УДК 621.391.18

А.В. Козленко, В.С. Авраменко, И.Б. Саенко, А.В. Кий

МЕТОД ОЦЕНКИ УРОВНЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД В КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ ГРАФА ЗАЩИЩЕННОСТИ

Козленко А.В., Авраменко В.С., Саенко И.Б., Кий А.В. **Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности.**
Аннотация. В работе показана актуальность проблемы оценки уровня защиты информации от несанкционированного доступа в компьютерных сетях. Целью работы является разработка метода оценки уровня защиты информации от несанкционированного доступа в компьютерных сетях на основе графа защищенности. Разработанный метод обеспечивает повышение эффективности управления защитой информации в компьютерных сетях за счет комплексного показателя защищенности, а также применения графа защищенности, учитывающего реальную структуру компьютерной сети и системы защиты информации.
Ключевые слова: информация, оценка уровня защиты, несанкционированный доступ, компьютерная сеть, коэффициент защищенности, граф защищенности.

Kozlenko A.V., Avramenko V.S., Saenko I.B., Kiy A.V. **Method of assessing the level of information protection against unauthorized access in computer networks on the basis of the security graph.**
Abstract. In this paper the urgency of the problem of assessing the level of information protection against unauthorized access in computer networks is shown. The purpose of the paper is the development of the method of assessing the level of information protection against unauthorized access in computer networks on the basis of the security graph. The developed method provides the increase in information security management efficiency in computer networks due to complex security metric, and also application of the security graph which considers real structure of a computer network and information security system.
Keywords: information, assessing the protection level, unauthorized access, computer network, security coefficient, security graph.

1. Введение. Нарушение нормального функционирования компьютерных сетей большинства промышленных, правительственных, банковских, оборонных и правоохранительных организаций вследствие несанкционированного доступа (НСД) к обрабатываемой в них информации влечет за собой значительный ущерб. Достижение научно-обоснованного уровня защиты информации от НСД обуславливает необходимость проведения оценки данного уровня на всех этапах жизненного цикла компьютерных сетей при различной степени полноты и достоверности имеющейся информации. Целью работы является разработка метода оценки уровня защиты информации от НСД в компьютерных сетях, обеспечивающего повышение эффективности управления защитой информации в организациях за счет комплексного показателя, учитывающего как характеристики процесса нарушений

безопасности, так и характеристики процесса защиты, а также применение графа защищенности, учитывающего реальную структуру компьютерной сети и системы защиты информации (СЗИ).

2. Релевантные работы. На современном этапе становление научного направления, связанного с исследованием и оценкой уровня защиты информации от НСД в компьютерных сетях, сдерживается отсутствием единого понятийного аппарата в области защиты информации от НСД, преобладанием в руководящих документах качественных подходов к оценке уровня защиты, ориентацией на статические условия функционирования систем защиты. Аттестация автоматизированных систем, сертификация средств вычислительной техники согласно требованиям действующих нормативных документов (руководящих документов ФСТЭК России, ГОСТ Р ИСО/МЭК 15408-2008, ГОСТ Р ИСО/МЭК 17799-2005) требует высокой квалификации персонала, обработки больших объемов данных и значительных временных затрат. К качественным подходам также можно отнести метод оценки уровня защиты информации от НСД на основе построения деревьев атак [1–3], основным недостатком которого является экспоненциальный рост времени на проведение оценки уровня защиты больших АС.

В условиях стремительного развития информационных технологий постоянно возникают новые виды угроз, что, в свою очередь, приводит к появлению новых уязвимостей программного и аппаратного обеспечения как самих компьютерных сетей, так и средств защиты информации. В таких условиях более перспективными являются количественные методы оценки уровня защиты информации от НСД.

Среди известных отечественных и зарубежных методик количественной оценки уровня защиты информации от НСД наибольшее распространение получил подход на базе анализа информационных рисков [4], в частности, модель системы обеспечения безопасности Клементса [5]. На основе анализа рисков созданы такие средства оценки защищенности как *Microsoft Baseline Security Analyzer* (*MBSA*) [6],*CRAMM, CounterMeasures, BCM-Analyser* [7], а также отечественные «Гриф» и «Риск Менеджер» [7]. Однако у данного подхода есть ряд существенных недостатков, а именно: не учитывается реальная структура компьютерной сети и СЗИ; стоимость потерь от несанкционированного доступа к информации оценивается в денежных единицах, что не всегда приемлемо; не полностью учитывается вариативность сценариев реализации НСД и динамические характеристики процесса защиты информации.

3. Описание метода. Уровень защиты информации в компьютерной сети от НСД определяется защищенностью каждого защищаемого ресурса. Для решения задачи оценки уровня защиты информации от НСД целесообразно использовать комплексные показатели защищенности, учитывающие как процессы нарушения безопасности ресурсов в компьютерной сети, так и процессы контроля и восстановления их защищенного состояния. В качестве такого показателя будем использовать коэффициент защищенности информации от НСД [8].

Предлагаемый метод оценки уровня защиты информации от НСД в компьютерных сетях состоит из следующих этапов (рис. 1):

1) сбор и анализ исходных данных;

2) расчет показателей защищенности отдельных ресурсов;

Рис. 1. Метод оценки уровня защиты информации от НСД в компьютерных сетях

3) построение графов защищенности по типам угроз безопасности информации;

4) расчет показателей защищенности всей информации в компьютерной сети;

5) оценка уровня защиты информации от НСД в компьютерной сети по выбранному критерию;

6) выработка рекомендаций по обеспечению требуемого уровня защиты информации от НСД в компьютерной сети должностным лицам, ответственным за защиту информации в организации.

Исходными данными для оценки уровня защиты информации от НСД в компьютерной сети являются:

1) перечень защищаемых ресурсов и их местоположение;

2) состав и параметры функционирования средств защиты ресурсов (количество, местоположение, защищаемые ресурсы, способ организации защиты);

3) интенсивности нарушений безопасности информационных ресурсов, рассчитываемые отдельно для трех основных типов угроз безопасности информации — угроз конфиденциальности, целостности и доступности (в расчете на наихудший случай, когда нарушитель «идеальный», т.е. имеет высокую квалификацию, отслеживает появление новых уязвимостей и способен мгновенно использовать их для НСД к информации, интенсивность нарушений безопасности ресурсов соответствует интенсивности появления уязвимостей в программно-аппаратном обеспечении компьютерной сети);

4) интенсивности восстановления защищенности ресурсов (зависят от количества должностных лиц, ответственных за защиту информации в организации, и от уровня их квалификации; также рассчитываются отдельно для трех основных типов угроз безопасности информации).

Также на этапе анализа исходных данных проводится анализ структуры, параметров и алгоритмов функционирования компьютерной сети.

После анализа исходных данных производится расчет показателей защищенности отдельных ресурсов. При этом для расчета коэффициентов защищенности ресурса используются следующие выражения:

$$K_{\text{зщ}}^{\text{К}} = \frac{\mu_{\text{вз}}^{\text{К}}}{\lambda_{\text{нб}}^{\text{К}} + \mu_{\text{вз}}^{\text{К}}}, K_{\text{зщ}}^{\text{Ц}} = \frac{\mu_{\text{вз}}^{\text{Ц}}}{\lambda_{\text{нб}}^{\text{Ц}} + \mu_{\text{вз}}^{\text{Ц}}}, K_{\text{зщ}}^{\text{Д}} = \frac{\mu_{\text{вз}}^{\text{Д}}}{\lambda_{\text{нб}}^{\text{Д}} + \mu_{\text{вз}}^{\text{Д}}}; \quad (1)$$

где $K_{\text{зщ}}^{\text{К}}, K_{\text{зщ}}^{\text{Ц}}, K_{\text{зщ}}^{\text{Д}}$ — коэффициенты защищенности ресурсов от угроз конфиденциальности, целостности и доступности, соответственно;

$\lambda_{\text{нб}}^{\text{К}}, \lambda_{\text{нб}}^{\text{Ц}}, \lambda_{\text{нб}}^{\text{Д}}$ — интенсивности нарушений конфиденциальности, целостности и доступности ресурсов, соответственно;

$\mu_{вз}^{К}, \mu_{вз}^{Ц}, \mu_{вз}^{Д}$ — интенсивности восстановления защищенности для конфиденциальности, целостности и доступности ресурсов, соответственно.

Для краткости запишем выражение (1) в виде

$$K_{зщ}^{К,Ц,Д} = \frac{\mu_{вз}^{К,Ц,Д}}{\lambda_{нб}^{К,Ц,Д} + \mu_{вз}^{К,Ц,Д}}, \quad (2)$$

и в дальнейшем будем пользоваться такой формой записи.

Для расчета показателей защищенности всей информации в компьютерной сети предложим подход, ориентированный на использование графов защищенности по типам угроз безопасности информации. Под *графом защищенности компьютерной сети* будем понимать совокупность связанных элементов, характеризующих состояние защищенности ее ресурсов [9].

Граф защищенности строится на основе анализа структуры, параметров и алгоритмов функционирования компьютерной сети, проведенном при анализе исходных данных. Данный этап требует высокой квалификации персонала и относительно больших временных затрат, поэтому основной объем работ по построению графов защищенности по типам угроз безопасности информации рекомендуется проводить на этапе проектирования компьютерной сети. В этом случае на этапе эксплуатации компьютерной сети для получения графов защищенности по типам угроз безопасности информации необходимо уточнить графы защищенности, полученные на этапе проектирования в соответствии с изменениями структуры, параметров и алгоритмов функционирования компьютерной сети, произошедшими к данному моменту эксплуатации.

При анализе компьютерной сети на предмет защищенности в первую очередь следует учитывать наличие альтернативных средств защиты (АСЗ), а также наличие ресурсов и/или способов их использования, эквивалентных по пригодности для достижения цели функционирования компьютерной сети. При этом следует руководствоваться следующими правилами [9]:

1) если для достижения цели функционирования компьютерной сети требуется защищенное состояние всех ресурсов (нарушение функционирования компьютерной сети происходит при нарушении безопасности хотя бы одного ресурса) и при этом для защиты ресурсов не используются дополнительные АСЗ (используемое средство или несколько средств защиты преодолеваются за счет использования уязвимости одного типа в одном или нескольких средствах защиты), а

также отсутствуют альтернативные с точки зрения защищенности резервные ресурсы (например, альтернативные по уязвимостям резервные программные и технические средства автоматизации), то такой компьютерной сети ставится в соответствие последовательный граф защищенности;

2) если для защиты ресурса кроме основного используются дополнительные средства защиты, альтернативные основному по способу защиты от реализации угроз, то такому ресурсу соответствует параллельный граф защищенности, число элементов в котором соответствует общему числу средств защиты данного ресурса;

3) если при нарушении безопасности ресурса имеются варианты решения соответствующей задачи компьютерной сети с использованием другого альтернативного ресурса (защищаемый ресурс компьютерной сети резервирован структурно, функционально и т. д.), то при допущении о нарушении безопасности в один момент времени только в отношении одного ресурса основной и резервные ресурсы образуют резервированную группу. В этом случае им ставится в соответствие параллельный граф защищенности.

В общем случае граф защищенности компьютерной сети может содержать как последовательные, так и параллельные соединения. Графы защищенности целесообразно строить отдельно для основных типов угроз безопасности информации — угроз конфиденциальности, целостности и доступности.

На основе построенных графов защищенности по типам угроз безопасности информации и рассчитанных показателей защищенности отдельных ресурсов проводится этап расчета показателей защищенности информации в компьютерной сети.

Выражения для расчета показателей защищенности информации в компьютерной сети для общего случая при допущении о том, что нарушения безопасности отдельных ресурсов являются независимыми событиями, можно получить, используя теорему умножения для независимых событий. При этом для последовательного соединения:

$$K_{\text{зщ КС}}^{\text{К,Ц,Д}} = \prod_{i=1}^{N_{\text{зр}}} K_{\text{зщ}\,i}^{\text{К,Ц,Д}}, \qquad (3)$$

где $K_{\text{зщ КС}}^{\text{К,Ц,Д}}$ — коэффициенты защищенности компьютерной сети;

$N_{\text{зр}}$ — количество защищаемых ресурсов;

$K_{\text{зщ}\,i}^{\text{К,Ц,Д}}$ — коэффициенты защищенности i-го ресурса.

Для параллельного соединения имеем:

$$K_{\text{зщ КС}}^{\text{К,Ц,Д}} = 1 - \prod_{i=1}^{N_{\text{зр}}} (1 - K_{\text{зщ } i}^{\text{К,Ц,Д}}) . \quad (4)$$

Для последовательного соединения при наличии неограниченных ресурсов на восстановление защищенности ресурсов для расчета коэффициентов защищенности может использоваться следующее выражение:

$$K_{\text{зщ КС}}^{\text{К,Ц,Д}} = \prod_{i=1}^{N_{\text{зр}}} \left(\frac{\mu_{\text{вз}}^{\text{К,Ц,Д}}}{\lambda_{\text{нб}}^{\text{К,Ц,Д}} + \mu_{\text{вз}}^{\text{К,Ц,Д}}} \right) . \quad (5)$$

При ограниченных ресурсах на восстановление защищенности (в один момент времени восстанавливается защищенность только одного ресурса) для последовательного соединения коэффициенты защищенности определяются следующим выражением:

$$K_{\text{зщ КС}}^{\text{К,Ц,Д}} = \frac{1}{\sum_{i=1}^{N_{\text{зр}}} \frac{N_{\text{зр}}!}{(N_{\text{зр}} - 1)!} \left(\frac{\lambda_{\text{нб}}^{\text{К,Ц,Д}}}{\mu_{\text{вз}}^{\text{К,Ц,Д}}} \right)^i} . \quad (6)$$

При резервировании ресурсов и применении АСЗ основных и резервных ресурсов граф защищенности имеет последовательно-параллельную структуру, а коэффициенты защищенности определяются следующим выражением:

$$K_{\text{зщ КС}}^{\text{К,Ц,Д}} = \prod_{i=1}^{N_{\text{зр}}} \left(1 - \prod_{j=0}^{N_{\text{рр}}^i} \prod_{k=0}^{N_{\text{асз}}^i} \left(1 - K_{\text{зщ } ijk}^{\text{К,Ц,Д}} \right) \right), \quad (7)$$

где $N_{\text{рр}}$ — количество резервных защищаемых ресурсов в резервированной группе;

$N_{\text{асз}}$ — количество АСЗ;

$K_{\text{зщ } ijk}^{\text{К,Ц,Д}}$ — коэффициенты защищенности i-го ресурса в j-й резервированной группе с применением k-го средства защиты.

Для последовательно-параллельного графа защищенности при постоянном использовании одинакового количества АСЗ($N_{\text{асз}}$) дополнительно к основным средствам($N_{\text{сз}}$), а также при одинаковых интенсивностях нарушения безопасности ресурсов и интенсивностях восстановления защищенности ресурсов расчетная формула имеет следующий вид:

$$K_{\text{зщ КС}}^{\text{К,Ц,Д}} = \left(1 - \left(1 - \frac{\mu_{\text{вз}}^{\text{К,Ц,Д}}}{\lambda_{\text{нб}}^{\text{К,Ц,Д}} + \mu_{\text{вз}}^{\text{К,Ц,Д}}}\right)^{N_{\text{сз}}+N_{\text{асз}}}\right)^{N_{\text{зр}}}. \quad (8)$$

После расчета показателя защищенности всей информации в компьютерной сети производится оценка уровня защиты информации от НСД по принятому критерию, после чего выявляются «узкие» места в системе защиты. Затем на основе полученных результатов разрабатываются рекомендации по обеспечению требуемого уровня защиты информации, адресованные должностным лицам, ответственным за защиту информации в компьютерной сети.

4. Пример реализации метода. Приведем пример оценки уровня защиты информации от НСД на основе предлагаемого метода. Рассмотрим следующий типовой вариант компьютерной сети организации. Положим, что каждый сотрудник организации имеет автоматизированное рабочее место (АРМ), функционирующее под управлением операционной системы *Microsoft Windows 7*, на которой находятся его пользовательские данные. В организации имеется 50 таких АРМ. Все АРМ объединены в компьютерную сеть с четырьмя серверами на базе операционной системы *Microsoft Windows 2008 Server*, на которых функционирует общесистемное и прикладное программное обеспечение (почтовый сервер, СУБД, *Web*-сервер, мгновенная система обмена сообщениями и т. д.). Два сервера объединены в отказоустойчивый кластер. Один из серверов является сервером единого времени.

Проведем анализ исходных данных. Критичные с точки зрения безопасности информации ресурсы расположены следующим образом: каждое АРМ содержит один критически важный защищаемый ресурс. Два сервера (С–1 и С–2), объединенных в отказоустойчивый кластер, обеспечивают функционирование СУБД *MS SQL Server 2008*и почтового сервера *MS Exchange Server 2010*организации. Следовательно, они содержат два защищаемых ресурса. Третий сервер (С–3), обеспечивающий функционирование *Web*-сервера предприятия и мгновенной системы обмена сообщениями, содержит два защищаемых ресурса. Четвертый сервер (С–4) выделен для функционирования системы единого времени и, следовательно, имеет один защищаемый ресурс. Для защиты указанных ресурсов от НСД используются одно основное средство защиты (СЗ) информации (для каждого пользователя и администратора предусмотрен личный пароль для входа в систему) и одно дополнительное АСЗ (аутентификация пользователей и администраторов по смарт-карте).

Для определения интенсивности нарушений безопасности ресурсов компьютерной сети организации проведен анализ общедоступной статистики по обнаружению уязвимостей в ОС *Windows* за последний год (использовалась база уязвимостей *National Vulnerability Database* [10]). Данный анализ показал, что интенсивность нарушений конфиденциальности информацииприблизительноравна9,96 нарушений/месяц ($\lambda_{нб}^{К} = 0{,}0138$ час$^{-1}$), интенсивность нарушений целостности информации — 9,75($\lambda_{нб}^{Ц} = 0{,}0135$ час$^{-1}$), интенсивность нарушений доступности информации —10,04($\lambda_{нб}^{Д} = 0{,}0139$ час$^{-1}$). Предположим, что должностные лица организации, ответственные за защиту информации, имеют численный состав и квалификацию, позволяющие восстанавливать конфиденциальность, целостность и доступность любого количества ресурсов за 3 часа.

Для расчета показателей защищенности отдельных ресурсов применим выражение (2). Тогда рассчитанные коэффициенты защищенности для пользовательских данных на АРМ равны: $K_{зщ\,РС}^{К} = 0{,}96$, $K_{зщ\,РС}^{Ц} = 0{,}961$, $K_{зщ\,РС}^{Д} = 0{,}96$.

Построим графы защищенности компьютерной сети организации от угроз конфиденциальности, целостности и доступности информации (приведены на рис. 2, 3 и 4, соответственно).

Применим правила расчета показателя защищенности всей информации в компьютерной сети с использованием рассчитанных значений показателей защищенности отдельных ресурсов.

На основе построенных графов защищенности по типам угроз безопасности информации и выражений (3), (4) и (8)получим для коэффициентов защищенности компьютерной сети от угроз конфиденциальности, целостности и доступности информации, соответственно, следующие значения: $K_{зщ\,КС}^{К} = 0{,}845$, $K_{зщ\,КС}^{Ц} = 0{,}849$ и $K_{зщ\,КС}^{Д} = 0{,}997$.

Контроль защищенности информации, обрабатываемой в компьютерной сети организации, по критерию пригодности $K_{зщ\,КС}^{К,Ц,Д} > 0{,}99$ позволяет сделать вывод о том, что система защиты информации от НСД в рассматриваемой компьютерной сети в целом не позволяет обеспечить требуемый уровень защиты. Он, в частности, достигнут лишь для одного типа угроз безопасности информации.

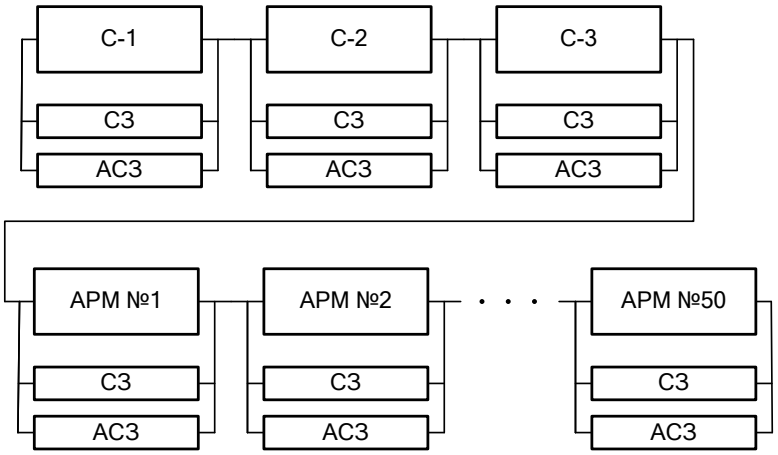

Рис. 2. Граф защищенности компьютерной сети организации от угроз конфиденциальности информации

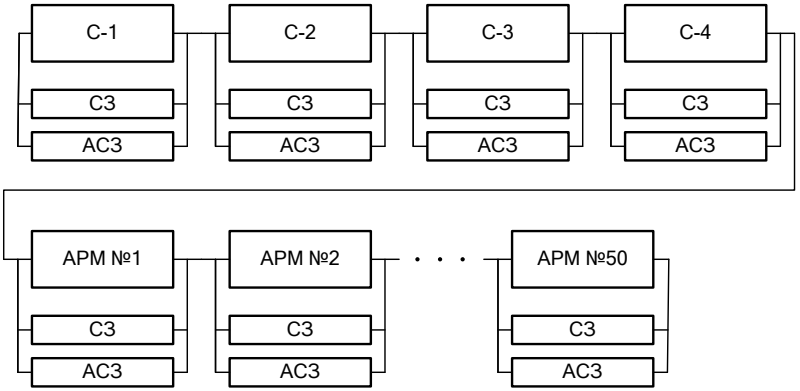

Рис. 3. Граф защищенности компьютерной сети организации от угроз целостности информации

Для достижения требуемого уровня защиты необходимо провести комплексные организационно-технические мероприятия. Например, при повышении квалификации администраторов безопасности до уровня, позволяющего восстанавливать защищенность ресурсов за

30 минут, коэффициенты защищенности повышаются до следующих значений: $K^{К}_{зщ\,КС} = 0{,}995$, $K^{Ц}_{зщ\,КС} = 0{,}995$ и $K^{Д}_{зщ\,КС} = 0{,}999$.

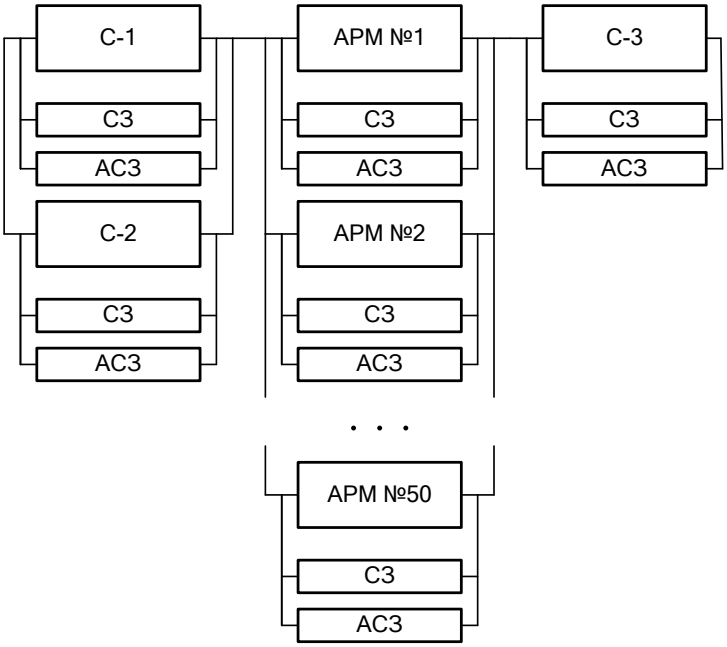

Рис. 4. Граф защищенности компьютерной сети организации от угроз доступности информации

При добавлении дополнительного АСЗ (например, контроль доступа по отпечатку пальца) коэффициенты защищенности возрастают еще больше до следующих значений: $K^{К}_{зщ\,КС} = 0{,}999$, $K^{Ц}_{зщ\,КС} = 0{,}999$ и $K^{Д}_{зщ\,КС} = 0{,}999$.

5. Заключение. Для решения задачи количественной оценки уровня защиты информации от НСД в компьютерных сетях разработан метод на основе графа защищенности, который, в отличие от уже использующихся, учитывает динамику и стохастическую неопределенность всех основных процессах защиты информации, а также реальную структуру компьютерной сети и СЗИ при расчете показателей защищенности; обеспечивает возможность получения количественных

оценок уровня защиты для различных типов угроз безопасности информации.

По мнению авторов, цель работы достигнута. Данный подход может представлять интерес как для разработчиков систем защиты информации, так и для должностных лиц, ответственных за защиту информации от НСД в организациях.

Литература

1. *Котенко И.В., Степашкин М.В., Богданов В.С.* Анализ защищенности компьютерных сетей на различных этапах их жизненного цикла // Изв. вузов. Приборостроение. Т.49, № 5, 2006, С.3–8.
2. *KotenkoI., Stepashkin M.* Attack Graph based Evaluation of Network Security // Lecture Notes in Computer Science, Vol. 4237, 2006. P.216–227.
3. *Котенко И.В., Степашкин М.В., Дойникова Е.В.* Анализ защищенности автоматизированных систем с учетом социоинженерных атак // Проблемы информационной безопасности. Компьютерные системы. 2011, № 3, С.40–57.
4. *Шумский А.А., Шелупанов А.А.* Системный анализ в защите информации: учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности. М.: Гелиос-АРВ, 2005. 224 с.
5. *Анищенко В.В., Криштофик А.М.* О необходимости разработки моделей защищенности объектов информационных технологий // Информатика, №1, 2005.
6. Microsoft Baseline Security Analyzer (MBSA) [электронный ресурс http:// www.microsoft.com/technet/security/tools/mbsahome.mspx].
7. *Сафонов А.* Практическое применение методов и средств анализа рисков // Информационная безопасность,№3, 2010. С. 42–43.
8. *Авраменко В.С., Козленко А.В.* Модель для количественной оценки защищенности информации от несанкционированного доступа в автоматизированных системах по комплексному показателю // Труды СПИИРАН, №13, 2010. С. 172–181.
9. *Авраменко В.С.* Модели защищенности информации от несанкционированного доступа в многорежимных автоматизированных системах и методы ее контроля в условиях неопределенности угроз // Информация и космос, №2, 2008. С. 87–95.
10. National Vulnerability Database Version 2.2 [электронный ресурс http://nvd.nist.gov].

Козленко Андрей Владимирович — адъюнкт Военной академии связи. Область научных интересов: оценивание и контроль защищенности информации, программирование, разработка комплексов программ. Число научных публикаций — 23. et-ak@yandex.ru; Военная академия связи, Тихорецкий проспект, 3, Санкт-Петербург, 194064, РФ; р.т. +7(812)247-9842.Научныйруководитель — В.С. Авраменко.

Kozlenko Andrey Vladimirovich — post-graduate student, Military academy of communications. Research interests: the information security estimation and control, programming, software complex development. The number of publications — 23. et-ak@yandex.ru; Military academy of communications, Tihoretskiy broad street, 3, St. Petersburg, 194064, Russia; office phone +7(812)247-9842. Scientific adviser — V.S. Avramenko.

Авраменко Владимир Семенович — канд. техн. наук, доцент; профессор кафедры Военной академии связи. Область научных интересов: автоматизированные системы управления, современные информационные технологии, оценивание и контроль защи-

щенности информации, автоматическое обнаружение нарушений безопасности информации на основе информационных образов, методы биометрической аутентификации. Число научных публикаций — 99. vsavr@yandex.ru; Военная академия связи, Тихорецкий проспект, 3, Санкт-Петербург, 194064, РФ; р.т. +7(812)247-9342.

Avramenko Vladimir Semenovich — PhD in Technical sciences, associate professor; professor, Military academy of communications. Research interests: automated control systems, modern information technologies, the information security estimation and control, automatic detection of information security violations on the basis of information images, biometric authentication methods. The number of publications — 99.vsavr@yandex.ru; Military academy of communications, Tihoretskiy broad street, 3, St. Petersburg, 194064, Russia; office phone +7(812)247-9342.

Саенко Игорь Борисович — д-р техн. наук, проф.; ведущий научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН. Область научных интересов: автоматизированные информационные системы, информационная безопасность. Число научных публикаций —250. ibsaen@mail.ru; СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Saenko Igor Borisovich — Ph.D., Doctor of Technical Sciences, professor; leading research scientist of laboratory of computer network security, SPIIRAS. Research interests: automated information systems, information security. The number of publications — 250. ibsaen@mail.ru; SPIIRAS, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Кий Андрей Вячеславович — адъюнкт Военной академии связи. Область научных интересов: разграничение доступа к информации. Число научных публикаций — 13. kiyarmy@rambler.ru; Военная академия связи, Тихорецкий проспект, 3, Санкт-Петербург, 194064, РФ; р.т. +7(812)247-9842.Научныйруководитель — Я.М. Копчак.

Kiy Andrey Vyacheslavovich — post-graduate student, Military academy of communications. Research interests: access control of information. The number of publications — 13.kiyarmy@yandex.ru; Military academy of communications, Tihoretskiy broad street, 3, St. Petersburg, 194064, Russia; office phone +7(812)247-9842. Scientific adviser — Y.M. Kopchak.

Рекомендовано СПИИРАН, заведующий научно-исследовательской лабораторией проблем компьютерной безопасности Котенко И.В., д-р техн. наук, проф.
Статья поступила в редакцию 23.03.2012.

РЕФЕРАТ

Козленко А.В., Авраменко В.С., Саенко И.Б., Кий А.В. **Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности.**

Нарушение нормального функционирования компьютерных сетей большинства промышленных, правительственных, банковских, оборонных и правоохранительных организаций вследствие НСД к обрабатываемой в них информации влечет за собой значительный ущерб. Достижение научно-обоснованного уровня защиты информации от НСД обуславливает необходимость проведения оценки данного уровня на всех этапах жизненного цикла компьютерных сетей при различной степени полноты и достоверности имеющейся информации. Целью работы является разработка метода оценки уровня защиты информации от несанкционированного доступа в компьютерных сетях, обеспечивающего повышение эффективности управления защитой информации в организациях за счет комплексного показателя, учитывающего как характеристики процесса нарушений безопасности, так и характеристики процесса защиты, а также применение графа защищенности, учитывающего реальную структуру компьютерной сети и системы защиты информации.

Для решения задачи количественной оценки уровня защиты информации от НСД в компьютерных сетях разработан метод на основе графа защищенности. Граф защищенности строится на основе анализа структуры, параметров и алгоритмов функционирования компьютерной сети, проведенном при анализе исходных данных. В общем случае граф защищенности компьютерной сети может содержать как последовательные, так и параллельные соединения.

Произведена оценка уровня защиты информации от НСД на основе предлагаемого метода на примере типовой локальной компьютерной сети организации. Выработаны рекомендации по обеспечению требуемого уровня защиты информации от НСД в компьютерной сети должностным лицам, ответственным за защиту информации в организации.

Разработанный метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности, в отличие от уже использующихся, учитывает динамику и стохастическую неопределенность всех основных процессов защиты информации, а также реальную структуру компьютерной сети и системы защиты информации при расчете показателей защищенности; обеспечивает возможность получения количественных оценок уровня защиты для различных типов угроз безопасности информации как на этапе разработки, так и на этапе эксплуатации компьютерных сетей.

По мнению авторов, цель работы достигнута. Данный подход может представлять интерес как для разработчиков систем защиты информации, так и для должностных лиц, ответственных за защиту информации от НСД в организациях.

SUMMARY

Kozlenko A.V., Avramenko V.S., Saenko I.B., Kiy A.V. **Method of assessing the level of information protection against unauthorized access in computer networks on the basis of the security graph.**

Violation of normal operation of computer networks for the majority of the industrial, governmental, bank, defensive and law-enforcement organizations owing to unauthorized access to the information, which is processed in them, involves a considerable damage. Achieving scientific and reasonable level of information protection against unauthorized access requires the assessment of the level at all stages of the life cycle of computer networks with varying degrees of completeness and accuracy of the information available. The goal of the paper is to develop a method for assessing the level of information protection against unauthorized access in computer networks, to ensure better management of the protection of information in organizations through integrated indicator that takes into account both the characteristics of security violation process, and characteristics of security process and also application of security graph, taking into account the real structure of a computer network and information security systems.

To meet the challenge of measuring the level of information protection against unauthorized access to computer networks, a method based on security graph is developed. The security graph is based on the analysis of the structure, parameters, and operation algorithms for a computer network, held in the analysis of the initial data. In general, the security graph for a computer network can contain both serial and parallel connections.

Assessment of the level of information protection against unauthorized access is made on the basis of the proposed method for the typical corporative LAN. Recommendations to ensure the required level of information protection against unauthorized access to computer network are made for officials responsible for the protection of information in the organization.

The developed method of assessing the level of information protection against unauthorized access in computer networks, on the basis of the security graph, in contrast to the already used takes into account the dynamics and stochastic uncertainty in all major processes of information protection, as well as the real structure of a computer network and information security system in calculating indicators of protection; provides the ability to obtain quantitative estimates of the level of protection for different types of threats to information security both at the stage of development and exploitation of computer networks.

According to the authors, the goal of the article is reached. The given approach can be of interest both for developers of information security systems and for the officials responsible for information security from unauthorized access in the organizations.