УДК 004.089

А.Г. Сабанов

Методика идентификации рисков процессов аутентификации

Предложена методика формирования дерева отказов и дерева событий в процессах аутентификации в соответствии с основными стандартами анализа надежности. Методика основана на рассмотрения основных процедур аутентификации, имеющих различную продолжительность во времени.

Ключевые слова: идентификация, методика, надежность, дерево отказов, дерево событий, риск, процесс, аутентификация.

При построении информационного общества [1] и развитии систем оказания государственных и муниципальных услуг в электронной форме на передний план выдвигаются понятия безопасности и надежности определения сторон взаимодействия. В работе [2] доказано, что указанные понятия тесно связаны друг с другом, а основой создания доверительных отношений для взаимодействующих сторон является сервис безопасности, называемый аутентификацией. Представим аутентификацию в виде двух связанных между собой процессов: подтверждения подлинности предъявленных претендентом идентификаторов и проверки принадлежности аутентификатора данному пользователю. Подлинность проверяется с помощью протоколов аутентификации, как правило, криптографическими методами, с использованием аутентификатора (секрета), о котором или о наличии которого (например, закрытого ключа сертификата электронной подписи или сертификата доступа) известно проверяющей стороне. Факт принадлежности проверяется с использованием электронного удостоверения (ЭУ), которое связывает наличие аутентификатора и идентификаторов (ИД) с конкретным пользователем [3]. Проектирование и эксплуатация систем идентификации и аутентификации (СИА) должны сопровождаться анализом рисков [4] и оценками надежности их работы [2].

Под надежностью аутентификации будем понимать такое состояние механизмов и элементов СИА, которое обеспечивает выполнение потока заявок на аутентификацию всех легальных пользователей в течение заданного интервала времени, но не позволяет злоумышленнику преодолеть реализуемые функции безопасной аутентификации за приемлемое время. Системы аутентификации относятся к разряду интеллектуальных систем, составными частями которых, как правило, являются мощная серверная (аппаратная и программная) и клиентская части, соединенные защищенными каналами связи. Для анализа рисков и исследования надежности выполнения основных процедур аутентификации сначала необходимо идентифицировать риски. Эта весьма сложная задача в силу многообразия используемых решений и применяемых технологий может быть разбита на этапы. Концептуальный подход рассмотрения двух важнейших этапов идентификации рисков будет рассмотрен в данной работе. Для снятия остаточных неопределенностей и проведения параметрических исследований требуется создание математических моделей, принципы построения которых разработаны в [5]. Как показано в [6], 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», передача заявки на авторизацию пользователя). При моделировании СИА также надо учитывать то, что при значительном числе зарегистрированных пользователей (например, более пятисот) системы аутентификации должны подчиняться законам систем массового обслуживания. Это требование предусматривает необходимость исследования поведения СИА 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. Применение стандартных подходов построения дерева отказов на основе классической теории надежности механизмов и машин для выполнения заданного набора функций таких сложных систем в интенсивно меняющихся условиях воздействия приводит к рассмотрению многообразия схем СИА, механизмов аутентификации и условий эксплуатации в зависимости от времени. Одним из возможных решений данной задачи является разработка методики определения дерева основных отказов, учитывающей особенности СИА в части выполнения проце-

дур аутентификации (т.е. основных функций) и охватывающей все типы систем и условий работы, вплоть до перехода к облачным вычислениям. Другими словами, предлагаемый подход основан на применении базовых принципов функциональной надежности [7] к анализу безопасности выполнения СИА основных процедур обработки заявок претендентов на авторизацию. Создание указанной методики позволит существенно сократить объем исследований при сохранении в виде объекта рассмотрения всего разнообразия СИА и условий их эксплуатации.

Вопросы оценки надежности аутентификации пользователей и применяемых при этом средств аутентификации активно обсуждаются специалистами, однако общепринятый научный подход и устоявшаяся терминология к исследованию этого весьма сложного процесса пока не выработаны. Целью данной статьи является выполнение подготовительного этапа анализа надежности – разработка методики построения дерева отказов и дерева событий для исследования безопасности и надежности аутентификации, а также введению таких базовых понятий для анализа изучаемых СИА, как отказ и опасный отказ.

Базовые понятия надежности процессов аутентификации. Сначала определим некоторые базовые понятия, которые будут использоваться в работе. Привычные для специалистов по информационной безопасности (ИБ) свойства защищенности информационной системы (ИС) применительно к СИА могут быть выстроены в порядке убывания приоритетов следующим образом: доступность, целостность, конфиденциальность. В работе [2] показано, что в понятие надежности кроме указанных свойств защищенности, входят такие свойства, как безотказность, сохранность (устойчивость к воздействиям) и ремонтопригодность.

Безотказность – свойство системы (объекта) непрерывно сохранять работоспособное состояние в течение некоторого времени (наработки). Под наработкой обычно понимается продолжительность времени работы системы или объем работы. Состоянием называется множество существенных свойств, которыми объект обладает в данный момент времени. Безотказность и доступность условно можно объединить в понятие минимизации простоев СИА, т.е. обеспечение непрерывности обслуживания заявок на аутентификацию.

Важнейшим понятием в теории надежности является понятие отказа. В ИС отказы происходят не всегда одинаково, различные способы отказа называются состояниями отказа. Состояния отказа отражают события ненадлежащего обслуживания. Применительно к СИА под отказом будем понимать отрицательный результат аутентификации и соответственно состояние отказа в авторизации легального пользователя.

Работоспособное состояние – это такое состояние объекта, при котором множество существенных свойств в полном объеме отвечает заданным требованиям.

Под опасным отказом будем понимать положительный результат прохождения процесса аутентификации злоумышленником.

Предположения. Для формирования дерева отказов и дерева событий введем следующие предположения, основанные на опыте проектирования, построения и анализе функционирования ряда промышленных СИА.

1. Основной поток заявок $\lambda_{л.п}$ на обслуживание СИА поступает от легальных пользователей системы, при этом заявки не содержат ошибок, а система и ее элементы не имеют отказов.

2. Среди массы заявок от легальных пользователей имеется некоторая часть некорректно оформленных заявок $\lambda_{ош.л.п} \in \lambda_{л.п}$. из-за непреднамеренных ошибок.

3. Из числа заявок от легальных пользователей имеется некоторая часть заведомо ложных заявок $\lambda_{з.л.л.п.} \in \lambda_{л.п}$. с целью выдать себя за пользователя с более привилегированными правами доступа. Таким образом, имеем соотношение: $\lambda_{ош.л.п} + \lambda_{ош.л.п} + \lambda_{з.л.л.п} = \lambda_{л.п}$.

4. В СИА поступает некоторая часть заведомо ложных заявок от злоумышленников $\lambda_{з.л.зл}$, пытающихся выдать себя за легальных пользователей: $\lambda_{з.л.зл} \cap \lambda_{л.п}$.

Введем ряд предположений о работе СИА:

1. СИА состоит из серверной и клиентской частей, связанных устойчивым каналом (каналами) связи.

2. Серверная часть состоит из нескольких связанных защищенным образом серверов (например, по протоколу IPSec), отказоустойчивость *OU* которых (по SLA – Service Level Agreement, соглашение об уровне обслуживания) $OU \geq 99{,}95\%$. Системное, прикладное и специальное программное обеспечение (ПО) – лицензионное, как правило, вовремя обновляется и обслуживается производителями.

3. Клиентская часть может быть представлена в виде следующих модификаций: компьютер пользователя с необходимым набором ПО и аутентификационной информацией (АИ) пользователя:

а) код доступа (логин, пароль);

б) логин и пароль плюс одноразовый пароль или усиленный неквалифицированный сертификат и ключ неквалифицированной подписи;

в) квалифицированный сертификат доступа и ключ подписи.

Для определенности будем считать, что в вариантах (б) и (в) АИ пользователя находится в некоем устройстве, связанном с конкретным пользователем. При этом связь пользователя с устройством осуществлена ЦР в виде ЭУ при выдаче пользователю АИ и находится в БД учетных записей.

Методика формирования модели дерева отказов. Проведем анализ видов и последствий отказов согласно рекомендациям [8, 9]. Как известно, этот метод позволяет определить возможные причины отказа элементов системы и события, породившие отказ.

Составим дерево отказов СИА в соответствии с пятиуровневой схемой. Верхний (первый) уровень – отказ системы. Второй уровень – отказ составных частей. Третий уровень – отказ элементов. Следующий уровень определяет события, порождающие отказ. Пятый уровень определяет виды воздействий, приводящих к отказу СИА.

Построение всего дерева отказов СИА в виде графа событий и последствий представляет собой трудночитаемый рисунок с множеством мелких значков и надписей. Поэтому выделим наиболее существенные виды отказов СИА, не пропуская, по возможности, наиболее критичные с точки зрения безопасности и надежности.

Для примера сначала рассмотрим некоторые отказы СИА, связанные с событиями, породившими отказ, в процедурах регистрации и хранения (табл. 1).

Таблица 1

Примеры дерева отказов, связанных с нарушениями ИБ, в процедурах регистрации и хранения аутентификационной информации

Уровень системы	Отказ СИА	Отказ СИА	Опасный отказ СИА (в процедуре регистрации)	Опасный отказ СИА (в процедуре хранения)
Уровень составных частей	Отказ в регистрации	Отказ в регистрации легальному пользователю	Злоумышленник зарегистрирован под видом легаль-ного пользователя	Злоумышленник владеет ИД и секретом (аутентификатором) легального пользователя
Уровень элементов	Отказ в приеме ИД	Отказ в результате проверки ИД	Проверки ИД не выявили обмана	Потеря конфиден-циальности секрета
События, порождающие отказ	Неполный набор представленных пользователем ИД	В базах данных ведомств не найдены ИД, соответствующие представленным пользователем	Поддельные документы на имя легального пользователя	Нарушение условий хранения секрета
Виды воздействия	Ошибка заявителя, попытка злоумышленника	Неполная база, сбой, вирусная атака	Атака класса «маскарад»	Хищение, копирование ИД и секрета (аутентификатора)

Также можно рассмотреть дерево отказов СИА, связанных с нарушениями ИБ, и для других процедур аутентификации. В табл. 2 приводятся примеры отказов, обусловленных нарушениями ИБ, в процедурах валидации, протоколах обмена и принятия решения.

Сформированное таким образом дерево отказов позволяет более четко идентифицировать вероятные события, которые могут привести к нарушениям ИБ при работе СИА. Рассмотрение отказов является одной из важных подготовительных процедур для идентификации рисков нарушения безопасности функционирования СИА. Следующей процедурой, согласно [9], является формирование модели дерева событий.

Формирование модели дерева событий. Согласно рекомендациям [8], необходимо выделить наиболее вероятные опасные события и оценить частоту их реализации.

Существует вероятность ошибки первого рода (СИА не авторизовала легального пользователя ИС). Рассмотрим возможные причины такого события:

1) пользователь неверно ввел свою АИ (например, забыл пароль в случае «а»);

2) перегрузка СИА ввиду большого числа одновременных заявок и/или время ожидания превысило некий порог ожидания;

3) отказ клиентской части (аппаратный или программный сбой);

4) отказ канала связи (аппаратный и/или программный);

5) отказ серверной части.

Также существует вероятность ошибки второго рода, когда СИА признала ИА правильной и авторизовала злоумышленника под именем легального пользователя.

Таблица 2

Примеры дерева отказов, связанных с нарушениями ИБ, в процедурах проверки валидности ЭУ, протоколах аутентификации и принятия решения

Уровень системы	Отказ СИА	Отказ СИА	Отказ СИА	Отказ СИА
Уровень составных частей СИА	Отказ в валидации	Отказ в работе протокола обмена	Отказ в процедуре принятия решения	Отказ в процедуре принятия решения
Отказ элементов	ЭУ пользователя не валидно	Отказ в клиентской части	Несовпадение предъявленного секрета с БД	Превышено время ожидания
События, порождающие отказ	Нет цепочки проверки сертификата, не работает служба OCSP\UDVCS	Не установлен драйвер, не выполнено обновление системного ПО	Подмена ИД и ЭУ на имя легального пользователя	Велика интенсивность потока заявок на аутентификацию для данной СИА, ошибки проектирования
Виды воздействия	Атака не сервер УЦ, выдавший ЭУ, сбои УЦ цепочки ЭУ	Вирусная атака, халатность администратора	Попытка злоумышленника	DDoS-атака

На основе анализа двенадцатилетнего опыта построения и эксплуатации ряда промышленных СИА выделим ряд вероятных опасных событий PHE_i, $i = 1, n$. Перечислим эти события и приведем грубую оценку частоты их реализации.

PHE_1. Целенаправленные действия злоумышленника при регистрации. Регистрация – одна из самых ответственных операций процессов аутентификации, существенно влияющая на безопасность, надежность и в конечном счете на доверие работы СИА. Тем не менее на момент написания данной работы процедура регистрации является одной из самых не затронутых регулированием. В ряде государственных ИС, например, для доступа на портал государственных услуг, как было признано представителем Минкомсвязи на конференциях 2013 г., и по день написания текста злоумышленник может зарегистрироваться под именем любого незарегистрированного в ЕСИА гражданина. Максимум усилий злоумышленника может потребоваться для подделки паспорта (который предъявлять требуют не везде, а при предъявлении не проверяют на «поддельность»), а сделать поддельную справку СНИЛС с истинным номером владельца не представляет трудности. Для краткости будем называть этот вид «маскарад» при регистрации. Оценим частоту такого события для существующих СИА в достаточно широких пределах: 10^{-7}–10^{-5} в год.

PHE_2. Злоумышленник для доступа к интересующим его информационным ресурсам может воспользоваться уязвимостями СИА. Поскольку требований ИБ к СИА пока нет, это опасное событие имеет вероятность осуществиться. Будем называть это событие «уязвимости СИА» и оценим частоту в пределах 10^{-5}–10^{-3}.

PHE_3. Этот тип вероятного опасного события (ВОС) может быть связан с действиями инсайдера. Помочь злоумышленнику пройти все рубежи СИА может легальный пользователь. Еще больше возможностей у администратора. Кратко назовем это событие «помощь инсайдера». Грубые оценки частоты: 10^{-6}–10^{-4}.

PHE_4. Завладение злоумышленником ИД и АИ легального пользователя. Это может быть кража, клонирование ИД и АИ, подсмотренный пароль, перехваченный PIN-код. Кратко назовем этот тип «кража ИД и АИ» и оценим частоту: 10^{-5}–10^{-3}.

PHE_5. Атака «вход по принуждению» встречается все реже и реже: 10^{-7}–10^{-5}.

PHE_6. Ошибки и/или целенаправленные действия злоумышленника при смене пароля, замене цифрового сертификата доступа или сценарии «забыл дома смарт-карту» [10]. Коротко назовем этот тип «смена АИ» и оценим частоту в пределах 10^{-5}–10^{-3}.

PHE_7. Данный тип ВОС связан с ошибками валидации ЭУ. Под валидацией будем понимать процесс проверки действительности сертификата доступа и цепочки сертификатов, для парольной защиты это процедура сличения хешей паролей (присланного претендентом и зарегистрированного в БД учетных записей). Короткое название – «ошибки валидации». Оценки частоты: 10^{-6}–10^{-4}.

PHE_8. Ошибки в принятии решения «свой–чужой». Процедура производится на серверах, вероятная частота подобного события 10^{-7}–10^{-5}.

PHE_9. Имитация доверяющей стороны. Особенно актуален такой тип ВОС при предоставлении Web –доступа, который становится все более распространенным. Фишинг (подмена сайта) является одним из актуальных ВОС, оценки частоты колеблются в пределах 10^{-4}–10^{-2}.

PHE_{10}. Подмена доверенной стороны или объекта (spoofing), оценим частоту 10^{-6}–10^{-4}.

PHE_{11}. Риск добровольной передачи персонального средства ИА другому сотруднику. Выявлено в ряде ИС государственных организаций. Частоту можно оценить в пределах 10^{-4}–10^{-2}. Средство борьбы – усиленная персонализация (совмещение смарт-карты, содержащей аутентификатор, с зарплатной или введение карт с технологией Match on Card).

PHE_{12}. Наконец, последним ВОС будем считать воздействие вредоносного программного обеспечения, вероятность заражения рабочих мест определяется политикой безопасности организации, в среднем по стране может быть оценена как 10^{-4}–10^{-2}.

В качестве следующего подготовительного этапа к оценке рисков и надежности работы СИА необходимо разработать рекомендации к обоснованию уровней приемлемого риска для перечисленных опасных событий. Для анализа рисков в конкретной организации также необходимо провести анализ последствий наступления опасных событий. Эти вопросы будут предметом продолжения исследования, начатого в данной статье.

Заключение. Предложенная методика построения модели дерева отказов и модели дерева событий для проведения оценок безопасности и надежности аутентификации представляет научный и практический интерес. Применение и развитие методики позволит проводить исследования безопасности, анализа рисков и определять характеристики надежности аутентификации при проектировании и эксплуатации СИА.

Литература

1. Распоряжение Правительства Российской Федерации от 20 октября 2010 г. № 1815-р «О государственной программе Российской Федерации «Информационное общество (2011–2020 годы)» [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2010/11/16/infobschestvo-site-dok.html свободный, дата проверки: 17.12.2013 г.

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

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

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

5. Сабанов А.Г. Концепция моделирования процессов аутентификации // Доклады ТУСУРа. – 2013. – № 3(29). – С. 71–75.

6. Сабанов А.Г. Основные процессы аутентификации // Вопросы защиты информации. – 2012. – № 3. – С. 54–57.

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

8. ГОСТ Р 51901.1-2002. Менеджмент риска. Анализ риска технологических систем. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200030153 свободный, дата проверки: 17.12.2013г.

9. ГОСТ Р 51901.12-2007. Метод анализа видов и последовательность отказов [Электронный ресурс]. – Режим доступа: http://www.opengost.ru/iso/13_gosty_iso/13110_gost_iso/4936-gost-r-51901.12-2007-mek-60812_2006-menedzhment-riska.-metod-analiza-vidov-i-posledstviy-otkazov.html свободный, дата проверки: 17.12.2013 г.

10. Аутентификация. Теория и практика. Обеспечение безопасного доступа к информационным ресурсам / А.А. Афанасьев и др.; под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. – М.: Горячая линия-Телеком, 2009. – 552 с.

Сабанов Алексей Геннадьевич
Канд. техн. наук, зам. ген. дир. 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.
Method of risks identity of authentication processes

In the paper we suggest a method of generation the fault tree and event tree according to dependability of analyzing standards for risks identity of authentication processes. The strategy is based on the consideration of major authentication procedures which differ in duration.
Keywords: identity, method, dependability, fault tree, event tree, risk, process, authentication.
