Забезпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах

УДК 681.513

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЯ

Александр Архипов, Андрей Ишутин*

*Национальный технический университет Украины «КПИ», *Компания UMC*

Анотація: **Оглянуто існуючі системи виявлення вторгнень, надана їх класифікація. Розглядаються методи та моделі виявлення аномалій, приведено декілька алгоритмів виявлення аномалій. Приведено постановку задачі розробки нової сучасної моделі виявлення вторгнень та вимоги до неї.**

Summary: **In this article the analysis of existing IDS is carried out, their classification is given, the advantages and lacks are described. The various methods of detection of anomalies are considered. The mathematical algorithms of detection of abnormal behaviour some IDS are given. The statement of a task of creation of modern model of detection of intrusions and main requirements showed to new model is given**.

Ключевые слова: **Безопасность, защита информации, системы обнаружения вторжений, методы обнаружения аномалий.**

I Введение

В настоящее время компьютерная техника используется практически во всех сферах человеческой деятельности. В современных компьютерных системах (КС) хранится и обрабатывается большое количество информации разной степени открытости: частная, коммерческая, банковская и другая. Созданные компьютерные сети являются удобным способом получения и передачи информации.

Вместе с тем растущий уровень сложности сетевых архитектур, повышение степени открытости сетей и все более тесная их привязка к Интернет делают актуальным вопрос безопасности информации. Получение несанкционированного доступа к КС, разглашение, изменение или уничтожение информации, нелегальное использование ресурсов или вывод системы из строя может иметь катастрофические последствия для собственников информации или систем. На сегодняшний день существует большое количество способов и средств несанкционированного доступа к КС: сетевые атаки, компьютерные вирусы, взломщики паролей и другие вредоносные программы.

В последние годы число информационных атак, зафиксированных в информационно-коммуникационных системах, неуклонно увеличивается [1, 2]. Причин этого явления несколько. Прежде всего, возросло количество уязвимостей, ежедневно обнаруживаемых в программном и аппаратном обеспечении КС. Кроме того, количество пользователей общедоступных сетей, в частности, Интернета, возрастает с каждым днем, причем доступ к глобальным сетям получают как отдельные клиентские рабочие станции, так и целые корпоративные сети. А с ростом числа пользователей увеличивается и количество потенциальных источников и объектов атаки. Следует также отметить, что сегодня программные средства для совершения атак стали весьма простыми, и обращение с ними не требует специальных знаний. В Интернете можно без труда найти немало программ, при помощи которых любой пользователь Сети сумеет организовать какую-либо атаку, направленную на активизацию известных уязвимостей.

Существующие на сегодняшний день средства защиты, такие как системы обнаружения вторжений (Intrusion Detection System, IDS), межсетевые экраны, различные системы разграничения доступа, антивирусные программы и другие не обеспечивают достаточный уровень защищенности КС. Основная причина в том, что большая часть этих средств способна противостоять только известным видам атак, вирусов и других нарушений безопасности.

Одним из наиболее перспективных направлений развития средств защиты информации являются системы обнаружения вторжений, использующие методы обнаружения аномалий. Изучение методов обнаружения аномалий базируется на том, что анализируя данные аудита и выявляя отклонения между текущими данными и данными, полученными за некоторый предыдущий период времени, можно различать законных и незаконных пользователей КС. Кроме того, данный подход позволяет обнаруживать авторизованных пользователей, выполняющих несанкционированные действия, т. е. злоупотребляющих своими привилегиями. Главное преимущество IDS, использующих методы обнаружения аномалий, в том,

что обнаружение не зависит от особенностей операционной системы (ОС), прикладного программного обеспечения (ПО), уязвимостей ОС и ПО, а также типов вторжения.

Рассмотрим подробнее существующие системы обнаружения вторжений и модели обнаружения аномалий.

II Классификация IDS

Классифицировать IDS можно по следующим параметрам.

По способу выявления атаки различают системы обнаружения злоупотреблений (misuse detection systems или signature-based) и системы обнаружения аномалий (anomaly detection systems или anomaly-based). Первый тип основан на сравнении информации с предустановленной базой сигнатур атак [3]. Недостаток систем данного типа – невозможность обнаружения новых, неизвестных видов атак. Второй тип основан на контроле частоты событий или обнаружении статистических аномалий [8, 13, 14]. Такие системы ориентированы на выявление новых типов атак. Недостатком является необходимость постоянного их обучения, а также высокий уровень ложных тревог.

По способу сбора информации об атаке различают network-based, host-based и application-based системы. Системы первого типа работают по типу сниффера, "прослушивая" трафик в сети и определяя возможные действия злоумышленников [4, 5]. Поиск атаки идет по принципу "от хоста до хоста". Системы второго типа, host-based, предназначены для мониторинга, детектирования и реагирования на действия злоумышленников на определенном хосте. Система, располагаясь на защищаемом хосте, проверяет и выявляет направленные против него действия. Третий тип IDS, application-based, основан на поиске проблем в определенном приложении. Кроме того, существуют гибридные IDS, представляющие собой комбинацию различных типов систем. В последнее время появились так называемые распределенные (distributed IDS, dIDS). Они состоит из множества IDS, которые расположены в различных участках большой сети и связаны между собой и с центральным управляющим сервером. Такая система усиливает защищенность корпоративной подсети благодаря способности собирать, обобщать и анализировать информацию, исходящую от разнообразных источников.

По времени анализа различают системы, работающие в реальном времени (online IDS) и системы, работающие в отложенном режиме (offline, periodic). Преимущество систем первого типа в том, что они могут зафиксировать и предотвратить атаку еще на этапе ее подготовки или на начальном этапе [6, 11]. Недостаток таких IDS – замедление (иногда существенное) работы КС. Offline-системы требуют гораздо меньше системных ресурсов. Активизируются они, как правило, в ночное или другое время, когда нагрузка на КС минимальна.

По способу реагирования различают пассивные и активные IDS. Пассивные просто фиксируют факт атаки, записывают данные в файл журнала и выдают предупреждения. Активные IDS не только определяют, но и пытаются остановить атаку, а также могут провести ответное нападение на атакующего. Наиболее распространенные типы активного реагирования – прерывание сессии и переконфигурирование межсетевого экрана.

III Математические модели обнаружения аномалий

Обнаружение вторжений остается областью активных исследований уже в течение двух десятилетий. Начало этому направлению было положено в 1980 г. статьей Джеймса Андерсона "Мониторинг угроз компьютерной безопасности" [7]. Несколько позже, в 1987 г. это направление было развито публикацией статьи "О модели обнаружения вторжения" Дороти Деннинг (Dorothy Denning) [8]. Она обеспечила методологический подход, вдохновивший многих исследователей и заложивший основу для создания коммерческих продуктов в области обнаружения вторжений. Ею была разработана универсальная модель экспертной системы обнаружения вторжения в реальном времени (IDES). Модель основывается на гипотезе, что нарушение безопасности может быть обнаружено путем мониторинга записей аудита системы на предмет аномальности ее работы. Универсальность модели заключается в том, что она не зависит от особенностей той или иной системы, прикладного окружения, уязвимостей системы и программ, типов вторжения, а также способности обнаруживать нарушения безопасности в широких пределах – от попыток проникновения извне до внутренних злоупотреблений. Модель включает в себя профили представления поведения субъектов по отношению к объектам в терминах метрических и статистических моделей и правила для получения знаний об этом поведении из записей аудита для обнаружения аномального поведения.

Модель состоит из шести основных компонент:

- субъекты – инициаторы активности на целевой системе, как правило, пользователи;

- объекты – файлы, команды, устройства, программы; объекты могут группироваться в классы; можно создавать другие структуры, например базы данных;
- записи аудита – регистрация всех действий субъектов по отношению к объектам (вход пользователя, выполнения команд, доступ к файлам);
- профили – структуры, которые характеризуют субъекта по отношению к объекту в терминах статистических метрик и моделей наблюдаемых действий; профили автоматически генерируются и инициализируются из шаблонов;
- записи об аномалиях – генерируются, когда обнаруживаются аномалии;
- правила действий – то, что должно выполняться при удовлетворении некоторого комплекса условий, которые обновляют профили, обнаруживают аномальное поведение и др.

Профиль включает в себя такие понятия как метрика и статистическая модель.

Метрика – это случайная переменная X, представляющая некоторую количественную меру произошедшего за период. Периодом может быть как фиксированный интервал времени (минуты, дни, недели и др.) так и время между двумя аудит-связанными событиями (например, время между входом в систему и выходом из нее). Есть три типа метрик:

- счетчик событий (например, количество логинов в час);
- временной интервал (например, между логинами);
- измерение ресурса (например, количество напечатанных страниц).

Цель *статистической модели* – определить, является ли новое наблюдение x_{n+1} переменной X аномальным по сравнению с предыдущими наблюдениями. IDES предлагает использование следующих моделей.

1. *Операционная модель* основывается на том, что каждое новое наблюдение переменной должно укладываться в некоторых границах. Если этого не происходит, то мы имеем дело с отклонением. Допустимые границы определяются на основании анализа предыдущих значений переменной. Данная модель может использоваться, если некоторое значение метрики можно аргументированно связать с попыткой вторжения (например, количество попыток ввода пароля более 10).

2. *Модель среднего значения и среднеквадратического отклонения* базируется на том, что все, что мы знаем о предыдущих наблюдениях ($x_1, \ldots, x_n$) некоторой величины – это ее среднее значение ($\mu = \sum x_i / n$) и среднеквадратическое отклонение $\sigma = sqrt((x_1^2 + \ldots + x_n^2) / (n\text{-}1) - \mu^2)$. Тогда новое наблюдение является аномальным, если оно не укладывается в границах доверительного интервала $\mu + d*\sigma$, где d – некоторая константа. Модель применима для измерения счетчиков событий, временных интервалов и используемых ресурсов. Преимуществом модели по сравнению с операционной является независимость оценки аномальности поведения от априорных знаний. Кроме того, необходимо отметить, что аномальность поведения зависит от значения доверительного интервала, и как следствие, понятие аномальности для пользователей системы может отличаться.

3. *Многовариационная модель* аналогична модели среднего значения и среднеквадратичного отклонения, но учитывает корреляцию между двумя или большим количеством метрик (использование цифровой подписи (ЦП) и числа операцій ввода-вывода, числа выполненных процедур входа в систему и время сессии).

4. *Модель Марковского процесса* применима только к счетчикам событий, рассматривая каждый тип событий как переменную состояния и используя матрицу переходов для характеристики частот переходов между состояниями. Наблюдение является аномальным, если вероятность перехода, определенная предыдущим состоянием и матрицей перехода, очень мала. Модель применима в том случае, если рассматривается множество команд, последовательность которых важна.

5. *Модель временных серий*. Использует временные периоды вместе со счетчиками событий и измерениями ресурса, учитывающая как значения наблюдений $x_1, \ldots, x_n$, так и временные интервалы между ними. Новое наблюдение является аномальным, если вероятность его появления за временой период низка. Преимуществом данной модели является учет временного сдвига между событиями, а недостаток – накладные расходы по вычислению по сравнению с моделью среднего значения и среднеквадратичного отклонения.

Кроме перечисленных моделей, могут также использоваться и другие.

Работа Dorothy Denning оставляет открытыми множество вопросов:

- обнаруживает ли данный подход вторжения; можно ли отличить аномалии, связанные с вторжением, от аномалий, связанных с другими факторами;
- позволяет ли данный подход обнаружить большинство, если не все вторжения или значительная их часть остается необнаруженными;

- какие метрики, статистические модели и профили нужно выбрать, чтобы обеспечить наилучшую различимость аномалий; каковы для них соотношения эффективность / стоимость; какие есть связи между типами аномалий и различными методами вторжения;
- как лучше спроектировать и реализовать систему;
- feedback, т. е. как система должна реагировать на вторжения;
- социальный аспект.

Множество авторов и научных коллективов попытались найти ответы на поставленные в [8] вопросы. Были предложены различные математические модели, алгоритмы и технические реализации простых и многоуровневых систем обнаружения вторжений.

Так, в работе [9] исследовалась возможность построения автоматических инструментов для анализа безопасности данных аудита IBM систем. Целью исследования была разработка аналитических методов обнаружения вторжений путем изучения поведения пользователей в системе.

В [10] была впервые экспериментально доказана возможность различения пользователей КС на основе их шаблонов поведения, а также отличать работу нормального пользователя от имитации вторжения. В основе идеи использовались концепции теории распознавания образов.

Одна из экспертных систем обнаружения вторжений была разработана и реализована в компании "SRI International" [11]. За основу была взята модель Dorothy Denning [8]. Разработанная IDES наблюдает за действиями пользователей, групп пользователей, удаленных хостов и всей системы и обнаруживает нарушения безопасности. Кроме этого, IDES имеет rule-based компонент (т. е. некую базу знаний), который позволяет обнаруживать не только внешние атаки, но и злоупотребления авторизованных пользователей. Для обнаружения вторжения используется специальный статистический алгоритм выявления аномального поведения. Суть алгоритма в следующем.

Для каждой записи аудита, сгенерированной пользователем, IDES формирует единственное статистическое значение T^2, которое показывает суммарную степень аномальности поведения пользователя в недалеком прошлом:

$$T^2 = (S_1, S_2, ..., S_n) C^{-1} (S_1, S_2, ..., S_n)^t,$$

где $S_1, S_2, \ldots S_n$ – наблюдаемые индивидуальные параметры, C^{-1} – матрица, обратная корреляционной матрице вектора (S_1, S_2, … S_n), C_{ik} – коэффициент корреляции между S_i и S_k, (S_1, S_2, … S_n)^t – транспонированный вектор.

Каждое значение S – некоторая статистика, рассчитываемая по значениям реальных данных. Например, пусть Q – время работы с ЦП, подчиняющееся нормальному закону распределения. Наблюдая за значениями Q в записях аудита и выбирая соответствующий интервал значений Q, можно построить частотное распределение Q. Допустим, было замечено следующее:

1% значений Q попадает в интервал от 0 до 1 миллисекунд;
7% в интервал от 1 до 2;
35% в интервал от 2 до 4;
18% в интервал от 4 до 8;
28% в интервал от 8 до 16;
11% в интервал от 16 до 32.

Алгоритм преобразования Q в S следующий.

Пусть P_m – относительная частота, с которой Q принадлежит m-му интервалу, а TPROB – сумма P_m и тех значений P, которые меньше или равны P_m. Для m-го интервала s_m – такое значение, для которого вероятность появления значений нормально распределенной переменной $N(0, 1)$ с математическим ожиданием равным 0 и дисперсией 1, больших по модулю, чем s_m, равно $TPROB$:

$$P(|N(0, 1)| \geq s_m) = TPROB_m \quad \text{или}$$

$$s_m = \Phi^{-1}\left(1 - \frac{TPROB_m}{2}\right),$$

где Φ – интегральная функция распределения нормальной случайной величины $N(0, 1)$. Значение S будет большим, если Q лежит в интервале от 0 до 1 или Q > 32, или S будет близким к нулю, если Q лежит в интервале от 2 до 4. Относительная частота принадлежности Q интервалу m определяется как:

$$P_m = \frac{1}{N_k} \sum_{j=1}^{k} W_{m,j} 2^{-b(k-j)},$$

где k – количество дней, прошедших с момента первого наблюдения, используемого в формировании массива исходных данных, применяемых для оценки P_m;

b – норма распада, которая определяется половиной времени наблюдения, затраченного для формирования массива исходных данных;
$W_{m,j}$ – количество записей аудита на j-й день, для которых Q принадлежит m-му интервалу;
N_k – экспоненциально взвешенное общее количество записей аудита с момента первого наблюдения:

$$N_k = \sum_{j=1}^{k} W_j 2^{-b(k-j)},$$

W_j – общее количество записей аудита на j-й день.

Разработанная IDES в принципе позволяет обнаруживать как известные злоупотребления авторизированных пользователей, так и неизвестные атаки. Однако ряд существенных недостатков ограничивает ее применение:

- большое количество ложных сигналов о вторжении;
- сложность подбора таких параметров наблюдения, которые наиболее точно способствовали бы обнаружению вторжений, а также взаимосвязь между параметрами;
- отсутствие информации о том, какая часть атак обнаруживается;
- большая сложность масштабируемости и расширяемости;
- большая стоимость переконфигурации системы и изменения статистического алгоритма;
- сложность использования при большом количестве пользователей.

Значительные исследования в области систем обнаружения вторжений проводились в Калифорнийском Университете Дэвиса Лоуренса (Lawrence Livermore Laboratories) [4]. В 1988 году проект Haystack в Lawrence Livermore Labs реализовал ещё одну версию системы обнаружения вторжения для военно-воздушных сил Соединённых Штатов. Так же, как и предыдущая IDES, эта система анализировала контрольный след, сравнивая его с определёнными образцами. Задачами Haystack было обнаружение различных типов вторжений: попытки взлома системы, проникновение в защищенные системы, утечки информации и таких известных типов атак, как «маскарад» и отказ в обслуживании.

Авторами был предложен свой алгоритм обнаружения вторжений. Алгоритм состоит из четырех основных этапов.

Первый шаг – генерирование вектора сессии вида $X = <x_1, x_2, \ldots x_n>$, где x_i – значение некоторого наблюдаемого параметра (атрибута) (например количество файлов или время работы ЦП). Вектор сессии отображает активность пользователя в данной сессии.

На втором этапе генерируется пороговый вектор T и вектор Бернулли B:

$$T= <t_1, t_2, \ldots t_n>, \quad B = <b_1, b_2, \ldots b_n>.$$

Пороговый вектор T представляет собой пороговые значения для каждого атрибута i: $t_i = <t_{i,\,min}, t_{i,\,max}>$. Вектор Бернулли B – это просто двоичный вектор, показывающий, какой из атрибутов превышает пороговые значения для данной группы пользователей:

$$b_i = \begin{cases} 0, & t_{i,\min} \le x_i \le t_{i,\max} \\ 1, & else \end{cases}.$$

Следующий шаг – генерирование весовой метки вторжения. Сама по себе метка не имеет значения, однако, знание распределения весовых меток для всех сессий можно использовать для определения нормы подозрительности сессии. Весовой вектор вторжения $W= <w_1, w_2, \ldots w_n>$ существует для каждой группы и типа вторжения. Каждое w_i показывает важность i-го атрибута для обнаружения особого типа вторжения. Поэтому, если $w_i>w_j$, то факт, что i-й атрибут превышает порог t_i – более полезный, чем факт, что j-й атрибут превышает порог t_j. Весовая метка вторжения определяется как сумма всех w_i, где i-й атрибут превосходит его порог t_i:

$$W = \sum_{i=1}^{n} b_i w_i .$$

На последнем шаге вычисляется норма подозрительности. Норма подозрительности показывает, какой процент сессий имеет весовую метку вторжения меньшую, чем весовая метка текущей сессии:

$$sq = \sum_{j=0}^{score} P_{n,j},$$

где $P_{n,j}$ – вероятность того, что случайная сессия будет иметь весовую метку вторжения $score = j$.

Преимуществом IDS Haystack является возможность определить важность наблюдения того или иного параметра для обнаружения различных типов вторжения. Однако, практически все вопросы, поставленные

в [8], остаются здесь открытыми.

Еще один подход для обнаружения аномального поведения предлагает Terran Lane [13, 14]. Для сравнения символьных последовательностей, представляющих собой поведение пользователей, предлагается использовать специальную меру подобия. Так, для последовательностей длиной l подобие между последовательностями $X = (x_0, x_1, \ldots x_{l-1})$ и $Y = (y_0, y_1, \ldots y_{l-1})$ определяется парой функций:

$$w(X,Y,i) = \begin{cases} 0 & if \quad i < 0 \; or \; x_i \neq y_i \\ 1 + w(X,Y,i-1) & if \quad x_i = y_i \end{cases};$$

$$Sim(X,Y) = \sum_{i=0}^{l-1} w(X,Y,i).$$

Для каждого пользователя сохраняется профиль D – набор последовательностей, выбранных из наблюдаемых действий:

$$Sim_D(X) = \max_{Y \in D} \{Sim(Y,X)\}.$$

Недостатком данного подхода является необходимость сохранять большое количество данных для каждого пользователя, т. е. все его последовательности. Авторы предлагают два метода для уменьшения объема баз последовательностей: в первом сохраняются не все образцы последовательностей, а, например, только последние n. Второй – метод кластеризации, при котором база последовательностей преобразуется в базу представителей классов элементов.

IV Постановка задачи

На основе анализа различных методов обнаружения аномалий можно сделать вывод, что на сегодняшний день не существует надежного способа защиты от неизвестных атак. Это также подтверждается тем фактом, что в настоящее время не существует системы обнаружения вторжений, работающих только по принципу обнаружения аномалий. Объясняется это рядом причин.

Во-первых, большинство предложенных методов обнаружения аномалий основываются на моделях, разработанных много лет назад [8]. Проблема в том, что эти модели не отражают многих особенностей современного состояния отрасли IT.

Во-вторых, предложенные модели не дают ни четких ответов, ни рекомендаций по ряду ключевых вопросов, например, как выбирать параметры наблюдения, как устанавливать границы для шкал измерения и другие.

В-третьих, все IDS, работающие по принципу обнаружения аномалий, имеют серьезные недостатки, которые ограничивают их широкое применение. Главные из них – это высокий уровень ложных тревог и необходимость обучения, сложность реконфигурации системы при введении нового субъекта наблюдения.

Поэтому, актуальной задачей на сегодняшний день является разработка новой, современной модели обнаружения вторжений, на основе которой в дальнейшем можно было бы спроектировать и реализовать систему обнаружения вторжений. Такая модель должна учитывать современный уровень аппаратного и программного обеспечения КС и давать ответы на ключевые вопросы:

- кто или что является субъектом/объектом наблюдения;
- какие действия в системе подлежат регистрации, наблюдению и анализу;
- какие существуют взаимосвязи между событиями, как они учитываются;
- какое поведение системы является нормальным, а какое – аномальным;
- какие используются методы измерения и как устанавливаются граничные параметры;
- как можно исключить или значительно уменьшить уровень ложных тревог;
- как исключить или минимизировать проблемы, связанные с добавлением новых субъектов/объектов;
- какие типы и методы вторжения обнаруживаются данной моделью.

Кроме этого, новая модель должна по возможности предложить решение тех проблем, которые ограничили бы ее практическое применение.

V Заключение

В работе проведен анализ существующих IDS, дана их классификация, описаны преимущества и недостатки. Приведены математические алгоритмы обнаружения аномального поведения некоторых IDS, приведена постановка задачи создания современной модели обнаружения вторжений и главные требования, предъявляемые к новой модели. Целью дальнейшего исследования является разработка указанной модели и ее практическая реализация.

Литература: ***1.*** *The CERT Coordination Center (CERT/CC), a center of Internet security expertise, http://www.cert.org/stats/cert_stats.html, 2005.* ***2.*** *Ю. Машевский, Перелом в развитии вредоносных программ, http://www.viruslist.com/ru/analysis.pubid=166969803, 29. 07. 2005.* ***3.*** *Lindqvist, Ulf & Porras, Phillip A. Detecting Computer and Network Misuse Through the Production-Based Expert System Toolset (P-BEST). Proceedings of the 1999 IEEE Symposium on Security and Privacy. Oakland, CA, May 9 – 12, 1999.* ***4.*** *Mukherjee, Biswanath; Heberlein, L. Todd; & Levitt, Karl N. (University of California, Davis). Network Intrusion Detection. IEEE Network 8, 3 (May/June 1994): 26 - 41.* ***5.*** *Vigna, Giovanni & Kemmerer, Richard A. (University of California, Santa Barbara). NetSTAT: A Network-Based Intrusion Detection Approach. Proceedings of the 14th Annual Computer Security Applications Conference. Scottsdale, AZ, Dec. 1998.* ***6.*** *Paxson, Vern. (Lawrence Berkeley National Laboratory). Bro: A System for Detecting Network Intruders in Real-Time, Proceedings of 7th USENIX Security Symposium. San Antonio, TX, January 1998.* ***7.*** *J. P. Anderson, Computer Security Threat Monitoring and Surveillance, James P. Anderson Co., Fort Washington, Pa. 1980.* ***8.*** *D. E. Denning, An Intrusion Detection Model, IEEE Trans. Software Eng., vol. 13, no. 2, Feb. 1987.* ***9.*** *H. S. Javitz, A. Valdes, D. E. Denning, and P. G. Neumann. Analytical Techniques Development for a Statistical Intrusion Detection System (SIDS) Based on Accounting Records. Technical report, SRI International, Menlo Park, California, July 1986.* ***10.*** *T. F. Lunt, J. van Horne, and L. Halme. Automated Analysis of Computer System Audit Trails. In Proceedings of the Ninth DOE Computer Security Group Conference, May 1986.* ***11.*** *Lunt, Teresa F., et al. (SRI International). A Real-Time Intrusion Detection Expert System (IDES).****12.*** *An Application of Pattern Matching in Intrusion Detection. Sandeep Kumar, Eugene H.Spafford, 1994.* ***13.*** *Temporal Sequence Learning and Data Reduction for Anomaly Detection Terran Lane, Carla E. Brodley, 1998.* ***14.*** *Machine Learning Techniques for the Domain of Anomaly Detection for Computer Security Terran Lane, 1998.* ***15.*** *The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection Stefan Axelson, 1999.* ***16.*** *S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. A. Longstaff. A sense of self for UNIX processes. In Proceedings of the 1996 IEEE Symposium on Security and Privacy, pages 120 – 128, Los Alamitos, CA, 1996. IEEE Computer Society Press.* ***17.*** *S. A. Hofmeyr, S. Forrest, and A. Somayaji. Intrusion detection using sequences of system calls. Journal of Computer Security, 6:151 – 180, 1998.* ***18.*** *M. Damashek. Gauging similarity with n-grams: Languageindependent categorization of text. Science, 267:843–848, Feb. 1995.* ***19.*** *Anderson, Debra, et al. (SRI International). Detecting Unusual Program Behavior Using the Statistical Component of the NextGeneration Intrusion Detection Expert System (NIDES) (SRICSL-95 -06). Menlo Park, CA: Computer Science Laboratory, SRI International, May 1995.* ***20.*** *W. Lee and S. J. Stolfo. Data mining approaches for intrusion detection. In Proceedings of the 7th USENIX Security Symposium, 1998.* ***21.*** *R. C. Carrasco and J. Oncina. Learning stochastic regular grammars by means of a state merging method. In Proceedings of the Second International ICGI Colloquium on Grammatical Inteference and Applications, pages 139 – 152, Alicante, Spain, 1994.* ***22.*** *D. Ron, Y. Singer, and N. Tishby. The power of amnesia: Learning probabilistic automata with variable memory length. Machine Learning, 25, 1996.* ***23.*** *L. R. Rabiner. A tutorial on Hidden Markov Models and selected applications in speech recognition. Proceedings of the IEEE, 77(2):257 – 286, 1989.* ***24.*** *А. Новиков, С. Кащенко, Моделирование поведения программного обеспечения с точки зрения безопасности, Правове, нормативне та метрологічне забезпечення систем захиту інформації в Україні, вип. 2, 2001 р.* ***25.*** *Политика безопасности. Краткий обзор защитных политик, http://www.securitylab.ru/analytics/216207.php, 06. 06. 2002.* ***26.*** *А. Астахов, Разработка эффективных политик информационной безопасности, http://www.osp.ru/cio/2004/01/070.htm, 30. 01. 2004.* ***27.*** *D. Wagner, D. Dean, Intrusion Detection via Static Analysis, Proceedings of the 2001 IEEE Symposium on Security and Privacy, May 14 – 16. 2001, p. 156 – 169.* ***28.*** *Wahbe, Lucco, Anderson, Efficient Software-Based Fault Isolation, Proceedings of the Symposium on Operating System Principles, 1993.* ***29.*** *William E. Perry. Effective Methods for Software Testing, Second Edition, Wiley, 2001.*

УДК 681.3

УЗАГАЛЬНЕНІ ЗАВАДОСТІЙКІ КОДИ В ЗАДАЧАХ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ В УМОВАХ ПРИРОДНИХ ВПЛИВІВ

Вячеслав Василенко
Національний авіаційний університет

Анотація: **Для використання в задачах забезпечення цілісності інформаційних об'єктів в умовах природних впливів пропонуються узагальнені завадостійкі коді.**