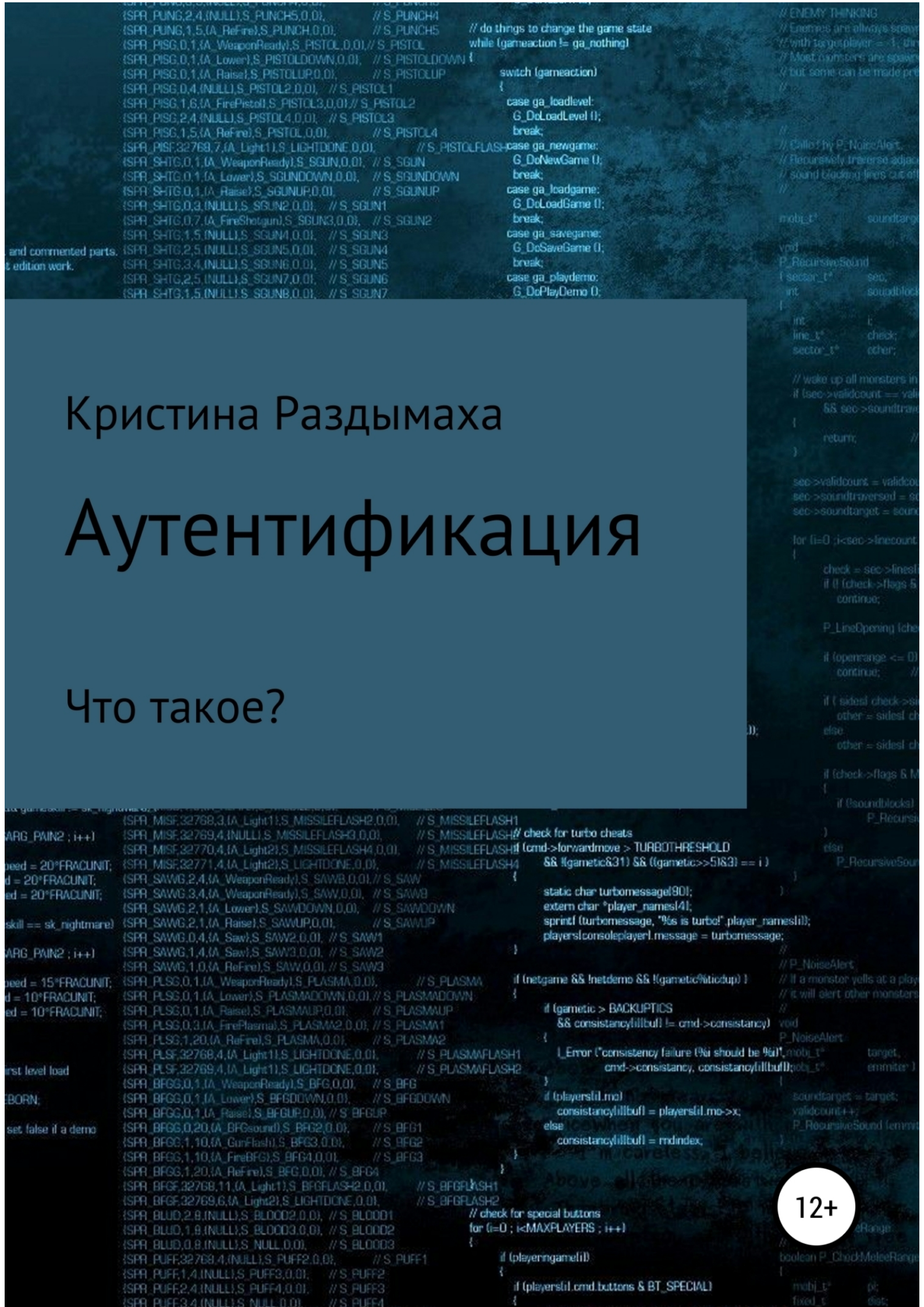


Кристина Раздымаха

Аутентификация

Что такое?

12+

Кристина Раздымаха

Аутентификация

«ЛитРес: Самиздат»

2020

Раздымаха К. В.

Аутентификация / К. В. Раздымаха — «ЛитРес: Самиздат», 2020

Данная книга предназначена как учебное пособие по термину "Аутентификация". В ней вы найдете полный разбор термина и его применение.

Кристина Раздымаха
Аутентификация

Введение

В настоящее время информационные системы (ИС) различного масштаба стали неотъемлемой частью базовой инфраструктуры государства, бизнеса, гражданского общества. Все больше защищаемой информации переносится в ИС. Современные информационные технологии не только обеспечивают новые возможности организации бизнеса, ведения государственной и общественной деятельности, но и создают значительные потребности в обеспечении безопасности для защиты информации.

Известно, что более 25 % злоупотреблений информацией в ИС совершаются внутренними пользователями, партнерами и поставщиками услуг, имеющими прямой доступ к ИС. До 70 % из них – случаи несанкционированного получения прав и привилегий, кражи и передачи учетной информации пользователей ИС, что становится возможным из-за несовершенства технологий разграничения доступа и аутентификации пользователей ИС. Совершенствование методов системы управления доступом и регистрации пользователей является одним из приоритетных направлений развития ИС.

1. Аутентификация

Аутентификацией называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

С древних времён перед людьми стояла довольно сложная задача – убедиться в достоверности важных сообщений. Придумывались речевые пароли, сложные печати, моноалфавитные шифры. Появление методов аутентификации с применением механических устройств сильно упрощало задачу, например, обычный замок и ключ были придуманы очень давно. Пример системы аутентификации можно увидеть в старинной сказке "Приключения Алим-Бабым и сорока разбойников". В этой сказке говорится о сокровищах, спрятанных в пещере. Пещера была загорожена камнем. Отодвинуть его можно было только с помощью уникального речевого пароля: "Сезам, откройся!"

В настоящее время в связи с обширным развитием сетевых технологий, автоматическая аутентификация используется повсеместно.

Для корректной аутентификации пользователя необходимо, чтобы пользователь предъявил аутентификационную информацию (информацию, которой обладает только сам пользователь и никто другой).

Обычно методы аутентификации классифицируют по используемым средствам. В этом случае указанные методы делят на четыре группы:

Элемент аутентификации	Субъект
Пещера 40 разбойников	Человек, знающий пароль
Регистрация в системе	Авторизованный пользователь
Банкомат	Владелец банковской карты

Характеристика
Пароль "Сезам, откройся!"
Тайный пароль
Банковская карта и персональный идентификатор

Хозяин системы
40 разбойников
Предприятие, которому принадлежит система
Банк

Механизм аутентификации
Волшебное устройство, реагирующее на слова
Программное обеспечение, проверяющее пароль
Программное обеспечение, проверяющее карту и персональный идентификатор

Механизм управления доступом
Механизм, отодвигающий камень от входа в пещеру
Процесс регистрации, управления доступом
Разрешение на выполнение банковских действий

2. Элементы системы аутентификации

Вне зависимости от того, является ли система аутентификации компьютерной, всегда обычно присутствует несколько элементов, и происходят определенные вещи. Прежде всего мы имеем конкретного человека или группу людей, которые должны проходить аутентификацию. Кроме того, нам необходима характеристика, которая отличает этого человека или группу людей от других. В – третьих, есть хозяин, который несет ответственность за использование системы, и в разграничении авторизованных пользователей от остальных людей полагается на механизм аутентификации. В-четвертых, нам необходим механизм аутентификации, чтобы проверить присутствие отличительной характеристики. В-пятых, при успешном прохождении аутентификации мы выдаем некоторые привилегии, используя для этого механизм управления доступом, и с помощью этого же механизма лишаем привилегий, если аутентификация была неуспешной.

В любой системе аутентификации обычно можно выделить несколько элементов:

– субъект, который будет проходить процедуру

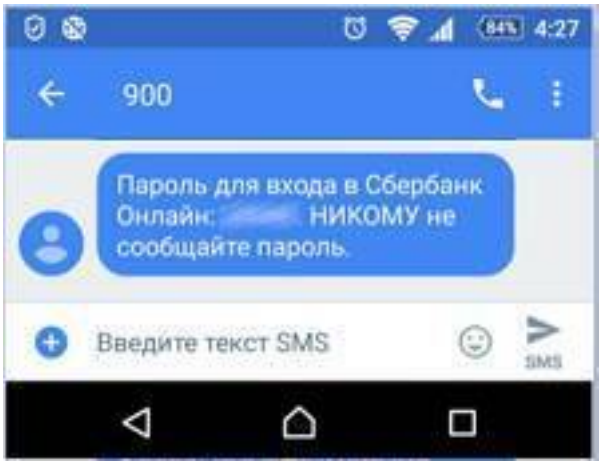
– характеристика субъекта – отличительная черта

– хозяин системы аутентификации, несущий ответственность и контролирующий её работу

– сам механизм аутентификации, то есть принцип работы системы

– механизм, предоставляющий определённые права доступа или лишающий субъекта таковых.

3. Парольная аутентификация



Парольная аутентификация –

самый распространенный вид аутентификации. Главное достоинство являются простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

4.Уникальность предмета

Уникальность предмета, по которому выполняется аутентификация пользователя компьютером, определяется информацией, которую он содержит. Для аутентификации часто используются следующие носители информации:

– USB-токены – представляют собой устройства с различной степенью интеллекта, подключаемые к порту USB компьютера;

– смарт-карты – по функциональности похожи на USB-токены, но работа с ними осуществляется с помощью специальных устройств, называемых ридерами смарт-карт;

– электронные таблетки iButton (или Touch Memory);

– карты с магнитной полосой.

5.Биометрическая аутентификация

Биометрическая аутентификация – это аутентификация пользователя по его уникальным биометрическим характеристикам. Уникальными являются следующие характеристики:

– отпечатки пальцев;
–узор радужной оболочки и структура сетчатки глаза, расположение слепого пятна глаза;
– черты лица;
– схема кровеносных сосудов рук, лица;
– геометрия кисти руки;
– рукописная подпись;

Конец ознакомительного фрагмента.