13. *Reynolds G., Schwarzbacher A.* Th. Reducing IT Costs through the Design and Implementation of a Thin Client Infrastructure in Educational Environments, *IEE Irish Signals and Systems Conference*. Dublin, 2006, pp. 28-30.
14. *Chugrinov A.V.* Doverennye seansy svyazi i sredstva ikh obespecheniya [Trusted sessions and their means of support], *Informatsionnaya bezopasnost'* [Information Security], 2010, No. 4, pp. 54-55.
15. Tekhnologiya «Zashchishchennyy tonkiy klient» [Technology "Secure thin client", *Prezentatsiya kompanii «ANCUD»* [Company presentation "ANCUD"]. Available at: http://ancud.ru/presentation.html (Accessed 13 November 2014).
16. *Gatchin Yu.A., Teploukhova O.A.* Realizatsiya kontrolya tselostnosti obraza operatsionnoy sistemy, zagruzhaemogo po seti na tonkiy klient [Implementation monitoring the integrity of the operating system image that is loaded over the network to the thin client], *Sbornik tezisov dokladov kongressa molodykh uchenykh. Elektronnoe izdanie* [The book of abstracts of the Congress of young scientists. Electronic edition]. St. Petersburg: Universitet ITMO, 2015.
17. *Hocking M.* Feature: Thin client security in the cloud, *Network Security,* 2011, Issue 6, pp. 17-19.

Статью рекомендовал к опубликованию к.т.н. А.П. Еремеев.

Тищенко Евгений Николаевич – ФГБОУ ВПО «РГЭУ (РИНХ)»; e-mail: celt@inbox.ru; 344002, г. Ростов-на-Дону, ул. Большая Садовая, 69; тел.: 89281440403; профессор; зав. кафедрой.

Буцик Кирилл Александрович – e-mail: akademik@spark-mail.ru; тел.: 89094084213; аспирант.

Деревяшко Вадим Вадимович – e-mail: godzevs@mail.ru; тел.: 89185340736; аспирант.

Tishenko Evgeniy Nikolaevich – FGBOU VPO "RSUE (RINH)"; e-mail: celt@inbox.ru; 69, Bolshaya Sadovaya street, Rostov-on-Don, 344002, Russia; phone: +79281440403; professor; head of department.

Butsik Kirill Alexandrovich – e-mail: akademik@spark-mail.ru; phone: +79094084213; postgraduate student.

Derevyashko Vadim Vadimovich – e-mail: godzevs@mail.ru; phone: +79185340736; postgraduate student.

УДК 004.771

Р.В. Сёмин, В.А. Новосядлый

ИССЛЕДОВАНИЕ ЗАДАЧИ АКТИВНОГО АУДИТА ПАРОЛЬНОЙ ПОЛИТИКИ В КОМПЬЮТЕРНЫХ СЕТЯХ

На настоящий момент угрозам информационной безопасности в компьютерных сетях уделяется большое внимание. Различные утечки баз данных с паролями показывают, что даже хорошо построенная система безопасности может быть уязвима по причине слабой парольной политики. Для обнаружения слабых сторон в парольной безопасности применяются методы активного аудита, а именно тесты на проникновение. В статье рассматривается непосредственно фаза атаки на объекты компьютерной сети. На результаты проведения тестов могут негативно влиять ряд факторов, которые приводят к возникновению так называемых «ложных срабатываний», вызванных ненадёжностью или недостаточной скоростью работы тех или иных узлов сети. К таким факторам, например, относится как само использование компьютерных сетей, так и использование прокси-серверов при проведении аудита. Особое внимание уделяется именно влиянию прокси-серверов на систему проведения аудита. Цель данного исследования – выявление характерных особенностей процесса активного аудита парольной политики и конструирование

математической модели, которая учитывает вероятность возникновения «ложных срабатываний» и позволяет её минимизировать. Вводятся понятия сбоя и успеха соединения при проведении теста на проникновение, используя случайную величину, показывающую вероятность установления успешных параллельных соединений через прокси-сервер. На основе созданной модели можно успешно найти необходимое пороговое значение максимально возможного количества параллельных соединений в секунду в необходимый момент времени суток. Это необходимо для того, чтобы максимизировать скорость проведения тестов на проникновение и в то же самое время минимизировать количество «ложных срабатываний».

Активный аудит; тесты на проникновение; математическая модель; соединения через прокси-сервер; удалённый аудит.

R.V. Semin, V.A. Novosiadlyi

ON THE PROBLEM OF ACTIVE AUDIT IN COMPUTER NETWORKS

Nowadays, computer security in computer networks is of great importance. Password leaks show that even if one construct a good security network there is always a possibility of security penetration due to weak passwords or password policy. Active security audit and its main tool – penetration testing – are capable of detecting weak points in password security. The process of active audit faces a number of issues that can affect audit results by causing false failures. One of the main issues is the usage of proxy servers. The goals of the article is to study the process of active password audit and to create a mathematical model that takes into account the probability of false failures and minimizes them. The mathematical model defines the probability of "failed" and "success" attempts of penetration tests using a random variable that shows the probability of parallel successful connections via proxy server. We assume it to have Gaussian distribution and find its EV and standard deviation on an experimental basis. Using the constructed model, we can find the maximum amount of successful connections per second at the exact time of day in order to maximize the speed of penetrations tests while having minimum amount of false failures.

Active audit; penetration testing; mathematical model; proxy server connection; remote audit.

Введение. Обеспечение информационной безопасности носит комплексный характер и содержит в себе как технические, так и организационные меры. По результатам "Trustwave 2013 Global Security Report" наиболее часто несанкционированный доступ к информации получается удаленно, в том числе через SQL-инъекцию. Основная цель атак – данные кредитных карт и адреса электронной почты. Проведенный анализ паролей, полученных в результате тестов на проникновение, показывает, что слабые пароли, наподобие "Welcome1", "Password1", "Hello123" все еще часто используются. Аналогичные выводы делаются и в отчете Министерства внутренней безопасности США.

Таким образом, можно сделать вывод, что угрозы слабой парольной защиты являлись и до сих пор являются одними из наиболее часто упоминаемых и встречающихся в компьютерных сетях. Этой угрозе были подвержены такие известные компьютерные системы, как LinkedIn, Steam и Hotmail, Yahoo, Gmail.

Надёжный канал, обеспечивающий конфиденциальность передаваемой информации, система авторизации, предотвращающая несанкционированный доступ, – всё это не позволяет обеспечить безопасность информации, если имеет место неграмотная политика паролей пользователей. Для уменьшения этой угрозы применяется периодический аудит безопасности. К сожалению, в большинстве случаев аудит ограничивается проверкой параметров парольной политики (требования к длине пароля, наличия в нём специальных символов и т.д.). Подобный аудит не обнаруживает угрозу слабой парольной защиты там, где парольная политика не действует или не может быть применена. Например, вычислительные средства, не входящие в домен, домашние ПК, коммутационное оборудование, пароли на шифрованные разделы и файлы и т.д.

Аудит требований парольной политики является частью пассивного аудита [6]. Сложность его проведения невысока, и на данный момент разработано достаточно много комплексов пассивного аудита как свободно распространяемых (Watcher, Open-AudIT), так и коммерческих (Nipper Studio, PVS). Для того чтобы устранить недостатки пассивного аудита, применяется "активный аудит" [6], немаловажной частью которого является так называемый "Penetration Testing", или "Испытание на проникновение" [11]. С точки зрения выявления слабой парольной защиты эти действия заключаются в обнаружении сетевых сервисов, доступных для подключения изнутри сети или снаружи неё, в зависимости от целей аудита.

Для выполнения активного аудита парольной защиты компьютерной системы применяется следующий комплекс шагов:

1. Определение перечня проверяемых узлов компьютерной сети.
2. Определение перечня проверяемых сервисов.
3. Обнаружение доступных сервисов из списка на проверяемых узлах.
4. Активная проверка существования угрозы слабой парольной защиты на обнаруженном сервисе.

Отдельным вопросом является определение того, какую парольную защиту следует относить к слабым. В рамках данного исследования будем считать защиту слабой, если нам удалось подобрать учётные данные для доступа к сервису с использованием словарей.

Активный аудит. Активный аудит состоит из набора различных тестов на проникновение, которые представляют собой реальные атаки на реальные компоненты системы, с использованием средств и каналов, часто используемых злоумышленниками.

Цель данного исследования – выявление характерных особенностей процесса активного аудита парольной политики, возникающих при проведении тестов на проникновение. Результаты тестов на проникновение могут дать важную информацию о степени защищённости системы. В то же самое время такие испытания достаточно трудоёмки и требуют дополнительной подготовки и предварительного учёта и оценки возможных рисков, с целью минимизировать риск причинения вреда тестируемой системе, поскольку последствия таких тестов могут не лучшим образом сказаться на работоспособности системы и её компонентов.

Тест на проникновение можно разделить на четыре фазы:

- планирование, – фаза, в которой задаются основные правила и цели теста. Непосредственно тесты в этой фазе не проводятся;
- обнаружение, – фаза, включающая в себя две подфазы. Первая представляет собой уже непосредственно тестирование, где происходит сбор информации и сканирование, проводится опознавание открытых портов и служб. Вторая подфаза – анализ уязвимостей, как человеческий, ручной, так и автоматический, который включает в себя сверку информации, полученной в первой подфазе, с базами данных уязвимостей;
- атака – ключевая фаза теста на проникновение. В большинстве случаев успешно использованная уязвимость не даёт максимальных привилегий для атакующего, а всего лишь расширяет его возможности. Атака проводится снова и снова до исчерпания всех возможностей и проверки всех потенциальных уязвимостей. В то время как предыдущая фаза только предоставляет информацию о возможных уязвимостях, фаза атаки даёт чёткий ответ и, в случае успеха, подтверждает наличие уязвимости;
- отчёт, – фаза, которая активна на протяжении всех остальных трёх фаз теста и собирает критическую информацию, характеризующую систему со стороны различных аспектов безопасности.

При проведении активного аудита возникает ряд особенностей, которые следует учесть для тщательного и качественного проведения аудита.

Во-первых, сеть и канал, в которых проводится тестирование, могут быть недостаточно надёжны. Во время проведения аудита следует учитывать необходимость повторного тестирования соединений в случае неудачи, с целью минимизировать влияние сторонних негативных факторов на соединение.

Во-вторых, проведение аудита может быть сопряжено с необходимостью использования прокси-серверов, как собственных, так и общедоступных. Собственные нужны, в первую очередь, благодаря тому, что позволяют легко вести статистику соединений, не нагружая функциональностью систему проведения аудита. В то же самое время, прокси-серверы налагают дополнительные трудности, сопряжённые как с дополнительным негативным влиянием на канал, так и текущим положением в сфере общедоступных прокси-серверов. Под негативным влиянием на канал подразумеваются дополнительные затраты времени, необходимые для установления соединения через прокси-сервер, а также скорость реагирования самого сервера, учёт его нагрузки и возможный отказ соединения в связи с перегруженностью. Под текущим положением понимается неполное несоответствие значительного процента общедоступных прокси-серверов протоколу, в частности неполное информирование об ошибке соединения с удалённым хостом.

Произведён выборочный анализ прокси-серверов протокола SOCKS 5, находящихся в свободном доступе. Результаты анализа приведены в табл. 1.

Таблица 1

Результаты анализа прокси-серверов на соответствие протоколу

База данных прокси-серверов	Размер выборки	Соответствуют протоколу, %
http://www.hidemyass.com/	40	62,5
http://hideme.ru/	19	68,4
http://www.socks-proxy.net/	50	64

Кроме того, прокси-серверы SOCKS5, функциональность которых предоставляется SSH-серверами, также не соответствует протоколу.

Математическая модель. В первую очередь, необходимо составить модель сети, в которой будет происходить аудит. В неё должны входить непосредственно вычислительное средство, с которого будет выполняться активный аудит, набор прокси-серверов, через которые будет происходить соединение с удаленными объектами исследуемой на уязвимости сети, и сами удаленные объекты. Схема представлена на рис. 1.

Обозначим через «Прокси 1», «Прокси 2»,…, «Прокси N» прокси-серверы протокола SOCKS5, которые будут использованы в системе. Через «Удаленный сервер 1», «Удаленный сервер 2»,…, «Удаленный сервер N» обозначим объекты исследуемой сети.

Вследствие неполного соответствия прокси-серверов протоколу невозможно точно классифицировать причину отрицательного результата при попытке установить соединение между системой, с которой инициирован аудит, и удаленным сервером. Причины могут быть следующие:

- отказ удалённого сервера (например, соединение было заблокировано межсетевым экраном);
- неожиданный обрыв соединения в силу программно-аппаратной ошибки на линии и её узлах;

- перегруженность прокси-сервера на момент попытки установления соединения;
- невозможность установить соединение и, как следствие, отказ установить соединение по прошествии времени ожидания/n-попыток установить соединение.

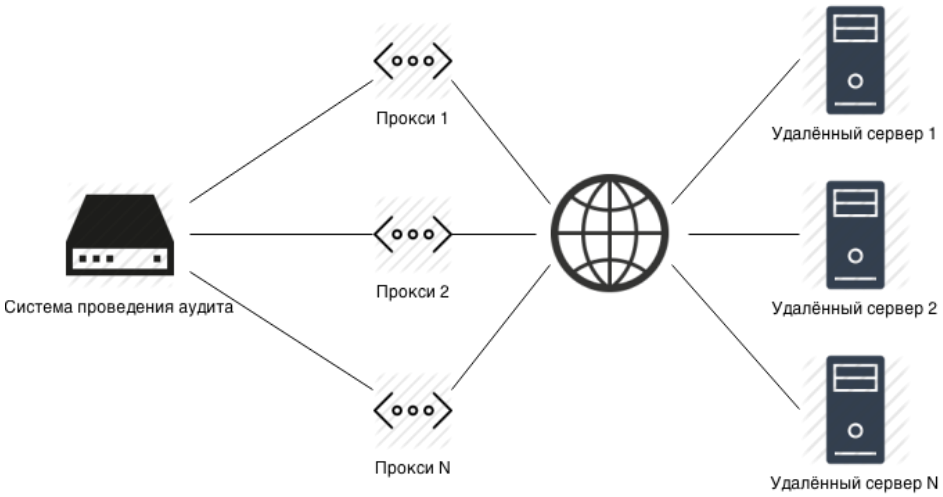

Рис. 1. Схема взаимодействия системы с объектами аудита

Сбоем прокси-сервера назовём событие, при котором был получен отрицательный результат попытки установить соединение с удалённым сервером. Следовательно, успехом назовём любое другое событие.

Введём вероятность успеха j-го прокси-сервера при n параллельных соединениях как случайную величину, зависящую от времени t и от количества соединений n, которые система собирается установить через данный прокси-сервер. Обозначим её как $Pr^j{}_{p-success}(t,n)$.

Данную вероятность в силу удаленности прокси-серверов следует устанавливать экспериментально. Для этого необходимо вести суточную статистику по прокси-серверам. Разобьём сутки на l промежутков.

Каждому промежутку поставим в соответствие весовую функцию $H_i'(t)$, которую определим позже.

Тогда вероятность успеха j-го прокси-сервера можно представить следующим образом:

$$Pr^j{}_{p-success}(t,n) =$$
$$= \sum_{i=-l+1}^{0} H_i'(b,t)P_{i+24}^j(n) + \sum_{i=1}^{l} H_i'(b,t)P_i^j(n) +$$
$$+ \sum_{i=l+1}^{2l} H_i'(b,t)P_{i-24}^j(n),$$

где $P_i^j(n)$ – случайная величина, показывающая вероятность того, что n-е параллельное соединение к доступному удаленному хосту будет успешным через j-й прокси-сервер в промежуток времени i. Соединения необходимо устанавливать к серверу, с которым успешное соединение гарантировано. Исходя из особенностей этой случайной величины, допустим, что она распределена по закону Гаусса.

В результате экспериментов необходимо выяснить две её характеристики – математическое ожидание и дисперсию. Наличие 1-го и 3-го слагаемых обусловлено необходимостью иметь корректное представление вероятности в начале и в конце суток. Для этого, также сделано допущение о схожести поведения соединения с прокси-серверов на протяжении 3-х суток.

Указанные величины будем вычислять, основываясь на следующем эксперименте: в *i*-й промежуток времени будем устанавливать максимально возможное количество соединений, повторяя процесс m раз, последовательно. Результат любого повторения будет слабо влиять на результат остальных. Будем вычислять математическое ожидание следующим образом:

$$M_i^j = \frac{\sum_{k=1}^{m} n_k}{m},$$

где n_k – количество соединений, установленных успешно на k-м из m повторений в промежуток времени i.

Далее в экспериментах было выбрано значение $m = 100$ и $l = 24$.

Среднеквадратичное отклонение будем вычислять по следующей формуле:

$$D_i^j = \sqrt{\frac{\sum_{k=1}^{m} n_k^2}{m} - \left(\frac{\sum_{k=1}^{m} n_k}{m}\right)^2}.$$

Таким образом, получаем:

$$P_i^j(n) = \frac{1}{D_i^j\sqrt{2\pi}} e^{\frac{-(n-M_i^j)^2}{2\left(D_i^j\right)^2}}.$$

Определим теперь весовую функцию $H_i'(t)$ как прямоугольную функцию, выраженную через аналитическое представление сглаженной функции Хевисайда:

$$H_i'(t) = \frac{1}{1+e^{-(t-i+1)}} - \frac{1}{1+e^{-(t-i)}},$$

где i = 1…24.

Весовая функция достигает своего максимального значения при $t = i + \frac{1}{2}$.

Экспериментально найдём математическое ожидание и дисперсию для выбранных 3-х прокси-серверов. На протяжении суток, каждый час, равновероятно в течение часа, будем проводить по 10 экспериментов для каждого прокси-сервера. За один эксперимент будем устанавливать 100 параллельных соединений.

Имея вероятности $Pr^j{}_{p-success}(t,n)$, введём $Pr^j{}_{parallel}(t,n)$ – вероятность установления *n* параллельных соединений на *j*-м прокси-сервере:

$$Pr^j{}_{parallel}(t,n) = \sum_{k=n}^{m} Pr^j{}_{p-success}(t,k).$$

Кроме вероятности успешности *n*-го соединения необходимо знать время, которое затрачивается на установку *n* параллельных соединений через *j*-й прокси-сервер. Для этого на тех же l промежутках введём функцию, показывающую скорость установлений соединения *n* параллельных соединений через *j*-й прокси-сервер в момент времени t:

$$C^j(t,n) = \sum_{i=1}^{l} T_i^j(n)\, H_i'(t),$$

где $T_i^j(n)$ – математическое ожидание случайной величины, показывающей время, необходимое на установление соединения при *n* параллельных соединениях для *j*-го прокси-сервера в промежуток времени *i*. Будем вычислять математическое ожидание следующим образом:

$$T_i^j(n) = \frac{\sum_{k=1}^{m} t_k^n}{m},$$

где t_k^n – время, потребовавшееся для установления соединения на k-м из m повторений.

Основную задачу будем ставить следующим образом – для набора прокси-серверов требуется подобрать такое значение n, при котором работа системы была наиболее эффективной, а именно, количество успешных соединений в секунду было максимальным, а количество неуспешных минимальным. Таким образом, в определённый момент времени t для j-го прокси-сервера необходимо решить следующую задачу оптимизации:

$$\frac{Pr^j{}_{parallel}(t,n)}{C^j(t,n)} \to max.$$

Решение этой задачи позволит оптимальным образом подбирать параметры функционирования системы активного аудита для того, чтобы обеспечить максимальную скорость проверки удаленных серверов при минимальном количестве сбоев, вызванных ограничением работы прокси-сервера.

Построим графики модели для n = 1,10,20,30…100 (рис. 1). Заметим, что в разное время суток оптимальными будут различные значения n.

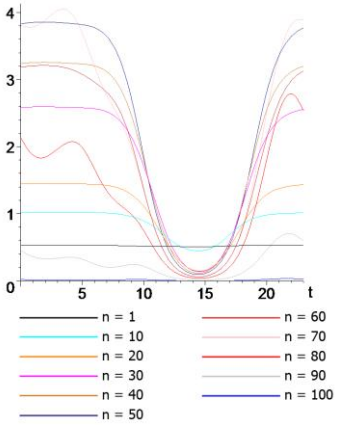

Рис. 1. Поведение модели при различных значениях n

Заключение. Исследована эффективность активного аудита парольной защиты в компьютерных сетях. Выявлены основные особенности, встречающиеся при проведении тестов на проникновение в сети, а именно: возможные сбои, связанные с загруженностью сети и её сегментов, приводящие к ложным результатам тестирования; отказ или некорректный ответ прокси-сервера, который может не соответствовать протоколу SOCKS5, также приводящие к некорректному выводу о результатах аудита.

В результате создана математическая модель системы активного аудита парольной политики в компьютерных сетях. Её основная характеристика – вероятность успеха n-го параллельного соединения через прокси-сервер. Полагая, что эта случайная величина имеет нормальное распределение, экспериментально вычислены математическое ожидание и дисперсия в разные временные промежутки тестирования модели. Введена случайная величина – вероятность установления n параллельных соединений для прокси-сервера. В итоге была сформулирована и решена задача оптимизации, отвечающая на вопрос – сколько задач аудита выполнять параллельно в момент времени t для достижения максимальной эффективности системы, а именно для максимизации такого показателя, как количество успешно завершённых задач в секунду.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Trustwave 2013 Global Security Report. http://www2.trustwave.com/rs/trustwave/ images/2013-Global-Security-Report.pdf.
2. *Coburn T.* The Federal Government's Track Record on Cybersecurity and Critical Infrastructure. http://www.hsgac.senate.gov/download/?id=8BC15BCD-4B90-4691-BDBA-C1F0584CA66A.
3. BBC News – LinkedIn passwords leaked by hackers. http://www.bbc.com/news/ technology-18338956.
4. BBC News – Valve's online game service Steam hit by hackers. http://www.bbc.co.uk/ news/technology-15690187.
5. *Fildes J.* BBC News – Technology – Scam hits more e-mail accounts. http://news.bbc.co.uk/ 2/hi/technology/8292299.stm.
6. *Rogers R., Ed Fuller E., Greg Miles G.* Network Security Evaluation. Using the NSA IEM. Syngress, 2005.
7. Watcher: Web security testing tool and passive vulnerability scanner. http://websecuritytool. codeplex.com.
8. Open-AudIT – The network inventory, audit, documentation and management tool. http://www.open-audit.org.
9. Network Security Audit Software for Firewalls, Switches and Routers. https://www.titania.com /nipperstudio.
10. Monitor Network Traffic Using The Passive Vulnerability Scanner. www.tenable.com/ products/passive-vulnerability-scanner.
11. *Scarfone K., Souppaya M., Cody A., Orebaugh A.* Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-115, 2008. – 80 c.
12. *Sayana S.A.* Approach-to-Auditing-Network-Security. Information Systems Audit and Control Association, 2003.
13. *Krutz R.L., Vines R.D.* Penetration Testing. The CISSP® and CAPCM Prep Guide: Platinum Edition. John Wiley & Sons, 2006.

REFERENCES

1. Trustwave 2013 Global Security Report. Available at: http://www2.trustwave.com/rs/ trustwave/images/2013-Global-Security-Report.pdf.
2. *Coburn T.* The Federal Government's Track Record on Cybersecurity and Critical Infrastructure. Available at: http://www.hsgac.senate.gov/download/?id=8BC15BCD-4B90-4691-BDBA-C1F0584CA66A.
3. BBC News – LinkedIn passwords leaked by hackers. Available at: http://www.bbc.com/news/ technology-18338956.
4. BBC News – Valve's online game service Steam hit by hackers. Available at: http://www.bbc.co.uk/news/technology-15690187.
5. *Fildes J.* BBC News – Technology – Scam hits more e-mail accounts. Available at: http://news.bbc.co.uk/2/hi/technology/8292299.stm.
6. *Rogers R., Ed Fuller E., Greg Miles G.* Network Security Evaluation. Using the NSA IEM. Syngress, 2005.
7. Watcher: Web security testing tool and passive vulnerability scanner. Available at: http://websecuritytool.codeplex.com.
8. Open-AudIT – The network inventory, audit, documentation and management tool. Available at: http://www.open-audit.org.
9. Network Security Audit Software for Firewalls, Switches and Routers. Available at: https://www.titania.com/nipperstudio.
10. Monitor Network Traffic Using The Passive Vulnerability Scanner. Available at: http://www.tenable.com/products/passive-vulnerability-scanner.
11. *Scarfone K., Souppaya M., Cody A., Orebaugh A.* Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-115, 2008, 80 p.

12. *Sayana S.A.* Approach-to-Auditing-Network-Security. Information Systems Audit and Control Association, 2003.
13. *Krutz R.L., Vines R.D.* Penetration Testing. The CISSP® and CAPCM Prep Guide: Platinum Edition. John Wiley & Sons, 2006.

Статью рекомендовал к опубликованию д.ф.-м.н., профессор В.С. Пилиди.

Сёмин Роман Вячеславович – ФГАНУ НИИ "Спецвузавтоматика"; e-mail: r.semin@niisva.org; 344002, г. Ростов-на-Дону, пер. Газетный, 51; тел.: 88632012817; м.н.с.

Новосядлый Василий Александрович – e-mail: nova@niisva.org; к.ф.-м.н.; зав. лаб.

Semin Roman Viacheslavovich – FSASE SRI "Specvuzavtomatika"; e-mail: v.grezin@niisva.org; 51, Gazetnyi, Rostov-on-Don, 344002; phone: +78632012817; junior research assistant.

Novosiadlyi Vasilii Aleksandrovich – e-mail: nova@niisva.org; cand. of phys.-math. sc.; head of lab.