УДК 004.089

А.Г. Сабанов

Концепция моделирования процессов аутентификации

Предложена концепция моделирования процесса аутентификации. Концепция основана на рассмотрении основных процедур аутентификации, имеющих различную продолжительность во времени. Процесс аутентификации рассматривается в условиях потока заявок на авторизацию различной интенсивности.

Ключевые слова: концепция, безопасность, надежность, моделирование, процесс, аутентификация.

Системы аутентификации относятся к разряду интеллектуальных систем, составными частями которых, как правило, являются мощная серверная (аппаратная и программная) и клиентская части. Для анализа рисков и исследования надежности выполнения основных процедур аутентификации требуется создание математических моделей [1, 2, 8–10]. При моделировании необходимо учитывать участие в процедурах и процессах подготовки и проведения аутентификации пользователей информационной системы (ИС). Аутентификация – это достаточно сложный процесс, состоящий из двух подпроцессов: подтверждения подлинности предъявленного пользователем идентификатора и проверки принадлежности пользователю аутентификатора, с помощью которого производится первый процесс.

Как показано в [3], процесс аутентификации можно рассматривать как цепь последовательных процедур: однократной (регистрация нового пользователя), длительной по времени (хранение) и часто повторяющихся (предъявление аутентификатора, протоколы обмена «клиент–сервер», валидация, принятие решения «свой-чужой», авторизация). При моделировании также надо учитывать то, что при значительном числе зарегистрированных пользователей (например, более пятисот) системы аутентификации должны подчиняться законам систем массового обслуживания. Это требует предусматривать возможность исследования поведения моделей в условиях случайного потока заявок на аутентификацию, который зависит от времени. Так, в корпоративных системах пик запросов на аутентификацию приходится на начало работы, а в информационных системах общего пользования (ИСОП) пиковые нагрузки в общем случае носят случайный характер.

Вопросы оценки безопасности и надежности аутентификации пользователей и применяемых при этом средств аутентификации активно обсуждаются специалистами, однако общепринятый научный подход к исследованию этого весьма сложного процесса пока не выработан. Целью данной статьи является разработка концепции моделирования для исследования безопасности и надежности аутентификации.

Моделирование процедур аутентификации. Для моделирования процесса аутентификации сначала следует разделить его на однородные по функциональным и вероятностно-статистическим характеристикам блоки. Основанием служит то, что разные блоки имеют существенно отличающиеся характеристики по времени. Например, процедура регистрации производится единожды и может быть относительно краткой по времени. Хранение аутентификационных данных и электронных удостоверений (ЭУ) – длительная процедура, к которой могут быть применены вероятностные и статистические методы. Остальные процедуры (проверка подлинности, валидация, принятие решения) тесно связаны с временем выполнения процедур и многократно повторяются – как минимум раз в день. В итоге получаем следующие блоки:

1) процедура регистрации не связана со временем (стационарный процесс);

2) процедура хранения связана со временем. Для моделирования применимо пуассоновское распределение;

3) протоколы обмена производятся за доли секунды, иногда за секунды; в этой процедуре необходимо строго учитывать отказы (имеются в виду отказы аппаратного и программного компонентов, случайные, неслучайные ошибки пользователей, атаки). Для моделирования возможно применение экспоненциального распределения;

4) в процедуре валидации (также производится за доли секунды) вероятность отказа для корпоративных закрытых систем мала, для ИСОП – велика;

5) процесс принятия решения (положительный или отрицательный результат прохождения процедуры аутентификации) – фактически ответ «да или нет» для пропуска (или отказа в проходе) к следующей процедуре (проверке соответствия учетной записи и идентификатора определенной роли доступа для последующей авторизации пользователя). Производится за доли секунды. Необходимо учитывать вероятность отказа и опасного отказа – принятие положительного решения для злоумышленника под видом легального пользователя.

Заметим, что вслед за процедурой хранения секрета и ЭУ следует процедура предъявления ЭУ для отработки протокола аутентификации. Способ предъявления аутентификатора полностью зависит от протокола аутентификации и его настроек. Например, для аутентификации клиента SSL/TLS и серверов в протоколе IPSec этот процесс происходит в автоматическом режиме. Следовательно, без потери общности задачи можно объединить блоки «хранение» и «протоколы» в один блок (рис. 1).

Рис. 1. Модель основных процессов удаленной аутентификации

При определении характеристик надежности и безопасности системы удаленной аутентификации будем иметь в виду прежде всего функциональную надежность и функциональную безопасность. Под функциональной надежностью понимаем способность системы выполнять предусмотренные функциональные задачи с приемлемым уровнем безошибочности в реальных условиях эксплуатации. Функциональную безопасность определим как способность системы выполнять предусмотренные функциональные задачи с заданным уровнем доступности, целостности и конфиденциальности. Для данных допущений на основе анализа блочной структуры системы аутентификации сформируем вероятностную модель типовой системы аутентификации для оценки ее стационарных характеристик.

Без потери общности решения попробуем дополнительно сократить число блоков по принципу однократности/многократности. Примем следующие допущения:

- определим процесс регистрации нового пользователя ИСОП в терминах теории надежности как процесс однократного срабатывания;
- объединим блоки хранения секретов и протоколы аутентификации в один блок «Подтверждение подлинности». Примем, что данный объединенный в один блок многократный процесс хранения и предъявления аутентификатора может быть представлен как пуассоновский (стационарный, ординарный, отсутствие последствий). Заметим, что данный процесс можно отнести к хорошо исследованному классу марковских процессов;
- блок валидации можно объединить с блоком принятия решения, поскольку данные процедуры связаны в цепочку последовательных действий, а результат последней процедуры явно зависит от результата предыдущей.

Сформулируем критерии отказа и опасного отказа для рассматриваемых модулей. Так, для модуля регистрации отказом будем считать отсутствие регистрации для легального пользователя, а опасным отказом – регистрацию злоумышленника под именем легального пользователя. Отказы в модулях подтверждения подлинности предъявленных претендентом идентификационных данных и отказ в модуле принятия решения об авторизации претендента относятся к штатной работе модулей, т.е. не сказываются на вероятностной модели работы всей системы в целом. Опасным отказом работы модуля принятия решения будем понимать положительный итог прохождения процедуры аутентификации для злоумышленника под видом легального пользователя.

В качестве критериев функциональных отказов для рассматриваемой системы можно принять ошибки в работе системы, не приводящие к остановке выполнения основных заданных функций работы системы. Другими словами, ошибки и сбои не должны превышать определенного порога, начиная с которого система удаленной аутентификации может перестать выполнять заданный набор функций.

Сумма вероятностей выходов из каждого состояния есть полная группа событий:

$$\sum_{i=1}^{n} P_i = 1,$$

где n – число состояний системы.

Стационарный поток заявок на аутентификацию. При количестве пользователей ИС больше определенного количества (например, 300) система аутентификации может рассматриваться как система массового обслуживания с интенсивностью входящего пуассоновского потока заявок λ. Если обозначить интенсивность обработки заявок системой аутентификации μ, то одним из определяющих работу системы параметров будет $\rho = \lambda/\mu$. Если $\rho < 1$, т.е. процесс может считаться стационарным (например, корпоративная ненагруженная система), процедуры перехода системы из одного состояния в другое можно моделировать с помощью цепочек Маркова [4, 5].

Обозначим состояния системы следующим образом (рис. 2):

1 – претендент на регистрацию послал запрос на сервер центра регистрации (ЦР) с целью зарегистрироваться в ИС;

2 – данные от претендента и сервера аутентификации имеются для проверки подлинности пользователя;

3 – имеются данные для проверки валидности ЭУ пользователя;

4 – на сервере имеются все данные для начала процесса авторизации;

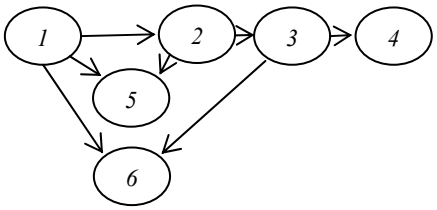

Рис. 2. Простейшая укрупненная модель процесса аутентификации

p_{ij} – вероятность перехода системы из состояния i в состояние j.

Например, p_{12} – вероятность перехода из состояния «*1*» в состояние «*2*», p_{34} – вероятность перехода системы из состояния готовности к процедуре валидации в состоянии готовности к авторизации пользователя.

Вектор вероятностей $\boldsymbol{P}$ можно определить из соотношения

$$\begin{Bmatrix} P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \\ P_6 \end{Bmatrix} = \begin{pmatrix} P_1, & P_2, & P_3, & P_4, & P_5, & P_6 \end{pmatrix} \cdot \begin{pmatrix} 0 & p_{12} & 0 & 0 & p_{15} & p_{16} \\ 0 & 0 & p_{23} & 0 & p_{25} & 0 \\ 0 & 0 & 0 & p_{34} & 0 & p_{36} \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

откуда можно найти выражения для стационарных вероятностей P_i того, что система находится в состоянии i ($i = 1, ..., 6$):

$$P_2 = P_1 \cdot p_{12};$$
$$P_3 = P_2 \cdot p_{23};$$
$$P_4 = P_3 \cdot p_{34};$$
$$P_5 = P_1 \cdot p_{15} + P_2 \cdot p_{25};$$
$$P_6 = P_1 \cdot p_{16} + P_3 \cdot p_{36}.$$

Выражения для вероятностей P_i ($i = 2, \ldots, 6$) можно выразить через P_1:

$$P_2 = P_1 \cdot p_{12};$$
$$P_3 = P_1 \cdot p_{12} \cdot p_{23};$$
$$P_4 = P_1 \cdot p_{12} \cdot p_{23} \cdot p_{34};$$
$$P_5 = P_1 \cdot (p_{15} + p_{12} \cdot p_{25});$$
$$P_6 = P_1 \cdot (p_{16} + p_{12} \cdot p_{23} \cdot p_{36}).$$

Из условия нормировки $\sum_{i=1}^{6} p_i = 1$ получаем:

$$P_1 \cdot \left(p_{12} + p_{12}p_{23}p_{34} + p_{15} + p_{12}p_{25} + p_{16} + p_{12}p_{23}p_{36}\right) = 1,$$

откуда

$$P_1 = \frac{1}{p_{12} \cdot \left(1 + p_{12} + p_{23}p_{34} + p_{25} + p_{12}p_{23}p_{16}\right) + p_{15}} = \frac{1}{A};$$

$$P_2 = \frac{p_{12}}{A}; \quad P_3 = \frac{p_{12}p_{12}}{A}; \quad P_4 = \frac{p_{12}p_{23}}{A}; \quad P_5 = \frac{p_{15} + p_{12}p_{25}}{A}; \quad P_6 = \frac{p_{16} + p_{12}p_{23}p_{36}}{A}.$$

Величина вероятностей переходов p_{12}, p_{23} и p_{34} может изменяться в диапазоне $0{,}8 < p_{ij} < 1$, величина вероятностей p_{15}, p_{25}, как правило, лежит в диапазоне $p_{j5} < 0{,}1$ для $j = 1, 2$; а вероятности p_{16} и p_{36} как минимум на два порядка меньше.

Каждый выделенный блок (см. рис. 1) можно расписать более подробно для моделирования основных процедур. Покажем это на примерах регистрации и простейшего протокола аутентификации.

Моделирование процедуры регистрации. Процедуру регистрации нового пользователя в системе аутентификации упрощенно можно представить в виде следующих состояний:

1. Претендент на регистрацию послал запрос на сервер ЦР с целью зарегистрироваться в ИС.
2. Идентификаторы претендента пришли на сервер вместе с запросом на регистрацию. С сервера ЦР высылается запрос на подтверждение наличия и совпадения полученных от претендента идентификаторов в базах, содержащих идентификационные данные граждан.
3. Получены ответы на запрос сервера. Если данные совпали, ЦР создает учетную запись претендента, который стал новым легальным пользователем ИС.
4. Центр регистрации создал или зарегистрировал аутентификатор нового легального пользователя в соответствии с его учетной записью.
5. ЦР выдал пользователю электронное удостоверение (например, в виде сертификата ключа проверки подписи) и аутентификатор в случае, когда аутентификатор был создан ЦР.

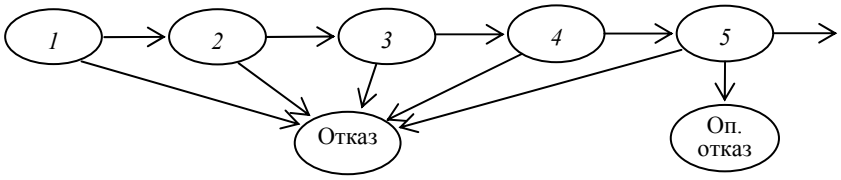

Рис. 3. Направленный граф состояний системы регистрации

В приведенных обозначениях состояний системы процесс регистрации можно представить в виде направленного графа [4, 6, 9], где состояния системы обозначены цифрами *1–5* (рис. 3).

Определим вероятность работы системы до возникновения первого функционального отказа:

$$P_{\Phi o} = 1 - P_1 + P_1(1 - P_2) + P_1P_2(1 - P_3) + P_1P_2P_3(1 - P_4) + P_1P_2P_3P_4(1 - P_5),$$

где P_1 – вероятность перехода системы из состояния «1» в состояние «2» (это соответствует отсутствию отказов «клиентской» части у претендента при формировании запроса: при личной явке в ЦР «отказом» может служить отсутствие паспорта или СНИЛС, неурочное время работы, отсутствие персонала в ЦР и т.д.); P_i – вероятность перехода из состояния «i» в состояние «i + 1», i = 2, 3, 4.

Определим вероятность функционального опасного отказа:

$$P_{\Phi Оп} = P_1P_2P_3P_4(1–P_5).$$

Для определения безопасности и надежности процедуры регистрации особенно важно определить параметры вероятности наступления опасного отказа, т.е. регистрации злоумышленника под именем легального пользователя системы.

Моделирование протоколов аутентификации. Для примера рассмотрим один из наиболее используемых в настоящее время протоколов аутентификации – простейший сетевой протокол аутентификации с применением логина пользователя в качестве его электронного удостоверения (*Id* пользователя) и пароля (password) в качестве секрета. Схема взаимодействия клиент–сервер приведена на рис. 4.

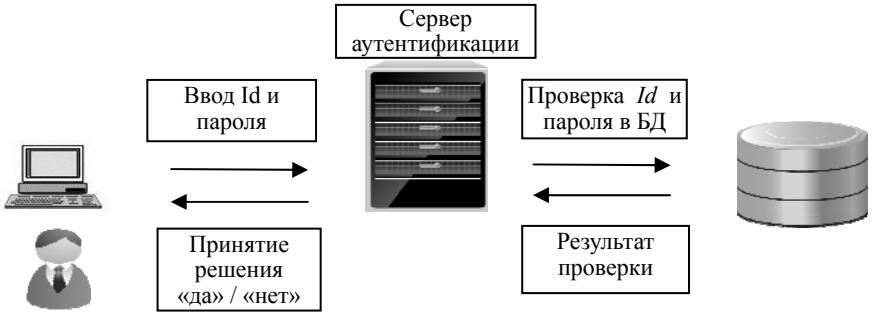

Рис. 4. Упрощенная схема протокола парольной аутентификации

Составим схему работы протокола, обозначив состояния системы:

1. Претендент на доступ к системе ввел логин и пароль.
2. Сервер аутентификации принял аутентификационные данные (АД) от претендента и переслал их для проверки соответствия в базу данных учетных записей (БДУЗ).
3. Присланные претендентом АД данные совпали с записями в БДУЗ.
4. Присланные претендентом АД не совпали с записями в БДУЗ.
5. Сервер аутентификации принял положительное решение о прохождении претендентом процедуры аутентификации.
6. Сервер аутентификации принял отрицательное решение о прохождении претендентом процедуры аутентификации.

Состояния системы «претендент – сервер аутентификации» могут быть представлены в виде направленного графа (рис. 5). По такому же принципу можно построить модели для наиболее часто используемых на практике протоколов аутентификации (Radius, Kerberos, SAML и т.д.).

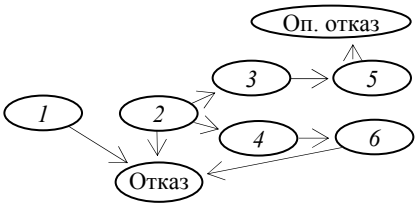

Рис. 5. Граф состояний системы парольной аутентификации

Реальные значения параметров вероятности P_i лежат в пределах 0,8–1. Для систем аутентификации это означает, что ошибки при вводе аутентификационных данных (в случае парольной защиты), сбои программного и аппаратного обеспечения могут приводить как к отказам или задержкам по времени, так и к опасным отказам с незначительной вероятностью [7, 10, 11].

Заключение. Предложенные выше модели для проведения оценок безопасности и надежности аутентификации представляют научный и практический интерес. Появление и развитие подобных моделей позволит проводить исследования безопасности и определение характеристик надежности аутентификации при проектировании и эксплуатации систем аутентификации. В развитие данной работы планируется исследование адекватности предложенных моделей и применение полученных соотношений к решению ряда практических задач.

Литература

1. Сабанов А.Г. Аутентификация при электронном обмене документами // Докл. Том. гос. ун-та систем управления и радиоэлектроники. – 2011. – № 2(24). – С. 263–266.

2. Сабанов А.Г. Об оценке рисков удаленной аутентификации как процесса // Электросвязь. – 2012. – № 4. – С. 27–32.

3. Сабанов А.Г. Методы исследования надежности удаленной аутентификации // Электросвязь. – 2013. – № 4. – С. 20–24.

4. Шубинский И.Б. Основы анализа сложных систем: учеб. пособие. – Л.: Министерство обороны СССР, 1986. – 256 с.

5. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. – Ульяновск: Печатный двор, 2012. – 296 с.

6. Кемени Дж. Кибернетическое моделирование. Некоторые приложения / Дж. Кемени, Дж. Снелл: пер. с англ. Б.Г. Миркина; под ред. И.Б. Гутчина. – М.: Советское радио, 1972. – 192 с.

7. Филькин К.Н. Информационно-управляющая система поддержки принятия решений при управлении информационной безопасностью территориально-распределенной организацией / К.Н. Филькин, С.Н. Филькин, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 83–86.

8. Исхаков С.Ю. Разработка методического и программного обеспечения для мониторинга работы локальных сетей / С.Ю. Исхаков, А.А. Шелупанов // Телекоммуникация. – 2013. – №6. – С. 16–20.

9. Шелупанов А.А. Метод построения графа связи альтернатив с исходами и графа предпочтений в задаче принятия решений / А.А. Шелупанов, Т.Ю. Зырянова // Вестник Тюм. гос. ун-та. – 2007. – № 5. – С. 101–106.

10. Миронова В.Г. Методология формирования угроз безопасности конфиденциальной информации в неопределенных условиях из возникновения / В.Г. Миронова, А.А. Шелупанов // Изв. Южного фед. ун-та. Технические науки. – 2012. – Т. 137, № 12. – С. 39–45.

11. Шелупанов А.А. Автоматизированная система предпроектного обследования информационной системы персональных данных «Аист-П» / А.А. Шелупанов, В.Г. Миронова, С.С. Ерохин, А.А. Мицель / Докл. Том. гос. ун-та систем управления и радиоэлектроники. – 2010. – № 1(1). – С. 14–22.

Сабанов Алексей Геннадьевич
Канд. техн. наук, зам. генерального директора ЗАО «Аладдин Р.Д.»,
доцент МГТУ им. Н.Э. Баумана, Москва
Тел.: 8-985-924-52-09
Эл. почта: asabanov@mail.ru; a.sabanov@aladdin-rd.ru

Sabanov A.G.

Authentication Process Modeling Strategy

A strategy of authentication process modeling is suggested. The strategy is based on the consideration of major authentication procedures that differ in duration. The authentication process is examined in authorization request flows of varying intensity.

Keywords: strategy, security, dependability, modeling, process, authentication.