистов, системных администраторов, администраторов безопасности различных сетей и систем.

Любая поисковая система в Интернет по запросу «аутентификация» предоставляет более 1 миллиона ссылок на различные информационные ресурсы. Этот очевидный факт подтверждает широкое распространение и использование механизмов аутентификации в практике обеспечения безопасности сетей, систем, различных приложений. Оценив интерес и востребованность данной технологии, мы решили взяться за дело.

Всю сложность воплощения нашей идеи мы поняли несколько позже, когда взялись за ее реализацию. Первая трудность состояла, главным образом, в том, чтобы объединить усилия специалистов зарубежных и российских компаний, признанных лидеров на рынке информационных технологий, таких, как компании Microsoft, Aladdin, Cisco Systems, Citrix, Oracle, Кристо-Про. При этом, помимо необходимых теоретических сведений, мы собирались предложить читателю различные решения, технологии и продукты для реализации задач по обеспечению безопасности доступа к данным и приложениям информационной системы организации, защищенных соединений. Речь идет как о представлении типовых решений, так и о возможной кастомизации продуктов под конкретные системы.

Другая сложность состояла в том, чтобы систематизировать, порой весьма противоречивые сведения, стили изложения, подходы к реализации решений в различных компаниях, и представить методически выверенные теоретические и практические материалы, в том числе и в виде готовых лабораторных работ для использования их в учебном процессе. Третья сложность состояла в том, чтобы преодолеть препону конкурентного противостояния компаний, создать полезную и, на наш взгляд, весьма своевременную и актуальную книгу без рекламы конкретных компаний. И наконец, любая работа, которая делается на общественных началах, зачастую страдает недостатком времени или возможности довести идею создания учебного пособия до логического завершения. Это обстоятельство явилось причиной отсутствия материалов в данной книге еще нескольких ведущих компаний — вендоров (IBM, Check Point Software Technologies, Сигнал-Ком, SUN и т. д.). Надеемся, что эти материалы войдут во второе издание данного учебного пособия. Потребовался весьма продолжительный период времени для решения организационных мероприятий, экспертизы и апробации материалов в учебных заведениях России, при проведении тренингов ИТ-специалистов, сотрудников служб информационной безопасности, студентов профильных ВУЗов и т. п.

К счастью, нам удалось преодолеть все эти трудности, и мы надеемся, что книга окажется полезной как в учебном процессе, так и в практической работе.

Учебное пособие состоит из теоретической и практической частей. Практическая часть содержит 9 лабораторных работ по типовым решениям с использованием продуктов различных компаний. Описание лабораторных работ можно найти по адресу в Интернет: <http://www.aladdin.ru/book/>

Согласно замыслу авторов, книга, которую Вы держите в руках, призвана открыть перед читателем суть и возможности технологии аутентификации, как базового элемента любой системы информационной безопасности современных компаний.

Специалистам, уже знакомым с данными технологиями, книга поможет систематизировать и расширить свои знания в части прикладного применения средств аутентификации и интеграции их с другими продуктами и решениями для защиты информации.

Развивать рынок аутентификации, способствовать повышению уровня и качества проектов в области ИТ-безопасности, а, главное, содействовать формированию четкого понимания ценности информации в современном мире — основная цель данной книги.

Мы искренне благодарим всех, кто поддерживал и продолжает поддерживать этот проект, помогает в его продвижении, а также распространении книги.

Особую благодарность выражаем Федеральной службе безопасности России (ФСБ России), Федеральной службе по техническому и экспортному контролю России (ФСТЭК России), Совету Безопасности Российской Федерации и Учебно-методическому объединению по образованию в области информационной безопасности за проявленный интерес, полезные замечания и конструктивную критику.

Отдельно хочется отметить вклад в работу при подготовке рукописи данной книги безвременно ушедшего из жизни руководителя аналитического отдела компании Aladdin, кандидата физико-математических наук Нахаева Ю.С.

Мы не планируем останавливаться на достигнутом результате и рассматриваем идею выпуска второго расширенного издания данной книги. Приглашаем к сотрудничеству всех заинтересованных специалистов, компании, ВУЗы.

Замечания, предложения и пожелания просьба направлять по адресу:

634050, Томск, пр-т Ленина, д.40

Институт системной интеграции и безопасности ТУСУР, Шелупанову А. А.

saa@udcs.ru

тел. 8 (3822) 413 426

129226 Москва, ул. Докукина, д. 16 корп. 1

ЗАО «Аладдин Р.Д.», генеральному директору Груздеву С. Л.

rg@aladdin.ru

тел. 8 (495) 223 0001

С уважением,

А. А. ШЕЛУПАНОВ,

Директор Института системной
интеграции и безопасности ТУСУР,
доктор технических наук, профессор

С. Л. ГРУЗДЕВ,

Генеральный директор компании Aladdin

Глава 1

ОБЩИЕ СВЕДЕНИЯ ОБ АУТЕНТИФИКАЦИИ

1.1. Основные понятия и определения

Процесс регистрации пользователя в любой системе состоит из трех взаимосвязанных последовательно выполняемых процедур: идентификации, аутентификации и авторизации.

Идентификация — процедура распознавания субъекта по его идентификатору. В процессе регистрации субъект предъявляет свой идентификатор системе, которая проверяет его наличие в своей базе данных. Субъекты с известными системе идентификаторами считаются легальными (законными), остальные относятся к нелегальным.

Аутентификация — процедура проверки подлинности субъекта, которая позволяет достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует. Для этого он должен подтвердить факт обладания некоторой информацией, которая может быть доступна только ему одному (пароль, ключ и т. п.).

Авторизация — процедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации. Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к ее ресурсам.

Для того чтобы обеспечить управление и контроль над данными процедурами, дополнительно используются процессы администрирования и аудита.

Администрирование — процесс управления доступом субъектов к ресурсам системы. Данный процесс включает:

- создание идентификатора субъекта (учетной записи пользователя) в системе;
- управление данными субъекта, используемыми для его аутентификации (смена пароля, издание сертификата и т. п.);
- управление правами доступа субъекта к ресурсам системы.

Аудит — процесс контроля (мониторинга) доступа субъектов к ресурсам системы, включающий протоколирование действий субъектов при их доступе к ресурсам системы в целях обнаружения несанкционированных действий.

Таким образом, в общем случае речь идет о пяти основных процедурах предоставления доступа к информации. При этом возможен различный подход к расстановке приоритетов при выполнении этих процедур.

1.2. Роль и задачи аутентификации. Место аутентификации в структуре основных направлений защиты информации

Независимо от типа системы аутентификации в ней всегда присутствуют пять элементов.

Первый элемент — конкретный человек или процесс, который должен проходить аутентификацию, — *субъект доступа*.

Второй элемент — опознавательный знак, *идентификатор*, который выделяет этого человека или этот процесс среди других.

Третий элемент — *отличительная характеристика* (аутентификатор), подтверждающая принадлежность идентификатора субъекту доступа.