3. *Иванова Т.А., Строкина Ю.Г.* Система организационно-технического управления комплексной безопасностью сложного объекта (на примере вуза) // Системы управления и информационные технологии. – 2012. – №2.1 (48). – С. 203-208.
4. *Левков А.А., Ильясов Б.Г.* Триадный подход к управлению интеллектуальными информационными системами (теоретические основы) // Вестник компьютерных и информационных технологий. – 2011. – № 4. – С. 3-6.
5. *Панин О.А.* Анализ эффективности интегрированных систем безопасности: принципы, критерии, методы // Системы безопасности. – 2006. – № 2. – С. 60-62.

Статью рекомендовал к опубликованию к.т.н. А.А. Бакиров.

Васильев Владимир Иванович – ФГБОУ ВПО «УГАТУ»; e-mail: Vasilyev@ugatu.ac.ru; г. Уфа, ул. К. Маркса, 12; тел.: 83472730672; зав. кафедрой ВТиЗИ; д.т.н.; профессор.

Иванова Татьяна Александровна – e-mail: iv_tatyana@list.ru; кафедра ВТиЗИ; к.т.н.; доцент.

Ильясов Барый Галеевич – e-mail: Ilyasov@tc.ugatu.ac.ru; тел.: 83472737835; кафедра ТК; зав. кафедрой; д.т.н.; профессор.

Vasilyev Vladimir Ivanovich – USATU; e-mail: Vasilyev@ugatu.ac.ru; 12, K. Marks street, Ufa, Russia; phone: +73472730672; the department of computer science and information security; head the department; dr. of eng. sc.; professor.

Ivanova Tatyana Aleksandrovna – e-mail: iv_tatyana@list.ru; the department of computer science and information security; cand. of eng. sc.; associate professor.

Ilyasov Bariy Galeevich – e-mail: Ilyasov@tc.ugatu.ac.ru; phone: +73472737835; the department of technical cybernetics; head the department; dr. of eng. sc.; professor.

УДК 004.056

А.Ю. Гуфан, К.И. Полюшкина

КУМУЛЯТИВНЫЙ ПОДХОД К ИСПОЛЬЗОВАНИЮ ВЕРОЯТНОСТНЫХ МЕТОДОВ ОБНАРУЖЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматривается несколько типичных задач из области контроля и обеспечения информационной безопасности, традиционно решаемых с использованием методов, дающих результаты в терминах вероятности истинности предположения о том, что безопасность была нарушена. Предлагается общий подход к совместному использованию результатов анализа нескольких объектов, относящихся к информационной системе, либо процессов, происходящих в ней, либо нескольких характеристик таких объектов или процессов. Показано, что интерпретация такой совокупности результатов анализа может дать более точную информацию о состоянии системы, чем простая дизъюнкция отдельных результатов, получаемых при анализе каждого объекта или процесса, или их характеристик по отдельности. Рассмотрены примеры задач стеганографического анализа, выявления вредоносных вложений в файлах неисполнимых форматов, поиска аномалий поведения пользователей информационных систем. Для каждой из этих задач выявлены особенности, критически влияющие на возможность и специфику применения к ним предлагаемого подхода и предложены пути преодоления связанных с этими особенностями проблем.

Аномалии поведения пользователей; нейронные сети; стеганографический анализ.

A.Y. Gufan, K.I. Polyushkina

CUMULATIVE APPROACH USING PROBABILISTIC METHODS FOR DETECTION INFORMATION SECURITY THREATS

The paper discusses some typical problems of information security control. Traditionally these problems are solved using techniques that give results in terms of probability of the fact that security was compromised. We proposed the general approach of joint use results of the analysis of several objects related to information system or processes, or more characteristics of objects or processes. It was shown that interpretation of such a set of results of analysis can provide more accurate information about the state of the system in comparison with a simple disjunction of individual results. It considers examples of tasks, such as steganography analysis, identifying malicious attachments in nonexecutable file formats, anomaly detection in behavior of users of information systems. For each of these tasks peculiarities were detected, that critically affect specificity of introduced approach application for them and ways to overcome problems related with these features were proposed.

User behavior anomalies; artificial neural networks; steganographic analysis.

Значительное количество задач контроля информационной безопасности (ИБ) относительно эффективно решается с помощью методов, сводящихся к прямому обнаружению практически однозначных признаков наличия угроз. Таковы, например, задачи обнаружения вредоносного программного обеспечения (ПО), где наиболее эффективными являются методы анализа, основанные на поиске сигнатур известных типов вредоносных вложений [1]. Такие методы позволяют справиться со значительной и важной частью проблем обеспечения безопасности информационных систем (ИС). Однако, часть задач обнаружения угроз безопасности методами такого типа не решается. Таковы, например, некоторые задачи обнаружения скрытых каналов передачи информации, эффективно решаемые статистическими методами, результатами работы которых являются не ответы бинарного типа, а оценки вероятности истинности гипотезы о наличии или реализации угроз ИБ.

В некоторых случаях средства обнаружения тех или иных угроз ИБ маскируют эту особенность метода обнаружения, лежащего в их основе: решение о том, какой из дискретных ответов об уровне угрозы выдать для дальнейшей обработки, принимается на основании сравнения результатов работы используемого метода анализа с заранее заданными или определяемыми адаптивно пороговыми значениями. Это, однако, следует считать техническим приемом, используемым для интерпретации результатов применения метода анализа ИС и для принятия последующих решений, а не имманентным элементом метода анализа.

Такой прием является очевидным и естественным в значительном количестве практически важных вопросов. Можно, однако, выделить обширные классы задач, в которых его применение не позволяет в полной мере воспользоваться информацией, получаемой непосредственно в результате статистического или иного анализа, о вероятности истинности гипотезы о нарушении ИБ.

В [2] рассмотрен один из таких классов задач, а именно – распространенная на практике ситуация использования методов стеганографического анализа применительно не к изолированному информационному объекту (контейнеру), а к группе объектов, объединенных общим происхождением. Автором [2] предложен подход, позволяющий на основе обработки всего массива результатов применения статистических методов анализа к каждому из контейнеров исследуемой группы, получить существенно более точные данные о наличии угрозы ИБ, чем на основе простого суммирования (конъюнкции) выводов, получаемых по результатам анализа каждого из контейнеров в отдельности.

Задача, исследованная в [2] обладает следующими важными особенностями, определяющими возможность именно такой имплементации идеи совместного рассмотрения совокупности многочисленных результатов анализа как единого целого:

1) имеются разумные причины с некоторыми оговорками считать результаты анализа разных контейнеров исследуемой группы независимыми величинами;
2) результаты анализа разных контейнеров можно считать одинаково распределенными случайными величинами;
3) ошибка второго рода ("ложноположительный результат") не являются недопустимыми.

По всей видимости, соблюдения этих условий на практике должно быть достаточно для того, чтобы оказался возможен метод оценки уровня угроз, аналогичный представленному в [2]. Такова, например, ситуация анализа журнальных записей межсетевых экранов с целью выявления признаков целенаправленной атаки на ресурсы защищаемой информационной системы.

Однако, в других ситуациях, когда одно или несколько из этих условий нарушаются, прямой перенос методики, представленной в [2], окажется невозможным. В настоящей работе предлагаются предварительные соображения относительно способов реализации концепции совместной интерпретации результатов анализа нескольких связанных информационных объектов в случае, когда особенности решаемой проблемы не согласуются с вышеперечисленными условиями.

1. Задачи, при решении которых результаты анализа отдельных объектов не следует интерпретировать как независимые случайные величины. В настоящее время весьма актуальной и популярной темой является исследование аномалий в поведении участников социальных сетей [3, 4]. Общая картина поведения и аномалии поведения множества пользователей социальных сетей складываются из особенностей поведения отдельных пользователей. Создается впечатление, что перенесение на эту область подхода, предложенного в [2], является естественным. Однако подразумеваемое содержание такой задачи состоит в том, что аномалии в картине поведения множества пользователей социальной сети обусловлены событиями реального мира или коррелируют с ними. А потому и картины поведения отдельных пользователей, формирующих отслеживаемую группу, не следует полагать взаимонезависимыми. Таким образом, первое из условий, перечисленных во введении, явным образом нарушается.

Одним из популярных подходов к обнаружению поведенческих аномалий пользователей социальных сетей является подход, основанный на использовании искусственных нейронных сетей (ИНС). Процедура применения таких методов выглядит как предварительное обучение ИНС (классификатора) на образцах нормальной активности пользователя и последующая проверка соответствия наблюдаемого поведения модели, с возможностью постоянного дообучения ИНС.

В большинстве публикаций по данному вопросу, например, в [4, 5], классификатор обучается лишь на положительных примерах, то есть только на действиях пользователя при его нормальной активности. Это связано с исходной постановкой задачи, имеющейся при исследовании аномалий поведения одного пользователя: как правило, речь идет о косвенном обнаружении взлома учетной записи и действий постороннего лица от имени пользователя, а образцов таких ситуаций, с возможностью их использования в качестве обучающего материала, обычно бывает меньше, чем необходимо для обучения ИНС. По той же причине, тестирование классификатора обычно проводят в формате кросс-теста, состоящего в том, что в процессе тестирования в качестве имитации вторжений используются действия других пользователей.

Приведем пример использования такого подхода. В качестве обучающей выборки для классификатора (реализованного посредством ИНС) возьмём набор векторов признаков, каждый из которых зафиксирован за одни сутки, для определён-

ного пользователя социального сервиса Twitter за некоторый промежуток, например, за месяц. Будем считать, что всё это время в социальной сети работал только один, легальный пользователь. Затем предложим ИНС классифицировать несколько векторов признаков за одни сутки: среди этих векторов присутствуют нелегальные (данные для других пользователей), и вектор легального пользователя, не участвующий в обучении нейронной сети. В векторы признаков, за исключением статистических данных, характеризующих активность пользователя, включён бинарный признак: предполагается, что у легального пользователя он равен единице "1".

Классификатор обучен на векторах признаков для одного пользователя, только на положительных примерах. По рис. 1 видно, что при попытке классифицировать ряд векторов легального и нелегальных пользователей, первый выделяется из остальных, то есть предсказание для него ближе всего к единице.

Рис. 1. Классификатор, обученный на векторах признаков для определённого пользователя ("gruppa_voina", "MedvedevRussia"), точнее всего классифицирует обозначающий рассматриваемый день вектор для данного пользователя среди других

Таким образом, видно, что достаточно эффективный инструментарий для обнаружения аномалий поведения отдельного пользователя существует и может быть с успехом использован на практике. Однако существенный интерес представляет вопрос о том, каким образом на основании такого инструментария могут быть разработаны методы для анализа и обнаружения аномалий поведения групп пользователей.

Следует оговориться, что при этом хотелось бы исключить очевидный вариант: применение в точности того же подхода, но обучение ИНС на материалах деятельности всей группы в целом. Практика показывает, что для группы от не-

скольких десятков пользователей поведение, охарактеризованное таким очевидным образом, оказывается достаточно однородным и малочувствительным к аномалиям, проявляющимся в поведении 10–15 % членов группы.

В ситуации, когда поведение пользователей социальной сети возможно было бы предположить взаимонезависимым или хотя бы не взаимообусловленным, эффективным мог бы быть прямой перенос на данный материал подхода, использованного в работе [2]. Однако, такие предположения в ситуации социальной сети являются обычно необоснованными. Использование подхода [2], тем не менее, возможно, при условии введения в него учета взаимообусловленности результатов анализа поведения отдельных пользователей в качестве самостоятельного фактора. Это может быть сделано на основе результатов анализа социального графа исследуемой группы [6,7]. А именно – учет влияния отдельных аномалий поведения на суммарный результат анализа должен быть поставлен в зависимость от меры близости отдельного пользователя с другими пользователями, синхронно с ним демонстрирующими аномалии. На основе подходящей к случаю (одной из многочисленных широко используемых – см. работы [6, 7] и ссылки в них) меры близости могут быть сформированы весовые коэффициенты, определяющие влияние результата, полученного для отдельного пользователя, на результат, получаемый для всей группы.

2. Ситуация, когда результаты анализа отдельных объектов не следует интерпретировать как одинаково распределенные случайные величины. Одной из важнейших задач в области ИБ является задача идентификации пользователя информационной системы (ИС) с целью предотвращения несанкционированного доступа к данным. Помимо проблемы идентификации пользователя в момент запроса доступа к ИС (идентификация "на входе"), собственной значимостью обладает проблема идентификации пользователя в процессе работы с ИС. В основе рассмотренных далее подходов к решению этой проблемы лежит предположение о том, что пользователь ИС демонстрирует собственное, уникальное поведение, по которому его можно отличить от другого пользователя (будем называть его нелегальным). В соответствии с этой гипотезой, можно сформировать некий эталонный вектор признаков поведения легального пользователя. При необходимости идентификации пользователя как легального или нелегального его наблюдаемое поведение сравнивается с эталонным.

При этом используются достижения такой достаточно развитой области науки об информационной безопасности, как обнаружение аномалий. Спектр методов, применимых к данной задаче, широк и включает использование генетических алгоритмов, конечных автоматов, марковских моделей, вейвлет-анализа, методов машинного обучения. В качестве характерного примера разберем один из достаточно эффективных методов решения задачи идентификации пользователя по его поведению, представленный в [4].

Авторы [4] используют схему принятия решения об аутентичности пользователя ПК, изображенную на рис. 2. Разработанная ими модель

- в реальном времени предсказывает динамические показатели на основе предыдущих значений. Решение о легальности/нелегальности пользователя базируется на количестве верно предсказанных нейронной сетью действий пользователя.
- в автономном режиме анализирует статистические данные, собранные в течение всего времени работы пользователя. На вход принимается набор признаков для конкретного промежутка времени. На выходе, если этот набор не участвовал в обучении, нейронная сеть выдаёт число из промежутка [0; 1] – вероятность "легальности" активности пользователя.
- выявление тенденций изменения поведения пользователя с течением времени.

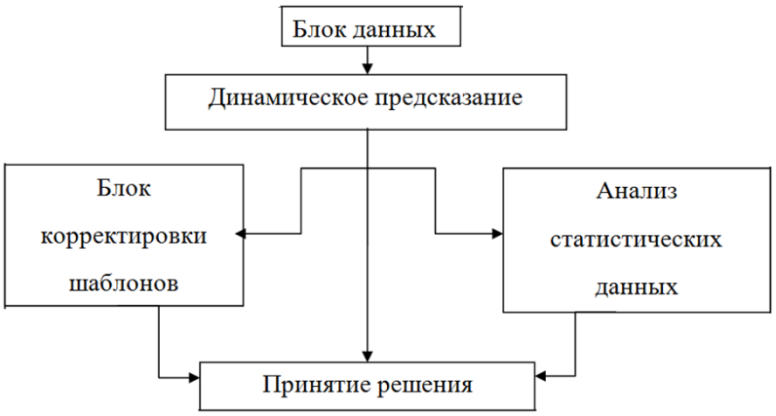

Рис. 2. Структура многокомпонентной нейросетевой системы моделирования поведения пользователя

Использованная авторами [4] модель обучаемая поведения пользователя базируется на аппарате искусственных нейронных сетей (ИНС). При разработке такой модели необходимо учитывать возможность эволюции поведения пользователя ПК со временем. Способность модели "забывать" устаревающие данные может быть организована, подобно подходу, представленному в [8], где была исследована зависимость текущего поведения пользователя от предыдущего: экстремумы автокорреляции наблюдаются при сдвигах кривых поведения в интервале от одной до восьми команд, поэтому был сделан вывод, что оптимальное количество учитываемых действий равно восьми.

$$p^i(n) = corr\left(\varepsilon_n^i,\ \mu_n^i\right), \qquad \varepsilon_n^i = \left(c_1^i,\ c_2^i,\ \ldots, c_{N_i-1}^i\right);$$
$$\mu_n^i = \left(c_{n+1}^i,\ c_{n+2}^i,\ \ldots, c_{N_i}^i\right);$$

где $p^i(n)$ – коэффициент корреляции для последовательности команд, зафиксированных за i-й сеанс; n – временное смещение между элементами последовательности (лаг).

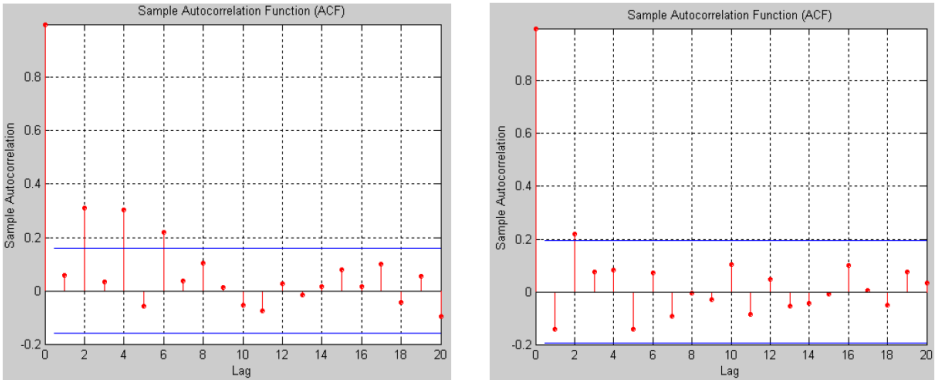

Рис. 3. Примеры автокорреляционных функций для разных пользователей

В [4] для этой функции модели выделен специальный агент, который, во-первых, в случае необходимости пополняет алфавит команд $A = (a_1,\ a_2, \ldots, a_N)$, и, во-вторых, вычисляет степень "оторванности" действий за последнюю сессию от других как суммарное расстояние Хемминга:

$$\varphi(g(s_{t\prime}), g(s_{t\prime\prime})) = \sum_{j=1}^{N} \chi\big(g(s_t'), g(s_t'')\big),$$

где вектор g – это набор бинарных признаков того, имела ли место команда в соответствующей сессии: $s_{t\prime}$ или $s_{t\prime\prime}$.

Эффективность данного подхода продемонстрирована на рис. 4: точность предсказания действий существенно падает при имитации вторжения (в нашем случае – подмене данных пользователя, для которого обучена ИНС данными другого пользователя).

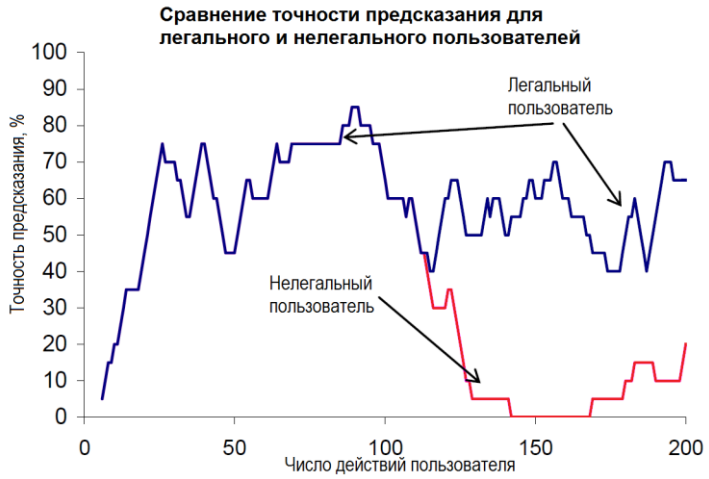

Рис. 4. Снижение точности предсказания действий пользователя в результате кросс-теста [4]

Таким образом, данный подход к решению задачи идентификации пользователя, а точнее – обнаружения аномалий поведения пользователя, в самом общем виде может быть описан как вычисление в процессе работы пользователя с ИС нескольких принципиально разнородных статистических характеристик и последующее их независимое сравнение с заранее обученными моделями. То есть в качестве данных, на основании которых принимается решение о том, имеет ли место несанкционированный доступ к ИС, выступает несколько величин (мер отличия разнообразных аспектов наблюдаемого поведения от обученной модели), которые можно считать в некотором специальном смысле случайными и не одинаково распределенными.

Прямое использование этих величин для обнаружения существенной аномалии поведения пользователя выглядит как простая конвертация значений каждой из них в отдельности в значение вероятности того, что пользователь, чье поведение исследовано, отличен от пользователя, чье поведение послужило материалом для обучения модели. При этом естественным способом принятия решений о том, что имеет место факт доступа к ИС пользователя, отличного от предполагаемого, базируется на двух принципах:

1. Решение по каждому фиксируемому параметру поведения принимается отдельно с использованием заранее заданных пороговых значений соответствующей величины отклонения результатов наблюдений от модели.
2. Окончательное решение принимается либо по итогам конъюнкции результатов, полученных по каждому параметру отдельно, либо в результате некоторой процедуры "голосования", проводимой на основании отдельных результатов.

При этом необходимо оговориться, что очевидно оптимальный с точки зрения точности результатов подход, основанный на построении не отдельных моделей для каждого аспекта поведения пользователя, а в целом для многомерного вектора признаков этого поведения и затем детекции аномалий по результатам сравнения всего комплекса наблюдений с этой моделью, обладает существенными недостатками, делающими его непрактичным:

1. Невозможность реализации системы обнаружения аномалий с архитектурой решающего ядра и подключаемых модулей фиксации и моделирования различных аспектов поведения пользователя. В случае формальной реализации такой архитектуры, подключение дополнительных модулей или отключение использовавшихся ранее, потребует полного переобучения модели, для многомерного вектора признаков.
2. Объем обучающих данных для многомерного вектора признаков с ростом числа его координат растет нелинейно, что должно привести к непрактичности процедуры предварительного обучения модели.

Однако имеются основания предполагать, что, по аналогии с результатами работы [2], совместный анализ результатов независимых сравнения нескольких аспектов поведения пользователя с моделями должен содержать больше информации об аномалиях в поведении пользователя, чем результат простого суммирования информации, содержащейся в каждом из сравнений в отдельности. Нам представляется наиболее естественной и практичной следующая возможность для такого совместного анализа комплекта результатов частных сравнений с моделями. Результаты, полученные в отдельности для каждого аспекта поведения пользователя следует проинтерпретировать в терминах вероятности истинности гипотезы о том, что угроза неаутентичности авторизованного пользователя не была реализована. Общая вероятность истинности такой гипотезы, получаемая на основании всего комплекса аспектов поведения, может быть в таком случае вычислена по принципу «включения-исключения»: $P_{global} = \sum_i P_i - \sum_{i,j} P_i P_j + \sum_{i,j,k} P_i P_j P_k - \cdots$. При этом в случае появления дополнительной информации о каком-либо аспекте поведения пользователя, либо признании части информации неактуальной, корректировка общей вероятности нереализации угрозы вычисляется заново с минимальными затруднениями.

3. Ситуация, когда ошибка второго рода крайне нежелательна. При решении проблемы обнаружения вредоносного ПО на компьютере, не включенном в ИС критически важного объекта, повышение вероятности «ложноположительного» результата анализа существенно ухудшает пользовательские характеристики системы обнаружения угроз ИБ и является крайне нежелательным. Значительный массив задач в этой области вполне удовлетворительно решается с помощью методов, подобных прямому поиску сигнатур известного вредоносного ПО [9] и для таких задач вопросы использования дополнительных возможностей совместной интерпретации результатов анализа нескольких информационных объектов неактуальны. Однако, и в этой области существуют важные классы задач, сколько-нибудь эффективно решаемых лишь с помощью методов вероятностного и статистического анализа. Так, например, в работе [1] представлено исследование возможностей решения задачи поиска вредоносных вложений по признаку наличия у них исполнимого загрузчика. При этом автором [1] разработан метод детекции исполнимого загрузчика, основанный на использовании скрытых марковских моделей. Алгоритм поиска исполнимого загрузчика в теле файла неисполнимого формата, предложенный и апробированный в этой работе, в общем виде выглядит следующим образом:

1. Методом исчерпывающего дизассемблирования всего тела файла строится карта всех инструкций, содержащихся в исследуемом файле (на основе спецификации Intel IA-32).
2. Для тех позиций файла, которые не входят в другие последовательности, строится последовательность инструкций, которая обрывается на позиции, начиная с которой далее не удается проинтерпретировать содержание файла как корректную инструкций.
3. На основе последовательностей, найденных в п. 2, алгоритмом Витерби находятся все подпоследовательности инструкций, соответствующие заранее обученной скрытой марковской модели исполнимой последовательности специального вида.
4. Если среди подпоследовательностей инструкций была хоть одна последовательность длиной больше заранее принятого порога, то она принимается за искомый загрузчик вложения.
5. Если в исследуемом файле был найден загрузчик, то файл считается содержащим вредоносное вложение.

Окончательное решение о том, что исследованный файл содержит исполнимый загрузчик, принимается на этапах 4–5, после интерпретации результатов сопоставления наблюдаемого содержания файла с вероятностной моделью. В той же работе [1] достаточно подробно исследован вопрос о возможности «пропуска», необнаружения части тела загрузчика при использовании предлагаемого автора подхода к его поиску. Поэтому в качестве метода исследования содержания файла разумно воспринимать шаги 1–3 вышеописанной процедуры, и результатом применения этих шагов после некоторой модификации шага 3 должна оказаться оценка вероятности присутствия исполнимого загрузчика в файле. Шаги же 4–5 представляют собой способ интерпретации этого результата.

Таким образом, методы, предложенные в [1] по важным формальным признакам подобны рассмотренным выше методам обнаружения аномалий поведения пользователей социальных сетей и ПЭВМ. Однако, к методам анализа файлов на предмет наличия в них вредоносного ПО предъявляются существенно иные требования по вероятностям ошибки второго рода. Поэтому перенос на эту тематическую область методов, предложенных в [2] и выше в настоящей работе, не является практичным. Тем не менее, для разработки в некотором роде аналогичных подходов здесь также существуют возможности.

Учтем одну особенность распространенной практики внедрения вредоносного ПО, а именно – частое наличие нескольких копий вредоносного ПО или нескольких вариантов вредоносного ПО на жестких дисках одной машины. В силу этого, обнаружение нескольких файлов, содержащих косвенные признаки присутствия вредоносных вложений, должно повышать уровень достоверности гипотезы о том, что факт вложения имеет место в действительности. Таким образом, совместный учет результатов анализа нескольких файлов должен основываться на принципе зависимости используемых при принятии решения пороговых значений для вычисляемых оценок вероятности наличия вложения в каждом отдельном файле от количества файлов, для которых оценка оказалась достаточно высокой.

Выводы. Таким образом, имеются основания утверждать, что в значительном количестве случаев, когда задачи контроля различных аспектов ИБ решаются с помощью методов, первоначальный результат применения которых представляет собой оценки вероятностных характеристик возможного нарушения ИБ, существуют возможности эффективно интерпретировать результаты анализа группы информационных объектов, либо процессов в ИС, или результаты анализа группы характеристик одного объекта либо процесса, таким образом, что получаемая при

этом информация окажется более содержательной, чем простая сумма информации, получаемой при анализе каждого объекта/процесса или их характеристик в отдельности. Однако, не удается выработать общих принципов построения такой интерпретации: применимость и эффективность различных приемов критически зависит от конкретных свойств исследуемых аспектов ИБ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Эдель Д.А.* Способ повышения эффективности средств выявления зараженных файлов на основе использования скрытых марковских моделей: дис. канд. техн. наук. – Таганрог, 2013.
2. *Елисеев А.С., Тикиджи-Хамбурьян А.Р.* Статистический стеганографический анализ источников контейнеров одинакового типа с использованием базового метода анализа отдельных контейнеров неизвестной структуры // Известия ЮФУ. Технические науки. – 2014. – № 2 (151). – С. 158-167.
3. *Comninos A.* Twitter revolutions and cyber crackdowns. User-generated content and social networking in the Arab spring and beyond / URL: https://www.apc.org/es/system/files/AlexComninos_MobileInternet.pdf (Дата обращения: 26.02.2014).
4. *Shelestov A., Skakun S., Kussul O.* Intelligent model of user behavior in distributed systems // International Journal "Information Theories & Applications". − 2008. − № 15. − С. 70-76.
5. *Cannady J.* Artificial neural networks for misuse detection // Proc. of the National Information Systems Security Conference. − 1998. − С. 443-456.
6. *Пушенко А.В., Хади Р.А.* Построение метрики для поиска скрытых групп при сетевом анализе // IX Всероссийский симпозиум по прикладной и промышленной математике (весенняя сессия). – 2008. − С. 1124.
7. *Пушенко А.В., Аграновский А.В.* Динамический поиск скрытых групп в социальных сетях // Десятая Международная научно-практическая конференция "Информационная безопасность 2008". – Таганрог: ТРТУ, 2008. − С. 234-236.
8. *Скакун С.В.* Математическое моделирование поведения пользователей компьютерных систем // Математические машины и системы. − 2005. − № 2. − С. 122-129.
9. *Brian Caswell, Jay Beale, James C. Foster*. Jeremy Faircloth "Snort 2.0 Intrusion Detection" // Syngress Publishing, 2003.

Статью рекомендовал к опубликованию д.ф.-м.н., профессор М.Ф. Куприянов.

Гуфан Александр Юрьевич – ФГАНУ НИИ «Спецвузавтоматика»; e-mail: a.gufan@niisva.org; 344002, г. Ростов-на-Дону, пер. Газетный, 51; тел.: +78632012817; д.ф.-м.н.; доцент; зав. лабораторией.

Полюшкина Ксения Ивановна – e-mail: fenetre@inbox.ru; бакалавр; инженер-программист.

Gufan Alexander Yurievich – FSASE SRI "Specvuzavtomatika"; e-mail: a.gufan@niisva.org; 51, Gazetny, Rostov-on-Don, 344002, Russia; phone: +78632012817; dr. of phis.-math. sc.; associate professor; head of laboratory.

Polushkina Xenia Ivanovna – e-mail: fenetre@inbox.ru; bachelor; software engineer.