https://doi.org/10.25559/SITITO.020.202403.748-759
УДК 004.492.3

Оригинальная статья

Задача разработки программного обеспечения проактивной защиты информации автоматизированной системы

Д. А. Абрамов*, В. Л. Токарев
ФГБОУ ВО «Тульский государственный университет», г. Тула, Российская Федерация
Адрес: 300012, Российская Федерация, Тульская область, г. Тула, проспект Ленина, д. 92
* sipai-dima@mail.ru

Аннотация

Представленная работа посвящена проблеме разработки систем проактивной защиты от угроз информационной безопасности, которая будет способна работать в режиме псевдореального времени и выявлять угрозы ИБ с минимальной задержкой, в случае её реализации на типовом аппаратном обеспечении. Представлена математическая модель, описывающая влияние негативных процессов на автоматизированную систему, вызванные как взаимодействием злоумышленника с заранее определёнными целями, действующего на основе формально описанной стратегии, так и случайные воздействия на автоматизированную систему, вызванные как действиями персонала, так и случайными факторами. Представлена методика реализации представленной модели, основанная на использовании множества упрощённых моделей, взаимодействующих на основе обобщенного алгоритма, позволяющего работать системе обеспечения безопасности в режиме псевдореального времени, но при этом обеспечивать повышенное быстродействие. Представлена предполагаемая структурная схема как всей системы, так и её частей, отвечающих за имитационное моделирование. Определён набор сенсоров необходимых для выделения нештатных ситуаций и предполагаемая архитектура системы поддержки принятия решений о наличии аномалии. Представлены методы определения показаний сенсоров и критерии их оценки. Описаны предполагаемые границы ответственности и сферы применения различных моделей, используемых в ядре системы поддержки принятия решения. Предложена методика построения системы оценивания количественных показателей качества работы предложенной системы защиты, а также описаны различные варианты её построения, которые позволят оценить способность системы противодействовать различным видам угроз информационной безопасности.

Ключевые слова: информационная безопасность, проактивная защита информации, имитационное моделирование, модели описания угроз информационной безопасности, системы поддержки принятия решений, детекторы нештатных ситуаций, методика оценки систем защиты информации, показатели эффективности систем защиты

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Абрамов Д. А., Токарев В. Л. Задача разработки программного обеспечения проактивной защиты информации автоматизированной системы // Современные информационные технологии и ИТ-образование. 2024. Т. 20, № 3. С. 748-759. https://doi.org/10.25559/SITITO.020.202403.748-759

Original article

The Task of Developing Software for the Proactive Information Protection of an Automated System

D. A. Abramov*, V. L. Tokarev
Tula State University, Tula, Russian Federation
Address: 92 Prospekt Lenina, Tula 300012, Russian Federation
* sipai-dima@mail.ru

Abstract

This work focuses on the development of proactive protection systems against information security threats that can operate in pseudo-real time mode and identify information security threats with minimal delay. These systems would be implemented on standard hardware and would help protect against information security risks. Present mathematical model is presented that describes the impact of negative processes on an automated system caused by both the interaction of an attacker with predetermined targets, acting on the basis of a formally described strategy, and random impacts on an automated system caused by both the actions of personnel and random factors. The article presents a methodology for implementing the presented model, based on the use of multiple simplified models interacting on the basis of a generalized algorithm, which allows the security system to operate in pseudo-real time mode, but at the same time ensure increased performance. The proposed structural diagram of both the entire system and its parts responsible for simulation modeling is presented. The proposed structural diagram of both the entire system and its parts responsible for simulation modeling is presented. A set of sensors required for identifying abnormal situations and a proposed architecture of a decision support system for the presence of an anomaly have been defined. Methods for determining sensor readings and criteria for their evaluation are presented. The proposed boundaries of responsibility and scope of application of the various models used in the core of the decision support system are described. A methodology for constructing a system for assessing quantitative indicators of the quality of the proposed protection system is proposed, and various options for its construction are described, which will allow assessing the system's ability to counteract various types of information security threats.

Keywords: information security, proactive information protection, simulation modeling, models for describing information security threats, decision support systems, anomaly situation detectors, methodics for assessing information security systems, performance indicators of information security systems

Conflict of interests: The authors declares no conflict of interest.

For citation: Abramov D.A., Tokarev V.L. The Task of Developing Software for the Proactive Information Protection of an Automated System. *Modern Information Technologies and IT-Education*. 2024;20(3):748-759. https://doi.org/10.25559/SITITO.020.202403.748-759

Введение

В современном мире количество преступлений, связанных с автоматизированной обработкой информации, ежегодно увеличивается более чем на 10-15%, что согласно исследованиям приводит к росту рынка услуг, связанных с информационной безопасностью не менее 6-10% в год[1]. Данное обстоятельство приводит к значительному росту интереса к направлениям, связанных с информационной безопасностью (ИБ). В области информационной безопасности на данный момент наибольшее распространение получает направление, связанное с проектированием систем ИБ. А наиболее развивающимся направлением обеспечения ИБ является обеспечение защиты от угроз, связанных с вирусным заражением рабочих станций, на основе превентивных технологий построения проективной защиты, защищаемых автоматизированных систем обработки информации [1-3].
Превентивные технологии, на которых построена проактивная защита, позволяют избежать потери времени и обезвредить новую угрозу еще до того, как она нанесет вред автоматизированной системе обработки информации (АС). В отличие от реактивных технологий, выполняющих анализ на основании записей баз Антивируса Касперского[2], превентивные технологии [4] распознают новую угрозу по последовательности действий, производимых некоторой программой.

Цель исследования
Разработка методики построения проактивной защиты информации автоматизированной системы, способной противодействовать заранее неизвестным, но формализованным угрозам информационной безопасности, без обновления базы знаний, способной работать в режиме псевдореального времени с минимальной задержкой при выявлении угроз.

Материалы и методы

Необходимость разработки проактивной защиты информации автоматизированной системы обусловлена также тем обстоятельством, что использование для принятия решений по совершенствованию системы обеспечения информационной безопасности (СОИБ) [5] защищаемой АС имеющейся статистики по различным происшествиям только фиксирует результаты работы существующих (существовавших) систем. Другими словами, статистика «бьет по хвостам» изменяющегося во времени процесса *n(t)* реализации негативных воздействий на АС.
Необходима разработка опережающих мер по борьбе с негативными воздействиями, связанных с прогнозированием развития [6] как алгоритмов реализации этих воздействий (в том числе, постоянно совершенствующихся способов и средств осуществления нарушителями АНВ), так и способов и средств борьбы с ними.

Моделирование процессов негативных воздействий на АС
Использование системного подхода к задаче разработки программного обеспечения проактивной защиты информации в АС обусловливает применение в качестве основы программного обеспечения моделей процессов негативных воздействий на АС и противодействия им СОИБ [7, 8].
Общая схема таких процессов может быть описана моделью (1), которая вместе с соответствующей методикой обеспечит возможность получения количественных оценок показателей качества (эффективности)[3] обеспечения безопасности защищаемых объектов.

$$N \times F \times H \xrightarrow{\mathrm{A}\left(\sigma_k^{IB}\right)} S \to W^{IB}(U) \qquad (1)$$

где N – множество негативных воздействий на АС; F – множество факторов, способствующих негативным воздействиям на АС; H – множество неопределенностей, сопровождающих негативные воздействия; $\mathrm{A}\left(\sigma_k^{IB}\right)$ – алгоритмы СОИБ защищаемой АС (алгоритмы противодействия негативному воздействию); $\sigma_k^{IB} \in \Sigma^{IB}$ – стратегия[4], применяемая СОИБ в k-й интервал времени, Σ^{IB} – множество возможных стратегий, используемых СОИБ; S – состояние защищаемой АС («негативное воздействие реализовано» или «негативное воздействие предотвращено»; U – множество величин ущерба, полученных АС в результате реализации негативных воздействий; W^{IB} – значение показателя эффективности обеспечения безопасности защищаемой АС, которое определяется по соответствующей методике с использованием информации, получаемой с помощью модели (1).

Под негативными воздействиями понимаются процессы n(t)∈N, являющиеся причиной негативных последствий для АС в виде ущерба u∈U определенного вида и масштаба. Случайный (вероятностный) характер процесса *n(t)* определяется наличием множества неопределенностей H. Примерами негативных воздействий могут быть не только противоправное воздействие нарушителя[5], но и: ошибки персонала в процессе функционирования АС; несоблюдение персоналом требований по обеспечению безопасности информации; нарушения работоспособности технических и программных средств АС; утечка информации по техническим каналам; помеховые воздействия на объекты информатизации со стороны физических полей, создаваемых различными техническими средствами, не входящих в состав АС; ошибки пользователей АС;

[1] Число кибератак в России и в мире [Электронный ресурс] // TAdviser, 2024. URL: https://www.tadviser.ru/a/665597 (дата обращения: 10.04.2024); Безопасность информационных систем [Электронный ресурс] // TAdviser, 2024. URL: https://www.tadviser.ru/a/274980 (дата обращения: 10.04.2024).

[2] Токарев И. Д., Волковский А. А. Анализ современных антивирусных программ // Современная техника и технологии: проблемы, состояние и перспективы: Материалы XII Всероссийской научно-практической конференции 24-25 ноября 2023 г. / Под ред. В. В. Гриценко. Рубцовск, 2023. С. 6-11. URL: https://www.rubinst.ru/sites/default/files/files/science/conference_materials/technical_collection-24.pdf (дата обращения: 10.04.2024).

[3] Токарев В. Л. Интеллектуальная система оперативного обнаружения вредоносных программ // Интеллектуальные и информационные системы. Интеллект – 2019 : Труды Всероссийской научно-технической конференции, Тула, 19-20 ноября 2019 года. Тула: ТулГУ, 2019. С. 258-263. EDN: EOLMMG

[4] Под стратегией здесь понимается один из возможных путей достижения цели – обеспечения информационной безопасности АС в условиях негативных воздействий.

[5] Нарушитель – лицо или группа лиц, совершающих или пытающихся совершить негативное(противоправное) воздействие на информацию в АС.

природные, техногенные воздействия и др.

Антагонистический характер процесса противоборства СОИБ с негативными воздействиями N в модели (1) учитывается стратегиями противоборства [9]:

$$\sigma_k^{IB} = P\left(\sigma_k^N, F\right), \quad \sigma^N \in \Sigma^N,$$
$$W\left(\sigma_k^{IB}\right) + W\left(\sigma_k^N, F\right) \approx 0, \qquad (2)$$

где σ_k^N – стратегия негативных воздействий на АС в *k*-й интервал дискретного времени, определяемого произошедшими событиями в АС; $P\left(\sigma_k^N, F\right)$ – правило выбора стратегии σ_k^{IB} на основе оценки стратегии нарушителя

$$\hat{\sigma}_{\mathrm{k}}^{\mathrm{N}} = \arg \min_{\hat{\sigma}_{\mathrm{k}}^{\mathrm{N}} \in \Sigma^N} \left\{ \sum_{i=k-m}^{k} \rho\left(n_i, \hat{n}_i\left(\hat{\sigma}^N, F\right)\right) \right\}, \qquad (3)$$

которая определяется на основе анализа совокупности параметров, характеризующих безопасность, как отдельных защищаемых информационных объектов АС, так и защищаемой АС в целом.

Следует подчеркнуть особую важность оценивания стратегии $\sigma_{\mathrm{k}}^{\mathrm{N}}$. Достоверная оценка $\hat{\sigma}_{\mathrm{k}}^{\mathrm{N}}$ позволит спрогнозировать достаточно точно негативное воздействие $\hat{\mathrm{n}}_{\mathrm{k}+1} \in N$ или воздействия, которые последуют в следующий интервал времени *k+1*. Это позволит уточнить шаги алгоритма $\mathrm{A}_j\left(\sigma_k^{IB}\right)$, $j = 1,\ldots, J$, реализующего стратегию σ_k^{IB}, и тем самым повысить значение показателя эффективности $W\left(\sigma_k^{IB}\right)$ СОИБ.

Обеспечение достоверности получаемых оценок требуется тщательная разработка модели нарушителя [10], включающей сведения о численности, оснащенности, подготовленности, его осведомленности об АС, о возможных стратегиях Σ^{N} и тактике действий потенциального нарушителя, его мотивации и преследуемых целях при совершении негативных воздействий на защищаемую АС.

Из всего этого следует, что построение модели (1) представляет собой сложную научную задачу.

Во первых, на исследуемую систему (защищаемую АС) действуют два основных взаимодействующих фактора. С одной стороны – действия *N* нарушителя, действующего в соответствии с некоторой, хорошо предсказуемой целью $g \in G$ и с некоторой, хуже предсказуемой стратегией $\sigma_{\mathrm{k}}^{\mathrm{N}} \in \Sigma^N$, и случайные негативные воздействия на систему, являющиеся результатом присутствия факторов $F \times H$. С другой стороны – действия СОИБ.

Во вторых, результатом их взаимодействия может служить показатель W^{IB}, для вычисления достоверной оценки которого требуется разработка специальной методики, так как существующие методики [11], основаны только на оценке величины ущерба, полученного после достижения цели нарушителя, что никак не позволит повысить эффективность проактивной защиты.

В третьих, существующие теории систем и системного анализа, а также накопленный опыт показывает [10], что такую многосвязную систему (1) отобразить одной моделью с требуемой точностью вряд ли удастся. Выход заключается в создании *моделирующей системы*, включающей множество моделей, часть из которых может быть создана с участием экспертов. В соответствии с теорией систем такая моделирующая система может быть обозначена классифицирована как «имитационная система». Причем понятие «имитационная система» не следует отождествлять с прививившимся за последнее время термином «имитационная модель», который обычно просто дублирует понятие «статистическая модель» (модель Монте-Карло).

Имитационная моделирующая система должна составлять основу компьютерной системы поддержки принятия решений – основу СОИБ.

Порядок ее разработки представляется следующим:

- обследование АС (изучение его топологии, выполняемых задач, кадрового и технического состава, алгоритмов и режимов функционирования и т. п.);
- обследование существующей на нем СОИБ (изучение ее кадрового состава и показателей его квалификации, инженерно-технических средств, режимов функционирования и используемых алгоритмов A^{IB} противодействия негативным воздействиям и т. п.);
- разработка моделей нарушителей и не их основе прогнозирование множества N возможных видов негативных воздействий в деятельность АС, их конечных результатов;
- прогнозирование множества Σ^{N}, а также алгоритмов их реализации $A\left(\sigma_k^{IB}\right)$,
- разработка метода оценки стратегии $\hat{\sigma}_{\mathrm{k}}^{\mathrm{N}}$, обеспечивающего выполнения требования (3);
- разработка системы поддержки принятия решений (2)[6];
- алгоритмизация и программная реализация модели (1);
- тестирование модели (1) с использованием имеющейся статистики по реализации негативных воздействий и противодействию им;
- разработка на основе модели (1) типовых сценариев функционирования СОИБ защищаемого объекта.

Не останавливаясь на очевидных элементах приведенного порядка, сделаем несколько замечаний по некоторым из них.

Прогнозирование множества Σ^{N} стратегий (типовых сценариев негативных воздействий на АС) на основе исследования метасистемы «АС – окружающая среда» и определения множества Σ^{IB} стратегий СОИБ является оперативной основой создания модели (1). Указанные стратегии содержат описание способов применения СОИБ, наиболее полно характеризую-

[6] Токарев В. Л. Компьютерная поддержка принятия решений : монография. М.: Изд-во СГУ, 2007. EDN: QJSEOX

щих их возможности в определенных условиях, и представляют собой также базу для создания методик оценки их качества (эффективности) [12, 13].

Имеющийся опыт создания больших систем различного назначения говорит о принципиальной необходимости и важности наличия подобных типовых стратегий, разработка которых требует, как правило, проведения специальных научно-исследовательских работ.

Отметим также обстоятельства, облегчающие и удешевляющие алгоритмизацию и программную реализацию моделирующей системы (1).

Во-первых, к этим обстоятельствам относится возможность включения в состав моделирующей системы (1) в качестве ее физических составляющих реальных систем и технических средств обеспечения безопасности конкретного защищаемого объекта (средств телевизионного наблюдения, охранной сигнализации, связи, технических и специальных средств контроля состояния объекта безопасности и т. п.). Эти средства могут использоваться как физические источники информации, в том числе, информации при моделировании действий нарушителей в условиях реального состояния АС.

Во-вторых, для реализации математической составляющей алгоритмов моделирующей системы (1) могут быть использованы имеющиеся на АС средства вычислительной техники.

Основными принципами построения имитационной моделирующей системы должны быть:

1) модульность построения, позволяющая набором стандартных модулей формировать модель (1) и проводить автономную отладку ее отдельных модулей;

2) открытость и гибкость структуры, позволяющая производить наращивание (корректировку) моделирующей системы (пополнение баз данных, подключение или отключение отдельных модулей) без коренной перестройки ее структуры и принципиального изменения содержания отдельных стандартных модулей;

3) соответствие вида и количества моделируемой информации данному уровню иерархии модели.

4) имитационный характер моделирующей системы, который позволяет вводить отдельным «блоком» эксперта (специалиста – оператора) для моделирования процессов, некоторые элементы которых по тем или иным причинам не могут быть формализованы.

Реализация этих принципов, во-первых, позволит создать моделирующую систему, соответствующую содержанию процессов функционирования СОИБ, и, во-вторых, обеспечит возможность проведения моделирования при приемлемых затратах времени и вычислительных ресурсов (что особенно важно при проведении многократных «прогонов» задач для получения устойчивых статистических результатов).

Структурная схема имитационной моделирующей системы

При создании математических моделей больших систем иерархической структуры их укрупнение путем простого «наращивания» информации в соответствии с увеличением числа элементов в моделях более высокого уровня, как показала практика, весьма затрудняет решение поставленных задачи даже при применении современных ЭВМ [14].

Выходом из положения является разработка комплекса взаимосвязанных моделей, организационный уровень которых соответствует минимально необходимому уровню применения рассматриваемого элемента системы. Как правило, этот уровень должен быть равным уровню штатной принадлежности элемента, функционирование которого моделируется.

Другими словами, речь о комплексе взаимосвязанных моделей [10], каждый блок которого на своем уровне обеспечивает наиболее полный (необходимый) учет влияния характеристик рассматриваемого элемента системы на показатель ее качества (эффективности) в целом.

По отношению к исследуемому уровню модели (1) все нижестоящие уровни должны моделироваться обобщенно (укрупненно), а вышестоящие уровни (в том числе и другие системы, взаимодействующие с моделируемой системой) должны представляться в виде исходных данных или ограничений[7].

Структурная схема имитационной моделирующей системы и взаимосвязи входящих в ее состав моделей отражены на рис. 1.

Р и с. 1. Структурная схема имитационной моделирующей системы

F i g. 1. Structural diagram of the simulation modeling system

Источник: здесь и далее в статье все рисунки составлены авторами.

Source: Hereinafter in this article all figures were drawn up by the authors.

Модели функционирования отдельных элементов СОИБ необходимы для оценки их влияния на процесс обеспечения безопасности АС в целом (в том числе на показатель качества этого обеспечения).

Модели процессов обеспечения безопасности должны разрабатываться с использованием моделей функционирования элементов СОИБ с учетом всех необходимых связей в структуре этой системы.

Модель процесса обеспечения безопасности защищаемого объекта [15] в целом должна учитывать ее взаимодействие со всеми другими внешними органами и системами, проводимое на основе единого алгоритма, согласованное по целям, задачам и времени.

[7] Токарев В. Л. Конструирование многоагентной системы для распознавания угроз информационной безопасности // Инновационное развитие науки и техники : Сборник статей VI Международной научно-практической конференции, Саратов, 10 декабря 2020 года. Саратов: Научная общественная организация «Цифровая наука», 2020. С. 10-20. EDN: ELXJFL

Реализация имитационной моделирующей системы

Исходной информацией для моделирования процесса негативных воздействий на *i*-ю АС являются:

- множество прогнозируемых стратегий Σ_i^N, характерных для *i*-й АС;.
- множество F_i факторов, способствующих реализации стратегий Σ^N или реализации негативных воздействий окружающей среды, направленных на *i*-ю АС;
- множества негативных воздействий N_i, направленных на *i*-ю АС [11];
- существующие стратегии Σ^{IB} СОИБ *i*-й защищаемой АС.

Множества Σ_i^N, F_i определяются экспертным методом, исходя из имеющегося опыта борьбы с негативными воздействиями, знания структуры, состава и особенностей защищаемой АС и её СОИБ, а также прогноза состояния элементов этих множеств на рассматриваемом временном интервале.

На основе этих исходных данных методами построения приближенных моделей [3] выстраивается моделирующая система (1). При этом неопределенности *H* при моделировании учитываются случайным образом в соответствии с их содержанием для конкретных стратегий $\sigma^N \in \Sigma^N$ и факторов F_i – реализацией распределений соответствующих случайных величин (функций).

В качестве метода получения устойчивых обобщенных результатов моделирования при реализации модели *M* был выбран метод статистических испытаний.

С использованием моделирующей системы определяется база знаний СОИБ – набор правил $P\left(\sigma_k^N, F\right)$

$$\left\langle N_i, F \right\rangle_i \xrightarrow{M} P\left(\sigma_k^N, F\right) \quad (4)$$

Отрицательные последствия некачественных решений (2) могут выражаться:

- в несвоевременности принятия решения $d\left(\hat{\sigma}_k^{IB}\right)$ (хотя и правильного, которого требовала создавшаяся ситуация),
- принятии решения, не позволяющего использовать все имеющиеся возможности СОИБ,
- непринятии какого-либо решения вообще (отсутствии реагирования на создавшуюся ситуацию).

Имитационная моделирующая система может быть использована как:

1) основа системы поддержки принятия решений (СППР) – главного модуля СОИБ.
2) исследовательская модель,
3) учебная модель,
4) модель мониторинга характеристик процесса негативных воздействий,
5) модель экспресс-оценок основных характеристик СОИБ,
6) основа методики количественной оценки характеристик СОИБ.

Система поддержки принятия решений на основе моделирующей системы может быть построена следующим образом.

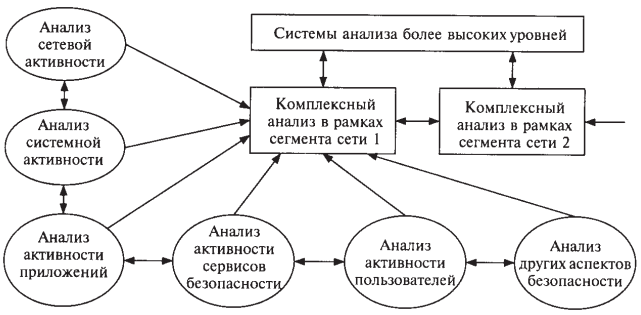
В различных точках защищаемой АС устанавливаются агенты (сенсоры) СОИБ, которые передают информацию на центральную консоль управления. Регистрационная информация может извлекаться из системных или прикладных журналов (технически несложно получать ее и напрямую от ядра ОС) либо добываться из сети АС с помощью механизмов активного сетевого оборудования или путем перехвата пакетов посредством установленной в режим мониторинга сетевой карты.

На уровне агентов (сенсоров) может выполняться фильтрация данных с целью уменьшения их объема. Это требует от агентов[8] некоторого интеллекта, но зато разгружает остальные компоненты системы.

Агенты передают информацию в центр распределения, который приводит ее к единому формату, возможно осуществляет дальнейшую фильтрацию, сохраняет в базе данных и направляет для анализа статистическому и экспертному компонентам. Один центр распределения может обслуживать несколько сенсоров.

Содержательный активный аудит начинается со статистического и экспертного компонентов. Если в процессе статистического или экспертного анализа выявляется подозрительная активность, соответствующее сообщение направляется решателю, который определяет, является ли тревога оправданной, и выбирает способ реагирования [16].

Архитектуру такой СОИБ можно представить в виде (рис. 2).



Р и с. 2. Архитектура системы поддержки принятия решений обнаружения негативных воздействий

F i g. 2. Architecture of a decision support system for detecting negative impacts

На одном уровне иерархии располагаются компоненты, анализирующие подозрительную активность с разных точек зрения. Например, на хосте могут располагаться подсистемы анализа поведения пользователей и приложений. Их может дополнять подсистема анализа сетевой активности [17]. Когда один компонент обнаруживает что-то подозрительное, то во многих случаях целесообразно сообщить об этом соседям либо для принятия мер, либо для усиления внимания к определенным аспектам поведения системы.

Датчики-сенсоры [18] аномалий идентифицируют необычное поведение, аномалии в функционировании отдельного объекта – трудности их применения на практике связаны с неста-

[8] Токарев В. Л. Конструирование многоагентной системы для распознавания угроз информационной безопасности // Инновационное развитие науки и техники : Сборник статей VI Международной научно-практической конференции, Саратов, 10 декабря 2020 года. Саратов: Научная общественная организация «Цифровая наука», 2020. С. 10-20. EDN: ELXJFL

бильностью самих защищаемых объектов и взаимодействующих с ними внешних объектов. В качестве объекта наблюдения может выступать сеть в целом, отдельный компьютер, сетевая служба (например, FTP-сервер), пользователь и т.д. Датчики срабатывают при условии, что негативные воздействия отличаются от «обычных» (законных) действий. Для этого необходима некоторая метрика, позволяющая определять «дистанцию» отклонения наблюдаемого поведения от штатного, принятого в АС, и «порог срабатывания» сенсора наблюдения. Меры и методы, обычно используемые в обнаружении аномалии, включают в себя следующие атрибуты:

1) пороговые значения. В качестве наблюдаемых параметров могут быть, например, количество файлов, к которым обращается пользователь в данный период времени, число неудачных попыток входа в систему, загрузка центрального процессора и т. п. Пороги могут быть статическими и динамическими (т. е. изменяться, подстраиваясь под конкретную систему);

2) статистические меры. Решение о наличии негативных воздействий делается по большому количеству собранных данных путем их статистической предобработки;

3) параметрические меры. Для выявления негативных воздействий строится специальный «профиль нормальной системы» на основе шаблонов (т. е. некоторой политики, которой обычно должна придерживаться защищаемая АС);

4) непараметрические меры. Здесь уже профиль строится на основе наблюдения за объектом в период обучения;

5) меры на основе правил (сигнатур). В период обучения СППР составляется представление о нормальном поведении объекта, которое записывается в виде специальных «правил». Получаются сигнатуры «нормального» поведения АС;

6) другие меры.

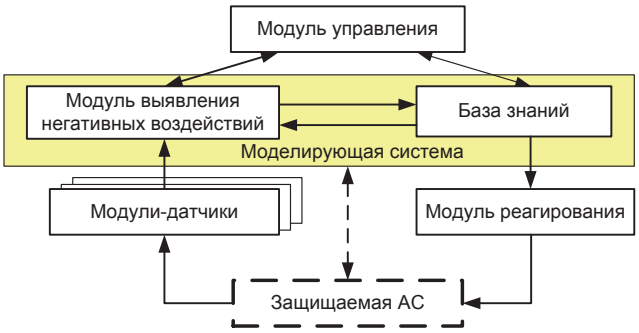
Две основные задачи: **1) построение профиля объекта, 2) определение граничных значений** характеристик поведения АС решаются с помощью моделирующей системы.

Достоинства такой СППР очевидны:

- они способны обнаруживать новые типы негативных воздействий, сигнатуры для которых еще не разработаны;
- обнаружения аномалий генерируют информацию, которая может быть использована для уточнения правил базы знаний СППР;
- они не нуждаются в обновлении сигнатур и правил обнаружения негативных воздействий.

Такая СППР представляет собой специализированное программно-аппаратное обеспечение с типовой архитектурой, включающей в себя следующие компоненты (рис. 3):

- модули-датчики для сбора необходимой информации о поведении АС;
- модуль выявления (распознавания) негативных воздействий, выполняющий обработку данных, собранных датчиками – первая основная компонента моделирующей системы (1);
- модуль хранения конфигурационной информации, базы правил, информации об обнаруженных негативных воздействиях и процедур логического вывода. Таким модулем, как правило, выступает база знаний – вторая основная компонента моделирующей системы (1);
- модуль реагирования на обнаруженные негативные воздействия;
- модуль управления компонентами СППР.



Р и с. 3. Архитектура СППР

F i g. 3. DSS architecture (Decision Support System – DSS)

Центральным компонентом СППР является специализированное программное ядро (моделирующая система), предназначенное для анализа данных, поступающих от сенсоров, и принятия решений о способах реагирования на подозрительные события. Стандартизация протоколов и форматов обмена данными между моделирующей системой с одной стороны и сенсорами и средствами реагирования с другой, позволяет применять общее программное ядро с различными типами сенсоров и средств реагирования.

Исследовательская модель призвана обеспечить получение необходимой информации для решения основных задач:

- выбора, обоснования и систематизации основных характеристик и показателей качества (эффективности) обеспечения безопасности защищаемых объектов;
- количественной оценки этих характеристик и показателей;
- исследования влияния топологии, состава и характеристик элементов АС на показатели качества обеспечения безопасности;
- исследования влияния внешних и внутренних факторов, способствующих реализации негативных воздействий на ОБ, на показатели качества обеспечения их безопасности;
- получения информации, необходимой для проведения теоретических обобщений, в том числе, получения статистических данных о состоянии СОИБ защищаемых объектов, исследований по обоснованию вероятностных характеристик процессов негативных воздействий на ОИБ (законов распределения случайных величин и функций, корреляционных и взаимно корреляционных функций и т. д.);
- выявления и прогнозирования «узких мест» с точки зрения качества обеспечения безопасности и выработки рекомендаций по ее совершенствованию;
- создания баз данных по характеристикам СОИБ защищаемых объектов.

Учебная модель (тренажер) призвана в наибольшей степени использовать возможности СОБ для отработки навыков действий их персонала при противодействии негативным воздействиям на ОБ и обеспечивать решение следующих основных задач:

- создания и развития баз данных по специальным учебным вариантам сценариев противоборства СОБ с негативными воздействиями; о моделирования работы СОБ при проведении «учебных игр» с их персоналом по результатам реализации того или иного из учебных сценариев;

- получения количественной информации, необходимой для оценки результатов обучения персонала СОБ;
- выявления «узких мест» с точки зрения наличия необходимых навыков и опыта работы персонала СОБ;
- проведение учений и тренировок персонала СОИБ защищаемой АС. Роль нарушителя при интерактивном моделировании должны выполнять высококвалифицированные специалисты СОИБ защищаемого объекта;
- выявление и последующая ликвидация имеющихся технологических и эксплуатационных уязвимостей АС;
- тренировка персонала СОИБ с целью получения и совершенствования им соответствующих навыков производственной деятельности.

Модель мониторинга характеристик процессов функционирования СОБ, определяющих их качество, призвана обеспечивать в режиме онлайн прогнозирование их поведения и принимать своевременные решения по недопущению возникновения нежелательных режимов их работы (перегрузки систем, сбоев в прохождении информации и т. п.) и в конечном итоге обеспечивать решение основных задач:
- выявления множества факторов, наиболее существенно влияющих на возникновение нежелательных режимов работы СОБ;
- получения необходимой информации для разработки способов мониторинга этих факторов в режиме он-лайн;
- отработки методов прогнозирования поведения СОБ по результатам оценок характеристик их функционирования;
- отработки способов предотвращения нештатных режимов работы СОБ по результатам прогнозирования значений их характеристик;
- оценки эффективности предлагаемых способов предотвращения нештатных режимов работы СОБ;
- отработки предложений по созданию программно-технических средств СОИБ, обеспечивающих решение задач реальными ОБ.

Модель экспресс-оценок основных характеристик СОИБ предназначена для руководящих органов, принимающих решения по их созданию и развитию и призвана обеспечивать решение следующих основных задач:
- оперативной оценки результатов изменений топологии, состава и характеристик инженерно-технических средств, состава и квалификации персонала, организации работы конкретных СОБ защищаемых объектов на показатели их качества (эффективности);
- оперативной оценки целесообразности рассмотрения тех или иных предложений по развитию существующих и созданию новых СОБ защищаемых объектов.

Разработка методики[9] количественной оценки характеристик СОИБ.

Основной конечной целью любой *методики* является количественная оценка некоторых характеристик (показателей качества) исследуемых объектов или процессов [19]. В соответствии с этим показатель качества СОИБ [20] определим следующим образом – это характеристика, описываемая количественно и позволяющая оценить свойство СОИБ с какой-либо одной стороны.

В настоящее время в научной и технической литературе кроме термина «показатель» используется также термин «критерий», которым часто придают один и тот же смысл. Представляется необходимым эти понятия четко различать.

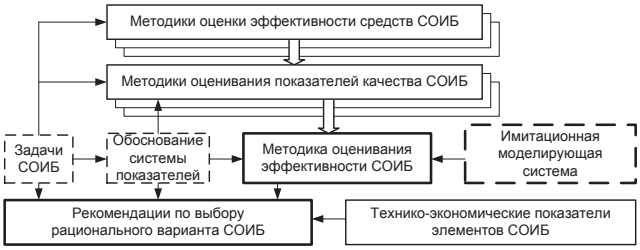
Понятие «*критерий*» (от греч. *criterion* - средство для суждения) определяет «признак, на основании которого производится оценка, определение или классификация чего-либо; мерило оценки». То есть, критерий – решающее правило (способ) [21], в соответствии с которым выбирается предпочтительный в некотором смысле вариант объекта, процесса из ряда альтернативных.

Критерий, таким образом, предполагает применительно к рассматриваемым альтернативным вариантам необходимость обоснования нашего представления (в том числе формального) о том, в каком же смысле рассматривается эта предпочтительность.

Следует заметить, что обоснование критерия в ряде случаев представляет собой самостоятельную сложную научную задачу.

Говоря о методиках количественной оценки характеристик (показателей качества) обеспечения безопасности защищаемых объектов [22], нужно заметить, что они должны соответствовать иерархии моделей комплексной имитационной моделирующей системы, так как выходные данные именно этих моделей будут являться входной информацией для методик.

Структурная схема комплексной методики количественной оценки качества (эффективности) СОБ защищаемого объекта и ее взаимосвязь с задачей обоснования рационального варианта этой системы отражена на рис. 4.



Р и с. 4. Структурная схема комплексной методики количественной оценки качества системы обеспечения безопасности

F i g. 4. Structural diagram of a comprehensive methodology for quantitative assessment of the quality of a security system

Комплексная методика количественной оценки качества СОИБ [23] защищаемых объектов в зависимости от специфики этих систем может основываться на существующих научных методах, применяемых в настоящее время для исследования и оценки характеристик сложных систем:
- методе получения оценок в результате интерактивного моделирования (использование модели М) процессов обеспечения безопасности защищаемых объектов;

[9] Напомним, что методика – способ реализации метода, т. е. конкретный алгоритм, процедура для проведения каких-либо нацеленных действий по реализации метода решения определенной задачи или достижения определенной цели. В то время как, метод – систематизированная совокупность шагов, действий, которые необходимо предпринять, чтобы решить определенную задачу или достичь определенной цели.

- методе получения оценок по результатам физического моделирования процессов;
- статистических методах обработки информации (дисперсионно-регрессионном анализе);
- различных комбинациях этих методов.

Каждый из указанных методов обладает специфическими преимуществами и недостатками, которые хорошо известны[10] [24, 25].

Обсуждение и заключение

Представленная в рамках данной работы, модель системы проактивной защиты автоматизированных систем от угроз информационной безопасности, основанная на использовании представленной модели, учитывающей как действия злоумышленника и его стратегию, так и случайные действия персонала, приводящие к негативным последствиям, реализованной на основе взаимодействия комплекса упрощённых моделей, осуществляемых на изложенной в работе методике, позволит получить систему защиты объектов от угроз ИБ, способную противодействовать на данный момент не известным, но поддающимся формализации угрозам ИБ, без обновления базы знаний, что может быть крайне актуально для решения задач, связанных с аппаратной реализацией средств защиты, а так же систем, устанавливаемых на объекты автоматизации, не имеющие канала связи, или объекты обновление базы знаний который в силу различных причин и ограничений затруднено. Возможность обеспечения защиты от заранее неизвестных, но формализуемых угроз ИБ без изменения базы знаний, позволит предложенной системе сохранять способность реагировать на события ИБ, в течении длительного времени, даже в случае сокращения процессов сервисного обслуживания, по сравнению и значительно снизить стоимость её обслуживания в сравнении с системами, не использующими данных подход.

Предложенный подход к проектированию СОИБ, является относительно универсальным, так как отсутствуют строгие ограничения на вид используемых данных и может быть использован для проектирования СОИБ, которые могут быть применены в различных предметных областях и на различных объектах информатизации, что позволяет получить СОИБ используемую широким кругом пользователей

Список использованных источников

[1] Cybersecurity and cybercrime: Current trends and threats / A. Kuzior [et al.] // Journal of International Studies. 2024. Vol. 17, No. 2. P. 220-239. https://doi.org/10.14254/2071-8330.2024/17-2/12

[2] A Systematic Literature Review on the Cyber Security / Yu. Perwej [et al.] // International Journal of Scientific Research and Management. 2021. Vol. 09, No. 12. P. 669-710. https://doi.org/10.18535/ijsrm/v9i12.ec04

[3] Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure / H. Riggs [et al.] // Sensors. 2023. Vol. 23, issue 8. Article number: 4060. https://doi.org/10.3390/s23084060

[4] Унижаев Н. В. Особенности моделирования угроз безопасности персональных данных для обеспечения достаточного уровня защищенности // Вопросы инновационной экономики. 2022. Т. 12, № 1. С. 95-110. https://doi.org/10.18334/vinec.12.1.114335

[5] Клишин Д. В., Чечулин А. А. Анализ стандартов обеспечения информационной безопасности // Системы анализа и обработки данных. 2023. № 1(89). С. 37-54. https://doi.org/10.17212/2782-2001-2023-1-37-54

[6] Анализ зарубежного опыта применения интеллектуальных методов в задачах защиты объектов критической информационной инфраструктуры финансового сектора / Н. В. Беспалова [и др.] // Инженерный вестник Дона. 2024. № 5(113). С. 76-91. EDN: CUNCOD

[7] Токарев В. Л., Сычугов А. А. Метод аудита защищенности автоматизированных систем // Моделирование, оптимизация и информационные технологии. 2019. Т. 7, № 1. С. 548-559. https://doi.org/10.26102/2310-6018/2019.24.1.036

[8] Bansal S., Ruby D., Bargoti R. A New Hybrid Ensemble Learning-Based Malware Detection Technique // Intelligent Computing, Smart Communication and Network Technologies. ICICSCNT 2023. Communications in Computer and Information Science ; ed. by P. Dassan, S. Thirumaaran, N. Subramani. Vol. 1970. Cham: Springer, 2024. P. 235-249. https://doi.org/10.1007/978-3-031-75957-4_20

[9] Токарев В. Л. Распознавание стратегии противодействующей стороны по текущим наблюдениям // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 2(32). С. 184-187. EDN: SEBGVJ

[10] Токарев В. Л. Формальные модели безопасности // Чебышевский сборник. 2021. Т. 22, № 1(77). С. 488-495. https://doi.org/10.22405/2226-8383-2021-22-1-488-494

[11] Борзенкова С. Ю., Токарев В. Л. Определение актуальных угроз на основе коэффициентов опасности деструктивных действий потенциального нарушителя системы информационной безопасности АСУ ТП // Промышленные АСУ и контроллеры. 2020. № 10. С. 52-55. https://doi.org/10.25791/asu.10.2020.1229

[12] Жук Р. В. Способ определения потенциала нарушителя безопасности информации и реализуемых им уязвимостей программного обеспечения // Труды учебных заведений связи. 2021. Т. 7, № 2. С. 95-101. https://doi.org/10.31854/1813-324X-2021-7-2-95-101

[10] Основы теории принятия решений для программистов: учеб. пособие / Н. А. Соловьев, Е. Н. Чернопрудова, Д. А. Лесовой. Оренбург: ОГУ, 2012. 187 с. URL: http://elib.osu.ru/bitstream/123456789/10122/1/3198_20120626.pdf (дата обращения: 10.04.2024); Глотова М. Ю., Самохвалова Е. А. Математическая обработка информации : учебник и практи-кум для СПО. 4-е изд., испр. и доп. М.: Изд-во Юрайт, 2024. 330 с. URL: https://urait.ru/bcode/562231 (дата обращения: 10.04.2024).

[13] Токарев В. Л., Сычугов А. А. Математическое обеспечение оценивания безопасности автоматизированных систем // Известия Тульского государственного университета. Технические науки. 2016. № 11-1. С. 157-165. EDN: XDYLNP

[14] Токарев В. Л., Сычугов А. А. Метод оценки уровня рисков безопасности узлов сети для повышения эффективности размещения иммунных детекторов // Моделирование, оптимизация и информационные технологии. 2020. Т. 8, № 3(30). С. 39. https://doi.org/10.26102/2310-6018/2020.30.3.021

[15] Токарев В. Л. Скрытые марковские модели в задаче обнаружения атак на компьютерные сети // Чебышевский сборник. 2021. Т. 22, № 5(81). С. 391-399. https://doi.org/10.22405/2226-8383-2021-22-5-391-399

[16] Ouiazzane S., Addou M., Barramou F. A Multi-Agent Model for Network Intrusion Detection // 2019 1st International Conference on Smart Systems and Data Science (ICSSD). Rabat, Morocco: IEEE Press, 2019. P. 1-5. https://doi.org/10.1109/ICSSD47982.2019.9003119

[17] Идентификация неявных угроз на основе анализа активности пользователя в интернет-пространстве / В. В. Бова [и др.] // Известия Южного федерального университета. Технические науки. 2020. № 3(213). С. 156-172. https://doi.org/10.18522/2311-3103-2020-3-156-172

[18] Адаптивная система защиты сенсорных сетей от активных атак / А. С. Басан, Е. С. Басан, О. Ю. Пескова [и др.] // Вопросы кибербезопасности. 2022. № 6(52). С. 22-39. https://doi.org/10.21681/2311-3456-2022-6-22-39

[19] Токарев В. Л., Сычугов А. А. Вариант системы оперативного обнаружения Malware // Известия Тульского государственного университета. Технические науки. 2017. № 10. С. 186-195. EDN: ZVLGJR

[20] Добрышин М. М. Подход к формированию обобщенного критерия оценки эффективности системы обеспечения информационной безопасности // Известия Тульского государственного университета. Технические науки. 2021. № 9. С. 113-121. https://doi.org/10.24412/2071-6168-2021-9-113-121

[21] Абрамов Д. А., Токарев В. Л. Методика автоматического выявления нештатных ситуаций на объектах общественного транспорта // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 4. С. 878-888. https://doi.org/10.25559/SITITO.18.202204.878-888

[22] Соловьев С. В., Язов Ю. К. Информационное обеспечение деятельности по технической защите информации // Вопросы кибербезопасности. 2021. № 1(41). С. 69-79. https://doi.org/10.21681/2311-3456-2021-1-69-79

[23] Вариант применения системной инженерии при синтезе системы обеспечения информационной безопасности / А. А. Кисляк, М. М. Добрышин, Д. Е. Шугуров, А. А. Горшков // Известия Тульского государственного университета. Технические науки. 2023. № 2. С. 71-76. https://doi.org/10.24412/2071-6168-2023-2-71-77

[24] Модель оптимального комплексирования мероприятий обеспечения информационной безопасности / П. Д. Зегжда, В. Г. Анисимов, Е. Г. Анисимов, Т. Н. Сауренко // Проблемы информационной безопасности. Компьютерные системы. 2020. № 2. С. 9-15. EDN: PPYPYM

[25] Белов А. С., Добрышин М. М., Шугуров Д. Е. Научно-методический подход к оцениванию качества систем обеспечения информационной безопасности // Приборы и системы. Управление, контроль, диагностика. 2022. № 11. С. 34-40. https://doi.org/10.25791/pribor.11.2022.1373

Поступила 10.04.2024; одобрена после рецензирования 21.06.2024; принята к публикации 29.08.2024.

Об авторах:

Абрамов Дмитрий Александрович, доцент кафедры информационной безопасности, ФГБОУ ВО «Тульский государственный университет» (300012, Российская Федерация, Тульская область, г. Тула, проспект Ленина, д. 92), кандидат технических наук, **ORCID: https://orcid.org/0000-0003-2813-1179,** sipai-dima@mail.ru

Токарев Вячеслав Леонидович, доцент кафедры информационной безопасности, ФГБОУ ВО «Тульский государственный университет» (300012, Российская Федерация, Тульская область, г. Тула, проспект Ленина, д. 92), доктор технических наук, профессор, **ORCID: https://orcid.org/0000-0002-9827-5250,** tokarev22@yandex.ru

Все авторы прочитали и одобрили окончательный вариант рукописи.

References

[1] Kuzior A., Tiutiunyk I., Zielińska A., Kelemen R. Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies*. 2024;17(2):220-239. https://doi.org/10.14254/2071-8330.2024/17-2/12

[2] Perwej Yu., et al. A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*. 2021;09(12):669-710. https://doi.org/10.18535/ijsrm/v9i12.ec04

[3] Riggs H., Tufail S., Parvez I., Tariq M., Khan M.A., Amir A., Vuda K.V., Sarwat A.I. Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensors.* 2023;23(8):4060. https://doi.org/10.3390/s23084060

[4] Unizhaev N.V. *Osobennosti modelirovaniya ugroz bezopasnosti personalnyh dannyh dlya obespecheniya dostatochnogo urovnya zaschischennosti* [Modeling threats to the personal data security to ensure a sufficient protection rate]. *Voprosy innovatsionnoy ekonomiki.* 2022;12(1):95-110. (In Russ., abstract in Eng.) https://doi.org/10.18334/vinec.12.1.114335

[5] Klishin D.V., Chechulin A.A. *Analiz standartov obespecheniya informatsionnoi bezopasnosti* [Analysis of information security standards]. *Sistemy analiza i obrabotki dannykh* = Analysis and Data Processing Systems. 2023;(1):37-54. (In Russ., abstract in Eng.) https://doi.org/10.17212/2782-2001-2023-1-37-54

[6] Bespalova N.V., et al. Analysis of foreign experience in the application of intelligent methods in the tasks of protecting objects of critical information infrastructure of the financial sector. *Ingineering Journal of Don*. 2024;(5):76-91. (In Russ., abstract in Eng.) EDN: CUNCOD

[7] Tokarev V.L., Sychugov A.A. Method of auditing the protection of automated systems. *Modeling, optimization and information technology.* 2019;7(1):548-559. (In Russ., abstract in Eng.) https://doi.org/10.26102/2310-6018/2019.24.1.036

[8] Bansal S., Ruby D., Bargoti R. A New Hybrid Ensemble Learning-Based Malware Detection Technique. In: Dassan P., Thirumaaran S., Subramani N. (Eds.) Intelligent Computing, Smart Communication and Network Technologies. ICICSCNT 2023. *Communications in Computer and Information Science.* Vol. 1970. Cham: Springer; 2024. p. 235-249. https://doi.org/10.1007/978-3-031-75957-4_20

[9] Tokarev V.L. Recognition of rival''s strategy using actions detection. *Proceedings of TUSUR University.* 2014;(2):184-187. (In Russ., abstract in Eng.) EDN: SEBGVJ

[10] Tokarev V.L. Formal Security Models. *Chebyshevskii Sbornik*. 2021;22(1):488-495. (In Russ., abstract in Eng.) https://doi.org/10.22405/2226-8383-2021-22-1-488-494

[11] Borzenkova S.Yu., Tokarev V.L. Determination of actual threats based on the risk factors of destructive actions of a potential violator of the information security system ACS TP. *Industrial Automatic Control Systems and Controllers.* 2020;(10):52-55. (In Russ., abstract in Eng.) https://doi.org/10.25791/asu.10.2020.1229

[12] Zhuk R.V. Method for Determining the Potential of an Information Security Intruder and Realizable Software Vulnerabilities. *Proceedings of Telecommunication Universities*. 2021;7(2):95-101. (In Russ., abstract in Eng.) https://doi.org/10.31854/1813-324X-2021-7-2-95-101

[13] Tokarev V.L., Sychugov A.A. Software Security Estimation of Automated Systems. *News of the Tula state university. Technical sciences.* 2016;(11-1):157-165. (In Russ., abstract in Eng.) EDN: XDYLNP

[14] Tokarev V.L., Sychugov A.A. Method for assessing the level of security risks of network nodes to improve the efficiency of placement of immune detectors. *Modeling, Optimization and Information Technology.* 2020;8(3):39. (In Russ., abstract in Eng.) https://doi.org/10.26102/2310-6018/2020.30.3.021

[15] Tokarev V.L. Hidden Markov Models in the Problem of Detecting Attacks on Computer Networks. *Chebyshevskii Sbornik*. 2021;22(5):391-399. (In Russ., abstract in Eng.) https://doi.org/10.22405/2226-8383-2021-22-5-391-399

[16] Ouiazzane S., Addou M., Barramou F. A Multi-Agent Model for Network Intrusion Detection. In: 2019 1st International Conference on Smart Systems and Data Science (ICSSD). Rabat, Morocco: IEEE Press; 2019. p. 1-5. https://doi.org/10.1109/ICSSD47982.2019.9003119

[17] Bova V.V., et al. Implicit Threats Identification Based on Analysis of User Activity on the Internet Space. *Izvestiya SFedU. Engineering Sciences.* 2020;(3):156-172. (In Russ., abstract in Eng.) https://doi.org/10.18522/2311-3103-2020-3-156-172

[18] Basan A.S., et al. Architecture of Adaptive Protection System for Sensor Network. *Voprosy kiberbezopasnosti* = Cybersecurity issues. 2022;(6):22-39. (In Russ., abstract in Eng.) https://doi.org/10.21681/2311-3456-2022-6-22-39

[19] Tokarev V.L., Sychugov A.A. Malware Detection Using Immune Detectors. *News of the Tula state university. Technical sciences.* 2017;(10):186-195. (In Russ., abstract in Eng.) EDN: ZVLGJR

[20] Dobryshin M. M. An approach to the formation of a generalized criterion for evaluating the effectiveness of an information security system. *News of the Tula state university. Technical sciences.* 2021;(9):113-121. (In Russ., abstract in Eng.) https://doi.org/10.24412/2071-6168-2021-9-113-121

[21] Abramov D.A., Tokarev V.L. Methodology for Automatic Detection of Emergency Situations at Public Transport Objects. *Modern Information Technologies and IT-Education*. 2022;18(4):878-888. (In Russ., abstract in Eng.) https://doi.org/10.25559/SITITO.18.202204.878-888

[22] Soloviev S.V., Yazov Yu.K. Information Support of the Activity for Technical Protection of Information. *Voprosy kiberbezopasnosti* = Cybersecurity issues. 2021;(1):69-79. (In Russ., abstract in Eng.) https://doi.org/10.21681/2311-3456-2021-1-69-79

[23] Kislyak A.A., et al. A variant of application of system engineering in the synthesis of the information security system. *News of the Tula state university. Technical sciences.* 2023;(2):71-76. (In Russ., abstract in Eng.) https://doi.org/10.24412/2071-6168-2023-2-71-77

[24] Zegzhda P.D., Anisimov V.G., Anisimov E.G., Saurenko T.N. Optimal Integration Model of Information Security Measures. *Problems of Information Security. Computer Systems*. 2020;(2):9-15. (In Russ., abstract in Eng.) EDN: PPYPYM

[25] Belov A.S., Dobryshin M.M., Shugurov D.E. Specification of Elements Qualitology Used at the Quality Estimation Systems of Support of Information Security. *Instruments and Systems: Monitoring, Control, and Diagnostics.* 2022;(11);34-40. (In Russ., abstract in Eng.) https://doi.org/10.25791/pribor.11.2022.1373

Submitted 10.04.2024; approved after reviewing 21.06.2024; accepted for publication 29.08.2024.

About the authors:

Dmitry A. Abramov, Associate Professor of the Chair of Information Security, Tula State University (92 Prospekt Lenina, Tula 300012, Russian Federation), Cand. Sci. (Eng.), **ORCID: https://orcid.org/0000-0003-2813-1179,** sipai-dima@mail.ru

Vyacheslav L. Tokarev, Associate Professor of the Chair of Information Security, Tula State University (92 Prospekt Lenina, Tula 300012, Russian Federation), Dr. Sci. (Eng.), Professor, **ORCID: https://orcid.org/0000-0002-9827-5250,** tokarev22@yandex.ru

All authors have read and approved the final manuscript.