УДК 004.056.5

А.С. Шабуров

Пермский национальный исследовательский политехнический университет,
Пермь, Россия

О РАЗРАБОТКЕ МОДЕЛИ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Обоснована актуальность проблемы компьютерных атак как наиболее опасной формы реализации угрозы информационной безопасности. Охарактеризованы информационные системы общего пользования, в наибольшей степени подверженные компьютерным атакам. Приведена оценка объектов критической информационной инфраструктуры – целей компьютерных атак. Особое внимание уделено требованиям российского законодательства, направленным на защиту критической информационной инфраструктуры. Приведена характеристика таргетированной компьютерной атаки, рассмотрены ее особенности. Предложены обобщенная структурная схема компьютерной атаки и последовательность формирования ее образа. Поставлена задача поиска эффективных алгоритмов обнаружения и анализа атак. Приведена обобщенная характеристика основных методов обнаружения и анализа компьютерных атак: методов анализа сигнатур и методов обнаружения аномальных отклонений. Проанализирована информация, необходимая для идентификации компьютерных атак. Предложены направления поиска правил для выявления эффективных способов обнаружения компьютерных атак. Поставлена задача развития алгоритмических моделей, обеспечивающих распознавание образа атаки на основании набора ее отличительных признаков. Сформулировано понятие адекватности моделей, рассмотренное в двух аспектах: адекватность прототипу и адекватность применения мер по защите информации. Приведены утверждения о целесообразности представления модели обнаружения компьютерных атак в виде композиции двух основных составляющих. Обозначена задача формирования моделей атаки на объекты критической информационной инфраструктуры. Предложена обобщенная схема формирования соответствующей модели на основе функционального подхода. Приведены необходимые аналитические выражения. Предложена теоретико-множественная модель, предполагающая построение полного множества безопасных состояний информационной системы и обнаружение на этой основе признаков компьютерных атак.

Ключевые слова: компьютерная атака, критическая информационная инфраструктура, защита информации, нейронные сети, метод обнаружения аномалий, анализ сигнатур, теория распознавания образов, функциональный подход.

A.S. Shaburov

Perm National Research Polytechnic University, Perm, Russian Federation

ON THE DEVELOPMENT OF A MODEL FOR DETECTING COMPUTER ATTACKS ON OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

The article deals with the relevance of the problem of computer attacks as the most dangerous form of information security threat materializing. It describes information systems of general use that are the most susceptible to computer attacks. The objects of critical information infrastructure are considered as the targets of computer attacks. Special focus was given to Russian legislative requirements directed to the protection of critical information infrastructure. The research considers the characteristics of the targeted computer attack and its features. The generalized structural scheme of the computer attack and the sequence of its form are examined. The article includes the search for effective algorithms for detection and analysis of the attacks. It presents the generalized characteristic of the main methods for detecting and analyzing computer attacks that are methods for analyzing signatures and methods for detecting abnormal deviations. The information needed to the identification of computer attacks is analyzed. The directions for searching and identifying the effective ways to detect computer attacks are suggested. There is the task to consider the development of algorithmic models providing the recognition of the image of an attack based on a set of its distinctive features. The concept of model adequacy is formulated, it is considered in two aspects: the adequacy of the prototype and the adequacy of the application of information protection measures. There are statements about the advisability of presenting the computer attack detection model in the form of a composition of two main components. The article includes the formation of models of attack on objects of a critical information infrastructure. There is the generalized functional scheme for the formation of the corresponding model.

There are necessary analytical expressions for the development of algorithms. The mathematical model of computer attack detection based on the functional approach is proposed. The use of the functional approach presupposes the full set construction of secure conditions of an informational system and its further detection of computer attacks signs.

Keywords: computer attack, critical information infrastructure, information security, neural networks, anomaly detection method, signature analysis, pattern recognition theory, functional approach.

Наиболее опасной формой реализации угрозы безопасности информации с точки зрения последствий их реализации является компьютерная атака. Актуальность данной проблемы подтверждается статистическим данными за истекший период 2016–2017 гг. [1]. Как правило, компьютерным атакам подвержены информационные системы (ИС) общего пользования, предполагающие значительное число субъектов, для которых функционируют данные системы, а также сложные и комплексные ИС, базирующиеся на аппаратно-программных платформах и устройствах различных производителей.

Особенно разрушительной по последствиям реализации компьютерная атака может быть в случае её воздействия на объекты критической информационной инфраструктуры (КИИ). Это послужило ключевым фактором для принятия Федерального закона «О безопасности

критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ, а также формирования и утверждения необходимых требований по безопасности информации со стороны государственных служб-регуляторов в области защиты информации [2].

В наибольшей степени опасность негативного компьютерного воздействия может проявляться для систем государственного управления, энергетического и транспортного секторов, систем связи и коммуникации, банковской сферы и др. Кроме того, дальнейшее внедрение информационных технологий во все сферы жизнедеятельности, а также реализация программы «Цифровая экономика Российской Федерации» только усугубят проблему компьютерных атак в ближайшей перспективе. Традиционно под понятием «компьютерная атака» (КА) понимается целенаправленное воздействие на информационные системы и информационно-телекоммуникационные сети программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих системах и сетях [3].

До недавнего времени обеспечение безопасности ИС осуществлялось посредством защиты от типовых, массовых информационных атак, таких как компьютерные вирусы, мошенничество, сетевые атаки, внутренние утечки и т.д. Типовые системы защиты информации стали иметь шаблонный вид и содержать в себе набор определенных, типовых средств (межсетевые экраны, антивирусные средства), которые позволяют парировать традиционные атаки. Значительную роль в повышении эффективности ИС сыграло внедрение современных комплексных решений, в том числе и применение DLP и SIEM-систем [4, 5, 6]. В то же время не все из комплексных и дорогостоящих решений в области информационной безопасности позволяли решить проблему компьютерных атак.

Тенденцией последних лет стало появление узконаправленных компьютерных атак (целевых, таргетированных), цель которых – конкретные коммерческие или государственные организации и их вычислительные сети. По мнению ряда специалистов, в ближайшее время количество подобных атак будет активно возрастать, что обусловливает необходимость их исследования и детального описания с точки зрения защищенности информационной составляющей [7].

Как правило, информационная атака предполагает наличие следующих структурных компонентов (рис. 1), необходимых и достаточных для достижения цели атаки, а именно:

– источник атаки (субъект атаки) – программа, ведущая атаку и осуществляющая непосредственное воздействие;

– используемые уязвимости ИС;

– вариант использования уязвимости ИС;

– объект информационной атаки, в качестве которого могут выступать: телекоммуникационные системы (ТС), автоматизированные системы (АС), информационно-управляющие системы (ИУС), распределенные ИУС (РИУС), и т.д.

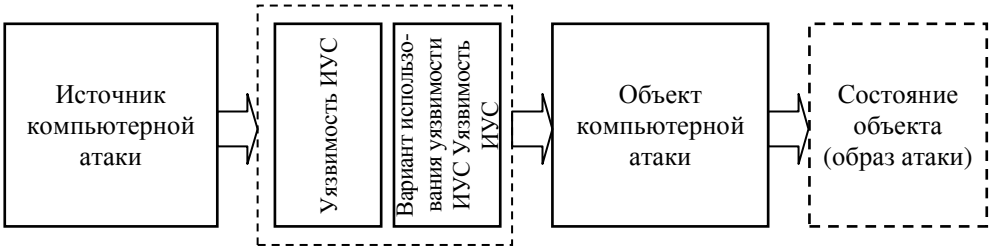

Рис. 1. Обобщенная схема формирования образа компьютерной атаки

Реализация воздействия компьютерной атаки, очевидно, приводит к изменению состояния объекта атаки, формируя ее образ как результат данного негативного воздействия. Анализ данного состояния может являться основой для формирования эффективного противодействия. Традиционно основой противодействия компьютерным атакам со стороны системы защиты информации является использование алгоритмов обнаружения и анализа атак. Как правило, методы обнаружения и анализа компьютерных атак декомпозируются на методы анализа сигнатур и методы обнаружения аномальных отклонений [8].

Методы анализа сигнатур предназначены для обнаружения известных атак и основаны на контроле программ и данных в критически важной информационной системе и эталонной сверке последовательности символов и событий в сети с базой данных сигнатур атак.

Методы обнаружения аномальных отклонений основываются на выявлении отклонений от нормального поведения системы и позволяют выявить неизвестные ранее компьютерные атаки.

Информация, необходимая для идентификации атак, представлена большим количеством данных аудита, и эффективный анализ этих данных требует внедрения автоматизированных алгоритмов. Применение систем обнаружения атак способствует повышению эффективности систем защиты информации в целом. Следовательно, эффективность применения тех или иных способов обнаружения компьютерных атак

предполагает развитие алгоритмических моделей, обеспечивающих распознавание образа атаки на основании набора отличительных признаков.

Разнообразие вариантов негативного информационного воздействия, которые могли бы служить объектами исследований, требует значительного упрощения для возможности их модельного представления, с учетом сохранения адекватности модели действительному образу атаки. Понятие адекватности моделей следует рассматривать в двух аспектах: адекватность прототипу (корректность описания соответствующей атаки) и адекватность главной цели – применение адекватных мер противодействия со стороны системы защиты [9, 10].

В литературе о системах обнаружения и анализа компьютерных атак приведенные методы не имеют достаточного математического описания. Как правило, они формализованы в виде способов и функций средств обнаружения компьютерных атак, используемых в инструментальных средствах, а также средств предупреждения и обнаружения компьютерных атак [11]. Модельное представление процессов обработки информации и связанных с ними процессов защиты информации является одним из этапов разработки и внедрения автоматизированных систем в защищенном исполнении различного назначения, в том числе для КИИ [12, 13].

Множество моделей компьютерных атак может быть описано прямым перечислением признаков в виде базы данных, что не всегда приемлемо из-за значительных потребностей памяти, либо заданием характеристического признака, позволяющего создавать модели непосредственно перед противодействием им. В любом случае целесообразно создать инструмент оперативного перечисления данных моделей, что особенно важно для объектов КИИ, имеющих свои специфические особенности.

Произвольную модель целесообразно представить в виде композиции двух основных составляющих, что позволяет разделить процессы генерации на две части:

1) синтез модели объекта КИИ, подверженной негативному информационному воздействию под влиянием компьютерной атаки;

2) синтез модели образа компьютерной атаки для адекватной защиты информации.

Следующим этапом должно стать рассмотрение свойств СЗИ, адекватности ее выбранной модели КИИ на основании имитационного моделирования полного множества возможных последствий атаки.

Таким образом, задачей моделирования является разработка генераторов (алгоритмов построения) соответствующих моделей атаки на КИИ и системы ее защиты, а также соответствующих методов исследования их защищенности. При этом КИИ является сложной по структуре и функционированию системой, традиционно представляемый набором состояний, изменяющихся как в штатном режиме функционирования, так и под воздействием последствий компьютерной атаки.

Подход к разработке системы защиты КИИ как к сложной системе предполагает в общем случае три уровня сложности: структурную сложность, сложность функционирования, сложность выбора варианта функционирования в многоальтернативных ситуациях компьютерной атаки [14]. Подобный взгляд требует моделирования с описанием всех уровней сложности в обобщенном виде, представленных на рис. 2.

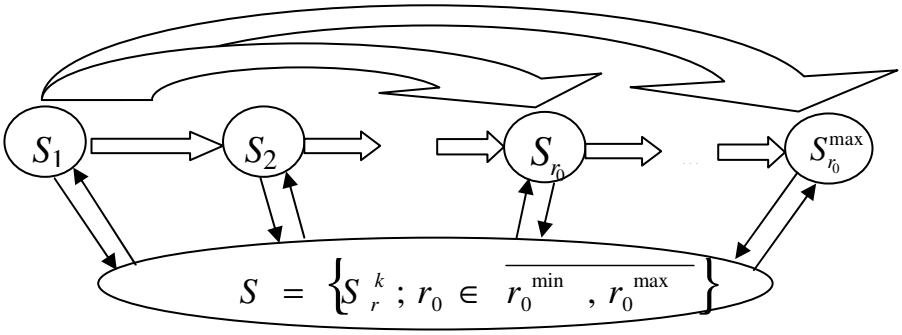

Рис. 2. Обобщенная функциональная схема формирования модели КИИ

На структурном уровне сложности описания функционирования КИИ (рис. 2) необходимо задать множество его основных состояний, важных с точки зрения реализации критически важных функций $S_0 = \left\{ S_{r_0} ; r_0 \in \overline{r_0^{min}, r_0^{max}} \right\}$, где r_0^{min} определяется необходимостью обеспечения нетревиальности модели КИИ, а r_0^{max} допустимой сложностью модели, обусловленной особенностями объектов КИИ.

Решение проблемы обнаружения компьютерной атаки предполагается на основе функционального подхода [15, 16].

Функциональное представление КИИ предполагает ее рассмотрение как выполнение элементарных функций, представляющих собой алгоритмы преобразования агрегированного пространства состояний самого объекта КИИ.

Сложность решения подобной задачи может быть обусловлена многогранностью и многофункциональностью описываемой информационной системы, для чего требуется детальный анализ алгоритмов ее безопасного функционирование через перечисление множества всех допустимых состояний.

Процесс агрегирования, являющийся ключевым понятием функционального подхода, заключается в построении агрегированного пространства состояний информационной системы – *Re,* которое отличается от настоящего рядом упрощений (укрупнений), но при определенных допущениях может рассматриваться как реальное.

В данном случае разработка функционального представления информационной системы осуществляется на основе анализа пространства параметров процессов в системе по установленным правилам и выявление тех параметров, которые характеризуют действие атаки. Элементарной функцией $fi \in F$ будем называть математическое описание соответствующего ей элементарного действия или композицию элементарных действий минимальной длины в виде алгоритма преобразования, определенного на всем пространстве агрегированных состояний информационной системы.

Описание алгоритма соответствующего преобразования требует построения области определения и области значений для каждой из элементарных функций. При этом областью определения элементарной функции системы будем называть полное подмножество ее состояний, каждое из которых для данного преобразования имеет образ, с ним не совпадающий.

Областью значений элементарной функции будем называть полное подмножество состояний информационной системы, каждое из которых для данного преобразования есть прообраз. При этом если:

$$S_f^{/} \subset S \tag{1}$$

– область определения функции *f* в *Re*, а

$$S_f^{//} \subset S \tag{2}$$

– область значений функции *f* в *Re*, то преобразование в *Re* согласно *f* опишется отображением:

$$G_f : S_f^{/} \to S_f^{//}. \tag{3}$$

В то же время предполагается, что в процессе конкретного элементарного действия изменению подвергаются лишь часть компонентов пространства, т.е. во внимание принимаются только те компоненты

агрегированного пространства состояний, которые имеют смысл для данного преобразования. Следовательно, для каждой элементарной функции *fi* строится абстрактное пространство состояний *Im* мерности $\dot{M} = \left\{\dot{X}_{\dot{k}}; \dot{k} = \overline{1, \left|\dot{M}\right|}\right\}$ с компонентами $\dot{X}_{j1}$, $j = \overline{1, \dot{M}_{i1}}$, в котором она полностью определена.

Следовательно, функция *fi* в общем случае не всюду определена на декартовом произведении:

$$\dot{S} = x_1 \times x_2 \times \ldots \times x_{\dot{M}_{i1}}, \tag{4}$$

или всюду определена на множестве состояний:

$$\dot{S}_f^{/} \subset \dot{S}, \tag{5}$$

где $S_f^{/}$ – есть область определения функции *f*.

$$\dot{S}_f^{//} \subset \dot{S} \tag{6}$$

– это область значения функции *f* в абстрактном пространстве *Im*. При этом отображением

$$G : \rho_i^M \leftrightarrow \dot{M}_i, \; s_n^{/} \in S \tag{7}$$

определяется состояние информационной системы на каждом шаге функционирования.

Значение компонентов абстрактного пространства в общем случае следующее:

$$\dot{X}_j = x_{j1} | x_{j2} | \ldots | x_{jk} | \ldots | x_{jk_j^{\max}}, \tag{8}$$

при этом $x_j = \left\{x_{jk}; k = \overline{1, K_j^{\max}}\right\}$.

Подпространства области определения и области значения элементарной функции принимают смысл отображений:

$$G_i^{/} : \rho_{i1}^M \leftrightarrow \dot{M}_i, \tag{9}$$

$$G_i^{//} : \rho_{i2}^M \leftrightarrow \dot{M}_i, \tag{10}$$

$$G_i : \rho_i^M = \rho_{i1}^M \cup \rho_{i2}^M \leftrightarrow \dot{M}_i = M_{i1}^{/} \cup M_{i2}^{/} \tag{11}$$

На рис. 3 представлена теоретико-множественная модель, описывающая процесс преобразования состояния в функциональной системе.

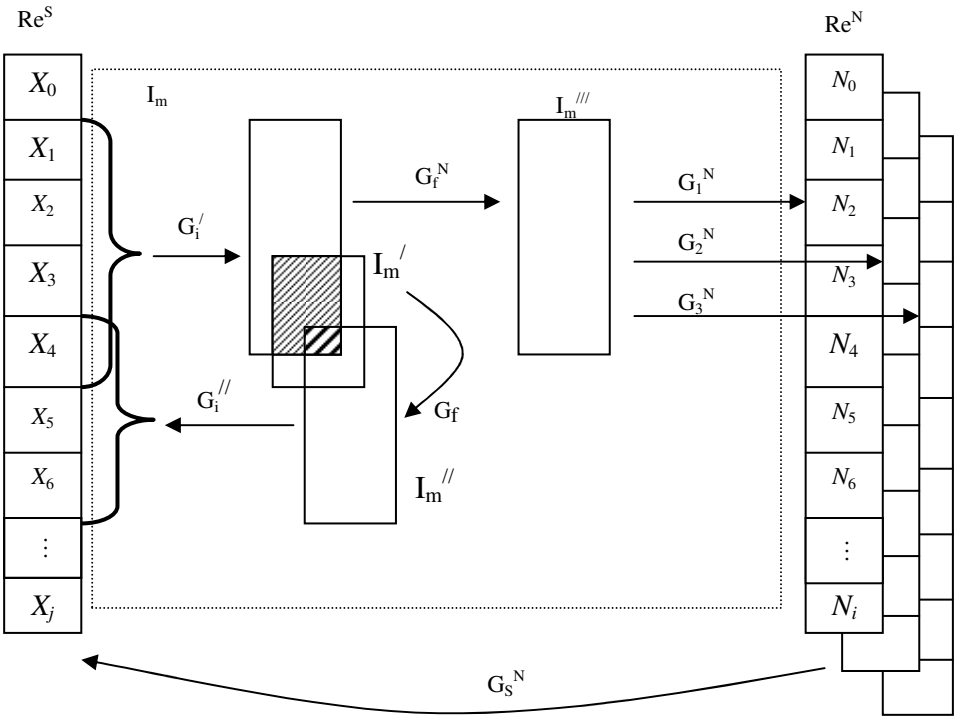

Рис. 3. Теоретико-множественная модель, иллюстрирующая процессы преобразования в функциональной системе

Процесс построения абстрактного пространства для элементарного преобразования заключается в последовательности этапов:

1) переходе из *R*e в *Im* для выполнения элементарной функции *f:*

$$S^{/}_{\rho^{M}_{f}} \rightarrow S^{/}_{\rho^{\dot{M}}_{f}}, \tag{12}$$

который описывается отображением:

$$G^{/}_{f} : S^{/}_{f} \rightarrow \dot{S}^{/}_{f} \ ; \tag{13}$$

2) преобразовании в *Im* согласно *f* как отображения:

$$\dot{G}_{f} : \dot{S}^{/}_{f} \rightarrow \dot{S}^{//}_{f}; \tag{14}$$

3) переходе из *Im* в *Re* после выполнения *f*:

$$S^{//}_{\rho^{\dot{M}}_{f}} \rightarrow S^{//}_{\rho^{M}_{f}}, \tag{15}$$

который описывается отображением:

$$G^{//}_{f} : \dot{S}^{//}_{f} \rightarrow S^{//}_{f}. \tag{16}$$

Критерий уровня наблюдаемости объекта КИИ N определяет уровень абстракции анализируемых событий в защищаемой системе и определяет границы применимости метода для обнаружения компьютерных атак в сетях. Традиционно в подобных системах рассматриваются следующие уровни наблюдаемости:

– наблюдение на уровне операционной системы отдельного узла сети;

– наблюдение на уровне сетевого взаимодействия объектов на узлах сети;

– наблюдение на уровне отдельных приложений узла сети;

– комбинация наблюдателей разных уровней.

В разработанной модели отображение G_S^N есть семантика наблюдаемости состояния, возникающая как образ состояния информационной системы посредством средств отображения информации, представляющий собой семантический код результата наблюдения. При этом каждый из элементов вектора наблюдаемости N несет информацию в зависимости от того, насколько наблюдаемость обеспечивает оценку состояния всей системы. Под наблюдаемостью информационной системы понимается степень соответствия семантического кода образа состояния информационной системы ее истинному состоянию.

Отображение G_f^N отдельных элементарных функций в абстрактном пространстве формирует конкретные образы отдельных компонентов как значения их наблюдаемости, причем каждая из них имеет свое проявление $G_{1,2,3}^N$ для различных уровней наблюдаемости разными средствами отображения.

Множества элементарных функций, объединенные в правильные композиции, представляют собой цепочки, отражающие поведение информационной системы в введенном пространстве состояний. При этом поведение $l \in F^*$ длины $|l|$ представляет собой кортеж:

$$l = f_{l_1} \circ f_{l_2} \circ \ldots \circ f_{l_{|l|}} \in F^*, \tag{17}$$

а $F_{mp} = \left\{ f^n ; n = \overline{1, |l|} \right\}$ – множество элементарных функций, соответствующих требуемому поведению информационной системы на каждом шаге n. При этом l можно обозначить отображением:

$$G_l = F_{mp} \to F, \tag{18}$$

$$(\forall f^n)(\exists! f_i) P(G_l(f^n) = f_i) . \tag{19}$$

Последний предикат утверждает о существовании единственно верного элементарного действия f_i на каждом шаге функционирования информационной системы. Отклонение от набора элементарных действий, в свою очередь, свидетельствует о наличии признака компьютерной атаки. Требуемый уровень наблюдаемости образа атаки может быть также реализован на основе внедрения нейронных технологий [17, 18].

Наиболее важными достоинствами моделей, основанных на нейронных сетях, являются способность адаптироваться к динамическим условиям и быстрота функционирования. Это особенно важно при работе систем защиты информации в режиме реального времени и необходимости оценки степени соответствия анализируемых данных эталонной модели [19, 20].

Таким образом, анализ количественного роста компьютерных атак на информационные системы, а также необходимость защиты объектов КИИ различного назначения требуют поиска наиболее эффективных способов обнаружения атак и применения имеющегося арсенала средств защиты информации. Разработанная модель позволяет представить информационную систему на основе функционального подхода, предполагающего решение задачи нахождения полного множества безопасных состояний ИС. Нахождение полного множества подобных состояний, в свою очередь, позволит определить признаки компьютерной атаки. Последующее распознавание характера атаки может осуществляться на основе системного анализа пространства параметров процессов в системе по установленным правилам и выявления тех параметров, которые характеризуют действие подобной компьютерной атаки.

Библиографический список

1. Анализ угроз информационной безопасности 2016-2017 [Электронный ресурс]. – URL: https://www.anti-malware.ru/analytics/Threats_-Analysis/Analysis_information_security (дата обращения: 21.03.2018).

2. О безопасности критической информационной инфраструктуры Российской Федерации (от 26.07.2017 № 187-ФЗ) // Доступ из справ.-правовой системы КонсультантПлюс.

3. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президен-

том РФ 03.02.2012 № 803) // Доступ из справ.-правовой системы КонсультантПлюс.

4. Шабуров А.С., Журилова Е.Е. Об особенностях интеграции DLP-решений в корпоративные информационные системы // Вестник УрФО. Безопасность в информационной среде. – Челябинск: Изд. центр ЮУрГУ, 2017. – № 3(25). – С. 5–12.

5. Шабуров А.С., Журилова Е.Е., Лужнов В.С. Технические аспекты внедрения DLP-системы на основе FalcongazeSecureTower // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2015. – № 4(16). – С. 57–67.

6. Шабуров А.С., Борисов В.И. О применении SIEM-систем для обеспечения безопасности корпоративных сетей, инновационные технологии, теория, инструменты, практика // Материалы VII Междунар. интернет-конф. молод. ученых, аспирантов, студ. – Пермь: Изд-во Перм. нац. исследоват. политехн. ун-та, 2016. – С. 249–254.

7. Positive Technologies. Кибербезопасность 2016-2017: от итогов к прогнозам [Электронный ресурс]. – URL: https://elibrary.ru/item.asp?id=29207621 (дата обращения: 21.03.2018).

8. Гамаюнов Д.Ю. Обнаружение компьютерных атак на основе анализа поведения сетевых объектов: дис. … канд. физ.-мат. наук. – М: Изд-во МГУ им. Ломоносова, 2007.

9. Шабуров А.С., Журилова Е.Е. Модель выявления каналов утечки информации в автоматизированных системах на основе симплекс-метода // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2017. – № 24. – С. 7–19.

10. Шабуров А.С., Борисов В.И. О применении сигнатурных методов анализа информации в SIEM-системах // Вестник УрФО. Безопасность в информационной среде. – Челябинск: Изд-во ЮУрГУ, 2015. – № 17. – С. 23–37.

11. Данилов А.Н., Шабуров А.С. Концептуальный подход в решении задачи обеспечения безопасности информационно-управляющих систем // Вестник Казан. гос. техн. ун-та им. А.Н. Туполева. – 2012. – № 1. – С. 113–119.

12. Шабуров А.С., Журилова Е.Е. Особенности реализации алгоритмов морфологического анализа в DLP-системах // Вестник УрФО. Безопасность в информационной сфере. – Челябинск, 2016. – № 2(20). – С. 23–28.

13. Шабуров А.С., Борисов В.И. Разработка модели защиты информации корпоративной сети на основе внедрения SIEM-системы // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2016. – № 19. – С. 111–124.

14. Екимов О.Б. Методика разработки учебно-лабораторного комплекса для исследования систем защиты информации сложных военно-технических объектов: дис. … канд. техн. наук. – Пермь: Перм. воен. ин-т ракет. войск, 2003. – 125 с.

15. Харитонов В.А. Основы теории живучести функционально избыточных систем: препринт №170. – СПб.: Ин-т Информатики и автоматизации Рос. акад. наук, 1993. – 60 с.

16. Шабуров А.С., Миронова А.А. Обнаружение компьютерных атак на основе функционального подхода // Вестник Пермского университета. Математика. Механика. Информатика. – 2015. – Вып. 4(31). – С. 110–115.

17. Шабуров А.С. Разработка модели распознавания компьютерных атак на основе нейронной сети // Нейрокомпьютеры: разработка, применение. – 2016. – № 8. – С. 67–72.

18. Шабуров А.С., Рашевский Р.Б. Применение нейронных сетей для обеспечения безопасности информационно-управляющих систем критически важных объектов // Нейрокомпьютеры: разработка, применение. – 2014. – № 12. – С. 31–35.

19. Шабуров А.С., Рашевский Р.Б. Практическое применение нейронных сетей для защиты информационно-управляющих систем критически важных объектов от DDOS-атак // Нейрокомпьютеры: разработка, применение. – 2015. – № 10. – С. 16–20.

20. Шабуров А.С. Алгоритм распознавания таргетированных компьютерных атак на основе нейронной сети // Нейрокомпьютеры: разработка, применение. – 2017. – № 6. – С. 60–64.

References

1. Analiz ugroz informatsionnoi bezopasnosti 2016-2017 [Analysis of information security threats 2016-2017], available at: https://www.anti-malware.ru/analytics/Threats_Analysis/Analysis_information_security (accessed 21 March 2018).

2. O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii (ot 26072017 № 187-FZ) [On the Security of the Criti-

cal Information Infrastructure of the Russian Federation (of July 26, 2017 No. 187-FZ)]. Dostup iz spravpravovoi sistemy Konsul'tantPlius.

3. Osnovnye napravleniia gosudarstvennoi politiki v oblasti obespecheniia bezopasnosti avtomatizirovannykh sistem upravleniia proizvodstvennymi i tekhnologicheskimi protsessami kriticheski vazhnykh ob"ektov infrastruktury Rossiiskoi Federatsii (utv. Prezidentom RF 03.02.2012 № 803) [The main directions of the state policy in the field of ensuring the safety of automated production and process control systems for critical infrastructure in the Russian Federation (approved by the President of the Russian Federation on February 3, 2012, No. 803)]. Dostup iz spravpravovoi sistemy Konsul'tantPlius.

4. Shaburov A.S., Zhurilova E.E. Ob osobennostiakh integratsii dlpreshenii v korporativnye informatsionnye sistemy [About features of integration DLP-solutions in corporateinformation systems]. *Vestnik Ural'skogo federal'nogo okruga. Bezopasnost' v informatsionnoi srede*. Cheliabinsk: Izdatel'skii tsentr Iuzhno-Ural'skogo gosudarstvennogo universiteta, 2017, no. 3(25), pp. 5-12.

5. Shaburov A.S., Zhurilova E.E., Luzhnov V.S. Tekhnicheskie aspekty vnedreniia dlpsistemy na osnove Falcongaze SecureTower [Technical aspects of implementation of DLP-systems based on Falcongaze SecureTower]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2015, no. 4(16), pp. 57-67.

6. Shaburov A.S., Borisov V.I. O primenenii SIEM-sistem dlia obespecheniia bezopasnosti korporativnykh setei, innovatsionnye tekhnologii, teoriia, instrumenty, praktika [On the application of SIEM-systems for the security of corporate networks, innovative technologies, theory, tools, practice]. *Materialy VII Mezhdunarodnoi internet-konferentsii molodykh uchenykh, aspirantov, studentov*. Perm': Permskii natsional'nyi issledovatel'skii politekhnicheskii universitet, 2016, pp. 249-254.

7. Positive Technologies. Kiberbezopasnost' 20162017: ot itogov k prognozam [Cybersecurity 2016-2017: from results to forecasts], available at: https://elibrary.ru/item.asp?id=29207621 (accessed 21 March 2018).

8. Gamaiunov D.Iu. Obnaruzhenie komp'iuternykh atak na osnove analiza povedeniia setevykh ob"ektov [Detection of computer attacks on the basis of the analysis of the behavior of network objects]. Ph.D.Thesis. Moscow: Moskovskii gosudarstvennyi universitet imeni M.V. Lomonosova, 2007.

9. Shaburov A.S., Zhurilova E.E. Model' vyiavleniia kanalov utechki informatsii v avtomatizirovannykh sistemakh na osnove simpleks-metoda [Model of identification of information leaks channels in automated systems based on the simplex-method]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2017, no. 24, pp. 7-19.

10. Shaburov A.S., Borisov V.I. O primenenii signaturnykh metodov analiza informatsii v SIEM-sistemakh [About the application of signature analysis method in the SIEM-systems]. *Vestnik Ural'skogo federal'nogo okruga. Bezopasnost' v informatsionnoi sfere*. Chelyabinsk: Iuzhno-Ural'skii gosudarstvennyi universitet, 2015, no. 17, pp. 23-37.

11. Danilov A.N., Shaburov A.S. Kontseptual'nyi podkhod v reshenii zadachi obespecheniia bezopasnosti informatsionno-upravliaiushchikh system [Conceptual approach in solving the problem of information-control systems security]. *Vestnik Kazanskogo gosudarstvennogo tekhnicheskogo universiteta imeni A.N. Tupoleva*, 2012, no. 1, pp. 113-119.

12. Shaburov A.S., Zhurilova E.E. Osobennosti realizatsii algoritmov morfologicheskogo analiza v DLP-sistemakh [Features of the implementation of algorithms for morphological analysis in DLP-systems]. *Vestnik Ural'skogo federal'nogo okruga. Bezopasnost' v informatsionnoi sfere*. Chelyabinsk, 2016, no. 2(20), pp. 23-28.

13. Shaburov A.S., Borisov V.I. Razrabotka modeli zashchity informatsii korporativnoi seti na osnove vnedreniia SIEM-sistemy [Developing protect the corporate network information model based on the introduction of SIEM-system]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2016, no. 19, pp. 111-124.

14. Ekimov O.B. Metodika razrabotki uchebno-laboratornogo kompleksa dlia issledovaniia sistem zashchity informatsii slozhnykh voenno-tekhnicheskikh ob"ektov [Methodology for the development of a training and laboratory complex for the study of information security systems for complex military-technical facilities]. Ph.D.Thesis. Perm': Permskii voennyi institut raketnykh voisk, 2003, 125 p.

15. Kharitonov V.A. Osnovy teorii zhivuchesti funktsional'no izbytochnykh system: preprint №170 [Fundamentals of the theory of survivability of functionally redundant systems: preprint №170]. Saint Petersburg: Institut Informatiki i avtomatizatsii Rossiiskoi akademii nauk, 1993. 60 p.

16. Shaburov A.S., Mironova A.A. Obnaruzhenie komp'iuternykh atak na osnove funktsional'nogo podkhoda [The detection of computer attacks based on the functional approach]. *Vestnik Permskogo universiteta. Matematika. Mekhanika. Informatika*, 2015, iss. 4(31), pp. 110-115.

17. Shaburov A.S. Razrabotka modeli raspoznavaniia komp'iuternykh atak na osnove neironnoi seti [Development of model for detection of computer attacks based on the neural network]. *Neirokomp'iutery: razrabotka, primenenie*, 2016, no. 8, pp. 67-72.

18. Shaburov A.S., Rashevskii R.B. Primenenie neironnykh setei dlia obespecheniia bezopasnosti informatsionno-upravliaiushchikh sistem kriticheski vazhnykh ob"ektov [Application of neural networks for security information and control systems of critical objects]. *Neirokomp'iutery: razrabotka, primenenie*, 2014, no. 12, pp. 31-35.

19. Shaburov A.S., Rashevskii R.B. Prakticheskoe primenenie neironnykh setei dlia zashchity informatsionno-upravliaiushchikh sistem kriticheski vazhnykh ob"ektov ot DDOS-atak [Practical application of neural networks to protect information management systems critical facilities from DDOS-attacks]. *Neirokomp'iutery: razrabotka, primenenie*, 2015, no. 10, pp. 16-20.

20. Shaburov A.S. Algoritm raspoznavaniia targetirovannykh komp'iuternykh atak na osnove neironnoi seti [Algorithm for recognizing targeted computer attacks based on a neural network]. *Neirokomp'iutery: razrabotka, primenenie*, 2017, no. 6, pp. 60-64.

Сведения об авторе

Шабуров Андрей Сергеевич (Пермь, Россия) – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: shans@at.pstu.ru).

About the author

Shaburov Andrey Sergeevich (Perm, Russian Federation) is a Ph.D. in Technical Sciences, Associate Professor of the Department of Automation and Telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: shans@at.pstu.ru).

Получено 25.04.2018