УДК 004.732

С.Ю. Исхаков, А.Ю. Исхаков, А.А. Шелупанов

Алгоритм применения краткосрочного прогнозирования для выявления инцидентов информационной безопасности посредством анализа сетевого трафика

Представлены материалы по расширению методического аппарата выявления инцидентов информационной безопасности путем применения методов визуализации к данным, полученным в результате использования краткосрочного прогнозирования. Рассмотрены способы повышения точности прогнозирования поведения сетевого трафика за счет автоматизации определения области допустимых значений и применения механизмов варьирования доверительных интервалов. Авторами представлен алгоритм применения метода Хольта–Винтерса для анализа сетевого трафика, позволяющий выявлять нетипичное поведение сетевых инфраструктур и своевременно обнаруживать инциденты. Существенным дополнением к алгоритму является предложенный механизм визуализации, применение которого обеспечивает возможность интерпретации полученных данных. При этом визуализация данных рассматривается как средство совершенствования методов управления инцидентами, поскольку информация о состоянии защищенности телекоммуникационной инфраструктуры может быть использована для обнаружения причин возникновения инцидентов и их расследования. Предложены варианты ускорения адаптации к реальным объектам сетевой инфраструктуры полученных моделей с помощью подбора коэффициентов, что позволяет снизить промежуток времени и объем данных, необходимые для начала формирования прогнозных значений. Рассмотрен лабораторный стенд и представлены результаты проведенных экспериментов, сформулированы основные преимущества предложенного подхода и выявленные технологические ограничения, что позволило определить задачи для следующих этапов исследования, в том числе проведения экспериментов по применению правил, ограничивающих глубину корреляции, для повышения стабильности работы и скорости поиска при больших объемах обрабатываемых данных.

Ключевые слова: алгоритм, краткосрочное прогнозирование, инцидент, сетевой трафик, визуализация.

doi: 10.21293/1818-0442-2018-21-4-44-50

Повсеместное применение сетевых технологий приводит не только к расширению возможностей инфокоммуникаций, но и к появлению новых угроз и векторов атак злоумышленников. При этом трафик, генерируемый пользователями корпоративных сервисов, является одним из наиболее полных и независимых источников информации о процессах, происходящих в ИТ-инфраструктуре предприятия, а результаты его анализа могут позволить получать информацию о протекании бизнес-процессов. Решение задачи по контролю и анализу сетевого трафика сопряжено с рядом важных аспектов в части анализа комбинаций запросов к различным сервисам, а также анализа состояния сегментов локальной сети и магистральных каналов связи. Большинство исследований в области анализа сетевого трафика, например [1–4], относятся к узким предметным областям и посвящены изучению трафика определенных классов. Однако характер сетевой активности различных пользователей и сервисных приложений имеет гетерогенную природу, поэтому применимость для анализа трафика некоторого единого метода на основе выделения устойчивых фрагментов и формирования шаблонов или пороговых значений, не представляется перспективным решением задачи.

По мнению авторов, наиболее актуальным подходом к анализу поведения сетевого трафика для выявления нетипичного поведения объектов инфраструктур, свидетельствующего о наступлении инцидентов информационной безопасности, является развитие алгоритмического аппарата по примене-

нию и адаптации методов краткосрочного прогнозирования, поскольку они позволяют выявлять тренды, относящиеся к коротким периодам, что позволяет делать краткосрочные прогнозы и повысить точность выявления инцидентов.

Кроме того, актуальным на сегодняшний день направлением в решении обозначенной задачи является развитие методических и практических наработок в части использования средств визуализации для совершенствования методов управления инцидентами. В статье также предлагаются механизмы расширения методического аппарата путем применения методов визуализации к данным, полученным в результате использования краткосрочного прогнозирования для выявления инцидентов информационной безопасности, поскольку информация о состоянии защищенности сетевой инфраструктуры может быть использована для обнаружения инцидентов, а также их расследования и принятия решений.

Экспоненциальное сглаживание временных рядов

Гетерогенная природа сетевого трафика и наличие нестационарных изменений обуславливают тот факт, что в процессе выявления инцидентов информационной безопасности наибольшую практическую ценность будут иметь краткосрочные прогнозы значений исследуемых параметров при условии, что глубина упреждения находится в рамках эволюционного периода. В [5–7] рассмотрены классификация методов прогнозирования и подходы к их применению в процессе выявления инцидентов и уста-

новлено, что основными преимуществами метода Хольта–Винтерса в рамках рассматриваемой задачи являются минимальный период определения трендов и возможность их учета при составлении прогнозных значений на следующие моменты времени. На текущем этапе исследования рассмотрены варианты применения этого метода совместно с механизмом визуализации на базе аналитической поисковой системы Elasticsearch [8].

При использовании вышеуказанного метода временной ряд представляется в виде суммы базовой компоненты, тренда и компонента сезонности, к каждому из которых применяется экспоненциальное сглаживание. Предполагается, что все компоненты изменяются во времени, а под периодом понимается единица временного ряда. При этом в (1) компонент сезонности за прошлый наблюдаемый период обозначен как c_{x+1-D} :

$$\hat{y}_{x+1} = a_x + b_x + c_{x+1-D}, \quad (1)$$

где $\hat{y}_{x+1}$ – прогноз на следующий период; x – текущий период; a_x – базовый компонент; b_x – тренд; c_x – компонент сезонности; D – длина сезона (в периодах).

Определение начальных значений компонент осуществляется в соответствии с формулами (2). При этом в случае с базовым компонентом оно является равным среднему арифметическому для первого сезона наблюдений:

$$a_0 = \sum_{x=1}^D \frac{y_x}{D}, \quad (2)$$

$$b_0 = \frac{1}{D} \left(\frac{y_{x=1} - y_1}{D} + \frac{y_{x=2} - y_2}{D} + \dots + \frac{y_{D+D} - y_D}{D} \right),$$

$$c_0 = y_1 - a_0,$$

где y_x – значение наблюдаемого параметра в текущий период.

Согласно (3) для получения прогнозируемого значения параметра с третьего периода к текущему значению необходимо применить коэффициенты α , β , γ , изменяющиеся в интервале (0,1). Применение этих коэффициентов позволяет распределить влияние на прогноз между текущим и предшествующим значением:

$$a_x = \alpha(y_x - c_{x-D}) + (1-\alpha)(a_{x-1} + b_{x-1}), \quad (3)$$

$$b_x = \beta(a_x - a_{x-1}) + (1-\beta)b_{x-1},$$

$$c_x = \gamma(y_x - a_x) + (1-\gamma)c_{x-D}.$$

В методических указаниях по выбору α , β , γ , например работы [4, 7, 10], определено, что возможность адаптировать прогноз за короткий промежуток времени достигается с помощью как минимум одного коэффициента. В проводимом исследовании для этой цели наилучшим образом подходит базовый компонент, поскольку γ определяет вклад сезонности, а β необходим для выявления линии тренда, которая изменяется медленнее других компонентов. При этом β следует выбирать так, чтобы сезон не составлял большую часть веса сглаживания.

Для выявления инцидента следует формировать прогноз на основе оценки предыдущих значений исследуемых показателей сетевого трафика и сравнивать его с текущим значением. Определение отклонений в поведении временных рядов может быть организовано путем проверки для каждой точки временного ряда вхождения этого значения в доверительный интервал, представленный в виде области допустимых значений.

В исследованиях [5–7, 9] показано, что при решении подобных задач применение четко определенных критериев и допустимых значений обуславливает высокую вероятность ошибок первого рода. Как было упомянуто ранее, гетерогенная природа трафика телекоммуникационных сетей обуславливает необходимость механизма варьирования области допустимых значений вместо применения четко определенных шаблонов и пороговых значений. В данной работе предлагается определять отклонения в тренде только после выявления определенного количества значений, не входящих в границы доверительного интервала, рассчитанного для данного момента времени.

На основании вышеизложенного можно сделать вывод, что поскольку наблюдение за различными параметрами сетевого трафика позволяет получать необходимые для применения метода Хольта–Винтерса временные ряды, а возможности этого метода позволяют выявлять краткосрочные тренды, то данный метод может быть использован для прогнозирования изменений параметров объектов сетевой инфраструктуры. Предложенный подход основан на сравнении ранее наблюдаемых значений с прогнозными значениями на текущий период, при том, что сравнение проводится на основе области допустимых значений, границы которых определяются для каждого вновь получаемого значения контролируемого параметра.

Алгоритм анализа сетевого трафика с помощью краткосрочного прогнозирования

Таким образом, в результате мониторинга параметров трафика между различными объектами сетевой инфраструктуры можно формировать временные ряды. Применение к таким рядам методов прогнозирования позволяет выявить тренды и отклонения в них, а полученные в результате данные могут быть обработаны аналитической поисковой системой Elasticsearch. Каждое наблюдаемое значение, выходящее за пределы доверительного интервала на данный период, помечается как факт сбоя в работе. К инциденту же относится факт превышения допустимого количества сбоев в пределах «плавающего окна». Данные о значениях контролируемых параметров помещаются в хранилище, а их расположение внутри хранилища определено созданными моделями объектов инфраструктуры. На рис. 1 представлен алгоритм анализа сетевого трафика, основанный на методе Хольта–Винтерса и позволяющий выявлять инциденты информационной безопасности посредством анализа сетевого трафика в рамках контроля параметров на исследуемом объекте.

Рис. 1. Алгоритм анализа сетевого трафика с помощью метода Хольта–Винтерса

Каждое новое значение перед помещением в хранилище сравнивается с прогнозированным на данный момент времени значением с учетом допускаемых отклонений. Если значение не укладывается в допустимый интервал возможных значений, увеличивается счетчик отклонений. После этого определяется состояние счетчика, и в случае превышения порога фиксируется инцидент. Затем заново рассчитываются коэффициенты, прогнозируемое значение и доверительный интервал. Используемые на рис. 1 обозначения представлены ниже.

- 1) L – величина «плавающего окна», $K \leq S$;
- 2) S – количество периодов наблюдения, составляющих один сезон;
- 3) $N_{\max}$ – максимальное число отклонений для определения момента фиксации инцидента;
- 4) N – счетчик числа отклонений;
- 5) $ADM(y_x)$ – область допустимых значений, определенная для y в момент времени x .

Рассмотренные выше ограничения обуславливают возможность применения алгоритма не ранее чем с третьего сезона наблюдения. Помимо непосредственного определения инцидентов, необходимо обеспечить механизм выявления причины его возникновения для адекватной реакции и проведения расследования, например, в случае резкого снижения объема трафика необходимо выяснить причину. Наступлению каждого инцидента предшествуют

различные события: сканирование сетевых ресурсов, попытки установить соединение, подозрительные вложения в почтовом трафике. Визуализация данных, полученных в ходе применения вышеизложенного алгоритма, позволяет объединить и группировать их для определения причины возникновения инцидента.

Визуализация данных как средство совершенствования методов управления инцидентами

Возможность визуализации информации о событиях и инцидентах в сетевой инфраструктуре позволяет не только реализовать новую форму представления данных, но и обеспечить механизмы их интерпретации и последующего принятия решений в отношении необходимости оперативной корректировки деятельности по реагированию на инциденты.

В [7, 9, 11] представлены подходы к формализации данной задачи, в [10] предложена методика для визуализации данных о состоянии топологии сетей различного масштаба. Основным недостатком данного методического обеспечения является направленность на визуальное представление топологии сети и состояния сетевых объектов (хостов). Ниже приведен предлагаемый механизм визуализации данных, полученных в результате применения методов краткосрочного прогнозирования к временным рядам, сформированным на основе контроля трафика сетевой инфраструктуры.

Шаг 1. Определение и выбор ИТ-активов, являющихся источниками данных в рамках конкретной решаемой задачи. Для каждого ИТ-актива, используемого в конкретной задаче необходимо определить механизмы транспорта информации о параметрах трафика (интерфейсы и протоколы взаимодействия).

Шаг 2. Провести анализ параметров с целью выделения тех, которые имеют практическую ценность для обнаружения инцидентов.

Шаг 3. В соответствии с рассмотренными выше методами разработать сбор информации и применение к ней краткосрочного прогнозирования.

Шаг 4. В соответствии с рассмотренными выше методами определить необходимость и разработать способы агрегации сообщений, определенных на шаге 3. В случае отсутствия необходимости агрегации для конкретного типа сообщений данный шаг может быть пропущен.

Шаг 5. Основываясь на рассмотренном выше алгоритме, организовать получение анализа сетевого трафика и формирование данных о сбоях и инцидентах, поскольку именно они будут являться данными, подлежащими визуализации. При этом необходимо определить принципиальные схемы событий, описывающих инциденты (определить субъекты, объекты и производимые действия).

Шаг 6. Обеспечить накопление событий и записей об инцидентах в хранилище, обеспечивающем возможность работы с большими данными и предоставляющем функции поиска, в том числе поиска с нечеткими условиями.

Шаг 7. Определить возможные для использования графические модели [10] и скорректировать их с учетом сценария работы сети. При определении моделей возможно использование критериев эффективности восприятия подсистемы визуализации [10].

Шаг 8. В соответствии с определенными на шаге 7 моделями реализовать визуализацию данных об инцидентах, извлекаемых из хранилища с помощью средств поиска, с использованием программных компонентов или отдельных продуктов.

Для практической реализации предложенного авторами механизма необходимо решить проблемы обработки больших данных. В [8, 12] представлены обзоры рынка современных решений в области визуализации данных, среди которых стоит отметить Elasticsearch. Это свободно распространяемая поисковая система с распределенным аналитическим ядром. Используется в составе с Logstash [8] и Kibana [Там же]. Для взаимосвязи компонентов используется платформа RabbitMQ [Там же]. На основании данных обзоров на текущем этапе исследований был выбран вышеуказанный продукт, основными преимуществами которого являются поддержка кластерной архитектуры (планируется к реализации на следующих этапах работы), централизованное хранение данных и возможность полнотекстового поиска в реальном времени по большим объемам разнотипных структур.

На базе стационарного компьютера был развернут стенд, имеющий следующие характеристики: 4-ядерный процессор с тактовой частотой 3,1 ГГц; 16 Гб ОЗУ, на котором установлен стек ELK в составе: Elasticsearch 6.2.0, Logstash 6.2.0, Kibana 6.2.0. Стенд был развернут на базе операционной системы CentOS 7. Скорость индексирования в Elasticsearch составила 15000 пакетов в секунду при средней загрузке каждого из ядер процессора 50%. Однако поскольку основной целью эксперимента была оценка времени поиска среди индексированных данных, были предприняты попытки отправки запросов в Elasticsearch. Среднее время поиска составило 1,02 мс при длине запроса 6 символов. На рис. 2 представлен пример визуализации данных.

Рис. 2. Пример визуализации данных использования метода Хольта-Винтерса для анализа загруженности одного из сетевых интерфейсов на маршрутизаторе с применением механизма доверительных интервалов

Несмотря на достигнутые результаты в части поиска данных, были выявлены следующие проблемы при обработке данных. Во-первых, стек ELK критичен к ошибкам типа «OutOfMemory» [14, 15], что приводит к частым перебоям в ходе его использования. Во-вторых, высокая скорость поиска в больших объемах данных сопровождается низким коэффициентом восстановления работоспособности

в случае перебоев, что зачастую приводит к безвозвратной потере данных.

Одним из наиболее практичных подходов является применение правил, ограничивающих глубину корреляции и разделение базы событий на онлайн- и архивную части. Например, события, произошедшие за последние сутки, хранятся в онлайн-базе, по истечении таймера помещаются в архивную часть. Для

работы с большим объемом данных применяются различные специализированные поисковые движки и инструменты визуализации.

На следующих этапах исследования будут проведены эксперименты по повышению стабильности работы и сохранности обрабатываемых данных. В некоторых публикациях [8, 10, 16] представлены данные смежных экспериментов. Ниже рассмотрены попытки сравнить полученные данные.

1. Аппаратные ресурсы. В большинстве рассмотренных примеров [10] используется распределение нагрузки на потоки в кластере из нескольких узлов (серверов). В данном случае использовались виртуальные машины на базе одного физического стенда, характеристики которого указаны выше.

2. Скорость индексирования и анализа используемых данных. В связи с невозможностью проведения экспериментов при равных условиях на идентичном оборудовании [8] проведение какой-либо количественной оценки по данному параметру не представляется возможным. Однако такие сравнения, вероятно, будут проведены на следующих этапах исследования.

3. Механизм обработки данных. В эксперименте, как и в большинстве смежных исследований [8, 10], применялась потоковая обработка.

4. Пул задач. Все рассмотренные задачи в смежных исследованиях имеют конкретную постановку, и получить результаты их сравнения в численном виде не представляется возможным. Однако на следующем этапе исследования будет возможно применение предлагаемого методического обеспечения для решения различных задач и получения количественных оценок будущих результатов.

Заключение

В ходе исследования разработан алгоритм применения метода Хольта–Винтерса для анализа сетевого трафика с целью выявления нетипичного поведения сетевых инфраструктур и обнаружения инцидентов информационной безопасности. В дополнение к этому алгоритму предложен механизм визуализации полученных данных для обеспечения возможности их интерпретации и принятия решений по выявлению причин и расследования инцидентов.

Среди достоинств предлагаемого подхода можно выделить регулярную корректировку критериев на основе предыдущих наблюдений и возможность выявления корреляций между не связанными между собой, на первый взгляд, значениями параметров контролируемых объектов. Кроме того, в процессе наблюдения допускается корректировка всех коэффициентов, что позволяет обеспечить требуемый уровень адекватности моделей. Ограничение в части требования накопления данных перед построением прогнозных значений в решении практических задач нивелируется исходя из принципов функционирования современных телекоммуникационных сетей, а также объемов и скорости передачи данных в них.

Предложенный механизм визуализации данных является обобщением методических и практических наработок авторов в части организации сбора и об-

работки данных о состоянии сетевой инфраструктуры для выявления инцидентов информационной безопасности. При этом визуализация данных предлагается к использованию в качестве средства совершенствования методов управления инцидентами, поскольку информация о состоянии защищенности инфраструктуры может быть использована для обнаружения причин возникновения инцидентов и их расследования.

Данная работа выполнена при поддержке РФФИ (проект № 16-47-700350 p_a).

Литература

1. Легков К.Е. Проведение экспериментов по сбору трафика и моделированию методики оценки изменения качества информационного обмена в инфокоммуникационной системе специального назначения // T-Comm. – 2014. – № 5. – С. 36–44.
2. Шелухин О.И. Сравнительный анализ характеристик обнаружения аномалий трафика методами крупномасштабного анализа / О.И. Шелухин, А.В. Панкрушин // T-Comm. – 2014. – № 6. – С. 65–69.
3. Моделирование информационной безопасности на основе многомерных матриц / А.Н. Громов, А.П. Тиунов, М.С. Фоменко, В.Г. Шахов // Омский научный вестник. – 2015. – № 2 (140). – С. 212–215.
4. Iskhakova A. Analysis of the vulnerabilities of the embedded information systems of IoT-devices through the honeypot network implementation / A. Iskhakova, R. Meshcheryakov, A. Iskhakov, S. Timchenko // Proceedings of the IV International research conference information technologies in science, management, social sphere and medicine (ITSMSM 2017). – 2017. – Vol. 72. – P. 363–367.
5. Aberrant Behavior Detection in Time Series for Network Monitoring [Электронный ресурс]. – Режим доступа: https://www.usenix.org/legacy/publications/library/proceedings/lisa2000/full_papers/brutlag/brutlag_html/index.html (дата обращения: 23.11.2018).
6. Исхаков С.Ю. Прогнозирование в системе мониторинга локальных сетей / С.Ю. Исхаков, А.А. Шелупанов, С.В. Тимченко // Доклады ТУСУР. – 2012. – № 1 (25), ч. 2. – С. 100–103.
7. Soni R.S. Inventory forecasting model using genetic programming and Holt-Winter's exponential smoothing method / R.S. Soni, D. Srikanth // 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017. – 2017. – P. 2086–2091.
8. Проноза А.А. Математические модели визуализации в SIEM-системах / А.А. Проноза, А.А. Чечулин, И.В. Котенко // Труды СПИИ РАН. – 2016. – № 46 (3). – С. 90–107.
9. Kalekar P.S. Time series Forecasting using Holt-Winters Exponential Smoothing [Электронный ресурс]. – Режим доступа: <https://labs.omniti.com/people/jesus/papers/holtwinters.pdf> (дата обращения 04.12.2018).
10. Милославская Н.Г. Визуализация информации при управлении информационной безопасностью информационной инфраструктуры организации / Н.Г. Милославская, А.И. Толстой, А.И. Бирюков // Научная визуализация. – 2014. – № 2 [Электронный ресурс]. – Режим доступа: <http://sv-journal.org/2014-2/06/ru/index.php?lang=ru>, свободный (дата обращения: 04.12.2018).
11. Семёнов Д.П. Визуализация процессов информационной безопасности // Актуальные проблемы авиации и космонавтики. – 2017. – Т. 2, № 13. – С. 230–232.

12. Корреляция SIEM. [Электронный ресурс]. – Режим доступа: <https://www.securitylab.ru/analytics/431459.php> (дата обращения: 23.11.2018).

13. Буйневич М.В. Способ визуализации модулей системы обеспечения информационной безопасности / М.В. Буйневич, В.В. Покусов, К.Е. Израйлов // Вестник Санкт-Петербургского университета государственной противопожарной службы МЧС России. – 2018. – № 3. – С. 81–90.

14. Abomhara M. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks / M. Abomhara, G.M. Kien // Journal of Cyber Security. – 2015. – Vol. 4. – P. 65–88.

15. Bajer M. Building an IoT Data Hub with Elasticsearch, Logstash and Kibana // 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). – 2017. – P. 63–68.

16. Son S.J. Performance of ELK stack and commercial system in security log analysis / S.J. Son, Y. Kwon // IEEE 13th Malaysia International Conference on Communications (MICC), 2017. – 2017. – P. 187–190.

Исхаков Сергей Юнусович

Канд. техн. наук, доцент каф. безопасности информационных систем (БИС)
Томского государственного университета систем управления и радиоэлектроники (ТУСУР)
Красноармейская ул., 146, г. Томск, Россия, 634045
Тел.: +7 (382-2) 70-15-29
Эл. почта: iskhakov.sy@gmail.com

Исхаков Андрей Юнусович

Канд. техн. наук, доцент каф. БИС ТУСУРа
Красноармейская ул., 146, г. Томск, Россия, 634045
Тел.: +7 (382-2) 70-15-29
Эл. почта: iskhakovandrey@gmail.com

Шелупанов Александр Александрович

Д-р техн. наук, профессор, ректор ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 51-05-30
Эл. почта: rector@tusur.ru

Iskhakov S.Y., Iskhakov A.Y., Shelupanov A.A.

Algorithm for applying short-term forecasting for detecting information security incidents through the network traffic analysis

This article is devoted to the expansion of the methodological apparatus for identifying information security incidents by applying visualization methods to data obtained as a result of the use of short-term forecasting. Ways to improve the accuracy of predicting the behavior of network traffic by automating the determination of the range of acceptable values and using the mechanisms of varying confidence intervals are considered. The authors presented an algorithm for applying the Holt-Winters method for analyzing network traffic, which makes it possible to identify the atypical behavior of network infrastructures and detect incidents in a timely manner. At the same time, data visualization is considered as a means of improving incident management methods, since information on the security status of the telecommunications infrastructure

can be used to detect the causes of incidents and investigate them. Options have been proposed for accelerating adaptation to real objects of the network infrastructure of the models obtained using selection of the coefficients of influence of the components, which makes it possible to reduce the time interval and the amount of data necessary to start the formation of predicted values. The laboratory bench was considered and the results of the experiments were presented, the main advantages of the proposed approach and the identified technological limitations were formulated, which allowed defining tasks for the next stages of the study, including conducting experiments on the application of rules limiting the depth of correlation, to increase the stability and speed of searching for large volumes of data processed.

Keywords: algorithm, short-term forecasting, incident, network traffic, visualization.

doi: 10.21293/1818-0442-2018-21-4-44-50

References

1. Legkov K.E. Conduct experiments on the collection and traffic modeling methodology for assessing changes in the quality of information exchange in the infocommunication system of special purpose. *T-Comm*, 2014. no. 5, pp. 36–44 (in Russ).

2. Sheluhin O.I., Pankrushin A.V. The comparative analysis of characteristics of network traffic's anomalies detection with methods of wavelet analysis. *T-Comm*, 2014, no. 6, pp. 65–69 (in Russ).

3. Gromov A.N., Tiunov A.P., Fomenko M.S., Shakhov V.G. Modeling information security based on multidimensional matrices. *Omsk scientific bulletin*, 2015, no. 2, pp. 212–215 (in Russ).

4. Iskhakova A., Meshcheryakov R., Iskhakov A., Timchenko S. Analysis of the vulnerabilities of the embedded information systems of IoT-devices through the honeypot network implementation. *Proceedings of the IV International research conference information technologies in science, management, social sphere and medicine (ITSMSSM 2017)*, 2017, vol. 72, pp. 363–367. 2017 (in Russ).

5. Brutlag J. Aberrant Behavior Detection in Time Series for Network Monitoring. *Proceedings of 14th Systems Administration Conference*. Available at: http://www.use-nix.org/events/lisa00/full_papers/brutlag/brutlag_html/index.html (accessed: November 20, 2018).

6. Iskhakov S.Y., Shelupanov A.A., Timchenko S.V. Forecasting in the system of LAN monitoring. *Proceedings of TUSUR University*, 2012, vol. 1, no. 2, pp. 100–103 (in Russ.).

7. Soni R.S., Srikanth D. Inventory forecasting model using genetic programming and Holt-Winter's exponential smoothing method. *2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2017, pp. 2086–2091.

8. Pronoza A.A., Chechulin A.A., Kotenko I.V. Mathematical models of visualization in SIEM systems. *SPIIRAS Proceedings*, 2016, vol. 3, no. 46, pp. 90–107.

9. Kalekar P.S. Time series Forecasting using Holt-Winters Exponential Smoothing. *OmniTI*. Available at: <https://labs.omniti.com/people/jesus/papers/holtwinters.pdf> (accessed: December 04, 2018).

10. Miloslavskaya N.G., Tolstoy A.I., Biryukov A.I. Visualization of information at management of information security of information infrastructure of the organization. *Scientific visualization*, 2014, no. 2 (in Russ). Available at: <http://sv-journal.org/2014-2/06/ru/index.php?lang=ru> (accessed: December 04, 2018).

11. Semenov D.P. Visualization of process of information security. *Aktual'nyye problemy aviatsii i kosmonavтики*. 2017, vol. 2, no/ 13, pp. 230–232 (in Russ).

12. Korrelyatsiya SIEM. Available at: <https://www.securitylab.ru/analytics/431459.php> (in Russ). (accessed: November 23, 2018).

13. Buinevich M.V., Pokusov V.V., Izrailov K.E. Method of visualizing the modules of the information security system. *Vestnik Sankt-Peterburgskogo universiteta GPS MCHS Rossii*. 2018, no. 3, pp. 81–90 (in Russ.).

14. Abomhara M., Kien G.M. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security*, 2015, vol. 4, pp. 65–88.

15. Bajer M. Building an IoT Data Hub with Elasticsearch, Logstash and Kibana. *5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, 2017, pp. 63–68.

16. Jon S.J., Kwon Y. Performance of ELK stack and commercial system in security log analysis. *IEEE 13th Malaysia International Conference on Communications (MICC)*, 2017, pp. 187–190.

Sergey Y. Iskhakov

PhD, Assistant Professor of Department of Information Systems Security, Tomsk State University of Control Systems and Radioelectronics (TUSUR)
146, Krasnoarmeyskaya st., Tomsk, Russia, 634045
Phone: +7 (382-2) 70-15-29
Email: iskhakov.sy@gmail.com

Andrey Y. Iskhakov

PhD, Assistant professor of Department of Information Systems Security, TUSUR
146, Krasnoarmeyskaya st., Tomsk, Russia, 634045
Phone: +7 (382-2) 70-15-29
Email: iskhakovandrey@gmail.com

Alexander A. Shelupanov

Doctor of Technical Sciences, Professor, Rector TUSUR
40, Lenina pr., Tomsk, Russia, 634050
Phone.: +7 (382-2) 51-05-30
Эл. почта: rector@tusur.ru