ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.089+621

МОДЕЛИ ДЛЯ ИССЛЕДОВАНИЯ БЕЗОПАСНОСТИ И НАДЕЖНОСТИ ПРОЦЕССОВ АУТЕНТИФИКАЦИИ

А. Г. Сабанов, заместитель генерального директора ЗАО «Аладдин Р.Д.», доцент МГТУ им. Н. Э. Баумана, к.т.н.; A. Sabanov@aladdin-rd.ru

Ключевые слова: *безопасность, надежность, модели, аутентификация.*

Введение. Вопросы разработки моделей для исследования интеллектуальных систем представляют собой отдельный класс сложных научных задач. Системы аутентификации относятся к разряду интеллектуальных систем, составными частями которых, как правило, являются мощная серверная (аппаратная и программная) и клиентская части. При моделировании также необходимо учитывать участие в процедурах и процессах подготовки и проведения аутентификации человека. 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 [1, 2], 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 500) 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 ряда простейших моделей для исследования безопасности и надежности аутентификации.

Моделирование процедур аутентификации. Для моделирования процесса аутентификации следует разделить его на однородные по функциональным и вероятностно-статистическим характеристикам блоки, поскольку разные блоки имеют существенно отличающиеся характеристики по времени. Например, процедура регистрации производится единожды и может быть относительно краткой. Хранение аутентификационных данных (АД) 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) регистрация — не связан со временем (стационарный процесс);

2) хранение — связан со временем. Применимо пуассоновское распределение;

3) протоколы обмена — отказы (отказы аппаратного и программного компонентов, случайные, неслучайные ошибки пользователей, атаки). Для моделирования возможно применение экспоненциального распределения;

4) валидация — вероятность отказа для корпоративных закрытых информационных систем (ИС) мала, для ИСОП — велика;

5) процедура принятия решения («свой-чужой») — простая; 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).

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 2 и 3 (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 (способность системы выполнять предусмотренные функциональные задачи с приемлемым уровнем безошибочности в реальных условиях эксплуатации) и функциональную безопасность (способность системы выполнять предусмотренные функциональные задачи с заданным уровнем доступности, целостности и конфиденциальности). С учетом 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:

- процесс регистрации нового пользователя ИСОП определяем в терминах теории надежности как процесс однократного срабатывания;
- блоки хранения секретов и протоколы аутентификации объединяем в один блок «Подтверждение подлинности». Принимаем, 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.

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 центра регистрации (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. ЦР создал или зарегистрировал аутентификатор нового легального пользователя в соответствии с его учетной записью.
5. ЦР выдал пользователю ЭУ (например, в виде сертификата ключа проверки подписи) и аутентификатор в случае, когда аутентификатор был создан ЦР.

В приведенных обозначениях состояний процесс регистрации можно представить в виде направленного графа, где состояния системы обозначены цифрами 1—5 (рис. 2):

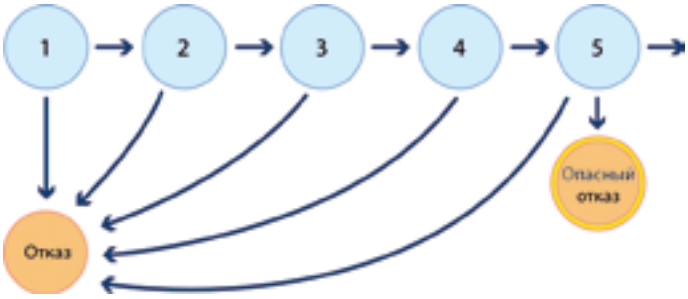

Рис. 2. **Граф состояний системы регистрации**

Определим вероятность работы системы до возникновения первого 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 «$i + 1$», $i = 2, 3, 4$.

Затем можно определить вероятность опасного отказа:

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

Типичные зависимости величин $P_{\Phi o}$ и $P_{\Phi\,Оп}$ от значений вероятности перехода от состоянию 1 к состоянию 2 при $P_2 = P_3 = P_4 = 0{,}9$ представлены на рис. 3.

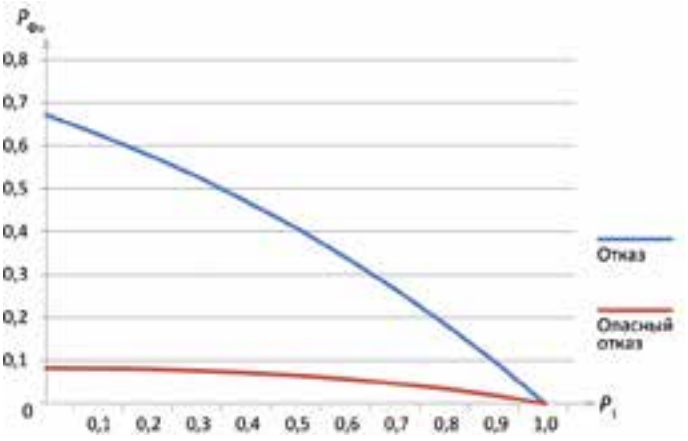

Рис. 3. **Вероятность наступления отказа и опасного отказа**

Как будет показано ниже, 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 часто 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**

Запишем схему работы протокола, обозначив состояния системы:

1. Претендент на доступ к системе ввел логин и пароль.
2. Сервер аутентификации принял аутентификационные данные 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.

Данные 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.).

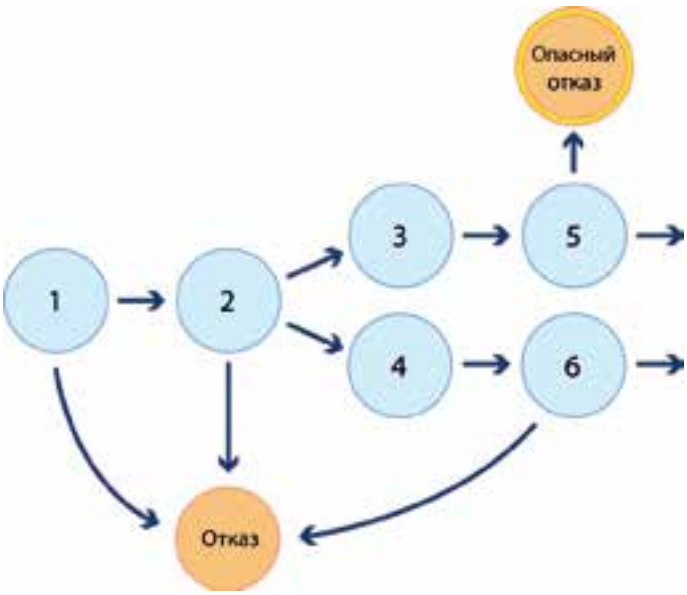

Рис. 5. **Граф состояний системы парольной аутентификации**

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. Для иллюстрации возможностей применения представленных моделей и оценки мер, обеспечивающих необходимый уровень надежности процесса аутентификации, рассмотрим классический пример из теории управления сложными объектами.

Представим блоки подтверждения подлинности, валидации и принятия решения в виде аналога ряда последовательно расположенной группы устройств r_i (рис. 6), обслуживающих поток заявок с интенсивностью λ и средним временем обслуживания t. Заявки, которые не были обслужены первым устройством, попадают на второе устройство, заявки, которые не были обслужены вторым устройством, попадают на устройства третьей группы, и т.д.

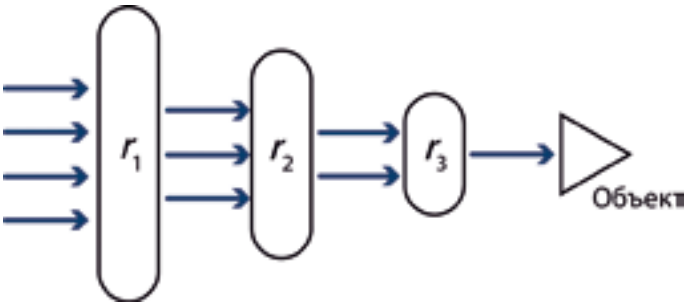

Рис. 6. **Ряд устройств, обслуживающих поток заявок**

Аналогом такой схемы является схема эшелонированной противотанковой обороны [3]. Танки противника, перед которыми поставлена цель — проникнуть на объект, должны преодолеть все эшелоны обороны. Попробуем оценить эффективность такой обороны, состоящей из однотипных устройств, в предположении показательных законов распределения времени между заявками с интенсивностью λ.

Определим вероятность того, что заявки получат отказ на устройствах первой группы и поступят на устройства второй группы, с помощью формулы Эрланга:

$$P_1 = a_1/d_1,$$

где $a_1 = \rho_1^r / r_1!$; $d_1 = \sum_{i=o}^{r_1} \frac{\rho_i}{i!}$.

Если устройства второй группы также будут заняты, заявки получат отказ. Вероятность такого события

$$P_2 = a_2/d_2,$$

где $a_2 = \frac{\rho^{\sum_{i=1}^{k} r_i}}{\left(\sum_{i=1}^{k} r_i\right)!}$; $d_2 = \sum_{i=0}^{r_1+r_2} \frac{\rho_i}{i!}$.

Если число таких групп k, вероятность прохода танков сквозь всю систему обороны равна

$$P_k = a_k/d_k,$$

где $a_k = \frac{\rho^{\sum_{i=1}^{k} r_i}}{\left(\sum_{i=1}^{k} r_i\right)!}$; $d_k = \sum_{i=0}^{k} \frac{\rho^{r_i}}{i!}$.

Для примера посчитаем вероятности, приняв значения $k = 1, 2, 3$. Поскольку $\rho = \lambda t$, положим интенсивность потока заявок $\lambda = 1$ и среднее время $t = 0{,}1$. Тогда

$$P_1 = a_1/d_1 = 0{,}1/1{,}1 = 0{,}0909;$$

$$P_2 = a_2/d_2 = 0{,}005/1{,}105 = 0{,}045249;$$

$$P_3 = a_3/d_3 = 0{,}000167/1{,}10516 = 0{,}000151,$$

из чего следует, что вероятность «прорыва танков» существенно уменьшается от эшелона к эшелону.

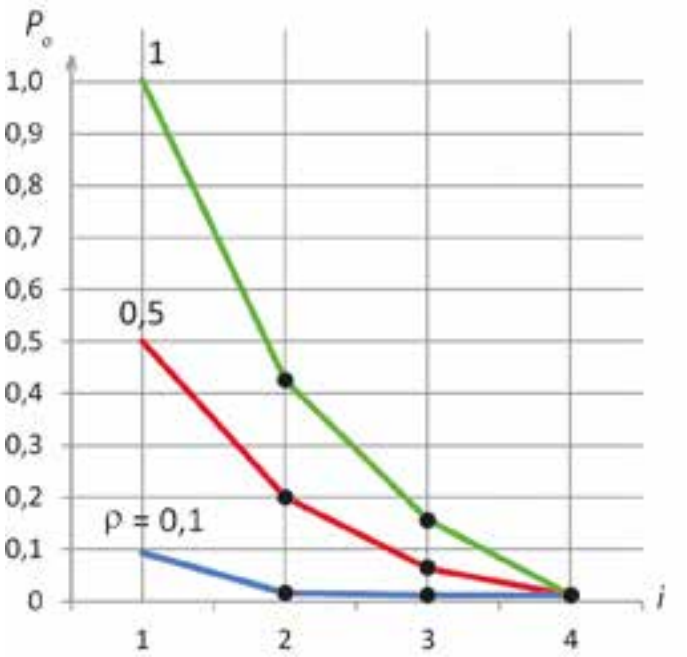

Рис. 7. **Расчет вероятности «прорыва танков»**

Добавим в расчеты четвертый «эшелон» и получим кривые вероятности отказа P_o от количества эшелонов $k = 0,\ldots,4$ в зависимости от интенсивности потока танков $\rho = \lambda t$ (рис. 7), из которых видно, что с уменьшением ρ «пропускная» способность обороны по мере увеличения числа эшелонов обороны падает менее интенсивно. Возвращаясь к задаче аутентификации, отметим, что интерпретация четырех «эшелонов» обороны будет соответствовать блокам предъявления идентификатора и аутентификатора, проверки подлинности аутентификатора, валидации и принятия решения. Полученные расчетным путем значения P_o должны соответствовать вероятности отказа в аутентификации. Причем в рассматриваемом случае отказ будет не смертелен: претенденту, как правило, дается минимум три попытки предъявления АД.

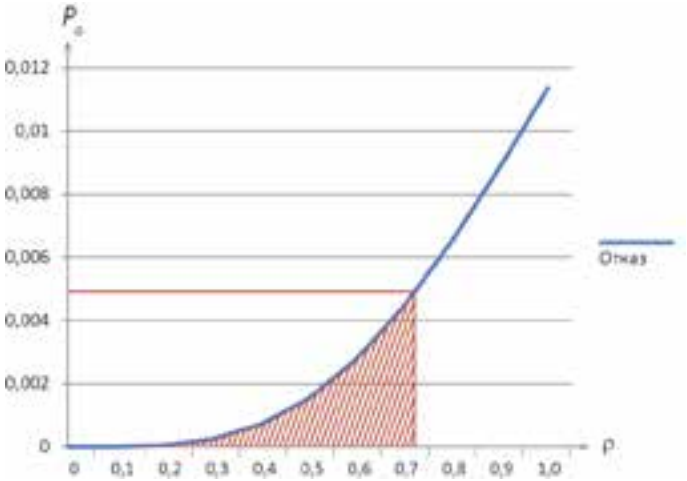

Рис. 8. **Пример расчета допустимых значений отказов в аутентификации**

Задача, таким образом, может сводиться к определению количества попыток аутентификации, а если их лимит выбран — количества резервных каналов для обеспечения заданного потока интенсивности заявок на аутентификацию в единицу времени. Пример расчета реальных значений одноканального потока заявок однократной парольной аутентификации с допустимым порогом отказа 5% представлен на рис. 8.

Полученные соотношения позволяют определить такие параметры, как вероятность безошибочной работы системы в условиях заданного потока заявок и вероятность безошибочной работы за заданное время [4].

Перспективы развития моделирования процессов аутентификации. Простейшие модели процедур аутентификации можно усложнять, последовательно вводя учет тех или иных параметров. Покажем, как учитывать влияние поглощения на примере укрупненной модели аутентификации (см. рис. 1). Работу системы аутентификации представим в виде направленного графа состояний (рис. 9), где 1 — регистрация нового легального пользователя системы выполнена; 2 — произведено подтверждение подлинности предъявленных претендентом (пользователем) аутентификационных данных; 3 — процедура принятия решения «свой-чужой» выполнена; 4 — состояние отказа аутентификации легального пользователя; 5 — состояние опасного отказа (аутентификация злоумышленника под видом легального пользователя).

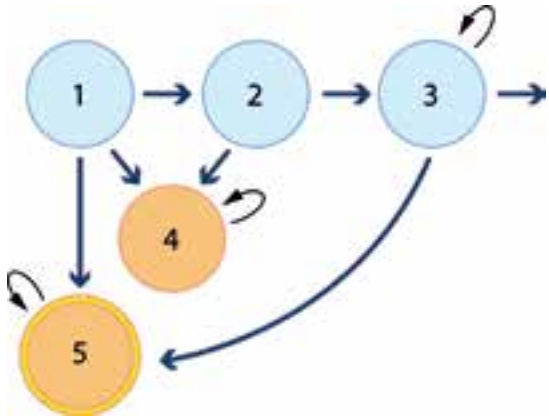

Рис. 9. **Граф состояний укрупненной вероятностной модели аутентификации**

Состояния системы 3—5 опишем в виде поглощающих состояний [4]. Обозначим вероятность переходов из одного состояния в другое:

p_{12} — вероятность перехода из состояния 1 (регистрация) в состояние 2 (подтверждение подлинности предъявленных идентификаторов);

p_{14} — вероятность перехода из состояния 1 в состояние 4 (отказ);

p_{15} — вероятность перехода из состояния 1 в состояние 5 (опасный отказ);

p_{23} — вероятность перехода из состояния 2 в состояние 3 (принятие решения);

p_{24} — вероятность перехода из состояния 2 в состояние отказа;

p_{33} — вероятность поглощения в состоянии 3; заметим, что $p_{33} \neq 1$;

p_{35} — вероятность перехода из состояния 3 в состояние опасного отказа;

p_{44} — вероятность поглощения в состоянии отказа, при этом $p_{44} = 1$;

p_{55} — вероятность поглощения в состоянии отказа, при этом $p_{55} = 1$.

Применим к данной модели теорию цепей Маркова для получения средних величин. Матрица переходов для такой схемы может быть записана в виде:

	1	2	3	4	5
1	0	p_{12}	0	p_{14}	p_{15}
2	0	0	p_{23}	p_{24}	0
3	0	0	p_{33}	0	p_{35}
4	0	0	0	1	0
5	0	0	0	0	1

(1)

Приведем полученную матрицу переходных вероятностей к каноническому виду, поставив поглощающие состояния первыми [5]:

$$\mathbf{P} = \cdots \begin{pmatrix} \mathbf{I} & \mathbf{O} \\ \mathbf{R} & \mathbf{Q} \end{pmatrix} \cdots =$$

	4	5	1	2	3
4	1	0	0	0	0
5	0	1	0	0	0
1	p_{14}	p_{15}	0	p_{12}	0
2	p_{24}	0	0	0	p_{23}
3	0	p_{35}	0	0	p_{33}

(2)

Фундаментальная матрица будет вычисляться по формуле $\mathbf{N} = (\mathbf{I} - \mathbf{Q})^{-1}$.

Матрица вероятностей поглощения равна $\mathbf{B} = \mathbf{NR}$. Решение уравнений (1) и (2) достаточно объемное, чтобы быть размещено в журнальной статье, поэтому заметим только, что предложенный подход позволит определить вероятность наступления отказа и опасного отказа более точно.

Заключение. Предложенные 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.

ЛИТЕРАТУРА

1. **Сабанов А. Г.** Методы исследования надежности удаленной аутентификации //Электросвязь.— 2013.— № 4.
2. **Сабанов А. Г.** Об оценке рисков удаленной аутентификации как процесса //Электросвязь.— 2012.— № 10.
3. **Шубинский И. Б.** Основы анализа сложных систем. Учеб. пособ.— Л.: Министерство обороны СССР, 1986.
4. **Шубинский И. Б.** Функциональная надежность информационных систем. Методы анализа.— Ульяновск: Печатный двор, 2012.
5. **Кемени Дж., Снелл Дж.** Кибернетическое моделирование. Некоторые приложения /Пер.с англ. Б. Г. Миркина. Под ред. И. Б. Гутчина.— М.: Сов. радио, 1972.

Получено 01.10.13