УДК 004.056.53
doi:10.31799/1684-8853-2024-1-44-55
EDN: MVWIFR

Научные статьи
Articles

Методика повышения защищенности сети передачи данных объектов критической информационной инфраструктуры при многоэтапных атаках

В. А. Липатников[a], *доктор техн. наук, профессор, старший научный сотрудник, orcid.org/0000-0002-3736-4743, lipatnikovanl@mail.ru*
А. А. Шевченко[a], *канд. техн. наук, старший научный сотрудник, orcid.org/0000-0001-9113-1089*
К. В. Мелехов[a], *адъюнкт, orcid.org/0009-0007-3474-412X*
Д. Ф. Ткачев[a], *канд. техн. наук, начальник отдела, orcid.org/0009-0004-2256-9270*
[a]*Военная академия связи им. Маршала Советского Союза С. М. Буденного, Тихорецкий пр., 3, Санкт-Петербург, 194064, РФ*

Введение: *стремительное развитие информационных технологий приводит к появлению новых угроз и уязвимостей в информационных системах в различных областях жизни общества, эксплуатация которых увеличивает вероятность успешной атаки злоумышленника. В связи с этим возникает необходимость исследовать методы повышения защищенности сетей передачи данных в условиях многоэтапных атак.* ***Цель:*** *повысить защищенность сети передачи данных путем проактивного управления безопасностью при многоэтапных атаках.* ***Результат:*** *разработана методика повышения защищенности сетей передачи данных при многоэтапных атаках на основе проактивного управления безопасностью. Методика включает в себя превентивный анализ динамики нарушителей, выявление несоответствий политики безопасности, определение параметров аномалий сетевого трафика, классификацию типов атак и определение геолокации нарушителей. Процесс обеспечения безопасности сети передачи данных был формализован с использованием математического аппарата теории марковских процессов с дискретными состояниями и непрерывным временем, что позволило получить зависимости вероятности обеспечения безопасности сети передачи данных от времени протекания различных подпроцессов системы информационной безопасности в наглядном графическом виде. Результаты моделирования показали, что предложенная методика позволяет повысить вероятность обеспечения безопасности сети передачи данных в течение заданного времени и, следовательно, создает условия для своевременного предоставления конечным пользователям услуг по обеспечению качества сети передачи данных.* ***Практическая значимость:*** *методика является математической основой системы информационной безопасности, учитывающей параметры процессов воздействия и защиты для принятия эффективных мер по парированию многоэтапных атак с использованием машинного обучения. Результаты исследования могут быть применимы при разработке или устранении неисправностей в системах информационной безопасности сетей передачи данных объектов критической информационной инфраструктуры.*

Ключевые слова *— проактивное управление, сеть передачи данных, многоэтапная атака, объект критической информационной инфраструктуры, метод машинного обучения, геолокация, информационная безопасность, аномалии, сетевой трафик.*

Для цитирования: Липатников В. А., Шевченко А. А., Мелехов К. В., Ткачев Д. Ф. Методика повышения защищенности сети передачи данных объектов критической информационной инфраструктуры при многоэтапных атаках. *Информационно-управляющие системы*, 2024, № 1, с. 44–55. doi:10.31799/1684-8853-2024-1-44-55, EDN: MVWIFR
For citation: Lipatnikov V. A., Shevchenko A. A., Melekhov K. V., Tkachev D. F. Methodology for improving the security of the data transmission network of critical information infrastructure objects under multi-stage attacks. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 1, pp. 44–55 (In Russian). doi:10.31799/1684-8853-2024-1-44-55, EDN: MVWIFR

Введение

В современных условиях геополитической нестабильности обеспечение безопасности объектов критической информационной инфраструктуры (КИИ), а именно информационных систем и в частности сетей передачи данных (СПД; Data Transmission Network — DTN), является актуальным направлением [1], которое включает в себя развитие методик повышения защищенности СПД от многоэтапных атак (МЭА; Multi-Stage Attack — MSA). Развитие IT-технологий и постоянный рост количества пользователей и аппаратных мощностей информационных систем приводит к неконтролируемому появлению новых уязвимостей в них, которые позволяют нарушителю получать доступ к СПД КИИ, сканировать ресурсы сети, повышать права доступа в атакуемом сегменте сети, внедрять скрипты, удаленно подключаться к оборудованию СПД и выключать его, искать конфиденциальную информацию, блокировать учетные записи пользователей [2, 3].

Воздействие МЭА приводит к повышению в СПД нелегитимной активности [4], которая влечет за собой изменение в пропускной способности телекоммуникационного оборудования (ТКО) СПД, задержки в каналах связи и потери кадров при передаче информации по СПД. Одновременно с этим при организации непрерывного и опера-

тивного контроля и обнаружения аномалий в трафике СПД появляются проблемы, связанные со сложной маршрутизацией потоков информации в СПД объектов КИИ. С другой стороны, СПД в данных условиях должна функционировать без сбоев и предоставлять качественные услуги конечным пользователям. Выявленные противоречия дают толчок для развития научно-методического аппарата обнаружения и прогнозирования МЭА, основанного на современных интеллектуальных технологиях, к числу которых можно отнести машинное обучение и анализ.

В работах [5–7] представлены способы, в которых делается акцент на управление информационной безопасностью (ИБ) инфраструктуры на основе выявления уязвимостей в процессе функционирования. В данных источниках управление ИБ является реактивным, так как не подразумевается прогнозирование развития атаки на сеть. Это позволяет сделать вывод, что вновь разрабатываемые способы и методики управления ИБ должны быть направлены на анализ не только динамики действий нарушителя, но и содержания блоков данных протоколов по этапам атаки. Наряду с этим одним из требований к управлению ИБ СПД является реализация способов контроля защищенности в режиме времени, близком к реальному. Отсюда вытекает противоречие между интенсивно развивающимися способами воздействия на СПД и их реализующими возможностями, с одной стороны, и применяемыми методами управления ИБ — с другой. Таким образом, необходимость оценки защищенности СПД объектов КИИ оказывается актуальной.

Целью данного исследования является повышение вероятности защищенности СПД в течение заданного времени на основе методики проактивного управления безопасностью при реализации противником МЭА. Проактивный характер управления безопасностью заключается в принятии решения по защите от МЭА на основе данных прогноза, действий нарушителя с учетом модели МЭА.

Задачей исследования является разработка методики повышения защищенности СПД при МЭА, основанной на прогнозировании стратегии вторжения нарушителя за счет применения интеллектуальных технологий.

Методика повышения защищенности СПД при МЭА

Структура СПД как объекта воздействия МЭА представлена на рис. 1.

Предполагаемая методика включает в себя взаимоувязанную последовательность подпроцессов, а именно содержит действия:

— превентивного анализа динамики действий нарушителя;

— обнаружения несоответствий политики безопасности;

— определения параметров аномалий сетевого трафика;

— классификации видов атак и получения полной информации;

— установления геолокации нарушителя [8, 9].

Методика управления защищенностью СПД при МЭА представлена в виде алгоритма (рис. 2). Алгоритм процесса функционирования системы информационной безопасности (СИБ; Information System Security — ISS) СПД при МЭА описывает полную последовательность подпроцессов управления СИБ СПД за один цикл.

В соответствии с отраслевыми нормативными документами прежде чем СИБ начнет функционировать в штатном режиме, СПД и СИБ вводят в эксплуатацию, что и было учтено в предлагаемом алгоритме.

Управление СИБ начинается с формирования исходных данных, а именно вырабатываются модели функционально-логической архитектуры СПД и используемых в СПД сетевых протоколов. Также весь входящий трафик представляется в виде модели цифрового потока.

Модель цифрового потока (N)-соединения ((N)-ЦПС) СПД есть определенная на периоде существования соединения алгебраическая система

$$A = <S, \{\oplus\}, \{R\}>, \quad (1)$$

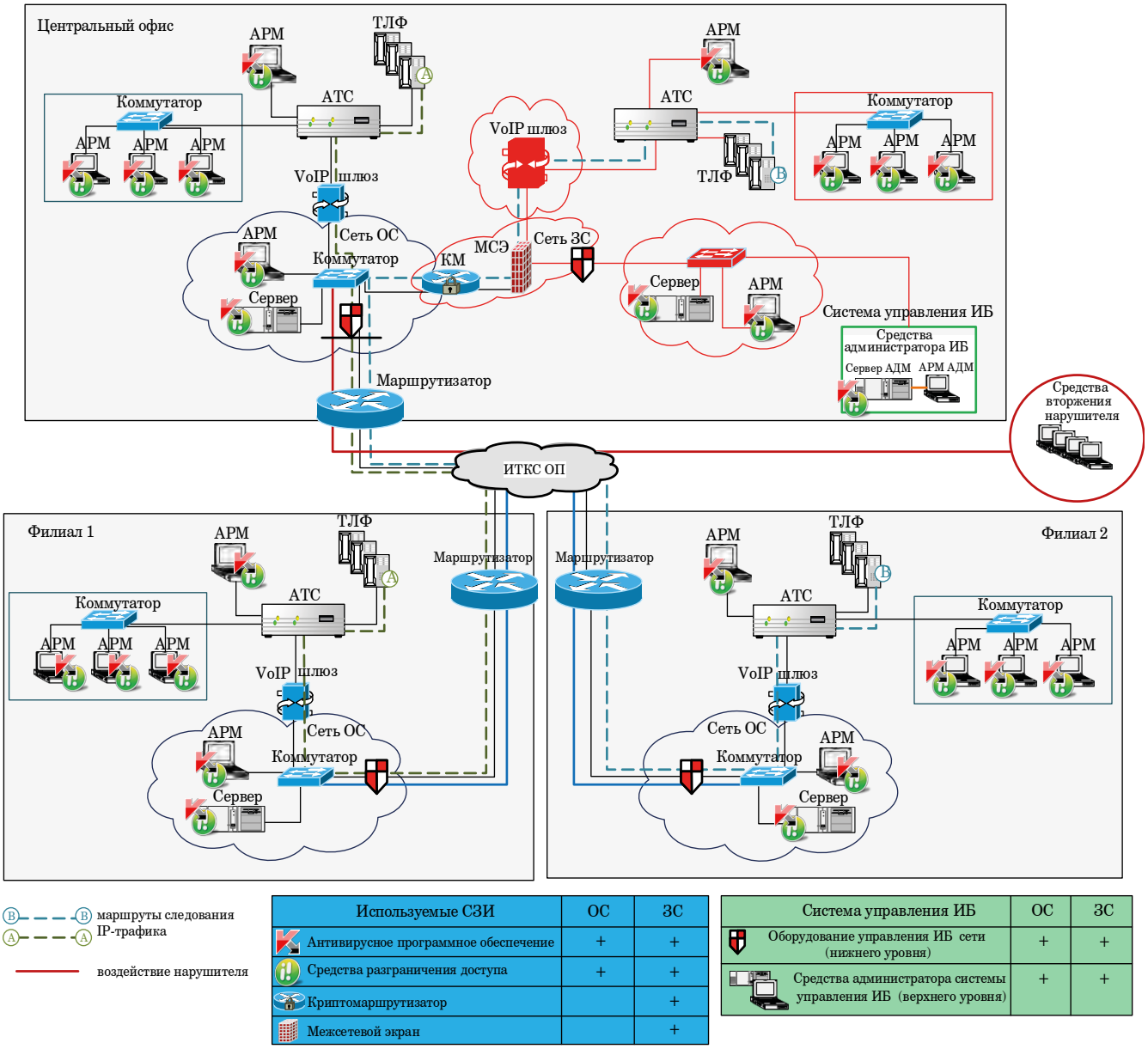
где S — множество структурных элементов (N)-ЦПС; $\oplus$ — операция конкатенации на множестве структурных элементов; R — бинарное отношение на множестве структурных элементов в (N)-ЦПС.

Модель в виде структуры (N)-ЦПС СПД, описываемого алгеброй вида (1), есть отношение строгого порядка, определенное на множестве структурных элементов и существующее на интервале, равном длительности существования соединения, т. е.

$$R = \{\forall(s_i, s_j, s_k) \in S, s_i R s_j \neq s_j R s_i, i \leq j;$$
$$s_i R s_j \wedge s_j R s_k \rightarrow s_i R s_k, i < j < k\}, \quad (2)$$

где s_i, s_j, s_k — структурные элементы (N)-ЦПС канального уровня.

В устройстве поиска информации [10, 11] на основе модели (цифрового потока) обеспечивается более высокая вероятность правильного распознавания информационного цифрового потока.



Используемые СЗИ	ОС	ЗС
Антивирусное программное обеспечение	+	+
Средства разграничения доступа	+	+
Криптомаршрутизатор		+
Межсетевой экран		+

Система управления ИБ	ОС	ЗС
Оборудование управления ИБ сети (нижнего уровня)	+	+
Средства администратора системы управления ИБ (верхнего уровня)	+	+

■ ***Рис. 1.*** Структура СПД как объекта воздействия МЭА: *АРМ* — автоматизированное рабочее место; *ТЛФ* — телефон; *АТС* — автоматическая телефонная станция; сеть *ОС* — сеть открытого сегмента; сеть *ЗС* — сеть закрытого сегмента; *КМ* — криптомаршрутизатор; *МСЭ* — межсетевой экран; *АДМ* — администратор; *ИТКС ОП* — информационно-телекоммуникационная сеть общего пользования; *СЗИ* — средства защиты информации

■ ***Fig. 1.*** Structure of DTN as an object of MSA impact: *АРМ* — automated workstation; *ТЛФ* — telephone; *АТС* — automatic telephone exchange; сеть *ОС* — open segment network; сеть *ЗС* — closed segment network; *КМ* — crypto router; *МСЭ* — firewall; *АДМ* — administrator; *ИТКС ОП* — public information and telecommunications network; *СЗИ* — information security tools

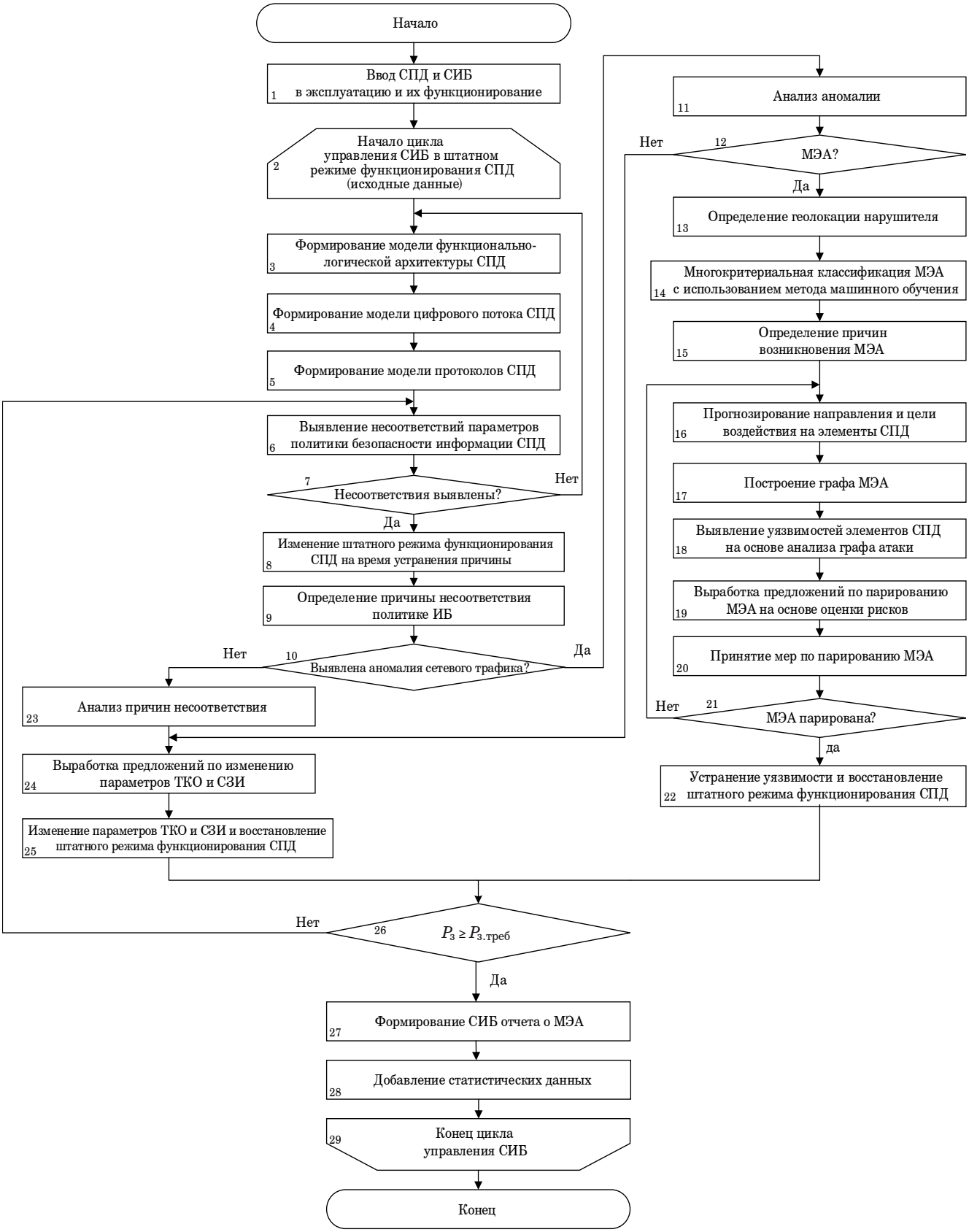
Далее в автоматическом режиме выявляются несоответствия параметров политики безопасности. В случае если несоответствия выявлены, то изменяется штатное функционирование СПД на время определения и устранения выявленных угроз. В результате установления причин несоответствия политики безопасности может быть определено, что триггером является аномалия сетевого трафика, которую необходимо подвергнуть анализу. Если выявится факт МЭА, то необходимо выполнить следующие действия:

— установить геолокацию нарушителя [12, 13];

— провести классификацию воздействия (данный процесс возможно реализовать методом машинного обучения);

— спрогнозировать тактику нарушителя и цель воздействия;

— на основе прогноза построить граф атаки;



■ ***Рис. 2.*** Алгоритм функционирования СИБ СПД при МЭА
■ ***Fig. 2.*** Algorithm of functioning of the ISS of DTN under the MSA

— определить уязвимости СПД, через которую нарушитель реализует МЭА [14, 15];

— с учетом оценки рисков выработать конкретные предложения по парированию МЭА и реализовать их.

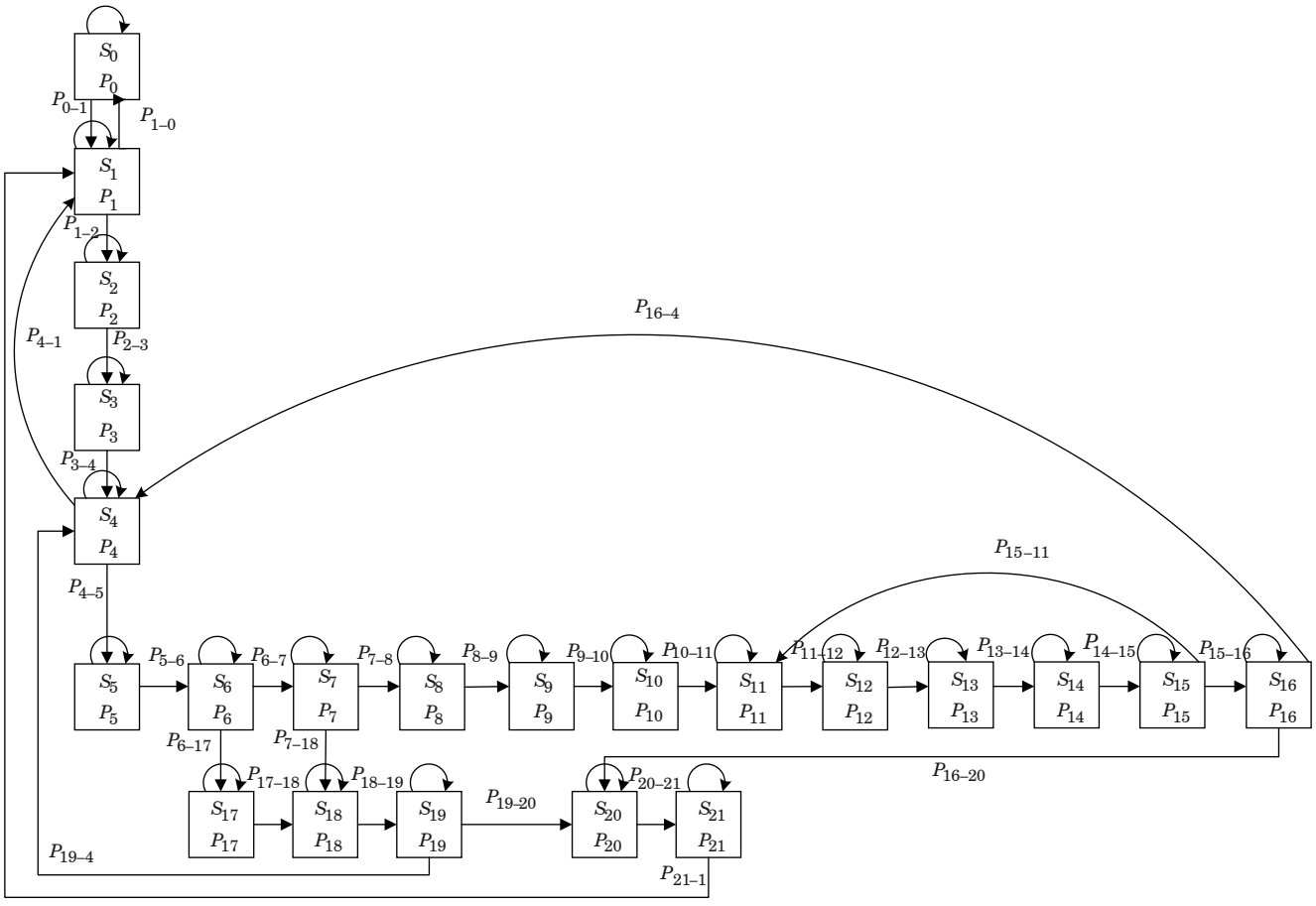
Вышеописанные процессы могут быть реализованы в автоматическом или ручном режиме и позволят восстановить штатный режим функционирования СПД.

Если же аномалия сетевого трафика не является причиной несоответствия, то проводится сравнение параметров настройки ТКО и СЗИ с правилами, установленными политикой безопасности. Далее установленные нарушения правил настройки ТКО и СЗИ устраняются в соответствии с выработанными предложениями [16, 17], после чего СПД продолжает свое функционирование в штатном режиме.

Цикл управления СИБ заканчивается тем, что проверяется уровень защищенности СПД после устранения несоответствий политике безопасности. Если уровень защищенности ниже требуемого, то необходимо повторно провести выявление несоответствий с последующим выполнением вышеописанных процессов, иначе формируется отчет о выявленном инциденте ИБ.

Для более детального исследования процесса функционирования СИБ СПД объекта КИИ при реализации МЭА данный процесс формализован в виде математической модели [18–21]. Модель представляет собой граф состояний СИБ, при этом переход одного стационарного состояния в другое происходит в произвольный момент времени и зависит только от параметров системы в данный конкретный момент времени [22, 23]. В результате строится граф состояний процесса функционирования СИБ СПД объекта КИИ при МЭА (рис. 3, табл. 1).

Показатель защищенности СПД зависит от сложившейся обстановки в информационном пространстве. Рассмотрим ситуацию, при которой осуществляется МЭА. В данном случае показатель защищенности определяется как вероятность нахождения СИБ в состоянии (S_{16}) устранения уязвимости и восстановления штатного режима функционирования СПД после парирования МЭА ($P_з$) [24, 25]. Вероятность $P_з$ принята за вероятность защищенности, если считать, что



■ ***Рис. 3.*** Граф состояний процесса функционирования СИБ СПД при МЭА

■ ***Fig. 3.*** Graph of the states of the process of functioning of the DTN ISS under MSA

■ ***Таблица 1.*** Процессы функционирования СИБ СПД при МЭА
■ ***Table 1.*** Processes of functioning of the DTN ISS under the MSA

Событие	Описание
S_0	Исходное состояние СИБ СПД
S_1	Формирование модели функционально-логической архитектуры СПД
S_2	Формирование модели протоколов СПД
S_3	Формирование модели цифрового потока СПД
S_4	Выявление несоответствий параметров политике безопасности информации СПД
S_5	Изменение штатного режима функционирования СПД на время устранения причины
S_6	Определение причины несоответствия политике безопасности
S_7	Анализ аномалии
S_8	Определение геолокации нарушителя
S_9	Многокритериальная классификация МЭА с использованием метода машинного обучения
S_{10}	Определение причин возникновения МЭА
S_{11}	Прогнозирование направления и цели воздействия на элементы СПД
S_{12}	Построение графа атаки
S_{13}	Выявление уязвимостей элементов СПД на основе анализа графа атаки
S_{14}	Выработка предложений по парированию МЭА на основе оценки рисков
S_{15}	Принятие мер по парированию МЭА
S_{16}	Устранение уязвимости и восстановление штатного режима функционирования СПД
S_{17}	Анализ причин несоответствия
S_{18}	Выработка предложений по изменению параметров ТКО и СЗИ
S_{19}	Изменение параметров ТКО и СЗИ и сохранение в журнал событий
S_{20}	Формирование СИБ отчета о МЭА
S_{21}	Добавление статистических данных

после парирования МЭА сразу же приступает к формированию отчета. Таким образом, вероятность защищенного состояния СПД примет вид

$$P_з = \frac{\lambda_0}{\mu_0}\left(\frac{\beta_1\beta_2\beta_3\lambda_{1-2}(\beta_2+\varphi)(\beta_3+\psi)((\beta_1+\eta)(\rho+\omega)-\beta_1\omega)+\beta_1^2\beta_2\beta_3\omega\lambda_{1-2}(\varphi(\beta_3+\psi)+\beta_2\psi)}{((\beta_1+\eta)(\beta_2+\varphi)(\beta_3+\psi)(\rho+\omega)-\beta_1\beta_2\beta_3\omega)((\beta_1+\eta)(\beta_2+\varphi)(\beta_3+\psi)(\rho+\omega)-\beta_1\omega)}\right)P_0.$$

Здесь

$$P_0 = \frac{1}{1+\frac{\lambda_0}{\mu_0}+\frac{\lambda_0\lambda_{1-2}}{\mu_0\lambda_{2-3}}+\frac{\lambda_0\lambda_{1-2}}{\mu_0\lambda_{3-4}}+C\left(+D\left(\begin{array}{c}1+\frac{\beta_1}{\lambda_{5-6}}+\frac{\beta_1}{\beta_2+\varphi}+\frac{\beta_1\beta_2}{(\beta_2+\varphi)(\beta_3+\psi)}+\\ \frac{1}{\lambda_{8-9}}+\frac{1}{\lambda_{9-10}}+\frac{1}{\lambda_{10-11}}+\\ +\left(\frac{1}{\lambda_{11-12}}+\frac{1}{\lambda_{12-13}}+\frac{1}{\lambda_{13-14}}+\frac{1}{\lambda_{14-15}}\right)\left(1+\frac{\alpha}{\varepsilon}\right)+\frac{1}{\varepsilon}\\ +\frac{\beta_1\varphi}{\lambda_{17-18}(\beta_2+\varphi)}+\frac{\beta_1(\beta_3+\psi)\varphi+\beta_1\beta_2\psi}{\lambda_{18-19}(\beta_2+\varphi)(\beta_3+\psi)}\end{array}\right)+\right)+}$$

$$+A+B+(A+B)\left(\frac{\rho}{\lambda_{20-21}}+\frac{\rho}{\mu_0}\right),$$

где

$$A = \frac{\lambda_0}{\mu_0}\frac{\begin{array}{c}\beta_1\beta_2\beta_3\lambda_{1-2}\times\\ \times(\beta_2+\varphi)(\beta_3+\psi)((\beta_1+\eta)(\rho+\omega)-\beta_1\omega)+\\ +\beta_1^2\beta_2\beta_3\omega\lambda_{1-2}(\varphi(\beta_3+\psi)+\beta_2\psi)\end{array}}{((\beta_1+\eta)(\beta_2+\varphi)(\beta_3+\psi)(\rho+\omega)-\beta_1\beta_2\beta_3\omega)\times};$$
$$\times((\beta_1+\eta)(\beta_2+\varphi)(\beta_3+\psi)(\rho+\omega)-\beta_1\omega)$$

$$B = \frac{\lambda_0}{\mu_0}\frac{\lambda_{1-2}\beta_1\left(\varphi(\beta_3+\psi)+\beta_2\psi\right)}{(\beta_1+\eta)(\beta_2+\varphi)(\beta_3+\psi)(\rho+\omega)-\beta_1\omega};$$

$$C = \frac{\lambda_0}{\mu_0}\frac{\lambda_{1-2}}{\beta_1+\eta}+\frac{\omega}{\beta_1+\eta}\left(A+B\right);$$

$$D = \frac{\beta_1\beta_2\beta_3}{(\beta_2+\varphi)(\beta_3+\psi)}.$$

Верификация с помощью программного обеспечения

Для оптимизации расчета процессов функционирования СИБ СПД при МЭА разработано программное обеспечение (ПО) на языке Python (рис. 4), позволяющее в наглядной форме получить вывод необходимых зависимостей.

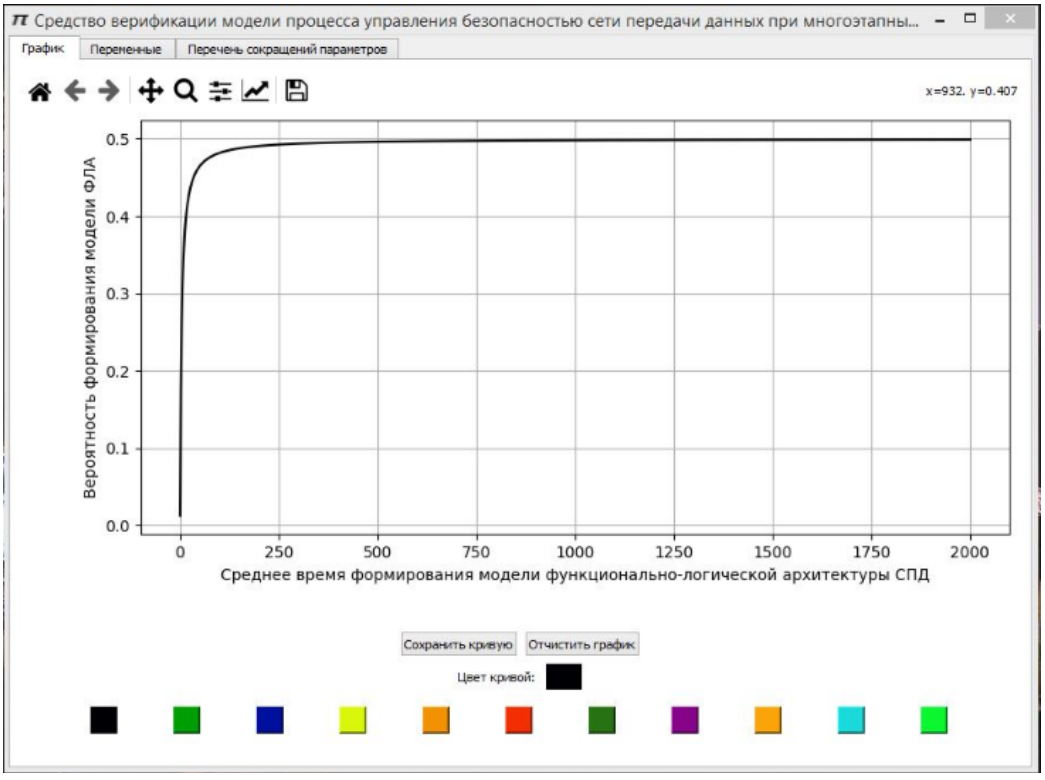
В разработанное ПО [26] были введены исходные данные из табл. 2 [27–30], являющиеся экспертными оценками. Программный продукт в автоматическом режиме построил зависимости вероятности защищенности СПД от различного времени определения причин несоответствия политике безопасности (от 0,005 до 0,05 мин) (рис. 5, *а*) и различного времени принятия мер по парированию МЭА (от 0,09 до 0,27 мин) (рис. 5, *б*).

Из рис. 5 следует, что увеличение времени определения геолокации нарушителя СИБ СПД при МЭА понижает защищенность $P_з$ ниже требуемого уровня 0,9. В связи с этим возможно определить требования к времени определения геолокации нарушителя в различных условиях функционирования СИБ СПД, например:

1) время определения геолокации нарушителя ≤ 0,495 мин при времени определения причины несоответствия политике безопасности за 0,05 мин;

2) время определения геолокации нарушителя ≤ 0,67 мин при времени принятия мер по парированию МЭА за 0,009 мин.

При количественных оценках для подтверждения новых предложений полученные результаты аналитического моделирования показали, что предложенный подход в сравнении с [31, 32] обеспечивает требуемый уровень достоверности



■ ***Рис. 4.*** Интерфейс ПО для оперативного расчета вероятностей защищенности СПД

■ ***Fig. 4.*** The software interface for quick calculation of DTN security probabilities

■ ***Таблица 2.*** Исходные данные для расчета оценки вероятности защищенности СПД при МЭА
■ ***Table 2.*** Input data for calculating the probability of protection of the DTN during the MSA

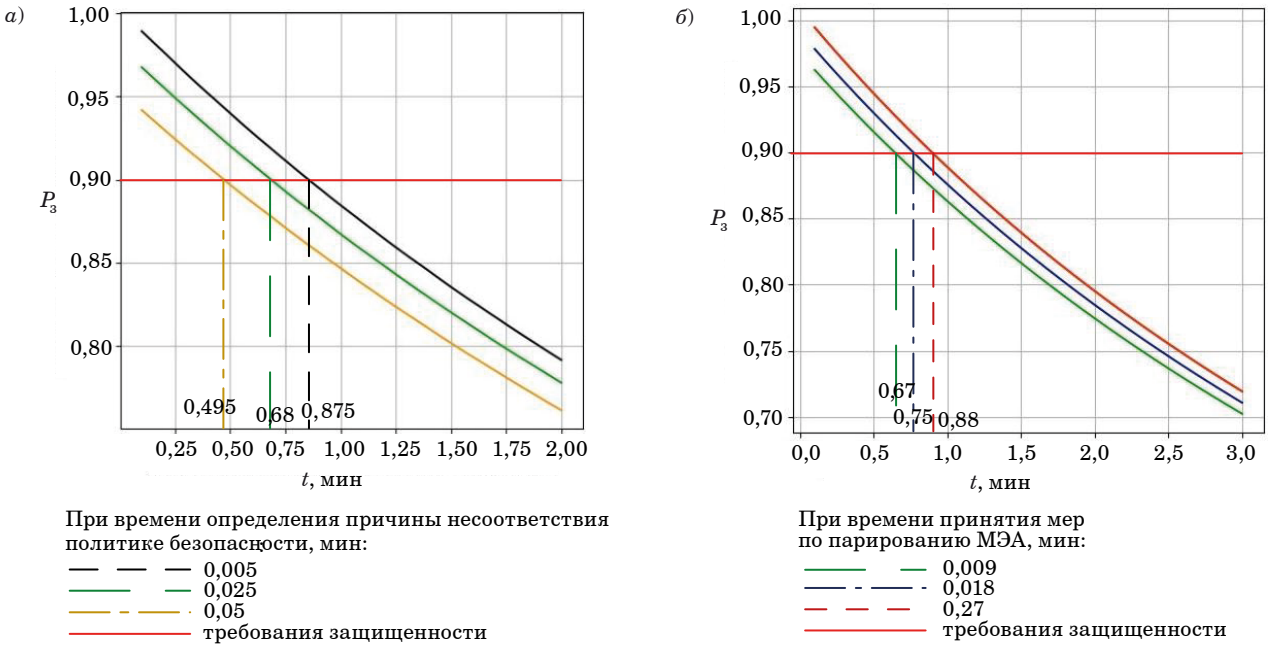
Событие	Описание	Значение, мин
S_0	Исходное состояние СИБ СПД	0,0055
S_1	Формирование модели функционально-логической архитектуры СПД	0,003
S_2	Формирование модели цифрового потока СПД	0,003
S_3	Формирование модели протоколов СПД	0,003
S_4	Выявление несоответствий параметров политике безопасности СПД	0,1
		0,001
S_5	Изменение штатного режима функционирования СПД на время устранения причины	0,052
S_6	Определение причины несоответствия политике безопасности	1
		0,005 0,025 0,05
S_7	Анализ аномалии	0,005
		3
S_8	Определение геолокации нарушителя	Переменная
S_9	Многокритериальная классификация МЭА с использованием метода машинного обучения	0,001
S_{10}	Определение причин возникновения МЭА	0,008
S_{11}	Прогнозирование направления и цели воздействия на элементы СПД	0,055
S_{12}	Построение графа атаки	0,051
S_{13}	Выявление уязвимостей элементов СПД на основе анализа графа атаки	0,051
S_{14}	Выработка предложений по парированию МЭА на основе оценки рисков	0,005
S_{15}	Принятие мер по парированию МЭА	0,09 0,18 0,27
		0,4
S_{16}	Устранение уязвимости и восстановление штатного режима функционирования	8
		8
S_{17}	Анализ причин несоответствия	0,5
S_{18}	Выработка предложений по изменению параметров ТКО и СЗИ	0,005
S_{19}	Изменение параметров ТКО и СЗИ и сохранение в журнал событий	8
		8
S_{20}	Формирование СИБ отчета о МЭА	0,5
S_{21}	Добавление статистических данных	0,005

принимаемых решений. Применение методики позволяет поднять значение вероятности защищенности СПД при МЭА выше 0,9.

Определено, что при использовании результатов моделирования можно реализовать способы повышения защищенности СПД от МЭА. Разработанный алгоритм может быть использован в уже существующих системах ИБ, поскольку он представляет собой инструмент выявления и прогнозирования МЭА. Проведены экспериментальная и теоретическая оценка эффективности предложений, а также сравнение с существующими методиками.

Заключение

Методика включает превентивный анализ динамики действий нарушителя, обнаружение несоответствий политике безопасности, опре-



■ ***Рис. 5.*** Зависимость вероятности защищенности от времени определения геолокации нарушителя при различном времени определения причин несоответствия политике безопасности (*а*) и принятия мер по парированию МЭА (*б*)

■ ***Fig. 5.*** The dependence of the probability of security on the time of determining the geolocation of the intruder at various times of taking measures of non-compliance with the information security policy (*а*) and parry the MSA (*б*)

деление параметров аномалий сетевого трафика, классификацию видов атак и определение геолокации нарушителя. Представлен алгоритм управления ИБ СПД КИИ при стохастической неопределенности.

Процесс обеспечения защищенности СПД был формализован с помощью математического аппарата теории марковских процессов с дискретными состояниями и непрерывным временем, что позволило получить зависимости вероятности защищенности СПД от времени различных подпроцессов СИБ в наглядном графическом виде. Результаты моделирования показали, что предложенная методика обеспечивает повышение вероятности защищенности СПД в течение заданного времени и как следствие дает условия для своевременного предоставления СПД качественных услуг конечным пользователям. Также результаты демонстрируют обоснованность временных параметров СИБ, максимизирующих время защищенности СПД при МЭА.

Дальнейшие исследования будут направлены на автоматизацию предлагаемой методики и ее синтез с другими известными способами защиты СПД, а также на интеллектуализацию процессов раннего обнаружения и анализа действий нарушителя в сети.

Литература

1. **Зеличенок И. Ю., Котенко И. В.** Выявление многошаговых атак при помощи рекуррентных нейронных сетей с применением слоев LSTM. *Региональная информатика (РИ-2022): материалы юбилейной XVIII Санкт-Петербургской междунар. конф.*, Санкт-Петербург, 26–28 октября 2022 г. СПб., 2022, с. 157–158.
2. **Зеличенок И. Ю., Котенко И. В.** Методы выявления многошаговых атак на компьютерные сети с помощью машинного обучения. *Региональная информатика (РИ-2022): материалы юбилейной XVIII Санкт-Петербургской междунар. конф.*, Санкт-Петербург, 26–28 октября 2022 г. СПб., 2022, с. 159–160.
3. **Котенко Д. И., Котенко И. В., Саенко И. Б.** Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы. *Труды СПИИРАН*, 2012, № 3(22), с. 5–30.
4. **Климов С. М.** *Методы и модели противодействия компьютерным атакам*. Люберцы, КАТАЛИТ, 2008. 316 с.
5. **Липатников В. А., Шевченко А. А., Косолапов В. С., Сокол Д. С.** Метод обеспечения информационной безопасности сети VoIP-телефонии с прогнозом стратегии вторжений нарушителя. *Информационно-управляющие системы*, 2022, № 1, с. 54–67. doi:10.31799/1684-8853-2022-1-54-67
6. **Visoottiviseth V., Sakarin P., Thongwilai J., Choobanjong T.** Signature-based and behavior-based

attack detection with machine learning for home IoT devices. *2020 IEEE Region 10 Conference (TENCON)*, Osaka, Japan, 2020, 16–19 November. IEEE, 2020, pp. 829–834. doi:10.1109/TENCON50793.2020.9293811

7. **Зегжда Д. П., Васильев Ю. С., Полтавцева М. А., Кефели И. Ф., Боровков А. И.** Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации. *Вопросы кибербезопасности*, 2018, № 2 (26), с. 2–15. doi:10.21681/2311-3456-2018-2-2-15, EDN: UYNEXS
8. **Williams J.** *Identification of IP Address using Fraudulent Geolocation Data*. Imperial College London, 15 June 2020. https://www.imperial.ac.uk/media/imperial-college/faculty-of-engineering/computing/public/1920-ug-projects/Williams,-James-(jw1317).pdf (дата обращения: 28.01.2023).
9. **Wang Z., Li H., Li Q., Li W., Zhu H., Sun L.** Towards IP geolocation with intermediate routers based on topology discovery. *Cybersecurity*, 2019, vol. 2, iss. 1. https://doi.org/10.1186/s42400-019-0030-2
10. Пат. RU 2100839 C1 РФ, МПК G06F 17/30. *Устройство поиска информации*, В. А. Липатников (РФ), А. М. Плотников (РФ), В. В. Якимовец (РФ). № 95108104/09; заявл. 18.05.1995; опубл. 27.12.1997, 11 с.
11. Пат. RU 2199148 C1 РФ, МПК G06F 17/30. *Устройство поиска информации*, В. А. Липатников (РФ), В. В. Якимовец (РФ), Д. Л. Хлыбов (РФ). № 2001120395/09; заявл. 20.07.2001; опубл. 20.02.2003, 18 с.
12. **Липатников В. А., Мелехов К. В., Задбоев В. А.** Способ определения локации злоумышленника в сети передачи данных сетевой инфраструктуры. *Транспорт России: проблемы и перспективы: материалы Междунар. науч.-практ. конф.*, Санкт-Петербург, 9–10 ноября 2022 г. СПб., 2022, с. 215–220. EDN: KDDQDW
13. **Taylor J., Devlin J., Curran K.** Bringing location to IP addresses with IP geolocation. *The Journal of Emerging Technologies in Web Intelligence*, 2012, vol. 4, no. 3, pp. 273–277.
14. **Коршунов Г. И., Липатников В. А., Шевченко А. А., Малышев Б. Ю.** Метод адаптивного управления защитой информационно-вычислительных сетей на основе анализа динамики действий нарушителя. *Информационно-управляющие системы*, 2018, № 4, с. 61–72. doi:10.31799/1684-8853-2018-4-61-72
15. **Ageev S., Kotenko I., Saenko I., Kopchak Y.** Abnormal traffic detection in networks of the Internet of things based on fuzzy logical inference. *Proc. of the 18th Intern. Conf. on Soft Computing and Measurements, SCM 2015*, Saint-Petersburg, 2015, 19–21 May. Saint-Petersburg, 2015, pp. 5–8. doi:10.1109/SCM.2015.7190394, EDN: WRWUMV
16. **Липатников В. А., Шевченко А. А., Яцкин А. Д., Семенова Е. Г.** Управление информационной безопасностью организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией. *Информационно-управляющие системы*, 2017, № 4, с. 67–76. doi:10.15217/issn1684-8853.2017.4.67
17. **Brezigar-Masten A., Masten I.** CART-based selection of bankruptcy predictors for the logit model. *Expert Systems with Applications*, 2012, vol. 39, no. 11, pp. 10153– 10159.
18. **Ju X., Chen V. C. P., Rosenberger J. M., Liu F.** Fast knot optimization for multivariate adaptive regression splines using hill climbing methods. *Expert Systems with Applications*, 2021, no. 171, p. 114565. doi:10.1016/j.eswa.2021.114565
19. **Clincy V., Shahriar H.** Web application firewall: Network security models and configuration. *2018 IEEE 42nd Annual Computer Software and Applications Conf. (COMPSAC)*, Tokyo, Japan, 2018, 23–27 July. IEEE, 2018, pp. 835–836. doi:10.1109/COMPSAC.2018.00144
20. **Шевченко А. А.** Математическая модель информационного противоборства двух систем в информационно-телекоммуникационном пространстве. *Инновационная деятельность в Вооруженных Силах Российской Федерации: труды всеармейской научно-практической конференции*, Санкт-Петербург, 14–15 октября 2020 г. СПб., 2020, с. 237–241. EDN: WZBIFU
21. **Ju X., Rosenberger J. M., Chen V. C. P., Liu F.** Global optimization on non-convex two-way interaction truncated linear multivariate adaptive regression splines using mixed integer quadratic programming. *Information Sciences*, 2022, no. 597, pp. 38–52.
22. **Ju X., Liu F., Wang Li., Lee W.-J.** Wind farm layout optimization based on support vector regression guided genetic algorithm with consideration of participation among landowners. *Energy Conversion and Management*, 2019, no. 196, pp. 1267–1281. doi:10.1016/j.enconman.2019.06.082
23. **Шевченко А. А.** Модель процесса защиты информационно-телекоммуникационной сети от несанкционированного воздействия. *Инновационная деятельность в Вооруженных Силах Российской Федерации*: *труды всеармейской научно-практической конференции*, Санкт-Петербург, 10–11 октября 2019 г. СПб., 2019, с. 166–173. EDN: NBCDWB
24. **Смирнова Е. В., Абачараева Э. Р.** Современные угрозы вирусных атак на компьютерные сети и критерии их оценивания. *Технологии инженерных и информационных систем*, 2020, № 3, с. 3–12. EDN: JQNNAV
25. **Pratap U., Canudas-de-Wit C., Garin F.** Average state estimation in presence of outliers. *2020 59th IEEE Conf. on Decision and Control (CDC)*, Jeju, Korea (South), 2020, 14–18 December. IEEE, 2020, pp. 6058–6063. doi:10.1109/CDC42340.2020.9303809
26. **Amma N. G. B., Selvakumar S., Velusamy R. L.** A statistical approach for detection of denial of service attacks in computer networks. *IEEE Transactions on*

Network and Service Management, 2020, vol. 17, no. 4, pp. 2511–2522. doi:10.1109/TNSM.2020.3022799

27. **Куликов А. Л., Бездушный Д. И., Шарыгин М. В., Осокин В. Ю.** Анализ применения метода опорных векторов в многомерной релейной защите. *Известия Российской академии наук. Энергетика*, 2020, № 2, с. 123–132. doi:10.31857/S0002331020020065, EDN: PVUKFW
28. Свидетельство о государственной регистрации программы для ЭВМ № 2023664605 Российская Федерация. *Средство верификации модели процесса управления безопасностью сети передачи данных при многоэтапных атаках*: № 2023663624: заявлено 27.06.2023: опубликовано 05.07.2023 Бюл. № 7 / Мелехов К. В., Липатников В. А., Петренко М. И., Шевченко А. А., Парфиров В. А., Мелихов И. А., Мезенин М. Е.; правообладатель Мелехов К. В. — Зарегистрировано в Реестре программ для ЭВМ.
29. **Липатников В. А., Тихонов В. А.** Распознавание вторжений нарушителя при управлении кибербезопасностью инфраструктуры интегрированной организации на основе нейро-нечетких сетей и когнитивного моделирования. *Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): сб. науч. ст. VIII Междунар. науч.-техн. и науч.-метод. конф.*, Санкт-Петербург, 27–28 февраля 2019 г. СПб., 2019, т. 4, с. 659–664. EDN: AWSFFH
30. **Karataş G., Akbulut A.** Survey on access control mechanisms in cloud computing. *Journal of Cyber Security and Mobility*, 2018, vol. 7, no. 3, pp. 1–36. doi:10.13052/2245-1439.731
31. **Lopez J., Rubio J.** Access control for cyber-physical systems interconnected to the cloud. *Comput. Netw.*, 2018, vol. 134, no. C, pp. 46–54.
32. **Yin A., Zhang C.** BOFE: Anomaly detection in linear time based on feature estimation. *2018 IEEE Intern. Conf. on Data Mining Workshops (ICDMW)*, Singapore, 2018, 17–20 November. IEEE, 2018, pp. 1128–1133. doi:10.1109/ICDMW.2018.00162

UDC 004.056.53
doi:10.31799/1684-8853-2024-1-44-55
EDN: MVWIFR

Methodology for improving the security of the data transmission network of critical information infrastructure objects under multi-stage attacks

V. A. Lipatnikov[a], Dr. Sc., Tech., Professor, Senior Researcher, orcid.org/0000-0002-3736-4743, lipatnikovanl@mail.ru
A. A. Shevchenko[a], PhD, Tech, Senior Researcher, orcid.org/0000-0001-9113-1089
K. V. Melekhov[a], Post-Graduate Student, orcid.org/0009-0007-3474-412X
D. F. Tkachev[a], PhD, Tech., Head of Division, orcid.org/0009-0004-2256-9270
[a]S. M. Budenny Military Academy of Communication, 3, Tikhoretskii Pr., 190064, Saint-Petersburg, Russian Federation

Introduction: The fast-paced development of information technologies leads to the emergence of new threats and vulnerabilities in information systems across various societal areas, the exploitation of which increases the probability of a successful attack by an intruder. Consequently, it is essential to research techniques for improving the security of data networks in the face of multi-stage attacks. **Purpose:** To improve the security of the data network by proactively managing security against multi-stage attacks. **Result:** We develop a methodology for improving the security of data transmission networks under multi-stage attacks based on proactive security management. The methodology includes preventive analysis of intruder dynamics, detection of security policy inconsistencies, determination of network traffic anomaly parameters, classification of attack types and determination of intruder geolocation. The process of ensuring the security of the data network has been formalized using the mathematical apparatus of the theory of Markov processes with discrete states and continuous time, which makes it possible to obtain the dependencies of the probability of data network security on the time of various sub-processes of the information security system in a clear graphical form. The results of modeling show that the proposed methodology provides an increase in the probability of data transmission network security within a given time and as a consequence provides conditions for timely provision of data transmission network quality services to end users. **Practical relevance:** The methodology is a mathematical basis for the information security system, taking into account the parameters of the impact and protection processes to take effective measures to parry multi-stage attacks using machine learning. The study's findings can be applicable in developing or troubleshooting information security systems for data transmission networks of critical information infrastructure objects.

Keywords — proactive management, data network, multi-stage attack, critical information infrastructure object, machine learning method, geolocation, information security, anomalies, network traffic.

For citation: Lipatnikov V. A., Shevchenko A. A., Melekhov K. V., Tkachev D. F. Methodology for improving the security of the data transmission network of critical information infrastructure objects under multi-stage attacks. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 1, pp. 44–55 (In Russian). doi:10.31799/1684-8853-2024-1-44-55, EDN: MVWIFR

References

1. Zelichenok I. Yu., Kotenko I. V. Detection of multi-step attacks using recurrent neural networks with LSTM layers. *Materialy yubilejnoj XVIII Sankt-Peterburgskoj Mezhdunarodnoj konferencii "Regional'naya informatika (RI-2022)"* [Proc. of the Anniversary XVIII St. Petersburg Intern. Conf. "Regional informatics (RI-2022)"]. Saint-Petersburg, 2022, pp. 157–158 (In Russian).
2. Zelichenok I. Yu., Kotenko I. V. Methods for detecting multi-step attacks on computer networks by using machine learning. *Materialy yubilejnoj XVIII Sankt-Peterburgskoj Mezhdunarodnoj konferencii "Regional'naya informatika (RI-2022)"* [Proc. of the Anniversary XVIII St. Petersburg Intern. Conf. "Regional informatics (RI-2022)"]. Saint-Petersburg, 2022, pp. 159–160 (In Russian).

3. Kotenko D. I., Kotenko I. V., Saenko I. B. Methods and tools for attack modeling in large computer networks: State of the problem. *SPIIRAS Proceedings*, 2012, iss. 3(22), pp. 5–30 (In Russian).
4. Klimov S. M. *Metody i modeli protivodejstviya komp'yuternym atakam* [Methods and models for countering computer attacks]. Lyubercy, KATALIT Publ., 2008. 316 p. (In Russian).
5. Lipatnikov V. A., Shevchenko A. A., Kosolapov V. S., Sokol D. S. Method for ensuring information security of a VoIP telephony network with a forecast of an intruder's intrusion strategy. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 1, pp. 54–67 (In Russian). doi:10.31799/1684-8853-2022-1-54-67
6. Visoottiviseth V., Sakarin P., Thongwilai J. Choobanjong T. Signature-based and behavior-based attack detection with machine learning for home IoT devices. *2020 IEEE Region 10 Conf. (TENCON)*, 2020, pp. 829–834. doi:10.1109/TENCON50793.2020.9293811
7. Zegzhda D. P., Vasilev U. S., Poltavtseva M. A., Kefele I. F., Borovkov A. I. Advanced production technologies security in the era of digital transformation. *Voprosy kiberbezopasnosti*, 2018, no. 2 (26), pp. 2–15 (In Russian). doi:10.21681/2311-3456-2018-2-2-15, EDN: UYNEXS
8. Williams J. *Identification of IP Address using Fraudulent Geolocation Data*. Imperial College London, 15 June 2020. Available at: https://www.imperial.ac.uk/media/imperial-college/faculty-of-engineering/computing/public/1920-ug-projects/Williams,-James-(jw1317).pdf (accessed 28 January 2023).
9. Wang Z., Li H., Li Q., Li W., Zhu H., Sun L. Towards IP geolocation with intermediate routers based on topology discovery. *Cybersecurity*, 2019, vol. 2, iss. 1. https://doi.org/10.1186/s42400-019-0030-2
10. Lipatnikov V. A., et al. *Ustrojstvo poiska informacii* [Information retrieval device]. Patent RF, no. RU 2100839 C1, 1997.
11. Lipatnikov V. A., et al. *Ustrojstvo poiska informacii* [Information retrieval device]. Patent RF, no. RU 2199148 C1, 2003.
12. Lipatnikov V. A., Melekhov K. V., Zadboev V. A. A method of detection of an intruder's location in the data network of the network infrastructure. *Materialy Mezhdunarodnoj nauchno-prakticheskoj konferencii "Transport Rossii: problemy i perspektivy"* [Proc. of the Intern. Scientific and Practical Conf. "Transport of Russia: problems and prospects"]. Saint-Petersburg, 2022, pp. 215–220 (In Russian). EDN: KDDQDW
13. Taylor J., Devlin J., Curran K. Bringing location to IP addresses with IP geolocation. *The Journal of Emerging Technologies in Web Intelligence*, 2012, vol. 4, no. 3, pp. 273–277.
14. Korshunov G. I., Lipatnikov V. A., Shevchenko A. A., Malyshev B. Y. Adaptive management of information network protection with analysis of intruder's actions. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 4, pp. 61–72 (In Russian). doi:10.31799/1684-8853-2018-4-61-72
15. Ageev S., Kopchak Y., Kotenko I., Saenko I. Abnormal traffic detection in networks of the Internet of things based on fuzzy logical inference. *Proc. of the IEEE 18th Intern. Conf. on Soft Computing and Measurements, SCM 2015*. Saint-Petersburg, 2015, pp. 5–8. doi:10.1109/SCM.2015.7190394, EDN: WRWUMV
16. Lipatnikov V. A., Shevchenko A. A., Yatskin A. D., Semenova E. G. Information security management of integrated structure organization based on a dedicated server with container virtualization. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2017, no. 4, pp. 67–76 (In Russian). doi:10.15217/issn1684-8853.2017.4.67
17. Brezigar-Masten A., Masten I. CART-based selection of bankruptcy predictors for the logit model. *Expert Systems with Applications*, 2012, vol. 39, no. 11, pp. 10153–10159.
18. Ju X., Chen V. C. P., Rosenberger J. M., Liu F. Fast knot optimization for multivariate adaptive regression splines using hill climbing methods. *Expert Systems with Applications*, 2021, no. 171, p. 114565. doi:10.1016/j.eswa.2021.114565
19. Clincy V., Shahriar H. Web application firewall: Network security models and configuration. *2018 IEEE 42nd Annual Computer Software and Applications Conf. (COMPSAC)*. IEEE, 2018, pp. 835–836.
20. Shevchenko A. A. Mathematical model of the information confrontation between two systems in the field of info-telecommunication. *Innovacionnaya deyatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii: Trudy vsearmejskoj nauchno-prakticheskoj konferencii* [Proc. of the All-Army Scientific and Practical Conf. "Innovative activities in the Armed Forces of the Russian Federation"]. Saint-Petersburg, 2020, pp. 237–241 (In Russian). EDN: WZBIFU
21. Ju X., Rosenberger J. M., Chen V. C. P., Liu F. Global optimization on non-convex two-way interaction truncated linear multivariate adaptive regression splines using mixed integer quadratic programming. *Information Sciences*, 2022, no. 597, pp. 38–52.
22. Ju X., Liu F., Wang Li., Lee W.-J. Wind farm layout optimization based on support vector regression guided genetic algorithm with consideration of participation among landowners. *Energy Conversion and Management*, 2019, no. 196, pp. 1267–1281. doi:10.1016/j.enconman.2019.06.082
23. Shevchenko A. A. Model of the information protection process of info-telecommunication network from unauthorized influence. *Innovacionnaya deyatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii: Trudy vsearmejskoj nauchno-prakticheskoj konferencii* [Proc. of the All-Army Scientific and Practical Conf. "Innovative activities in the Armed Forces of the Russian Federation"]. Saint-Petersburg, 2019, pp. 166–173 (In Russian). EDN: NBCDWB
24. Smirnova E. V., Abacharaeva E. R. Modern threats of computer networks virus attacks and their evaluation criteria. *Technologies of Engineering and Information Systems*, 2020, no. 3, pp. 3–12 (In Russian). EDN: JQNNAV
25. Pratap U., Canudas-de-Wit C., Garin F. Average state estimation in presence of outliers. *2020 59th IEEE Conf. on Decision and Control (CDC)*. IEEE, 2020, pp. 6058–6063. doi:10.1109/CDC42340.2020.9303809
26. Amma N. G. B., Selvakumar S., Velusamy R. L. A statistical approach for detection of denial of service attacks in computer networks. *IEEE Transactions on Network and Service Management*, 2020, vol. 17, no. 4, pp. 2511–2522. doi:10.1109/TNSM.2020.3022799
27. Kulikov A. L., Bezdushniy D. I., Sharygin M. V., Osokin V. Yu. The support vector machine application analysis in multidimensional relay protection. *Proceedings of the Russian Academy of Sciences. Power Engineering*, 2020, no. 2, pp. 123–132 (In Russian). doi:10.31857/S0002331020020065, EDN: PVUKFW
28. Melekhov K. V., et al. *Sredstvo verifikacii modeli processa upravleniya bezopasnost'yu seti peredachi dannyh pri mnogoetapnyh atakah* [A tool for verifying the data network security management process model during multi-stage attacks]. Certificate Russian Federation No. 2023664605, 2023.
29. Lipatnikov V. A., Tikhonov V. A. Recognition of offenders actions in the management of cyber security of the integrated organization infrastructure on the basis of neuro-fuzy networks and cognitive modeling. *Sbornik nauchnyh statej VIII Mezhdunarodnoj nauchno-tekhnicheskoj i nauchno-metodicheskoj konferencii "Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2019)* [Proc. of the VIII Intern. Scientific-Technical and Scientific-Methodological Conf. "Current problems of information and telecommunications in science and education"]. Saint-Petersburg, 2019, vol. 4, pp. 659–664 (In Russian). EDN: AWSFFH
30. Karataş G., Akbulut A. Survey on access control mechanisms in cloud computing. *Journal of Cyber Security and Mobility*, 2018, vol. 7, no. 3, pp. 1–36. doi:10.13052/2245-1439.731
31. Lopez J., Rubio J. Access control for cyber-physical systems interconnected to the cloud. *Comput. Netw.*, 2018, vol. 134, no. C, pp. 46–54.
32. Yin A., Zhang C. BOFE: Anomaly detection in linear time based on feature estimation. *2018 IEEE Intern. Conf. on Data Mining Workshops (ICDMW)*. IEEE, 2018, pp. 1128–1133. doi:10.1109/ICDMW.2018.00162