Plavan Aleksey Igorevich, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstoy Street, Samara, 443010, Russian Federation; PhD Student of Information Security Department. Tel. +7 927 736-50-55. E-mail: aleksej.plavan@ya.ru

References

1. Bocetta S. So long, ransomware: organizations brace for cryptojacking. URL: https://www.dataversity.net/so-long-ransomware-organizations-brace-for-cryptojacking (accessed: 28.08.2020).
2. Sheluhin O.I., Sakalema D.Zh., Filinova A.S. *Detection of Intrusions into Computer Networks (Network Anomalies)*. Moscow: Gorjachaja linija–Telekom, 2013, 220 p. (In Russ.)
3. Branitskij A.A., Kotenko I.V. Analysis and classification of methods for detecting network attacks. *Trudy SPII RAN*, 2016, no. 45, pp. 207–244. (In Russ.)
4. Zhao S. et al. Real-time network anomaly detection system using machine learning. *11th International Conference on the Design of Reliable Communication Networks (DRCN)*, Kansas City, MO, 2015, pp. 267–270.
5. Stukach O.V. Testing statistical hypotheses. URL: http://ieee.tpu.ru/system/hypotez.htm (accessed: 22.07.2020). (In Russ.)
6. Brownlee J. How to use ROC curves and precision-recall curves for classification in Python. URL: https://machinelearningmastery.com/roc-curves-and-precision-recall-curves-for-classification-in-python (accessed: 22.07.2020).
7. hping3 – network testing. URL: http://its27.ru/2019/05/27/hping3-testing-network (accessed: 20.06.2020). (In Russ.)
8. hping3 Package Description. URL: https://tools.kali.org/information-gathering/hping3 (accessed: 20.06.2020).
9. Kartashevskij V.G., Pozdnjak I.S. Filtering monitored traffic as a way to detect intrusions. *Vestnik UrFO*, 2019, no. 1 (31), pp. 17–22. (In Russ.)
10. Kartashevskij V.G. *Basics of Queuing Theory*. Moscow: Gorjachaja linija–Telekom, 2013, 130 p. (In Russ.)
11. Shapiro L. DDoS attacks. Part 2. Arsenal of the enemy. *BIT*, 2015, no. 6, pp. 24–27. (In Russ.)

Received 21.09.2020

УДК 004.4

РАЗРАБОТКА МЕТОДА МОНИТОРИНГА АНОМАЛЬНОГО ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ В РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ: ПОСТРОЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ

Ряполова Е.И., Преснов А.А., Цветкова К.Е.
Оренбургский филиал Поволжского государственного университета телекоммуникаций и информатики, Оренбург, РФ
E-mail: presnov.aleksey@mail.ru

Статья посвящена разработке системы мониторинга аномального поведения пользователя в распределенных информационно-вычислительных системах и построению математической модели разрабатываемой системы. Проведен анализ современных методов поведения пользователя информационной системы. Главное внимание уделено тому, что существующие методы защиты информационных систем имеют ряд недостатков, исправить которые возможно при использовании разрабатываемого метода, который осуществляет защиту как от внутренних, так и от внешних нарушителей. Для разработки системы мониторинга аномального поведения пользователя в распределенных информационно-вычислительных системах необходимо решить ряд задач: провести анализ методов мониторинга поведения пользователей в информационной системе; построить целевую функцию и выбрать критерии для оценки качества методов анализа аномального поведения пользователей. В исследовании использованы методы теории информационной безопасности, теории автоматов, теории распознавания образов и теории проектирования вычислительных систем.

Ключевые слова: *аномальное поведение пользователей, мониторинг поведения пользователей, системы информационной безопасности, распределенная информационная система, автоматная модель, DLP-системы*

Введение

В современном мире проблеме защиты информации уделяется особое внимание, информация имеет достаточно высокую цену, порой превышающую материальные объекты. Чтобы защитить информацию, государственные и коммерческие организации внедряют большое количество средств защиты информации: антивирусы, межсетевые экраны, системы обнаружения вторжений, средства разграничения доступа. Однако статистические данные показывают ежегодное увеличение атак на распределенные информационно-вычислительные системы.

Подобные проблемы с безопасностью связаны с тем, что в большинстве случаев данные подходы защиты недостаточно эффективны и не позволяют достичь требуемого уровня защиты системы. Поэтому возникает задача разработки метода, позволяющего повысить достоверность распознавания (идентификации) нарушителя.

На сегодняшний день одним из подобных методов является метод анализа поведения пользователя. Данный метод частично реализован в системах противодействия утечек информации (DLP) и системах обнаружения вторжений (IDS). Анализ поведения пользователя в системе сводится к анализу их поступков для защиты в первом случае от внутренних, во втором – внешних угроз, что в полной мере нельзя назвать анализом поведения пользователя. Акцент необходимо сделать на понимании понятия поведения – осознанной, взаимосвязанной последовательности действий пользователя.

Следовательно, разработанный метод должен позволять комплексно контролировать поведение пользователя и выявлять в нем аномалии с целью повышения достоверности идентификации нарушителя как внутреннего, так и внешнего.

За основу была взята автоматная модель Гогена-Мезигера, где каждый поступок пользователя представляется в виде состояния автомата, при этом система при каждом действии может переходить из одного разрешенного состояния только в несколько других, но в отличие от базовой модели в разрабатываемой проверяется корректность перехода не только по данным из текущего состояния, но и из всей предыстории действий пользователя [19].

Достоинствами данного подхода являются:

– возможность определения несанкционированного доступа (НСД) на ранней стадии реализации угрозы;

– возможность обнаружения атак со стороны внешних и внутренних нарушителей;

– возможность определения ранее неизвестных угроз;

– выявление аномалий в поведении пользователя и их пресечение;

– незначительное потребление ресурсов системы при мониторинге поведения;

– скрытность работы: пользователь не замечает анализа и фиксации своих действий в системе;

– удобство использования: система не загружает пользователей системы какими-либо дополнительными действиями.

Следует отметить, что данный класс методов по борьбе с НСД является новым, и в данный момент на российском рынке программного обеспечения (ПО) системы защиты информации (СЗИ) практически нет систем, осуществляющих анализ поведения пользователя в распределенных информационно-вычислительных системах.

Для защиты автоматизированных систем (АС) от НСД применяют различные системы аппаратных и программных средств защиты от внешних и внутренних нарушителей. По статистике за 2019 год [1–4], НСД является одной из самых распространённых угроз информационной безопасности (ИБ), при этом соотношение внешних и внутренних угроз составляет 45 и 55 % [5–9], что показывает большую опасность со стороны внутренних нарушителей, около трети всех угроз НСД были успешно реализованы [10; 11]. На основании этого следует, что существующие средства и методы защиты от НСД недостаточно эффективны.

Обзор патентов и научных работ показал, что для распознавания аномального поведения пользователя развиваются такие средства и методы, как: DLP-системы [16–18], средства анализа поведения пользователя на сайте, система адаптивного управления и контроля создания сигнатур вирусов на основе поведения пользователей [20], IDS/IPS-системы [21], нейронная система обнаружения аномального поведения вычислительных процессов микроядерных операционных систем [23], система обнаружения аномального поведения абонентов телефонной сети [24]. В таблице 1 указаны основные методы и угрозы рассматриваемы в DLP-системах.

Из таблицы 1 видно, что в DLP-системах используется три основных метода детектирования: «Лингвистический анализ», «Цифровой отпечаток» и «Контроль по шаблонам».

Таблица 1. Основные методы и угрозы в DLP-системах

Методы защиты DLP/ Угрозы на DLP	Лингвистический анализ	Статистические технологии (цифровой отпечаток)	Контроль по шаблонам
Отправка конфиденциальных документов по сети на печать или на съемное устройство в первоначальном виде	+	+	–
Отправка конфиденциальных документов с удалением «стоп-слов»	–	+	–
Стеганография	–	–	–
Физическое воздействие	–	–	–
Изменение кодировки	–	–/+	+
Уход за стандартную область документа	–/+	–	–
Формальное изменение текста	–	–	+
Использование другого языка	–	+	–
Изменение формата передаваемой информации	–	–/+	+

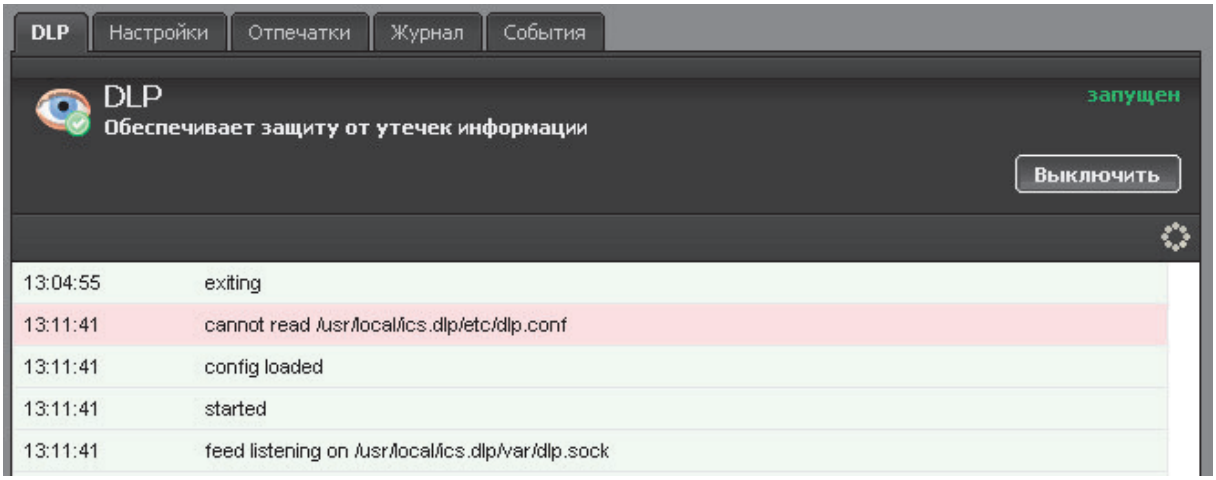

Рисунок 1. Экранная форма DLP-системы [16]

Как показывает статистика утечек информации, злоумышленники знают о подобных недостатках DLP-систем и часто их используют. Так практически во всех подобных системах не решены или плохо реализованы меры по защите от следующих угроз: стеганография (возможность видоизменения файла, его формата, формы, размера содержания – осуществить передачу конфиденциальной информации путем сокрытия самого факта передачи конфиденциальной информации), физическое воздействие (фотографирование, ксерокопирование, запоминание, переписывание конфиденциальной информации). С учетом определенных угроз построена таблица сравнительных характеристик методов обнаружения утечек.

Особую сложность для DLP-систем представляют угроза использования злоумышленником стеганографии для сокрытия информации. Одним из перспективных методов для обнаружения утечки информации, скрытой методами стеганографии, является подход на основе аномальной активности пользователя.

Современные DLP-системы являются эффективными для обнаружения непреднамеренных утечек данных или действий злоумышленников, которые не имеют достаточной квалификации и принципов работы средств информационной защиты. Для повышения эффективности систем предотвращения утечек необходимо разработать модели и средства защиты на основе идентификации аномального поведения сотрудников. На рисунке 1 показан пример работы с DLP-системой.

Средства анализа поведения пользователя на сайте применяются для увеличения числа заказов, покупок и других желаемых от посетителей действий, при этом анализируют, на каких страницах они задерживаются, каким маршрутом они перемещаются по страницам сайта, почему могут не доходить до целевых страниц (например,

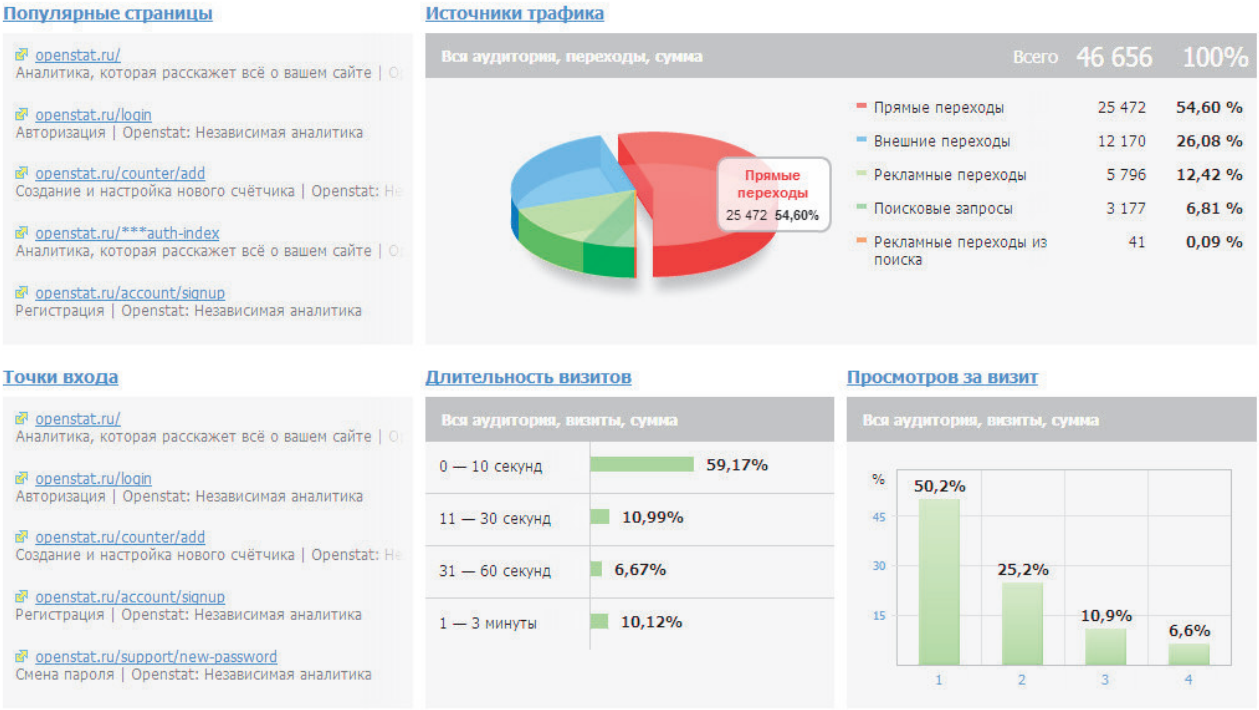

Рисунок 2. Экранная форма средства «Яндекс.Метрика» для анализ поведения пользователя на сайте [18]

до страницы заказа товара), какие страницы затрудняют поиск информации на сайте, какие страницы привлекают больше всего внимания. В качестве инструментов для анализа поведения пользователей могут использоваться: LiveInternet, Яндекс.Метрика, Google Analytics и внутренние сервисы анализа статистики.

Анализ заключается в выявлении характерных особенностей поведения посетителей. Если это был успешный посетитель, который совершил заказ, то нужно проанализировать, что он увидел на сайте, на что обратил внимание, когда купил. На этом и строится управление поведением и отслеживание результата. На рисунке 2 представлен пример работы со средством «Яндекс.Метрика» для анализа поведения пользователя на сайте.

Патент на систему адаптивного управления и контроля создания сигнатур вирусов на основе поведения пользователей включает в себя этап отслеживания произошедших событий в операционной системе, инициированных действиями пользователя на персональном компьютере. Согласно способу, формируют контекст, содержащий действия, совершенные пользователем, и события, инициированные совершенными действиями, а также осуществляют анализ сформированного контекста с помощью правил регулирования.

Кроме того, выявляют действие, совершенное пользователем на основе указанного анализа, при этом выявленное действие является запрещенным действием для пользователя, но при этом данное действие не было заблокировано. Такое действие необходимо отнести к запрещенным и создать соответствующую сигнатуру.

IDS-системы – это аппаратно-программные средства, предназначенные для выявления фактов неавторизованного доступа в компьютерную систему или сеть [21].

Системы обнаружения вторжений (СОВ, IDS) и межсетевой экран относятся к средствам обеспечения информационной безопасности, межсетевой экран отличается тем, что ограничивает поступление на хост или подсеть определенных видов трафика для предотвращения вторжений и не отслеживает вторжения, происходящие внутри сети. СОВ, напротив, пропускает трафик, анализируя его и сигнализируя при обнаружении подозрительной активности. Обнаружение нарушения безопасности проводится обычно с использованием эвристических правил и анализа сигнатур известных компьютерных атак. На рисунке 3 показан пример работы с СОВ «Prelude IDS».

Детекторы аномалий определяют ненормальное (необычное) поведение на хосте или в сети. Они предполагают, что атаки отличаются от «нормальной» (законной) деятельности и могут, следовательно, быть определены системой, которая умеет отслеживать эти отличия. Детекторы аномалий создают профили, представляющие собой нормальное поведение пользователей, хостов

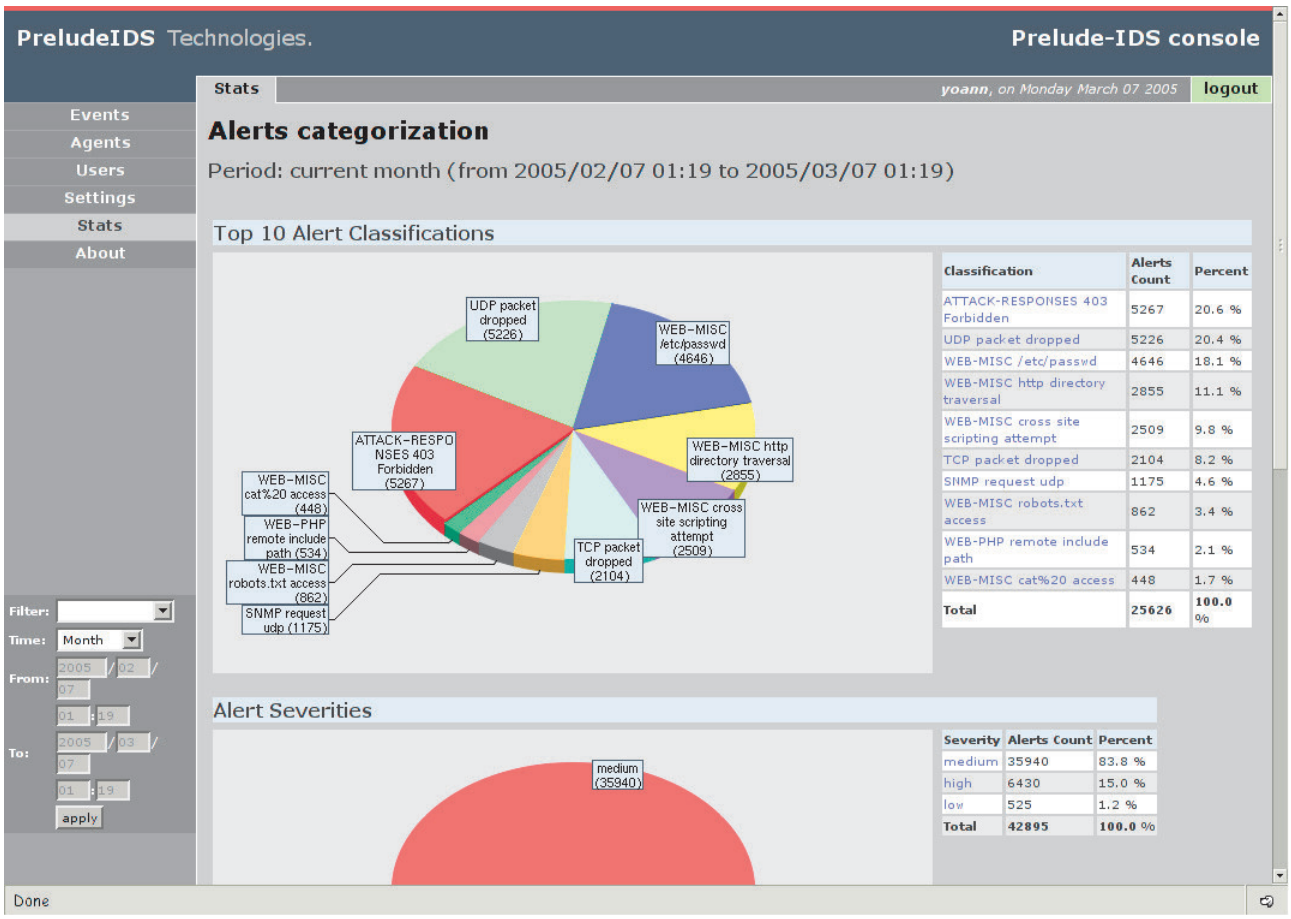

Рисунок 3. Экранная форма IDS-системы [21]

или сетевых соединений. Эти профили создаются, исходя из данных истории, собранных в период нормального функционирования. Затем детекторы собирают данные о событиях и используют различные метрики для определения того, что анализируемая деятельность отклоняется от нормальной.

Системы IPS можно рассматривать как расширение IDS, так как задача отслеживания атак остается одинаковой. Однако они отличаются в том, что IPS должна отслеживать активность в реальном времени и быстро реализовывать действия по предотвращению атак. Возможные меры – блокировка потоков трафика в сети, сброс соединений, выдача сигналов оператору. Также IPS могут выполнять дефрагментацию пакетов, переупорядочивание пакетов TCP для защиты от пакетов с измененными SEQ и ACK номерами.

Некоторые коммерческие IDS включают ограниченные формы определения аномалий, мало кто полагается исключительно на данную технологию. Определение аномалий, которое существует в коммерческих системах, обычно используется для определения зондирования сети или сканирования портов. Тем не менее определение аномалий остается предметом исследований в области активного определения проникновений и, скорее всего, будет играть возрастающую роль в IDS следующих поколений.

Системы обнаружения аномального поведения основаны на том, что им известны некоторые признаки, характеризующие правильное или допустимое поведение объекта наблюдения. Наиболее распространенной реализацией технологии обнаружения злоумышленного поведения являются экспертные системы.

Нейронная система обнаружения аномального поведения вычислительных процессов микроядерных операционных систем

В нашем исследовании будет использована модель вычислительного процесса в микроядерной операционной системе, основанная на собранной статистической информации о штатном поведении вычислительных процессов, отличающаяся тем, что она может быть использована для решения задачи распознавания аномального поведения вычислительных процессов и выявления новых типов атак с неизвестными сигнатурами [23].

Метод заключается в построении шаблона поведения пользователя на основе нескольких

Таблица 2. Сравнение средств и методов анализа поведения пользователя

Средство или метод / Функция защиты	DDLP	IIDS/ IPS	Нейронная система обнаружения аномального поведения вычислительных процессов микроядерных операционных систем	Метод анализа аномального поведения пользователя на основе автоматной модели
Защита от внутренних угроз (инсайдеров)	+	–	+	+
Защита от негативных действий в сети	–	+	–	+
Защита от случайных/ непреднамеренных действий	–	–	–	+
Защита от ранее неизвестных угроз	–	–	+	+

недель наблюдения абонентов в телефонной сети, и впоследствии обнаружения звонков, которые выходят за рамки текущего шаблона [24].

Учитывая случайную природу совершения телефонного звонка по отношению к оператору, для анализа поведения можно исходить из предположения, что число звонков за определенный промежуток времени будет распределено по распределению Пуассона.

Все перечисленные работы анализируют поведение пользователя в определенной среде и имеют ряд ограничений, в то время как предлагаемый метод универсален:

– применяется для защиты как от внешних, так и от внутренних нарушителей;

– для принятия решения о разрешении или запрещении последующих действий пользователя анализируются все предыдущие действия (состояния) пользователя, если для анализа недостаточно данных, то пользователю необходимо выполнить ряд дополнительных действий либо повторить предыдущие;

– обучаем: в процессе работы создаются базы сигнатур разрешенных и запрещенных состояний;

– обеспечивает скрытность работы: пользователь не замечает анализа и фиксации своих действий в системе;

– удобен в использовании: не накладывает на пользователя выполнение дополнительных, длительных операций;

– отличается незначительным потреблением ресурсов системы при мониторинге поведения пользователя.

Сравнительная характеристика существующих методов анализа поведения пользователя с разрабатываемыми представлена в таблице 2.

Как видно из таблицы 2, предлагаемый метод анализа аномального поведения пользователя превосходит по функционалу существующие методы, являясь при этом универсальным средством для детектирования действий пользователя и предотвращения НСД с его стороны, а также при использовании в комплексе ведет к повышению достоверности распознавания нарушителя компьютерной системы, при этом не загружая систему трудоемкими вычислениями. Следует отметить, что существующие на российском рынке DLP-системы плохо адаптированы под русский язык.

Выбор оптимального решения или сравнение двух альтернативных решений проводится с помощью некоторой зависимой величины (функции), определяемой проектными параметрами.

Основной целью разработки метода является повышение достоверности распознавания (идентификации) нарушителя на основе анализа аномального поведения пользователя. Следует отметить, что достоверность распознавания характеризуется наличием и количеством ошибок первого и второго рода.

Пусть дана выборка $X = (X_1, \ldots, X_n)^T$ из неизвестного совместного распределения P^X и поставлена бинарная задача проверки статистических гипотез: H_0 и H_1, где H_0 – нулевая гипотеза; H_1 – альтернативная гипотеза. Предположим, что статистический критерий задан формулой

$$F : R^n \to \{H_0, H_1\},$$

где каждой реализации выборки $X = x$ сопоставляется одна из имеющихся гипотез, и возможны следующие четыре ситуации.

1. Распределение P^X выборки X соответствует гипотезе H_0, и она точно определена статистическим критерием, то есть $f(x) = H_0$.

2. Распределение P^X выборки X соответствует гипотезе H_0, но она неверно отвергнута статистическим критерием, то есть $f(x) = H_1$.

3. Распределение P^X выборки X соответствует гипотезе H_1, и она точно определена статистическим критерием, то есть $f(x) = H_1$.

Таблица 3. Выявление ошибок первого и второго рода

Верная гипотеза / результат применения критерия	H_0	H_1
H_0	H_0 (верно принята)	H_0 (ошибка второго рода)
H_1	H_0 (ошибка первого рода)	H_0 (верно отвергнута)

4. Распределение P^X выборки X соответствует гипотезе H_1, но она неверно отвергнута статистическим критерием, то есть $f(x) = H_0$.

Во втором и четвертом случае говорят, что произошла статистическая ошибка, и её называют ошибкой первого и второго рода соответственно.

В таблице 3 представлено соотношение гипотез и результата применения критерия, так при пересечении $H_0 – H_0$ будет верно принято действий, $H_1 – H_1$ будет верно отвергнуто действие пользователя, в остальных случаях $H_0 – H_1$ и $H_1 – H_0$ будет принято неверное решение, которое приведет к появлению ошибок первого и второго рода.

Целевая функция отражает зависимость от повышения достоверности распознавания нарушителя с вероятностью реализации и количеством ошибок первого и второго рода.

Таким образом, целевая функция задачи повышения эффективности идентификации запрещенных действий пользователя определяется минимизацией ошибок первого и второго рода при $Z \leq Z_{доп}$ и имеет следующий вид:

$$E_C = \left[e_A (1-\alpha) - z_A \alpha \right] P_A + \\ + \left[e_B (1-\beta) - z_B \beta \right] P_B \rightarrow \max,$$

где e_A и e_B – экономия и возможный денежный доход от верного распознавания действий пользователя; z_A и z_B – затраты от неверного распознавания действий пользователя; α и β – соответственно, ошибки первого и второго рода при определении правомочности действий пользователя; P_A и P_B – априорные вероятности событий, соответствующих подаче команд пользователем для выполнения операций до контроля, соответственно, санкционированных и несанкционированных; Z и $Z_{доп}$ – соответственно, реальные и допустимые затраты на создание системы контроля.

Из приведенного выражения видно, что чем меньше ошибки первого и второго рода, тем выше значение целевой функции. Мониторинг значений (состояний) функции перехода $\delta(s, x)$, соответствующей конкретному пользователю, позволяет вести контроль санкционированных операций в компьютерной системе.

Необходимо минимизировать число аномальных действий пользователя, реализация которых приведёт к появлению ошибок первого и второго рода.

Технология обнаружения атак путем идентификации аномального поведения пользователя основана на следующей гипотезе: аномальное поведение пользователя (атака или какое-нибудь враждебное действие) часто проявляется как отклонение от нормального поведения. События (поступки) при попытке вторжения отличаются от событий нормальной деятельности и используют различные сигнатуры для определения отклонения от нормального состояния.

Если можно было бы однозначно описать профиль нормального поведения пользователя, а именно однозначно определить критерии для оценки аномальности поведения, то любое отклонение от них можно идентифицировать как аномальное поведение. Однако аномальное поведение не всегда является атакой, например, одновременную посылку большого числа запросов от администратора сети система защиты может идентифицировать как атаку типа «отказ в обслуживании». Преобладание фото- и видеоматериалов в трафике, большой объем передаваемой информации, использование ПК в нерабочее время также могут быть примером аномального поведения.

При настройке и эксплуатации систем обнаружения аномального поведения пользователя имеется ряд сложностей:

– построение профиля нормального поведения пользователя является трудно формализуемой и трудоемкой задачей, требующей от администратора большой предварительной работы;

– определение граничных значений характеристик поведения пользователя для снижения вероятности появления ошибок первого и второго рода.

Для составления профиля нормального поведения пользователя может использоваться следующая информация:

– обычное число входов в данное время в течение дня, предполагаемое самое раннее время входа, предполагаемая максимальная длительность входа;

– предполагаемый тип использования ресур-

сов, который должна поддерживать данная вычислительная система;

– число IP-адресов, с которыми были взаимодействия, объемы переданного/полученного трафика (пакетов), число клиентских (серверных) портов TCP/UDP, на которых были взаимодействия, количество сессий, число уникальных значений типов и кодов ICMP, количество появлявшихся уникальных битов в поле флагов TCP-заголовка и др.;

– попытка запустить или установить программное обеспечение, которое относится к категории системных программ;

– попытка изменения процесса загрузки ОС или внесение изменений в BIOS;

– создание новых разделов на диске;

– установка драйвера;

– попытка добавить нового пользователя в системе или изменить уже имеющийся;

– попытка загрузки операционной системы в безопасном режиме;

– действия, направленные на заполнения анкет, регистрацию на неизвестном сайте с вводом личных/конфиденциальных данных;

– работа в Internet через прокси-серверы или использование ПО для обеспечения анонимности;

– частота чтения и записи некоторых файлов, число отказов на запросы чтения или записи некоторых файлов и другие параметры доступа к файлам.

Технология обнаружения аномалий ориентирована на выявление новых типов атак, однако ее недостатком является необходимость постоянного обучения.

На данный момент нет систем, автоматически анализирующих все действия пользователя при работе с распределенной информационно-вычислительной системой. Такая возможность частично реализована в системах обнаружения атак и системах противодействия утечки конфиденциальной информации, но и там аспект анализа поведения пользователя достаточно узок и нет полноценного анализа поведения пользователя, – рассматривается лишь определенный перечень поступков пользователя в информационной системе.

Заключение

Предложенный подход к разработке системы мониторинга аномального поведения пользователя в распределенных информационно-вычислительных системах призван повысить их защищенность, – в банковской системе, например, за счет повышения достоверности распознавания несанкционированных транзакций клиентов и сотрудников. Подход применим для защиты межбанковских переводов, переводов пользователя при онлайн-банкинге с домашнего компьютера или смартфона и работе с банкоматом в общественном месте.

Литература

1. Развитие информационных угроз в первом квартале 2019 года // Все об интернет-безопасности. URL: http://securelist.ru/analysis/malware-quarterly/19176/razvitie-informacionnyx-ugroz-v-pervom-kvartale-2019-goda (дата обращения: 20.12.2020).
2. Анализ угроз информационной безопасности // Портал об интернет-безопасности. URL: https://www.anti-malware.ru/analytics/Threats_Analysis (дата обращения: 20.12.2020).
3. Kaspersky Security Bulletin 2019. Эволюция угроз информационной безопасности в бизнес-среде // Все об интернет-безопасности. URL: https://securelist.ru/analysis/ksb/27519/kaspersky-security-bulletin-2015-evolyuciya-ugroz-informacionnojbezopasnosti-v-biznes-srede (дата обращения: 20.12.2020).
4. Развитие информационных угроз во втором квартале 2019 года. Статистика // Все об интернет-безопасности. URL: https://securelist.ru/analysis/malware-quarterly/29062/it-threat-evolution-in-q2-2016-statistics (дата обращения: 20.12.2020).
5. Статистика реальных инцидентов ИБ в индустриальных системах // Все об интернет-безопасности. URL: http://www.securitylab.ru/blog/personal/Business_without_danger/38672.php (дата обращения: 20.12.2020).
6. Средства защиты от внутренних угроз // Информационная безопасность. URL: http://www.itsec.ru/articles2/techobzor/sredstva-zaschity-ot-vnytrennih-ugroz (дата обращения: 20.12.2020).
7. Угрозы информационной безопасности: обзор и оценка. Комплексная защита информации на предприятии // Проактивная защита компьютера от вредоносных программ. URL: http://rus.safensoft.com/security.phtml?c=791 (дата обращения: 20.12.2020).
8. Источники угроз информационной безопасности России // Международные отношения. URL: http://textbooks.studio/uchebnik-mejdunarod-nie-otnosheniya/istochniki-ugroz-informatsion-noy-bezopasnosti.html (дата обращения: 20.12.2020).

9. Внутренние и внешние угрозы информационной безопасности // Защита информации. URL: http://www.shpionam.net/vnutrennie-i-vneshnie-ugrozi-infbezopas-nosti.htm (дата обращения: 20.12.2020).
10. Угрозы информационной безопасности // Информационная безопасность. URL: http://www.kirillykk.narod.ru/ugroz.html (дата обращения: 20.12.2020).
11. Угрозы ИБ // Угрозы информационной безопасности. URL: https://ru.wikipedia.org/wiki/Угрозы_Информационной_безопасности (дата обращения: 20.12.2020).
12. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации // Информатика и системы управления. 2012. № 1 (31). С. 28–35.
13. Несанкционированный доступ к источникам конфиденциальной информации // Техника для спецслужб. URL: http://www.bnti.ru/showart.asp?aid=726&lvl=04 (дата обращения: 20.12.2020).
14. Защита рабочих станций от несанкционированного доступа при помощи Secret Disk Enterprise // Компания «Аладдин РД». URL: https://www.aladdin-rd.ru/company/pressroom/articles/44855 (дата обращения: 20.12.2020).
15. Компьютерная безопасность. Требования к функциональной безопасности системных средств и средств защиты информации // Информационные технологии в бизнесе. URL: http://www.npp-itb.spb.ru/publications/1.html (дата обращения: 20.12.2020).
16. Сравнение DLP-систем 2019 // Открытые системы. URL: http://www.osp.ru/win2000/2008/02/4871088 (дата обращения: 20.12.2020).
17. Расширенный анализ рынка DLP-систем в России 2014–2019 // Информационная безопасность. URL: https://www.antimalware.ru/analytics/Market_Analysis/extended_analysis_russian_dlp_market (дата обращения: 20.12.2020).
18. Сравнение DLP-систем // Открытые системы. URL: https://www.osp.ru/winitpro/2014/01/13039197 (дата обращения: 20.12.2020).
19. Модель Гогена – Мезигера // Модели защиты. URL: http://256bit.ru/besopas/indefik119.html (дата обращения: 20.12.2020).
20. Система адаптивного управления и контроля создания сигнатур вирусов на основе поведения пользователей // Информационный справочник. URL: http://www.findpatent.ru/patent/253/2534935.html (дата обращения: 20.12.2020).
21. IDS/IPS-системы обнаружения и предотвращения вторжений и хакерских атак // Информация и безопасность. URL: http://www.altell.ru/solutions/by_technologies/ids (дата обращения: 20.12.2020).
22. Системы обнаружения и предотвращения вторжений // Сетевые технологии. URL: http://netconfig.ru/server/ids-ips (дата обращения: 20.12.2020).
23. Нейронная система обнаружения аномального поведения вычислительных процессов микроядерных операционных систем // Сетевые технологии. URL: http://tekhnosfera.com/neyrosetevaya-sistema-obnaruzheniya-anomalnogo-povedeniya-vychislitelnyh-protsessov-mikroyadernyh-operatsionnyh-sistem (дата обращения: 20.12.2020).
24. Система обнаружения аномального поведения абонентов телефонной сети // Системы обнаружения аномалий. URL: http://www.academia.edu/8525607 (дата обращения: 20.12.2020).

Получено 25.12.2020

Ряполова Елена Ивановна, к.п.н., доцент кафедры математических и естественно-научных дисциплин Оренбургского филиала Поволжского государственного университета телекоммуникаций и информатики (ОФ ПГУТИ). 460060, Российская Федерация, г. Оренбург, ул. Салмышская, 47, кв. 101. Тел. +7 906 843-86-00. E-mail: ananeva_ei@mail.ru

Преснов Алексей Андреевич, к.п.н., доцент, директор ОФ ПГУТИ. 460022, Российская Федерация, г. Оренбург, ул. Пролетарская/Юркина, 249/76. Тел. +7 922 855-09-99. E-mail: presnov.aleksey@mail.ru

Цветкова Кристина Евгеньевна, к.п.н., доцент, зам. директора по учебной работе ОФ ПГУТИ. 460022, Российская Федерация, г. Оренбург, ул. Пролетарская/Юркина, 249/76. Тел. +7 987 776-97-97. E-mail: ke-tsvetkova@mail.ru

DEVELOPMENT OF A METHOD FOR MONITORING ANAMOUS BEHAVIOR OF A USER IN A DISTRIBUTED INFORMATION COMPUTER SYSTEM: BUILDING A MATHEMATICAL MODEL

Ryapolova E.I., Presnov A.A., Tsvetkova K.E.
Orenburg Branch of the Volga State University
of Telecommunications and Informatics, Orenburg, Russian Federation
E-mail: presnov.aleksey@mail.ru

The article is devoted to the analysis of the problem of developing a monitoring system for anomalous user behavior in distributed information computing systems and the construction of a mathematical model of the developed system. The study analyzes modern methods for analyzing user behavior in the information system. The main attention is paid to the fact that the existing methods of protecting information systems have a number of shortcomings, which can be corrected when using the developed method, while the method provides protection from both internal and external violators. To develop a monitoring system for abnormal user behavior in distributed information computing systems, it is necessary to solve a number of problems: to analyze methods for monitoring user behavior in the information system; build an objective function and select criteria for assessing the quality of methods for analyzing anomalous user behavior in a distributed information computing system. The study used the methods of information security theory, automata theory, pattern recognition theory and the theory of computing systems design.

Keywords: *abnormal user behavior, monitoring of user behavior, information security systems, distributed information system, automaton model, DLP systems*

DOI: 10.18469/ikt.2021.19.1.11

Ryapolova Elena Ivanovna, Orenburg Branch of the Povolzhskiy State University of Telecommunications and Informatics, apt. 101, 47, Salmyshskaya Street, Orenburg, 460060, Russian Federation; Associate Professor of Department of Mathematical and Natural Science Disciplines, PhD in Pedagogy, Associate Professor. Tel. +7 906 843-86-00. E-mail: ananeva_ei@mail.ru

Presnov Aleksey Andreyevich, Orenburg Branch of the Povolzhskiy State University of Telecommunications and Informatics, 249/76, Proletarskaya Street / Yurkina Street, Orenburg, 460022, Russian Federation; Director of Orenburg Branch of the PSUTI, Head of Department of Humanities and Socio-economic Disciplines, PhD in Pedagogy, Associate Professor. Tel. +7 922 855-09-99. E-mail: presnov.aleksey@mail.ru

Tsvetkova Kristina Evgenievna, Orenburg Branch of the Povolzhskiy State University of Telecommunications and Informatics, 249/76, Proletarskaya Street / Yurkina Street, Orenburg, 460022, Russian Federation; Deputy Director for educational work of Orenburg Branch of the PSUTI, PhD in Pedagogy, Associate Professor Department of Humanities and Socio-economic Disciplines. Tel. +7 987 776-97-97. E-mail: ke-tsvetkova@mail.ru

References

1. IT threat evolution Q1 2019. Everything about internet security. URL: http://securelist.ru/analysis/malware-quarterly/19176/razvitie-informaci-onnyx-ugroz-v-pervom-kvartale-2019-goda (accessed: 20.12.2020). (In Russ.)
2. Analysis of information security threats. Internet security portal. URL: https://www.anti-malware.ru/analytics/Threats_Analysis (accessed: 20.12.2020). (In Russ.)
3. Kaspersky Security Bulletin 2019. The Evolution of Information Security Threats in the Business Environment. Everything about internet security. URL: https://securelist.ru/analysis/ksb/27519/kaspersky-security-bulletin-2015-evolyuciya-ugroz-informacionnojbezopasnosti-v-biznes-srede (accessed: 20.12.2020). (In Russ.)

4. IT threat evolution Q2 2019. Statistics. Everything about internet security. URL: https://securelist.ru/analysis/malware-quarterly/29062/it-threat-evolution-in-q2-2016-statistics (accessed: 20.12.2020). (In Russ.)
5. Statistics of real information security incidents in industrial systems. Everything about internet security. URL: http://www.securitylab.ru/blog/personal/Business_without_danger/38672.php (accessed: 20.12.2020). (In Russ.)
6. Means of protection against internal threats. Information Security. URL: http://www.itsec.ru/articles2/techobzor/sredstva-zaschity-ot-vnytrennih-ugroz (accessed: 20.12.2020). (In Russ.)
7. Information Security Threats: Review and Assessment. Comprehensive information protection at the enterprise. Proactive protection of your computer against malware. URL: http://rus.safensoft.com/security.phtml?c=791 (accessed: 20.12.2020). (In Russ.)
8. Sources of threats to information security in Russia. Sources of information security threats. URL: http://textbooks.studio/uchebnik-mejdunarodnie-otnosheniya/istochniki-ugroz-informatsionnoy-bezopasnosti.html (accessed: 20.12.2020). (In Russ.)
9. Internal and external threats to information security. Protection of information. URL: http://www.shpionam.net/vnutrennie-i-vneshnie-ugrozi-infbezopas-nosti.htm (accessed: 20.12.2020). (In Russ.)
10. Information security threats. Information Security. URL: http://www.kirillykk.narod.ru/ugroz.html (accessed: 20.12.2020). (In Russ.)
11. Information security threats. Information security threats. URL: https://ru.wikipedia.org/wiki/Ugrozy_Informatsionnoj_bezopasnosti (accessed: 20.12.2020). (In Russ.)
12. Mironova V.G. Confidential Information Security Intruder Model. *Informatika i sistemy upravlenija*, 2012, no. 1 (31), pp. 28–35. (In Russ.)
13. Unauthorized access to sources of confidential information. Equipment for special services. URL: http://www.bnti.ru/showart.asp?aid=726&lvl=04 (accessed: 20.12.2020). (In Russ.)
14. Protecting workstations from unauthorized access with Secret Disk Enterprise. Aladdin RD company. URL: https://www.aladdin-rd.ru/company/pressroom/articles/44855 (accessed: 20.12.2020). (In Russ.)
15. Computer security. Requirements for the functional safety of system tools and information protection tools. Information technology in business. URL: http://www.npp-itb.spb.ru/publications/1.html (accessed: 20.12.2020). (In Russ.)
16. Comparison of DLP systems 2019. Open systems. URL: http://www.osp.ru/win2000/2008/02/4871088 (accessed: 20.12.2020). (In Russ.)
17. Extended analysis of the DLP systems market in Russia 2014-2019. Information Security. URL: https://www.antimalware.ru/analytics/Market_Analysis/extended_analysis_russian_dlp_market (accessed: 20.12.2020). (In Russ.)
18. Comparison of DLP systems. Open systems. URL: https://www.osp.ru/winitpro/2014/01/13039197 (accessed: 20.12.2020). (In Russ.)
19. The Gauguin-Mesiger model. Protection models. URL: http://256bit.ru/besopas/indefik119.html (accessed: 20.12.2020). (In Russ.)
20. A system for adaptive management and control of virus signature generation based on user behavior. Information reference book. URL: http://www.findpatent.ru/patent/253/2534935.html (accessed: 20.12.2020). (In Russ.)
21. IDS / IPS systems for detection and prevention of intrusions and hacker attacks. Information and security. URL: http://www.altell.ru/solutions/by_technologies/ids (accessed: 20.12.2020). (In Russ.)
22. Intrusion detection and prevention systems. Network technologies. URL: http://netconfig.ru/server/ids-ips (accessed: 20.12.2020). (In Russ.)
23. A neural system for detecting anomalous behavior of computing processes in microkernel operating systems. Network technologies. URL: http://tekhnosfera.com/neyrosetevaya-

sistema-obnaruzheniya-anomalnogo-povedeniya-vychislitelnyh-protsessov-mikroyadernyh-operatsionnyh-sistem (accessed: 20.12.2020). (In Russ.)
24. A system for detecting anomalous behavior of telephone subscribers. Anomaly detection systems. URL: http://www.academia.edu/8525607 (accessed: 20.12.2020). (In Russ.)

Received 20.12.2020

ТЕХНОЛОГИИ ЦИФРОВОЙ ЭКОНОМИКИ

УДК 004.852

МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ ДЛЯ РАСПОЗНАВАНИЯ ЧЕЛОВЕЧЕСКОЙ АКТИВНОСТИ С ИСПОЛЬЗОВАНИЕМ ДАТЧИКОВ ОКРУЖАЮЩЕЙ СРЕДЫ

Трошин А.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: a.v.troshin77@yandex.ru

Распознавание человеческой активности представляет собой быстро развивающуюся область исследований, целью которой является определение типа поведения людей на основе собираемых данных. Системы распознавания человеческой активности находят широкое применение в медицине, спорте, производстве и многих других сферах. Данные для систем распознавания могут быть получены при помощи видеонаблюдения, а также с использованием различного рода датчиков. Датчики окружающей среды обладают рядом преимуществ: простота, дешевизна и широкое применение в системах «умного дома». Для обработки данных в системах распознавания часто используются методы машинного обучения. Данная статья посвящена приложению различных методов машинного обучения к распознаванию человеческой активности на основе данных, полученных с датчиков окружающей среды «умного дома».

Ключевые слова: *методы машинного обучения, распознавание человеческой активности, датчики окружающей среды*

Введение

Распознавание человеческой активности (Human Activity Recognition – HAR) является быстро развивающейся областью исследований, целью которой является идентификация действий людей на основе собираемых данных [1–3]. Распознавание человеческой активности находит широкое применение в медицине: диагностика ряда заболеваний, уход за пожилыми людьми и инвалидами; в производстве: отслеживание действий и реакции персонала в различных ситуациях; в спорте: оценка уровня подготовки спортсменов.

В настоящее время существует два основных направления развития систем HAR, определяемых типом используемых данных [1–3]: системы на основе видеонаблюдения и системы на основе данных, собираемых с различного вида датчиков. В системах первого типа данные представляют собой видеоизображения человеческой деятельности, которые необходимо отнести к заранее определенным классам. В системах второго типа данными являются показания датчиков, закрепляемых на теле человека или устанавливаемых в окружающей человека среде, на основе этих данных требуется классифицировать текущую человеческую активность.

Несмотря на то что в области распознавания изображений были получены впечатляющие результаты, внедрение систем HAR на основе видеонаблюдения на практике может привести к ряду затруднений. Во-первых, для надежной работы таких систем необходимо получение изображений высокого разрешения и четкости, что может потребовать использования достаточно дорогостоящих видеокамер. Во-вторых, мониторинг активности в нескольких помещениях, а также наличие различных закрывающих обзор объектов делает необходимым использование нескольких видеокамер, что значительно удорожает внедрение систем данного типа. И в-третьих, распознавание активности с помощью видеонаблюдения в личных помещениях, что актуально, например, при наблюдении за пожилыми людьми, часто может быть неприемлемо из-за нарушения частной жизни и раскрытия персональных данных [1–3].

Большое распространение умных устройств, таких как смартфоны и фитнес-браслеты, которые уже снабжены встроенными датчиками,