УДК 004.056
DOI: 10.26102/2310-6018/2023.40.1.006

Интеллектуальная поддержка обнаружения инцидентов информационной безопасности

В.Л. Токарев, А.А. Сычугов✉

Тульский государственный университет, Тула, Российская Федерация
unwaiter@mail.ru✉

Резюме. Актуальность исследования обусловлена необходимостью автоматизации процессов обнаружения и идентификации инцидентов информационной безопасности для своевременного запуска процессов реагирования, что, в свою очередь, позволит снизить влияние как преднамеренных, так и случайных инцидентов информационной безопасности на защищенность информации в автоматизированных системах различного назначения. В основу предлагаемых решений положены методы искусственного интеллекта, а в качестве выстраиваемого средства интеллектуальной поддержки обнаружения инцидентов информационной безопасности – система поддержки принятия решений. В статье предложены модели, математические зависимости и методы решения задач автоматического обнаружения, идентификации инцидентов информационной безопасности, а также их локализации, для чего, среди прочего, используется теория нечетких множеств. Рассмотрены возможные стратегии локализации инцидентов ИБ. Сформулированы процедуры реагирования на инциденты информационной безопасности, а также их ликвидации, что, в свою очередь, позволяет строить системы интеллектуальной поддержки решения задачи оперативного обнаружения инцидентов информационной безопасности. Приведены примеры событий. Материалы статьи представляют практическую ценность при построении систем превентивной защиты информации, что является на сегодняшний день одним из перспективных направлений теории и практики обеспечения защиты информации.

Ключевые слова: инциденты информационной безопасности, превентивная защита информации, системы искусственного интеллекта, математическая логика, автоматизированные системы.

Для цитирования: Токарев В.Л., Сычугов А.А. Интеллектуальная поддержка обнаружения инцидентов ин-формационной безопасности. *Моделирование, оптимизация и информационные технологии.* 2023;11(1). URL: https://moitvivt.ru/ru/journal/pdf?id=1271 DOI: 10.26102/2310-6018/2023.40.1.006

Intelligent support for detecting information security incidents

V.L. Tokarev, A.A. Sychugov✉

Tula State University, Tula, Russian Federation
unwaiter@mail.ru✉

Abstract. The relevance of the study is due to the need to automate the processes of detecting and identifying information security incidents for the timely launch of response processes, which, in turn, will reduce the impact of both intentional and accidental information security incidents on information security in automated systems for various purposes. The suggested solutions are based on artificial intelligence methods, and as a built-in means of intellectual support for the detection of information security incidents, a decision support system is employed. The article proposes models, mathematical dependencies and methods for solving problems of automatic detection, identification of information security incidents as well as their localization, for which, among other things, fuzzy set theory is used. Possible strategies for localizing information security incidents are considered. Procedures for responding to information security incidents as well as their elimination are formulated, which, in turn,

allows building intelligent support systems for solving the problem of prompt detection of information security incidents. Examples of events are given. The materials of the article are of practical value for building systems of preventive information protection, which is currently one of the promising areas of theory and practice of ensuring information protection.

Keywords: information security incidents, preventive information protection, artificial intelligence systems, mathematical logic, automated systems.

For citation: Tokarev V.L., Sychugov A.A. Intelligent support for detecting information security incidents. *Modeling, Optimization and Information Technology*. 2023;11(1). URL: https://moitvivt.ru/ru/journal/pdf?id=1271 DOI: 10.26102/2310-6018/2023.40.1.006 (In Russ.).

Введение

Применяемые политики информационной безопасности (ИБ) и принятые меры и средства не могут полностью гарантировать защиту информации в автоматизированных системах (АС), сервисах или компьютерных сетях из-за наличия оставшихся в АС слабых мест (уязвимостей), которые делают возможным появление инцидентов информационной безопасности. Инциденты ИБ способны оказывать негативные воздействия (как прямые, так и косвенные) на деятельность организации. Кроме того, появление новых угроз становится причиной новых, ранее не встречавшихся инцидентов ИБ, для которых отсутствуют готовые рецепты реагирования. Таким образом, для любой организации, серьезно озабоченной обеспечением своей информационной безопасности, важно своевременно (ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности) [1]:

– обнаруживать и распознавать (классифицировать) возникающие инциденты ИБ;

– оповещать об их обнаружении всех заинтересованных лиц и реагировать на инциденты ИБ, включая активацию соответствующих защитных мер для предотвращения (или уменьшения негативных последствий) и восстановления защищенности АС после результатов негативных последствий;

– ввести превентивные меры по защите информации в АС, исключающих появление подобных инцидентов в будущем.

Одним из способов обеспечения своевременности обнаружения инцидентов ИБ, их классификации и реагирования на них является автоматизация указанных процессов. Поэтому, целью работы является повышение своевременности обнаружения инцидентов ИБ за счет решения задачи интеллектуальной поддержки обнаружения, идентификации инцидентов ИБ, что позволит своевременно запустить процесс реагирования и, тем самым, существенно снизить влияние инцидентов ИБ на защищенность информации в автоматизированных системах различного назначения.

Материалы и методы

Пусть множество инцидентов информационной безопасности $Y = \{y_i, i=1,\ldots,7\}$, множество источников информации: $S = \{s_i, i=1,\ldots,7\}$. Примеры описаний инцидентов и источников можно найти в [1].

Информацию множества S источников, составляет множество фактов, на основании которых принимаются решения о наличии $y \in Y$ или отсутствии $y \notin Y$ инцидента ИБ в текущий интервал времени t наблюдения за состоянием информационной безопасности.

Под реагированием на инциденты ИБ понимается последовательность некоторых действий $R(t) = \{r_1, r_2, \ldots, r_n\}$ как простых (приостановка работы автоматизированной

системы, сообщение администратору об инциденте, регистрация его и сохранение свидетельств), так и сложных, требующих выполнения набора определенных действий (анализ, классификация, локализация, выявление и ликвидация последствий инцидента ИБ).

Тогда представленную задачу можно сформулировать следующим образом.

Предполагается, что вся информация, получаемая от источников $s_k \in S$ хранится в специальной базе данных «ИНЦИДЕНТЫ», в которой каждому источнику s_k соответствует определенная запись – строка таблицы, с которой связана хранимая процедура (триггер x_k), выполняемая автоматически при появлении некоторого события $f \in F$.

Требуется, по информации, получаемой от множества триггеров X, автоматически (без участия оператора, администратора и др.) оперативно обнаруживать, классифицировать инцидент (отнесения к одному из видов $y \in Y$) и запускать процесс реагирования $R(t)$ на него.

В качестве способа решения этой задачи предлагается использовать методы систем искусственного интеллекта, а в качестве выстраиваемого средства интеллектуальной поддержки обнаружения инцидентов ИБ – систему поддержки принятия решений (СППР) [2, 3, 4, 6, 7, 8, 9, 10].

За основу базы знаний такой СППР принимается соответствие

$$F \to Y, \tag{1}$$

в котором F – конечное множество событий ИБ, $Y = \{y_1, y_2, \ldots, y_7\}$ – множество инцидентов ИБ.

Имея такую модель, задачу обнаружения инцидентов ИБ можно решить с помощью правила заключения исчисления высказываний [5]:

$$\hat{Y} = \rho[F(X), (F \to Y)], \tag{2}$$

где $\rho[\cdot]$ – правило логического вывода (заключения), $F(X)$ – вектор фактов, полученных в результате использования информации от множества X.

Правило заключения в классическом варианте [5] имеет вид: ρ: $\frac{P, P \to Q}{Q}$, если посылка (вектор фактов) P и импликация $P \to Q$ истинны, то истинно заключение Q.

Отсюда следует, что: 1) для решения задачи необходимо и достаточно построить модель $(F \to Y)$, поскольку значения $F(x)$ всегда можно получить от множества указанных источников X; 2) поскольку посылка F – вектор событий, отдельная группа которых F_i соответствует одному единственному инциденту y_i, состав которой может иметь различное число событий, т. е. количество событий в группе – случайное число, то вместо классического правила заключения целесообразно использовать нечеткое правило заключения:

$$\overleftrightarrow{\rho}: \frac{F(X),\ F(X) \to M_Y(X) = \{\mu_i(X),\ i = 1,\ldots,7\}}{max\{\mu_i(X),\ i = 1,\ldots,7\} \to y_i} \tag{3}$$

Идентификация инцидента информационной безопасности.

Модель (1) можно представить в виде двудольного графа, отвечающего следующим требованиям: 1) множество вершин разбито на две доли F и Y, 2) любые две вершины смежные тогда и только тогда, когда они принадлежат разным долям.

В модели (1) вершины доли F составляют события f_j а вершины второй доли – инциденты $y_i \in Y$. Такой граф можно представить в форме списков смежности $L = \{l_{y1}, l_{y2}, \ldots, l_{y7}\}$, где l_{yi} – список вершин (событий) левой части графа $(F \to Y)$, связанных с вершиной y_i и соответствующих определенной группе F_i. С каждой вершиной $y_i \in Y$

связан счетчик St_i, значение которого увеличивается на единицу при совпадении выявленного события $f_i(x)$ с одной из вершин списка смежности l_{yi}.

С помощью счетчика определяются значения функции принадлежности для каждого инцидента $\{\mu_i(X),\ i = 1,\ldots,7\}$:

$$\mu_i(X) = \frac{\langle St_i \rangle}{n_i}, \quad i = 1,\ldots,7 \tag{4}$$

где n_i – мощность (число вершин) подмножества $F_i \subseteq F$, все вершины которого связаны с вершиной $y_i \in Y$.

Это позволяет в соответствии с выражением (3) выполнить дефазификацию полученного нечеткого подмножества: $max\{\mu_i(X),\ i = 1,\ldots,7\} \rightarrow y_i$.

Тогда задача идентификации инцидентов сводится к задаче обхода вершин левой части вершин графа $(F \rightarrow Y)$ с целью подсчета числа совпадений обнаруженного события $f_k(x)$ с событием f_{ji} в каждом списке смежности.

Для снижения размерности задачи обхода вершин левой части графа (1) события $f \in F$ разбиваются на классы: A – множество событий на физическом уровне информационной инфраструктуры АС; B – множество событий на уровне сетевого оборудования; C – множество событий на уровне сетевых приложений и сервисов; D – множество событий, связанных с определением потенциальных целей атаки и получением представления о сервисах, работающих на атакуемой АС, то есть проведение разведки с целью получения представления об окружающей АС сетевой топологии и о том, с кем обычно эта АС связана обменом информации; и о потенциальных уязвимостей АС или непосредственно окружающей ее сетевой среды; H – множество событий на уровне операционных систем; G – множество событий на уровне технологических процессов, приложений, бизнес-процессов.

Тогда поиск совпадения с вершиной состоит из двух шагов: 1) определения класса события $F_j(x)$; 2) поиска совпадения $f_{ij}(x) \approx f_{ij} \in F_i$ внутри класса F_i.

Примеры событий множеств A, B, C, D, H, G можно найти в справочной и нормативной информации, например, в [1].

Например, инциденту y_1 – возникновение угрозы «отказ в обслуживании», соответствует список смежности $(a_{14}, a_{15}, a_{16}, b_{01}, b_{02}, b_{03}, c_{05}, c_{06}, c_{07}) \rightarrow y_1$. А инциденту y_3 – возникновение угрозы «Сбор информации», соответствует список смежности $(a_{04}, b_{20}, c_{09}, d_{01}, d_{0_2}, d_{03}, d_{04}, h_{02}) \rightarrow y_3$.

Результаты

Предложенный метод интеллектуальной поддержки обнаружения, идентификации инцидентов ИБ позволяет сформулировать процедуры реагирования на инциденты ИБ.

Процесс реагирования запускается сразу после идентификации конкретного инцидента $y_i \in Y$:

$$\pi(y_i) \rightarrow R = \{r_1, r_2, \ldots, r_{10}\},$$

где: r_1 – приостановить работу; r_2 – выдать сообщение непосредственному руководителю и администратору информационной безопасности; r_3 – выполнить регистрацию инцидента; r_4 – сохранить свидетельства инцидента.

После указанных действий выдаются указания о необходимости принятия мер по анализу (r_5), классификации (r_6), локализации (r_7), выявлению (r_8), ликвидации (r_9), закрытию (r_{10}) инцидентов ИБ.

Анализ инцидента ИБ (r_5)**.**

В процессе проведения анализа:

1) устанавливаются дата и время совершения инцидента ИБ; ФИО, должность и подразделение нарушителя ИБ;

2) исследуются информационная инфраструктура, включая как аппаратную, так и программную составляющие;

3) анализируются носители данных.

Анализ завершается сбором данных, свидетельствующих о причинах или источнике возникшего инцидента. По результатам устанавливаются причины инцидента и лица, виновные в его возникновении.

Классификация (r_6). Классификационными признаками являются: 1) степень тяжести для деятельности организации; 2) вероятность повторного возникновения; 3) виды источников угроз информационной безопасности; 4) преднамеренность возникновения; 5) виды объектов информационной инфраструктуры, пораженных при реализации инцидента; 6) уровень информационной инфраструктуры; 7) свойства информационной безопасности; 8) тип инцидента; 9) сложность обнаружения; 10) сложность закрытия.

Локализация инцидента ИБ (r_7). Этап локализации инцидента ИБ представляет собой действия, направленные на определение и ограничение функционирования информационных ресурсов, на которых обнаружены признаки зарегистрированного инцидента ИБ с целью предотвращения его дальнейшего распространения.

Цель локализации инцидента ИБ состоит в том, чтобы предотвратить следующие возможные действия злоумышленника: нарушения конфиденциальности, целостности или доступности информации вследствие несанкционированного доступа к ней; несанкционированное вмешательство в работу информационного ресурса; использование информационного ресурса для атаки на смежные ресурсы.

К примерам возможных стратегий, которые могут применяться при локализации инцидентов ИБ, можно отнести:

1. Применение блокировок (использование межсетевого экрана). Например, с использованием межсетевого экрана можно заблокировать информационные потоки с IP-адресов, с которых распространяется ВПО, шпионское ПО, неразрешенное ПО, а также IP-адресов почтовых ретрансляторов, источников «фишинга» и «спама» или известных IP-адресов хостов нарушителей. Почтовые блокировки включают фильтрацию вложений, строк тем и адресов отправителей. Для предотвращения доступа к неразрешенным или вредоносным веб-сайтам, или хостам (узлам) могут применяться блокировки URL-адресов и доменных имен.

2. Отключение зараженного информационного ресурса (группы ресурсов) от сети позволяет предотвратить: 1) заражение остальной части сети, 2) НСД и, соответственно, нарушение конфиденциальности, целостности и доступности информации, 3) дальнейшее заражение или сдерживание злонамеренных действий в информационной инфраструктуре или в отдельном сегменте сети. Это поможет информационным ресурсам корректно функционировать и при этом не распространять вредоносную активность на остальную часть инфраструктуры.

3. Осуществлять мониторинг вредоносной активности (в некоторых случаях может быть целесообразным), ограничив при этом возможности злоумышленника атаковать другие информационные ресурсы.

4. Выключение. В случае установления факта того, что дальнейшее функционирование информационного ресурса приведет к уничтожению (потере) данных в информационной инфраструктуре организации, в качестве меры сдерживания может быть принято решение о прекращении функционирования информационного ресурса. Если будет установлено, что определенный информационный ресурс, например, сервер

электронной почты или веб-сервер, должен быть выключен до тех пор, пока не будет предотвращено распространение ВПО, то функционирование данного сервера должно быть приостановлено[1].

5. Изменения маршрутизации осуществляются с целью устранения маршрута, по которому действует злоумышленник, препятствуя злоумышленнику получить доступ к информационным ресурсам, которые могут являться объектами атаки, а также блокирования механизмов передачи (распространения) ВПО между «зараженными» информационными ресурсами.

6. Отключение процессов подразумевает отключение процессов, которые могли быть использованы при компьютерной атаке.

7. Отключение учетных записей пользователей подразумевает отключение учетных записей тех пользователей, которые могли быть использованы при компьютерной атаке[2].

Выявление последствий инцидента ИБ **(r_8)** от реализации инцидента ИБ заключается в прогнозировании как прямого, так и косвенного ущербов.

Определяются затронутые инцидентом ИБ информационные ресурсы и обстоятельства, способствовавшие его совершению.

К примерам признаков негативного воздействия на элементы информационной инфраструктуры, которые выявляются в ходе анализа можно отнести: а) нештатную сетевую активность объекта воздействия компьютерной атаки; б) созданные, модифицированные, удаленные файлы, каталоги, параметры настройки ПО, включая ПО средств ЗИ; в) отклонения от эталонных (допустимых) параметров конфигурации операционной системы (ОС), и ПО, включая ПО средств ЗИ; г) отклонения от эталонного (допустимого) состава, установленного в ОС, ПО; д) отклонения от эталонного (допустимого) содержания системных и защищаемых файлов; е) выполненные потенциально вредоносные команды, в том числе расположенные в оперативной памяти СВТ; ж) признаки, идентифицирующие источник компьютерной атаки; з) признаки сбоев, перезагрузок, остановок и других нарушений в штатной работе ПО, признаки нарушений функционирования сетевых служб, аномального использования системных ресурсов; и) другую информацию, характерную отдельным типам компьютерных инцидентов, компьютерных атак.

При оценке негативного воздействия на элементы информационной инфраструктуры в результате инцидента ИБ должны оцениваться: 1) трудозатраты, связанные с проведением мероприятий по реагированию на компьютерный инцидент; 2) время простоя функционирования информационных ресурсов; 3) вред, причиненный интересам лица, ответственного за эксплуатацию элемента информационной инфраструктуры, подверженного воздействию, пользователя (пользователей) элемента информационной инфраструктуры, подверженного воздействию, в том числе связанного с нарушением конфиденциальности, целостности и доступности сведений, обрабатываемых данным объектом; 4) вред, причиненный организации, в том числе репутационные потери, экономический ущерб и иной вред; 5) финансовые затраты на восстановление штатного функционирования информационных ресурсов.

[1] Следует иметь в виду, что выключение сервера может отрицательно сказаться на работе конкретных пользователей, сервисов и различных критических процессов.

[2] Любые изменения в информационных ресурсах, включая действия по локализации, могут привести к потере (уничтожению) информации об инциденте ИБ (цифровых свидетельств). Следует убедиться, что вся необходимая для установления причин инцидентов ИБ информация (цифровые свидетельства) собрана в полном объеме перед внесением каких-либо системных изменений.

Переход на следующий этап реагирования на инцидент ИБ осуществляется после того, как руководитель (его заместитель или ответственный за отработку компьютерного инцидента) подразделения по управлению инцидентами ИБ убедится в достаточности выполненных действий и наличии заполненной соответствующей информации в карточке инцидента ИБ.

Ликвидация последствий инцидента ИБ **(r_9)** включает проведение следующих мероприятий:

На уровне сети: 1) внесение изменений в параметры настроек ПО, функционирующего в информационных ресурсах, вовлеченных в компьютерный инцидент; 2) подключение резервных ресурсов (каналы связи, серверное оборудование, виртуальные машины, оборудование из состава запасных инструментов и принадлежностей); 3) внесение изменений в архитектуру информационных ресурсов, вовлеченных в компьютерный инцидент, включая соответствующую проектную документацию; 4) миграция (перемещение) виртуальных машин в сторонние виртуальные инфраструктуры.

На уровне прикладного или специального ПО: 1) выполнение настройки безопасной конфигурации информационного ресурса, вовлеченного в компьютерный инцидент; 2) восстановление из актуальных резервных копий файлов, баз данных, конфигурационных файлов, подвергшихся модификации при компьютерном инциденте; 3) восстановление удаленных файлов, в том числе с использованием специальных инструментальных средств; 4) удаление ПО, вовлеченного в компьютерный инцидент и всех его файлов с последующей установкой актуальной версии данного ПО и актуальных обновлений безопасности.

На уровне ОС: 1) удаление следов вредоносной активности; 2) восстановление ОС в целом объекта воздействия; 3) настройка безопасной конфигурации ОС; переустановка ОС и ПО с последующей установкой актуальных обновлений безопасности.

Ключевыми процессами устранения последствий и причин инцидентов являются: 1) определение параметров нарушения, его характера; 2) анализ действий нарушителя и сценария нападения; 3) блокирование действий нарушителя; 4) блокирование работы информационной системы; 5) смена паролей; 6) переустановка поврежденного ПО; 7) восстановление нарушенной конфигурации ПО; 8) восстановление поврежденной информации.

Закрытие компьютерного инцидента (r_{10}) после получения подтверждений о принятии всех мер, предусмотренных на этапах локализации инцидента ИБ и выявлении и ликвидации его последствий, при условии, что проведенное тестирование показало достаточность принятых мер.

Заключение

Особенностью предложенного метода интеллектуальной поддержки решения задачи оперативного обнаружения инцидентов информационной безопасности является возможность его применения при построении систем превентивной защиты информации, что является на сегодняшний день одним из перспективных направлений теории и практики обеспечения защиты информации.

СПИСОК ИСТОЧНИКОВ

1. Васильева И.Н. *Расследование инцидентов информационной безопасности.* СПб.: Изд-во СПбГЭУ; 2019. 113 с.

2. Manish G., Chandra B. A framework of intelligent decision support system for Indian police. *Journal of Enterprise Information Management.* 2014:27(5):512–540. DOI: 10.1108/JEIM-10-2012-0073.
3. Jain G.P.-W. a. L. Recent Advances in Intelligent Decision Technologies. *Lecture Notes in Computer Science.* 2007:4692:567–571.
4. Witten I., Frank E. *Data Mining: Practical Machine Learning Tools and Techniques.* San Francisco: Morgan, Kaufmann; 2005. 558 p.
5. Судоплатов С.В., Овчинникова Е.В. *Математическая логика и теория алгоритмов.* М.: «ИНФРА-М»; 2004. 162 с.
6. Sanzhez-Marre M., Gibert K. *Evolution of Decision Support Systems.* University of Catalunya; 2012. n. pag.
7. Luenberger D.G., Yinyu Ye. *Linear and Nonlinear Programming*. International Series in Operations Research & Management Science; 2021. n. pag.
8. Power D.J. *Decision support systems: Concepts and resources for managers*. Greenwood Publishing Group; 2002. n.pag.
9. Ltifi H., Trabelsi G., Ayed M., Alimi A. Dynamic Decision Support System Based on Bayesian Networks. *(IJARAI) International Journal of Advanced Research in Artificial Intelligence,* 2012;1(1):22–29.
10. Burnside E.S., Rubin D.L., Fine J.P., Shachter R.D., Sisney G.A., Leung W.K. Bayesian network to predict breast cancer risk of mammographic microcalcifications and reduce number of benign biopsy results: initial experience. *Radiology,* 2006;240(3):666–673.

REFERENCES

1. Vasilyeva I.N. *Investigation of information security incidents : a manual.* Saint Petersburg: Publishing house of Saint Petersburg State University of Economics; 2019. 113 p. (In Russ.).
2. Manish G., Chandra B. A framework of intelligent decision support system for Indian police. *Journal of Enterprise Information Management.* 2014:27(5):512–540. DOI: 10.1108/JEIM-10-2012-0073.
3. Jain G.P.-W. a. L. Recent Advances in Intelligent Decision Technologies. *Lecture Notes in Computer Science.* 2007:4692:567–571.
4. Witten I., Frank E. *Data Mining: Practical Machine Learning Tools and Techniques.* San Francisco: Morgan, Kaufmann; 2005. 558 p.
5. Sudoplatov S.V., Ovchinnikova E.V. *Mathematical logic and theory of algorithms*. M.: «INFRA-M», 2004. 162 p. (In Russ.).
6. Sanzhez-Marre M., Gibert K. Evolution of Decision Support Systems. University of Catalunya; 2012. n. pag.
7. Luenberger D.G., Yinyu Ye. Linear and Nonlinear Programming. International Series in Operations Research & Management Science; 2021. n. pag.
8. Power D.J. Decision support systems: Concepts and resources for managers. Greenwood Publishing Group; 2002. n.pag.
9. Ltifi H., Trabelsi G., Ayed M., Alimi A. Dynamic Decision Support System Based on Bayesian Networks. (IJARAI) International Journal of Advanced Research in Artificial Intelligence, 2012;1(1):22–29.
10. Burnside E.S., Rubin D.L., Fine J.P., Shachter R.D., Sisney G.A., Leung W.K. Bayesian network to predict breast cancer risk of mammographic microcalcifications and reduce number of benign biopsy results: initial experience. Radiology, 2006;240(3):666–673.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Токарев Вячеслав Леонидович, доктор технических наук, профессор, кафедра информационной безопасности, Институт прикладной математики и компьютерных наук, Тульский государственный университет, Тула, Российская Федерация.
e-mail: unwaiter@mail.ru

Vyacheslav L. Tokarev, Doctor of Technical Sciences, Professor, Information Security Department, Institute of Applied Mathematics and Computer Science, Tula State University, Tula, Russian Federation.

Сычугов Алексей Алексеевич, доктор технических наук, доцент, кафедра информационной безопасности, Институт прикладной математики и компьютерных наук, Тульский государственный университет, Тула, Российская Федерация.
e-mail: xru2003@yandex.ru
ORCID: 0000-0002-3959-6994

Aleksey A. Sychugov, Doctor of Technical Sciences, Associate Professor, Information Security Department, Institute of Applied Mathematics and Computer Science, Tula State University, Tula, Russian Federation.

Статья поступила в редакцию 05.12.2022; одобрена после рецензирования 19.12.2022; принята к публикации 23.01.2023.

The article was submitted 05.12.2022; approved after reviewing 19.12.2022; accepted for publication 23.01.2023.