49. *Dalla Preda M., Christodorescu M., Jha S.,Debray S.* Semantic-based approach to malware detection // Proc. of the 34th Annual ACM SIGPLAN-SIGACT Symp.on Principles of Programming Languages, 2007, p. 377-388.

50. *Варновский Н.П., Захаров В.А., Кузюрин Н.Н., Шокуров А.В., Подловченко Р.И., Щербина В.С.* О применении методов деобфускации программ для обнаружения сложных компьютерных вирусов // Известия ТРТУ, Таганрог, Изд-во ТРГУ, 2006, т. 7, с. 66-72.

51. *Madou M., Anckaert B., De Sutter B., De Bosschere K.* Hybrid static-dynamic attacks against software protection mechanisms // Proc. of the 5th ACM Workshop on Digital Rights Management, 2005, p. 75-82.

52. *Collberg, C.S. Myles G., Huntwork A.* Sandmark - a tool for software protection research // IEEE Security & Privacy, v. 1, N 4, 2003, p. 40-49.

53. *Madou, M.; Van Put, L.; De Bosschere, K.* Loco: an interactive code (de)obfuscation tool // Proc. of ACM SIGPLAN 2006 Workshop on Partial Evaluation and Program Manipulation, 2006.

**В.В. Анищенко, Ю.В. Земцов**
Беларусь, г. Минск, ОИПИ НАН Беларуси

## МЕТОДИКА ИСПЫТАНИЙ СИСТЕМ ОБНАРУЖЕНИЯ АТАК

В настоящее время многие исследовательские и коммерческие организации тестируют и оценивают системы обнаружения атак (СОА) для определения эффективности каждого продукта, сравнения их друг с другом и обоснования выбора лучшего из них. Многие системные администраторы и администраторы безопасности также производят свои собственные оценки таких продуктов, чтобы принять решение о целесообразности их использования в своих средах. Однако подобные оценки СОА обычно включают в себя неформальное сравнение заявляемых разработчиками функциональных возможностей и, в лучшем случае, проверку относительных признаков сигнатур программных продуктов, т. е. производится определенное количество запланированных атак на тестируемую сеть, а испытатель подсчитывает количество сигналов тревоги действительно соответствующих производимым атакам, а также количество ложных сигналов тревоги. Результаты такого теста могут дать общее представление о сигнатурах, но они не дают точной оценки и не обеспечивают доверительные данные для того, чтобы делать заключение о преимуществе в эффективности той или иной системы [1]. В условиях обилия предложений СОА и отсутствия объективных критериев их оценки крайне тяжело сделать обоснованный выбор. Таким образом, особенно актуальна задача разработки методики испытаний СОА, основанной на формальных моделях и позволяющей получить для функциональных возможностей СОА количественные оценки.

Для оценки функциональных возможностей СОА существует ряд методик. Например, методика, предназначенная для оценки функциональных возможностей СОА, встраиваемых в канал связи и перехватывающих весь сетевой трафик на входе в защищаемую сеть, т.е. анализ данных с целью обнаружения атак выполняется в СОА на основе информации, собираемой на уровне сети. Однако существуют СОА, в которых применяются не только датчики уровня сети, но и датчики уровня операционной системы, предназначенные для сбора данных с целью обнаружения атак, не выявляемых на сетевом уровне [2]. Сбор данных на уровне операционной системы подразумевает получение информации о событиях критичных для обеспечения безопасности в защищаемой сети на основе последовательностей системных вызовов, сведений об использовании ресурсов системы, записей из журналов аудита операционной системы и журналов приложений и т.д. Кроме то-

го, в СОА анализ собранной датчиками информации может осуществляться децентрализовано, на основе нескольких компонент СОА, в каждой из которых может быть реализован свой метод анализа. Существуют более универсальные методики оценки функциональных возможностей СОА, применимые к большему количеству классов СОА. Основу подобных методик, как правило, составляет система качественных показателей, отражающих наличие или отсутствие тех или иных функциональных механизмов в СОА.

Основным достоинством указанных методик является возможность достаточно подробно проанализировать функциональные свойства СОА на предмет соответствия политике безопасности, используемой в защищаемой сети, вне зависимости от архитектуры СОА и реализованных в ней методов обнаружения атак. Однако использование только качественных и отсутствие количественных показателей существенно затрудняет оценку функциональных возможностей СОА и обоснование выбора СОА для эксплуатации в конкретной защищаемой сети, особенно в случае наличия нескольких СОА с практически одинаковыми функциональными возможностями. Таким образом, оценка практической применимости СОА должна основываться на анализе выполнения требований, предъявляемых политикой безопасности информации в защищаемой сети. Степень соответствия СОА этим требованиям может быть оценена на основе двух наборов показателей, характеризующих функциональные возможности СОА [2].

Первый набор представляет собой ряд показателей, позволяющих оценить функциональность СОА, т. е. возможность ее применения в специфических условиях конкретной сети. Внутри данного набора показатели подразделены на группы в соответствии с характером требований к СОА, которые могут быть предъявлены политикой безопасности информации: показатели обнаружения, показатели безопасности, показатели реагирования [2].

Показатели обнаружения определяют соответствие СОА требованиям в части, касающейся выявления и распознавания атак:

− возможность обнаружения атак в условиях применения криптографических средств защиты информации, передаваемой по каналам связи;

− возможность обнаружения атак в режиме реального времени, т. е. выявление факта атаки непосредственно во время ее осуществления;

− возможность обнаружения атак на уровне сети и/или на уровне операционной системы;

− возможность обнаружения неизвестных атак.

Показатели безопасности определяют соответствие СОА общим требованиям, предъявляемым к программному и аппаратному обеспечению защищаемой сети с целью предотвращения попыток НСД к информации:

− применение защищенных механизмов взаимодействия между компонентами СОА для реализации функций управления;

− устойчивость к атакам;

− ограничение доступа к компонентам СОА.

Показатели реагирования определяют соответствие СОА требованиям к ее поведению в случае обнаружения атаки на защищаемую сеть:

− возможность реагирования СОА в режиме реального времени;

− пассивное реагирование;

− активное реагирование.

Второй набор включает ряд показателей, характеризующих эффективность применения СОА в защищаемой сети для обнаружения атак и реагирования на них:

− точность обнаружения атак – характеризует наличие ошибок в результатах анализа;

− производительность СОА – характеризует возможность выполнения СОА функций по обнаружению атак без чрезмерного потребления ресурсов защищаемой сети;

− полнота обнаружения атак – характеризует способность СОА обнаруживать все возможные атаки;

− оперативность обнаружения атак – характеризует способность СОА производить анализ событий и обнаруживать атаку так быстро, чтобы у СОА оставалось время обеспечить поддержку принятия решений персоналом, отвечающим за безопасность информации.

Рассмотрим методику, определяющую порядок оценки функциональных возможностей некоторой СОА при ее применении в специфических условиях конкретной сети и предоставляющую возможность принятия решения, обоснованного показателями, по выбору СОА для эксплуатации в указанной сети. В общем случае процесс оценки функциональных возможностей СОА подразделяется на два этапа: подготовительный этап и этап тестирования. Основной задачей подготовительного этапа является формулирование требований к СОА для эксплуатации в конкретной сети на основе рассмотренных качественных показателей, что позволит определить соответствие функциональных возможностей оцениваемых СОА положениям принятой в защищаемой сети политики безопасности. Формулирование требований к СОА должно производиться на основе сведений о функционировании защищаемой сети:

− данные о сетевой инфраструктуре, включающие информацию об архитектуре сети, используемых протоколах, соответствующих канальному сетевому и транспортному уровням модели взаимодействия открытых систем;

− данные о критических элементах защищаемой сети и выполняемых ими функциях (предоставляемых сетевых сервисах и доступе к сетевым ресурсам). Под критическим понимается элемент защищаемой сети, работоспособность которого является необходимым условием обеспечения нормального процесса функционирования защищаемой сети.

Анализ сведений о функционировании сети позволит создать перечень элементов сети (маршрутизаторы, серверы приложений, серверы баз данных и т.д.), возможность обнаружения атак, которые являются необходимым для СОА условием эксплуатации [3]. На основе составленного перечня элементов определяется список известных на текущий момент уязвимостей аппаратного и программного обеспечения и перечень атак, эксплуатирующих указанные уязвимости, обнаружение которых необходимо. В результате формируется тестовая выборка атак для оценки функциональных возможностей СОА. Завершается подготовительный этап определением состава стенда (перечня аппаратного и программного обеспечения), достаточного для проведения тестирования СОА и структуры стенда [4]. Основное требование, предъявляемое к стенду − предоставление возможностей по моделированию реализаций всех известных на данный момент угроз безопасности информации.

Этап тестирования включает анализ документации, развертывание оцениваемой СОА, а также проведение натурных испытаний по проверке работоспособности СОА.

В процессе анализа документации необходимо определить на основе предложенного набора показателей соответствие заявленных производителем функциональных возможностей СОА требованиям, сформулированным на подготовительном этапе.

В процессе развертывания СОА необходимо:

− определить состав и места размещения датчиков, осуществляющих сбор первичной информации, компонент анализа, компонент управления;

− установить аппаратное и программное обеспечение СОА и произвести начальную настройку СОА;

− определить соответствие определенных в СОА настроек по умолчанию политике безопасности информации защищаемой сети;

− оценить трудоемкость процесса развертывания и начальной настройки СОА.

В процессе натурных испытаний на основе сформированной тестовой выборки атак производится моделирование действий злоумышленников, направленных на получение несанкционированного доступа, а также регистрируются результаты (успешное, неуспешное) и длительность действий СОА по выявлению, распознаванию, реагированию на атаки. По завершении тестирования определяется соответствие фактических (определенных по результатам тестирования) функциональных возможностей СОА предъявленным требованиям.

По зафиксированным результатам и длительностям действий СОА и в соответствии с описанной методикой производится вычисление значений показателей точности и производительности СОА, а также показателей полноты и оперативности обнаружения атак.

Предложенная методика испытаний позволяет вне зависимости от архитектуры СОА и реализованных в ней методов обнаружения атак решать задачи сравнительного анализа систем, которые обладают схожими функциональными возможностями. Однако для того, чтобы данная методика могла применяться для доказуемой оценки СОА, она должна опираться на универсальные для любой СОА количественные показатели [5].

В данной работе предлагается новая формальная модель СОА, специально предназначенная для количественной оценки эффективности. Условимся представлять СОА как упорядоченный конечный набор взаимосвязанных величин, т. е. кортеж (**Д**анные; **С**остояния; **Ф**ункциональные признаки; **З**нания; ***В***ыбор; ***О***тображение; ***П***рофилирование; ***К***лассификация), в котором первые 4 величины являются структурами данных, а последние четыре – процедурами их обработки.

Приведем краткую характеристику элементов кортежа:

1. Источник данных **Д** для сетевой СОА представляет собой поток сетевых пакетов, а для СОА уровня операционной системы – поток системных вызовов.

2. Множество возможных состояний **С** указывает на принадлежность элемента данных, например, сетевого пакета, к штатному либо аномальному типу (возможна детализация вплоть до конкретного вида атаки).

3. Вектор функциональных признаков $\mathbf{\Phi} = (\boldsymbol{\phi}_1, \boldsymbol{\phi}_2, \ldots \boldsymbol{\phi}_n)$ содержит конечное число параметров, каждый из которых определяет одно из свойств элемента данных. Например, $\boldsymbol{\phi}_1$ может быть сетевым протоколом (TCP, UDP), а $\boldsymbol{\phi}_2$ – номером порта.

4. База знаний **З** содержит информацию о типовых профилях нормальных и/или аномальных потоков данных. Точная структура базы знаний может быть уникальной для каждой отдельно взятой СОА в зависимости от модели, положенной в основу СОА, будь то нейронная сеть, набор правил, статистическая модель, база сигнатур либо комбинация подобных моделей [6].

5. Процедура выбора функциональных признаков ***В*** предназначена для выделения наиболее существенных свойств $\boldsymbol{\phi}_i$ элементов данных.

6. Процедура отображения данных ***О*** реализует предварительное преобразование и отображение данных в пространстве функциональных признаков, т.е. ***О*****:Д → Ф.**

7. Процедура определения профилей ***П*** представляет собой процесс создания базы знаний **З** на основании информации о функциональных признаках и соответствующих им возможных состояниях.

8. Процедура классификации представляет собой операцию отображения вектора функциональных признаков в определенные состояния, т. е. ***К*****:Ф → С.**

Большинство СОА функционируют в три этапа: выбор функциональных признаков, определение профилей и собственно обнаружение. Выбор функциональных признаков является одной из первичных процедур при разработке СОА и обычно выполняется только единожды. Как только функциональные признаки определены, можно перейти к процедуре определения профилей, которая должна осуществляться на обучающей выборке достаточно большого объема. Данное действие может выполняться как однократно для создания базы, так и многократно для ее актуализации и настройки. Собственно процедура обнаружения выполняет основную функцию СОА и осуществляется на протяжении всего жизненного цикла системы.

Для простоты изложения далее ограничимся рассмотрением СОА, основывающейся на обнаружении аномальной активности, т. е. множество возможных состояний которой имеет только два элемента: **С** = {*Норма*, *Аномалия*}. Введем также в рассмотрение три случайные величины *X, Y, Z*. Пусть случайная величина *X* представляет собой возможные входные данные СОА, принимая с некоторой вероятностью значения из множества **Д**. Случайная величина *Y* – сигнал тревоги СОА, принимающая с определенной вероятностью значения во множестве **С**. Случайная величина *Z* – промежуточное представление входных данных с использованием функциональных признаков из **Ф**. Таким образом, процесс обнаружения являет собой ни что иное, как цепь Маркова: $X \to Z \to Y$ (данные → преобразование → сигнал тревоги), согласно которой входные данные последовательно проходят две процедуры обработки: отображение данных ***О*** и классификацию ***К***. Соответственно, получение *Z* из *X* является результатом отображения ***О***, а дальнейшее получение *Y*, т. е. генерация сигнала тревоги, – результат классификации ***К***.

Примечательно, что анализ представленной цепи Маркова удобно проводить с помощью аппарата теории информации [7], поставив в соответствие операции кодирования процедуру отображения данных ***О***, а операции декодирования – классификацию ***К***. Однако необходимо заметить, что переопределенные нами операции кодирования и декодирования для СОА уже не будут гарантировать безошибочной передачи. Тем не менее, именно качество подобной передачи данных и будет являться ключом к количественной оценке эффективности СОА.

Воспользуемся понятиями энтропии *H* и взаимной информации *I,* чтобы определить три метрики для оценки СОА.

*Метрика 1*. Коэффициент обнаружения $\text{СОА}_{\text{обн.}}$ определяется как взвешенная взаимная информация между случайными величинами *X* и *Y*, т. е.

$$\text{СОА}_{\text{обн.}} = I(X; Y)/H(X) = 1 - (H(X|Y)/H(X)),\ \text{СОА}_{\text{обн.}} \in [0; 1].$$

Коэффициент $\text{СОА}_{\text{обн.}}$ показывает насколько правильно СОА отличает нормальные входные данные от аномальных.

*Метрика 2.* Коэффициент отображения $\text{СОА}_{\text{отобр.}}$ определяется как взвешенная взаимная информация между случайными величинами *X* и *Z*, т. е.

$$\text{СОА}_{\text{отобр.}} = I(X; Z)/H(X) = 1 - (H(X|Z)/H(X)),\ \text{СОА}_{\text{отобр.}} \in [0; 1].$$

Коэффициент $\text{СОА}_{\text{отобр.}}$ показывает, насколько полно СОА выполняет отображение данных в пространстве функциональных признаков. Например, если

$СОА_{отобр.} = 1$, то можно говорить о том, что при отображении $X \to Z$ потери существенной для СОА информации не происходит.

*Метрика 3.* Коэффициент классификации $СОА_{клас.}$ определяется как взвешенная разница взаимной информации $I(X, Y; Z)$ и $I(Y, Z)$, т. е.

$$СОА_{клас.} = 1 – (I(X, Y; Z) – I(Y, Z))/H(X) = 1 – I(X; Z|Y)/ H(X),\ СОА_{клас.} \in [0; 1].$$

Коэффициент $СОА_{клас.}$ показывает насколько значимые потери существенной для СОА информации происходят во время процедуры классификации. При $СОА_{клас.} = 1$ можно говорить об идеальной реализации процесса классификации.

Для того чтобы предложенные метрики можно было использовать на практике для количественной оценки эффективности СОА, необходим механизм перехода от данных, которые можно получить во время испытаний, например, относительные частоты атак, ложных сигналов тревоги и пропущенных атак [8], к случайным величинам *X*, *Y*, *Z*. Подобный переход возможен благодаря построению переходной матрицы для данной цепи Маркова с учетом того, что энтропия

$$H(X) = – \nu_{атак}\log(\nu_{атак}) – (1 – \nu_{атак})\log(1 – \nu_{атак.}),$$

где $\nu_{атак}$ – относительная частота атак во входных данных.

Анализ предложенных метрик для оценки эффективности СОА позволяет сделать следующие замечания по повышению эффективности СОА:

– повысить $СОА_{отобр.}$ можно путем модификации либо увеличения числа функциональных признаков **Ф** (например, добавление такого параметра как полезная нагрузка сетевого пакета), а также путем улучшения алгоритмов предварительного преобразования и отображения данных ***О*** в пространстве функциональных признаков **Ф** (например, включение этапа нормализации трафика).

– повысить $СОА_{клас.}$ можно за счет улучшения качества процедуры классификации ***К*** либо за счет повышения полноты и общности базы знаний **З**. Для СОА, основывающейся на обнаружении аномальной активности, это значит уточнение профиля штатного режима работы на обучающей выборке большого размера. Для сигнатурной СОА данная задача сводится к уточнению самих сигнатур, а также увеличению их количества с целью максимального покрытия множества известных уязвимостей.

Примечательно, что повысив коэффициенты $СОА_{отобр.}$ и $СОА_{клас.}$, мы автоматически повысим $СОА_{обн.}$ , т.к. $СОА_{обн.} = (СОА_{отобр.} + СОА_{клас.}) – 1$, тем самым повысив эффективность СОА в целом.

Таким образом, предлагаемая методика содержит метрики, которые позволяют не только количественно оценить эффективность СОА, но также в полной мере соответствуют формализованной модели СОА. Это дает возможность связывать количественные оценки с конкретными процедурами обнаружения атак, что, в свою очередь, способствует принятию обоснованных и доказуемых решений при разработке, модификации и настройке СОА.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Puketza N., Zhang K.* A methodology for testing intrusion detection systems. IEEE Transactions on Software Engineering. – 1996. – Vol. 22(10). – P. 719–729.

2. *Бородакий Ю.В., Куликов Г.В., Непомнящих А.В.* Методика оценивания функциональных возможностей систем обнаружения вторжений на основе ранжирования степени опасности атак. Информационное противодействие угрозам терроризма. – 2006. – № 7. – С. 67 – 78.

3. *Лукацкий А.В.* Обнаружение атак. – СПб.: БХВ-Петербург, 2003. – 608 с.

4. *Земцов, Ю.В.* Обнаружение аномальной активности на основе усеченной процедуры последовательного анализа. Информатика. – 2006. – № 3(11). – С. 91–100.

5. *Amoroso E., Kwapniewski R.* A Selection Criteria for Intrusion Detection Systems. – Proc. of the Ann. Computer Security Applications Conf. – 1998. – P. 280–288.

6. *Denning D.* An Intrusion Detection Model. IEEE Transactions on Software Engineering. – 1987. – Vol. 13. – P. 222–232.

7. *Guofei G., Fogla P.* Measuring intrusion detection capability: an information-theoretic approach. ACM Symposium on Informaion, Computer and Communications Security. – 2006. P. 90–101.

8. *McHugh J.* Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory. ACM Transactions on Information and System Security. – 2000. – P. 262–294.

**Е.В. Горковенко**
Казахстан, г. Алматы, Институт проблем информатики и управления

## ОРГАНИЗАЦИЯ ИНТЕРФЕЙСА И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ С МАНДАТНЫМ УПРАВЛЕНИЕМ ДОСТУПА

Технология создания безопасного канала предусматривает как шифрование данных, так и разграничение доступа к сетевым ресурсам. Контроль доступа пользователей к ресурсам локальной сети должен осуществляться в соответствии с политикой безопасности организации, которой принадлежит локальная сеть. Эффективное разграничение доступа к сетевым ресурсам может быть обеспечено только при надежной аутентификации всех пользователей. При взаимодействии с физически удаленными пользователями значительно сложнее обеспечить доступ к сетевым ресурсам только лиц, имеющих на это определенные полномочия. При удаленном взаимодействии важна надежная аутентификация и пользователя и оборудования, поскольку подмена пользователя или маршрутизатора приводит к тому, что данные из корпоративной сети могут передаваться не тем лицам, которым они предназначены, что ведет к реализации несанкционированного доступа (НСД). В классических моделях мандатного управления доступом процесс проецирования прав на защищаемые субъекты осуществляется логически, на основе вывода (да/нет) об аутентичности субъекта. Это наиболее уязвимое место, которое разработчики информационных систем пытаются устранить за счет организации различных схем аутентификации субъектов, в том числе с использованием средств криптографии. Другим подходом в решении данной проблемы является создание так называемой "доверительной компьютерной базы" (ДКБ), цель которой - гарантировать защищенность вычислений заданного пространства. Практика доказывает отсутствие четких гарантий в части обеспечения безопасности ДКБ.

Предлагается рассмотреть организацию многоуровневой защиты, отвечающей полномочной политике информационной безопасности и реализовывающей функции защиты в сетевом многопользовательском варианте в распределенных компьютерных системах. Организация интерфейса в информационных системах с мандатным управлением – доступом (рис.1) направлена, с одной стороны, на выполнение запросов пользователей к информационным ресурсам, а с другой, на поддержку работы администратора без нарушения правил доступа по разрешению запросов к информации различного уровня секретности. Интерфейс организован таким образом, что администратор имеет возможность работать только с базой данных многоуровневой защиты, однако не имеет непосредственного доступа к информационных ресурсам.

Интерфейс пользователя включает в себя:

- процесс аутентификации пользователя;
- формирование текущего запроса к информационным ресурсам;