УДК 004; 621.398
doi:10.31799/1684-8853-2022-1-54-67

Научные статьи
Articles

Метод обеспечения информационной безопасности сети VoIP-телефонии с прогнозом стратегии вторжений нарушителя

В. А. Липатников[a], *доктор техн. наук, профессор, orcid.org/0000-0002-3736-4743, lipatnikovanl@mail.ru*
А. А. Шевченко[a], *научный сотрудник, orcid.org/0000-0001-9113-1089*
В. С. Косолапов[a], *адъюнкт, orcid.org/0000-0001-8464-779X*
Д. С. Сокол[a], *оператор роты (научной), orcid.org/0000-0002-1532-8872*
[a]*Военная академия связи им. Маршала Советского Союза С. М. Буденного, Тихорецкий пр., 3, Санкт-Петербург, 194064, РФ*

Введение: *развитие технологий в сфере информации и телекоммуникации, а также унификация сетей и, в частности, построение распределенных сетей VoIP-телефонии позволяют сформулировать проблему, заключающуюся в том, что известные методы управления защитой VoIP сетей в современных условиях недостаточно эффективны, так как учитывают только одну сторону информационного противоборства.* ***Цель:*** *разработать метод обеспечения информационной безопасности сети VoIP-телефонии, позволяющий повысить вероятность защищенности VoIP сети путем уменьшения затрачиваемого времени, необходимого для анализа действий нарушителя, анализа и обработки рисков в условиях воздействия нарушителя.* ***Результаты:*** *на основе предложенной структуры системы управления информационной безопасностью, интегрируемой в VoIP сеть, разработан метод обеспечения информационной безопасности сети VoIP-телефонии в условиях воздействия нарушителя за счет внедрения процессов поддержки принятия решения в системе управления информационной безопасностью VoIP сети с использованием распределенных по сегментам интеллектуальных средств обнаружения вторжений. Данный метод позволил построить граф событий действий нарушителя, на основе которого проведено математическое моделирование атак MiTM и SPIT на сеть VoIP-телефонии. В результате моделирования получена зависимость успешного воздействия от внутренних и внешних характеристик атак, которая является основой разработанного программного обеспечения, позволяющего получить значения вероятности защищенности VoIP сети от степени воздействия нарушителя для дальнейшего выбора адекватных мер по управлению информационной безопасностью сети VoIP-телефонии. Метод включает в себя процессы анализа цифрового потока и определения параметров протоколов и профилей атак нарушителей.* ***Практическая значимость:*** *разработанный метод предоставляет возможность исследовать вопросы по защищенности сети VoIP-телефонии, на которую проводится воздействие со стороны нарушителей.*

Ключевые слова *— VoIP сеть, информационная безопасность, MiTM, SPIT, марковский случайный процесс, модель атаки.*

Для цитирования: 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

For citation: 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

Введение

Развитие технологий в сфере информации и телекоммуникации, а также унификация сетей и, в частности, построение распределенных сетей VoIP-телефонии повлияло на число исследований проблем, связанных с обеспечением информационной безопасности [1].

Ужесточение требований к средствам защиты информации (СЗИ) влечет за собой более детальное исследование вопросов информационной безопасности (ИБ). Разрабатываются новые методы обеспечения ИБ. Одним из них является способ, позволяющий формировать управляющие воздействия на СЗИ и объекты сети на основе анализа информации о нарушителе, полученной с помощью ложной инфраструктуры [2]. Существуют способы, которые позволяют управлять сетевой безопасностью за счет фиксации уязвимостей сети одновременно с ее функционированием [3, 4]. В вышеперечисленных решениях управление обеспечением ИБ носит реактивный характер, не учитывается прогнозирование воздействий на сеть.

Вывод по обзору релевантных работ [2–4] заключается в том, что при разработке методов ИБ недостаточно уделено внимание анализу динамики действий нарушителя. Одним из требований, которые предъявляются к информационно-вычислительным системам (ИВС), включая и VoIP сети, является реализация способа находить аномалии и возможные вторжения со стороны нарушителей в реальном времени. Возникает противоречие между современными и развивающимися возможностями нарушителей по вторжениям в сети и существующими способами защиты VoIP сети.

В связи с этим результаты анализа релевантных работ позволяют утверждать, что задача защиты инфраструктуры VoIP сети от вторжений со стороны внешних и внутренних нарушителей актуальна.

Целью исследования является повышение вероятности защищенности VoIP сети путем уменьшения времени, необходимого для проведения анализа динамики действий нарушителя, анализа и обработки рисков.

Задачей исследования является разработка метода управления ИБ для VoIP сети с прогнозированием воздействий на основе интеллектуальных технологий [5]. Для этого необходимо декомпозировать задачу на частные подзадачи: разработать структуру системы управления (СУ) ИБ, интегрируемой в VoIP сеть; разработать структурные схемы модулей распознавания вторжения с прогнозированием и оценки рисков ИБ за счет внедрения интеллектуальной системы; разработать алгоритм метода управления ИБ VoIP сети; разработать модели атак на сеть VoIP-телефонии.

Метод обеспечения информационной безопасности сети VoIP-телефонии

Распределенная VoIP сеть (рис. 1) может подвергаться информационному вторжению со стороны нарушителя.

Предлагаемый метод обеспечения ИБ содержит взаимоувязанную последовательность процессов [3]. Предложено обнаруживать, анализировать действия и прогнозировать реализацию атак на VoIP сеть с последующим блокированием нарушителя.

Аналогично [6] в целях сокращения времени реагирования СЗИ ($t_{СЗИ}$) предложена структурная схема СУ ИБ (рис. 2) с учетом внедрения интеллектуальной системы обнаружения вторжений (ИСОВ) [7]. Данные об инцидентах безопасности собираются с оборудования сети и СЗИ с помощью протоколов обмена служебной информацией. После чего проводятся унификация, фильтрация и установление приоритета полученной информации о безопасности сети. Далее оценивается защищенность сети на основе данной структурированной информации. Одновременно с этим строится прогноз воздействия и риска от него [8–10].

Нижний уровень работы ИСОВ предполагает обработку событий, происходящих в сегменте VoIP сети, и принятие мер в соответствии с их влиянием на ИБ с использованием модуля, представленного на рис. 3, *а* [11]. Данный модуль позволяет провести обработку возникающих или изменяющихся рисков.

Верхний уровень ИСОВ предполагает прогнозирование воздействия на VoIP сети с использованием другого модуля (рис. 3, *б*).

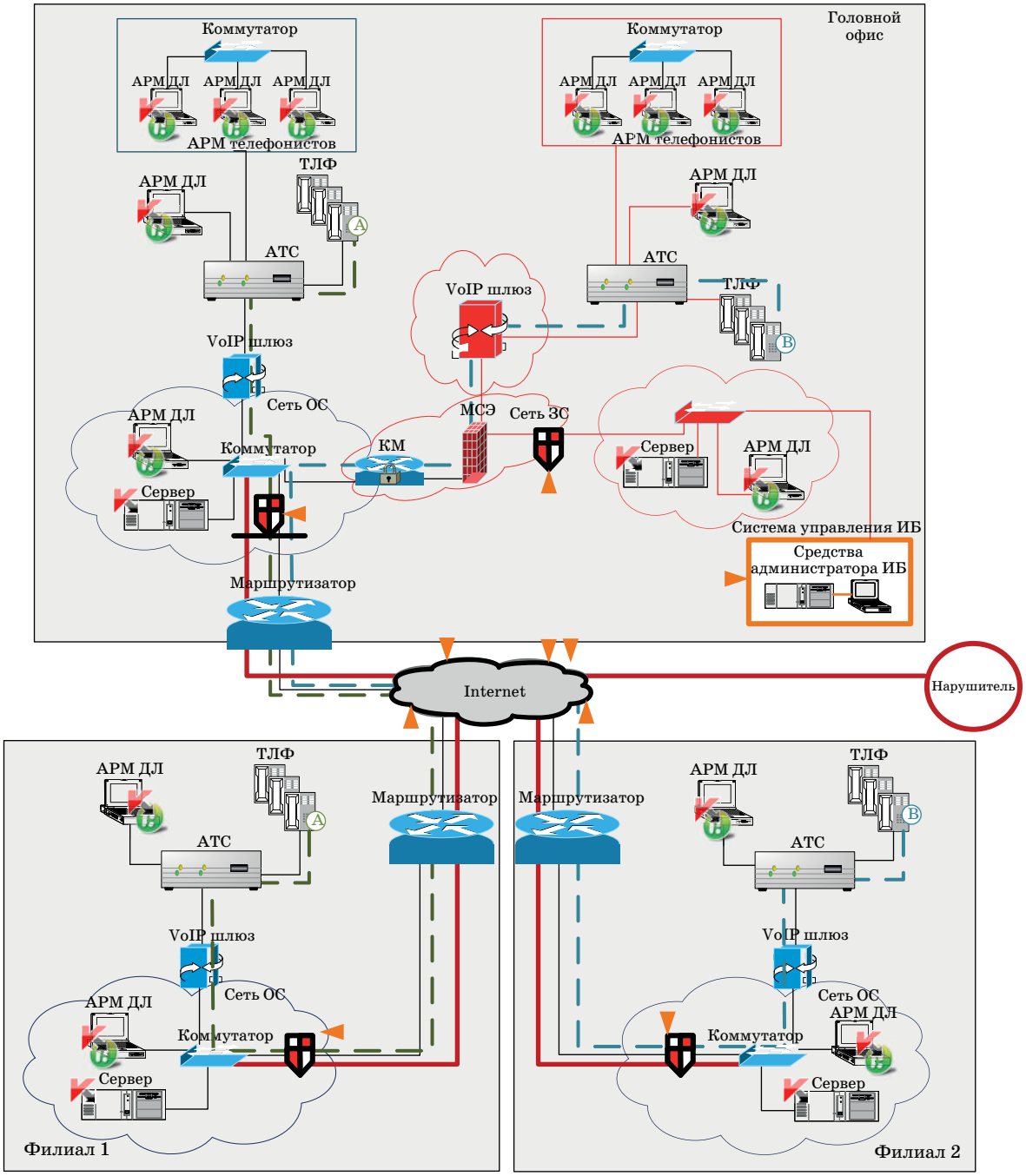
Прогнозирование воздействия и риска от него предлагается реализовать на основе интеллектуальных технологий, а именно модулярной гибридной системы прогнозирования временных рядов. Суть заключается в том, что прогнозы сравниваются по критериям, например точности, актуальности или соответствию горизонту прогнозирования [12].

В целях выявления уязвимостей VoIP сети на основе тестирования сети и пополнения базы данных (БД) угрозами несанкционированного действия (НСД) за счет анализа действий противника в ложной инфраструктуре VoIP сети разработан алгоритм метода обеспечения ИБ VoIP сети (рис. 4). Он позволяет реализовать наблюдение, выделение признаков атаки в пакетах сообщений, поступающих в VoIP сеть, и распознавание вторжения с выбором реализации способа защиты.

Системе управления ИБ необходимо произвести сбор информации о уязвимостях VoIP сети, текущей защищенности, сбор статистики и анализ действий нелегитимного пользователя, прогнозирование уровня защищенности с учетом анализа динамики действий нелегитимного пользователя, выработку стратегий противодействия и рекомендаций по корректировке работы СЗИ.

Уязвимость VoIP сети — это свойства VoIP сети и СЗИ, при которых нелегитимный пользователь методом вторжения нарушит защищенность информации. Поэтому в целях эффективного управления ИБ и своевременного устранения угроз безопасности предложено выявлять уязвимости на этапе, когда злоумышленник находится вне реальной сети, запущенной в VoIP сети в процессе ее функционирования.

Суть данного решения заключается в том, что идет получение пакетов сообщений от нелегитимных пользователей, которые не идентифицируются как угроза ИБ, а также в целях пополнения БД известных угроз в СУ ИБ формируются массивы, имитирующие ресурсы VoIP сети [13]. Также формируются виртуальные контейнеры на выделенном сервере в СУ ИБ на основе данных о VoIP сети и запускаются в работу в режиме функционирования VoIP сети. Принимаются на выделенном сервере пакеты сообщений от нелегитимного пользователя, пока соединение с нелегитимным пользователем не будет разорвано. Нелегитимный пользователь, работая с данным сервером, предполагает, что он находится в реальной VoIP сети, и проводит подготовку и реализацию вторжения. Действия нелегитимного пользователя ре-

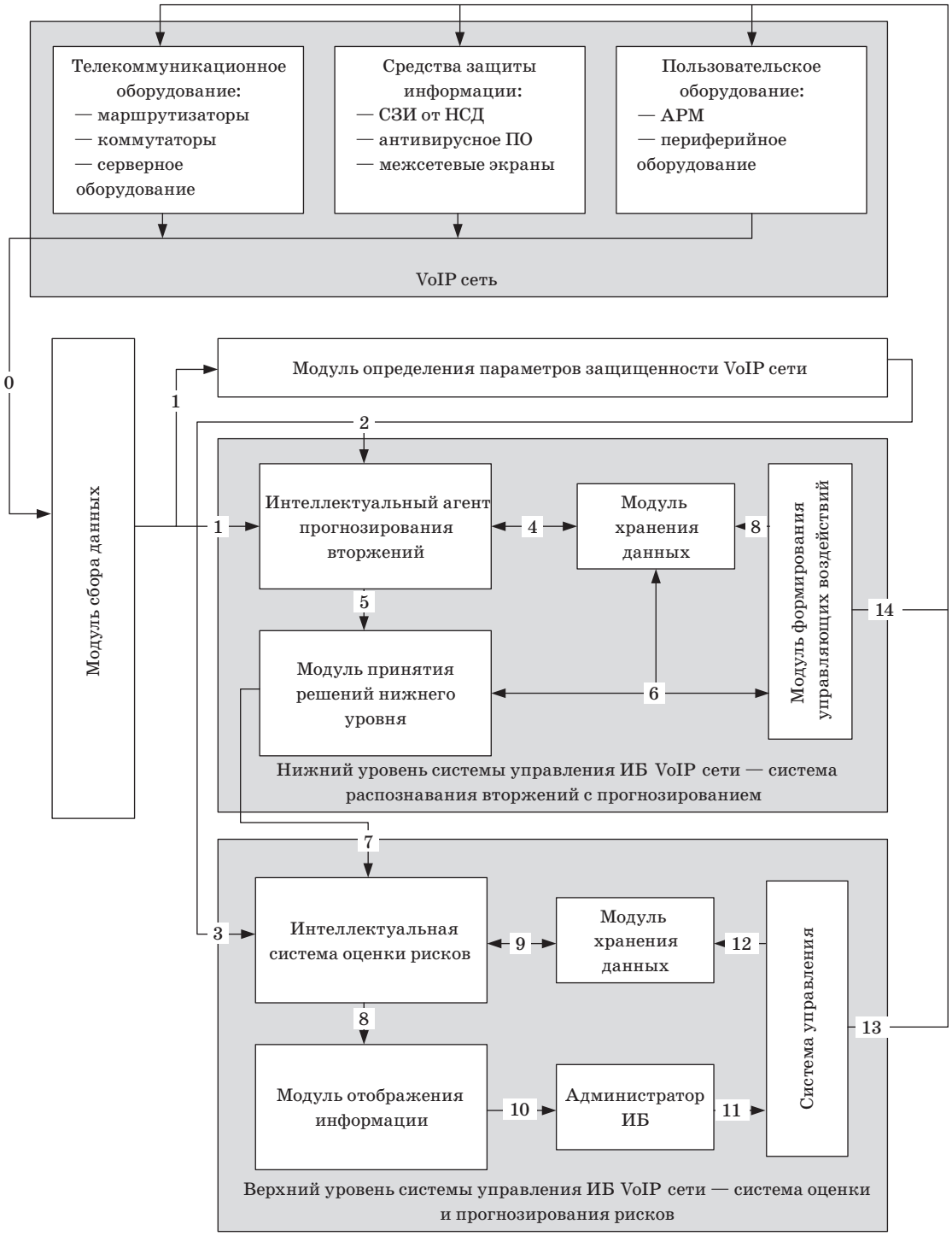


	Процессы реализации управления ИБ верхнего уровня
	Маршруты следования IP-трафика
	Воздействие нарушителя
Сеть ОС	Сеть открытого сегмента
Сеть ЗС	Сеть закрытого сегмента
АТС	Автоматическая телефонная станция
ТЛФ	Телефонный аппарат
АРМ ДЛ	Автоматизированное рабочее место должностного лица

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

Стандартные СЗИ	ОС	ЗС
Антивирусное программное обеспечение	+	+
Средства разграничения доступа	+	+
Криптомаршрутизатор (КМ)	–	+
Межсетевой экран (МСЭ)	–	+

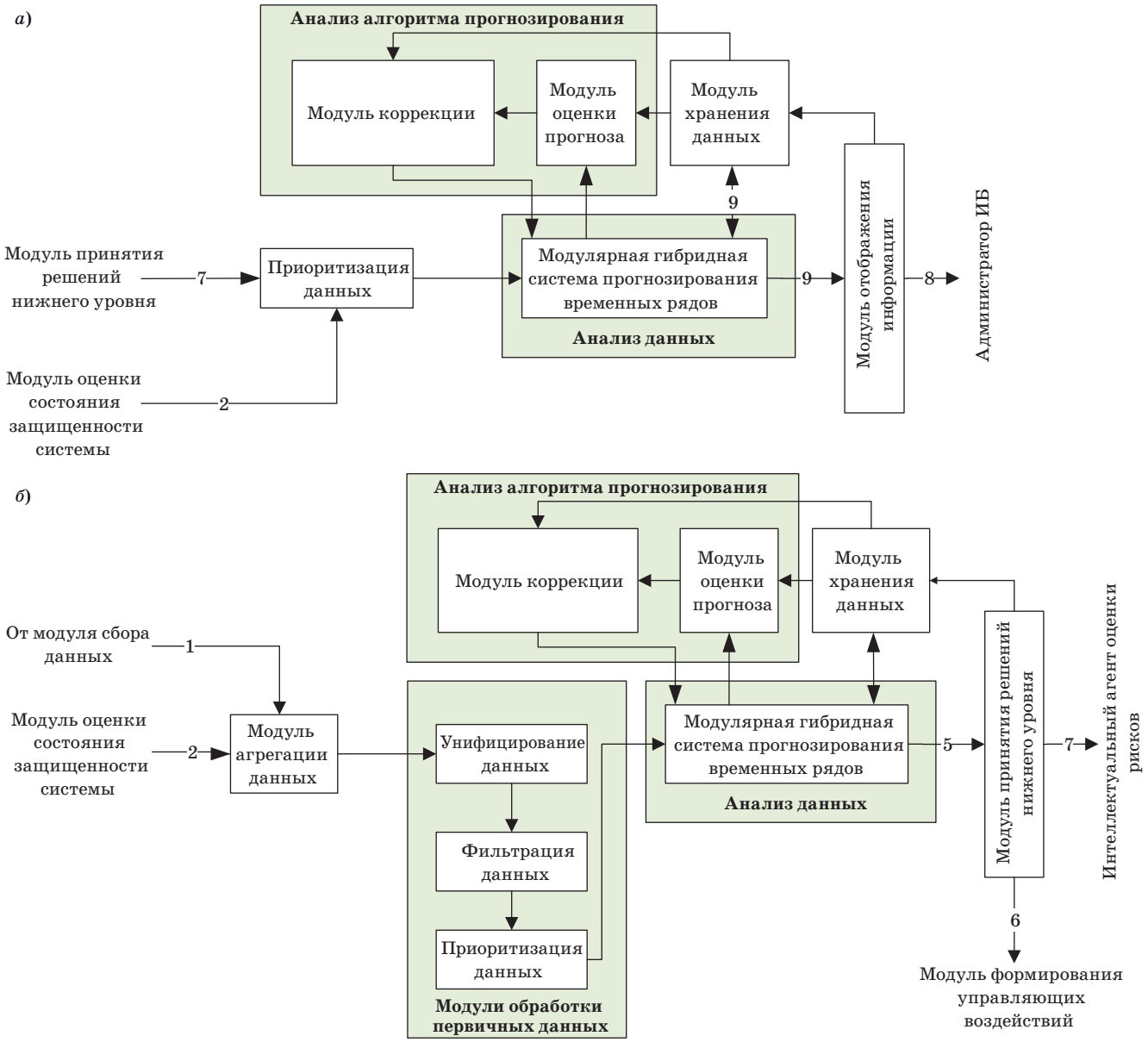
■ ***Рис. 1.*** VoIP сеть с интегрированной в нее СУ ИБ
■ ***Fig. 1.*** VoIP network with integrated IS management system



■ ***Рис. 2.*** Система управления ИБ с использованием ИСОВ
■ ***Fig. 2.*** Information security management system using intelligent intrusion detection system

гистрируются. В случае реализации угроз ИБ данные по действиям нелегитимного пользователя регистрируются и записываются в массив как новая угроза ИБ, тем самым пополняя БД. Далее проводится анализ, на основе которого принимается решение по изменению настроек СЗИ сети VoIP.

Анализ действий противника на сети VoIP осуществляется за счет моделирования атак на основе теории графов.



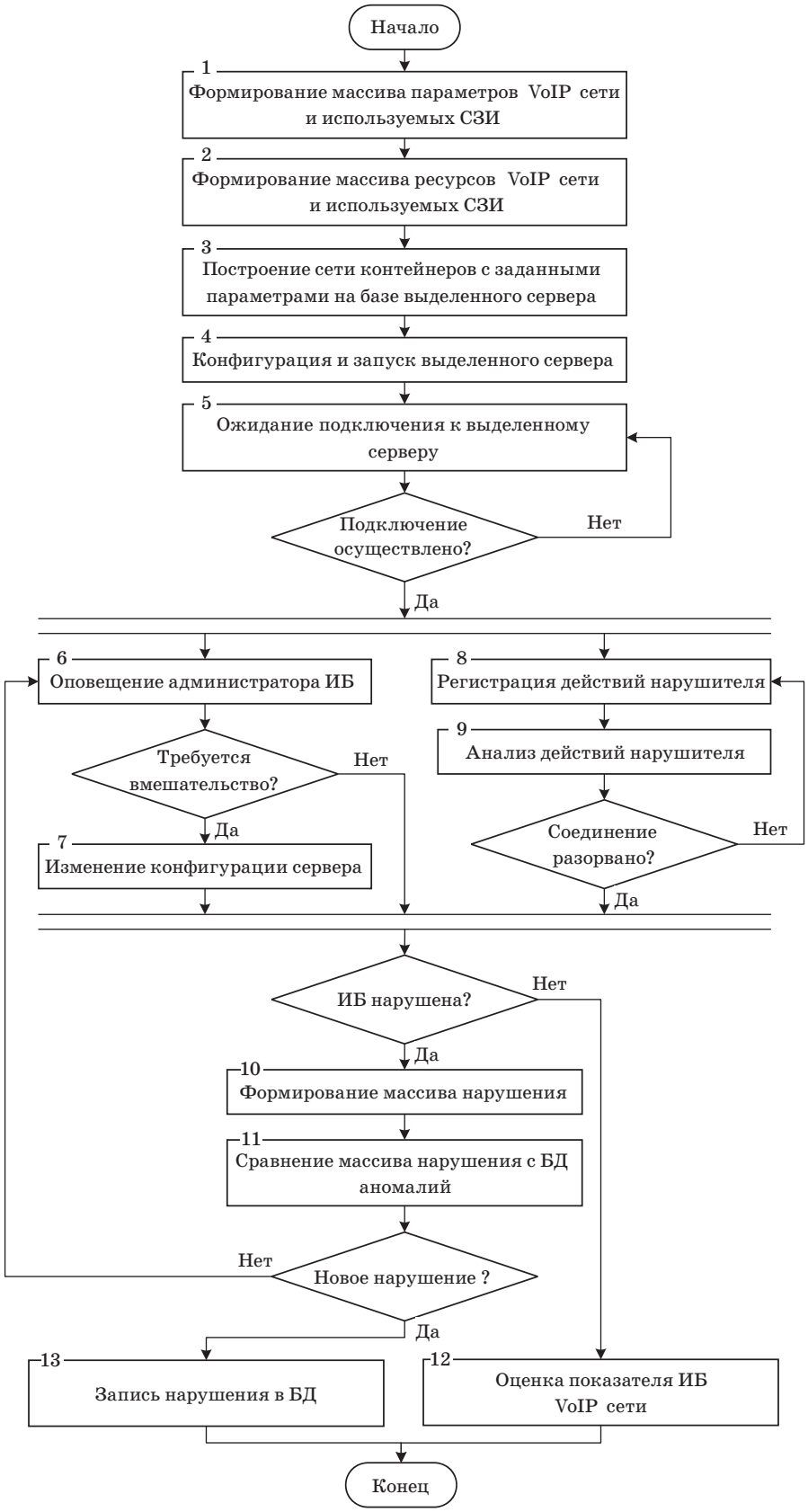
■ ***Рис. 3.*** Структура модуля интеллектуальной оценки рисков (*а*) и прогнозирования воздействия (*б*)
■ ***Fig. 3.*** The structure of the intelligent risk assessment module (*а*) and impact prediction module (*б*)

Модели действий нарушителя

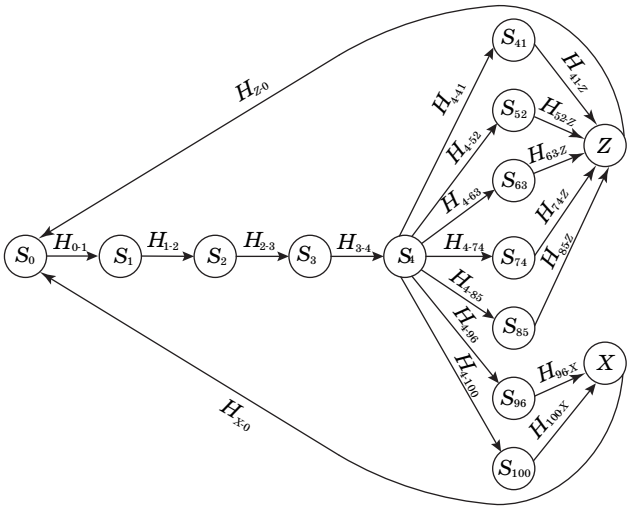
Одной из задач обеспечения ИБ VoIP сети является анализ воздействия, результатом которого являются параметры атаки. Данное действие необходимо для оценки эффективности системы обеспечения ИБ. В результате строится граф реализации угроз [14] и формируются рекомендации по корректировке настроек СЗИ.

Учтены нарушители в виде обычного посетителя организации и администратора информационной сети, который подключает ЭВМ. Если нарушитель первого типа знает логин и пароль от администрирования сети, то сразу авторизуется на сервере. Если не знает, то он подбирает логин и пароль (брутфорс (англ. *brute force*) — атака путем автоматического перебора паролей (иногда связки логинов-паролей), наиболее длительный и простой вид взлома) и авторизуется на сервере. После чего нарушитель администрирует свое устройство в сегменте сети и начинает сканировать сеть SIP (Session Initiation Protocol) сканером и находит список VoIP-устройств. После удачного поиска VoIP-устройств реализует атаку. На рис. 5 представлен граф реализации угроз VoIP сети [15].

Состояния нарушителя при реализации угроз описаны в табл. 1.



■ ***Рис. 4.*** Алгоритм метода обеспечения ИБ VoIP сети
■ ***Fig. 4.*** Algorithm of the VoIP network security method



■ ***Рис. 5***. Граф реализации угроз
■ ***Fig. 5***. Threat realization graph

■ ***Таблица 1***. Состояния нарушителя при реализации угроз
■ ***Table 1***. The state of the intruder during the implementation of threats

Состояние	Описание
S_0	Исходное состояние
S_1	Подготовка к воздействию
S_2	Сканирование нарушителем ИВС на наличие VoIP-устройств с помощью SIP-сканера
S_3	Сбор информации об объекте воздействия
S_4	Выбор осуществления типа атаки
S_{41}	Засорение канала передачи данных путем спама
S_{52}	Нагрузка с большим воздействием на VoIP-оборудование
S_{63}	Отправка постоянных пакетов данных на сеть VoIP
S_{74}	Создание виртуальных VoIP-устройств
S_{85}	Изменение ID-устройства
S_{96}	Перехват голосовых и медианных пользователей
S_{100}	Изменение пароля администратора ИВС
Z	Реализация отказа в обслуживании
X	Реализация угрозы хищения информации

Рассмотрены две атаки: человек посередине (Man in the Middle, MiTM) и спам для интернет-телефонии (Spam Over Internet Telephony, SPIT), так как они являются часто используемыми и наносящими большой материальный ущерб предприятию [16].

1. *Модель процесса нарушения безопасной передачи информации в сетях VoIP-телефонии при атаке MiTM*.

Перехват данных — самая большая проблема в сетях VoIP-телефонии, обусловлено это тем, что данные в стеке протоколов TCP/IP передаются в открытом виде [17]. Нарушителем выделяется маршрутизатор, который образует беспроводную сеть Wi-Fi. Определяется машина, на которой установлен анализатор трафика, например WireShark. Далее через netsh подготавливается точка доступа SSID (Service Set Identifier). Нарушитель в ходе разведки получает учетные данные для создания общей точки доступа с таким же названием и таким же паролем доступа, как на машине с WireShark. После чего перезагружается роутер, чтобы отключить всех клиентов. В этот момент включается двойник доступа. В итоге сетевое взаимодействие осуществляется через двойника доступа. Далее запускается WireShark и прослушивается трафик от клиентов.

Состояния нарушителя при реализации угрозы MiTM описаны в табл. 2.

■ ***Таблица 2***. Состояния нарушителя при реализации угрозы MiTM
■ ***Table 2***. The state of the intruder when the MiTM threat is implemented

Состояние	Описание
S_0	Исходное состояние
S_1	Постановка задачи на воздействие
S_2	Генерация пароля для входа в систему
S_3	Вход в систему под учетной записью «администратор»
S_4	Просмотр пароля и имени точки доступа на роутере для дальнейшего создания двойника на своем устройстве
S_5	Имитация ложной точки доступа
S_6	Обращение в Интернет через ложную точку доступа
S_7	Вывод из строя роутера с помощью DDoS-атаки
S_8	Ввод в сеть ложной точки доступа вместо атакуемого роутера
X	Реализация угрозы хищения информации

2. *Модель процесса нарушения безопасной передачи информации в сетях VoIP-телефонии при атаке SPIT.*

Данный вид воздействия возможен при помощи программ дозвона, таких как Spitter, по номерам из БД, с донесением заранее записанного голосового сообщения, с заранее пройденной авторизацией с помощью похищенных логинов и паролей от SIP учетных записей [18]. В отличие от спама, рассылаемого по e-mail в виде сообщений, вероятность прослушивания голосовых сообщений пользователями считается выше.

Состояния нарушителя при реализации угрозы SPIT описаны в табл. 3.

Разработана математическая модель активного нарушителя (рис. 6) [15], позволяющая рассчитать вероятностно-временные характеристики атаки в зависимости от значений вероятностей промежуточных атак [19, 20].

Определены вероятности нахождения нарушителя в различных состояниях реализации угрозы P_0, ..., P_8:

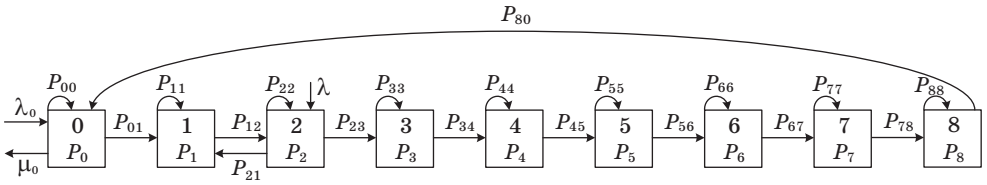
$$\begin{cases} P_0 = \dfrac{1}{1+\alpha\dfrac{\mu_0}{\beta_7}\left(1+\dfrac{\beta_7}{\beta_6}\left(1+\dfrac{\beta_6}{\beta_5}\left(1+\dfrac{\beta_5}{\beta_4}\left(1+\dfrac{\beta_4}{\beta_3}\left(1+\dfrac{\beta_3}{\beta_2}\left(1+\dfrac{\lambda+\beta_2}{\beta_1}\right)\right)\right)\right)\right)\right)}; \\ P_1 = \left(\alpha\cdot\dfrac{(\lambda+\beta_2)\beta_3\beta_4\beta_5\beta_6\beta_7\mu_0}{\beta_1\beta_2\beta_3\beta_4\beta_5\beta_6\beta_7}\right)\cdot\left(\dfrac{1}{1+\alpha\dfrac{\mu_0}{\beta_7}\left(1+\dfrac{\beta_7}{\beta_6}\left(1+\dfrac{\beta_6}{\beta_5}\left(1+\dfrac{\beta_5}{\beta_4}\left(1+\dfrac{\beta_4}{\beta_3}\left(1+\dfrac{\beta_3}{\beta_2}\left(1+\dfrac{\lambda+\beta_2}{\beta_1}\right)\right)\right)\right)\right)\right)}\right); \\ \ldots \\ P_8 = \alpha\cdot\left(\dfrac{1}{1+\alpha\dfrac{\mu_0}{\beta_7}\left(1+\dfrac{\beta_7}{\beta_6}\left(1+\dfrac{\beta_6}{\beta_5}\left(1+\dfrac{\beta_5}{\beta_4}\left(1+\dfrac{\beta_4}{\beta_3}\left(1+\dfrac{\beta_3}{\beta_2}\left(1+\dfrac{\lambda+\beta_2}{\beta_1}\right)\right)\right)\right)\right)\right)}\right), \end{cases} \quad (1)$$

где $\alpha = \dfrac{\lambda_0}{\mu_0}$, λ_0 — плотность потока задач на вторжение; μ_0 — плотность потока успешных вторжений; β_1, ..., β_7 — плотность выполнения задач нарушителем по вторжению согласно состояниям при MiTM- и SPIT-атаках.

■ ***Таблица 3.*** Состояния нарушителя при реализации угрозы SPIT

■ ***Table 3.*** The state of the intruder when the SPIT threat is implemented

Состояние	Описание
S_0	Исходное состояние
S_1	Постановка задачи на воздействие
S_2	Генерация пароля для входа в систему
S_3	Вход в систему под учетной записью «администратор»
S_4	Поиск SIP-абонентов
S_5	Обнаружение SIP-телефонов в сети и в режиме офлайн
S_6	Хищение данных для авторизации учетных SIP-записей
S_7	Вход в систему с похищенных учетных SIP-записей
S_8	Запуск программного обеспечения (ПО) Spitter
H	Реализация угрозы хищения информации



■ ***Рис. 6***. Граф состояния нарушителя при реализации угроз MiTM и SPIT на VoIP сеть
■ ***Fig. 6***. The intruder's state graph when the MiTM and SPIT threat is implemented on the VoIP network

Вероятности воздействия $P_в = P_0 + P_8$, так как, с одной стороны, нарушитель в «состоянии 8» успешно завершает реализацию угроз MiTM и SPIT на VoIP сеть, после чего, вероятнее всего, принимает решение на следующее воздействие на защищаемую инфраструктуру, с другой стороны, без корректной работы нарушителя в «состоянии 0» реализация угроз MiTM и SPIT на VoIP сеть невозможна [13]. С учетом вышесказанного система (1) примет вид

$$P_в = \frac{1+\alpha}{1+\alpha\frac{\mu_0}{\beta_7}\left(1+\frac{\beta_7}{\beta_6}\left(1+\frac{\beta_6}{\beta_5}\left(1+\frac{\beta_5}{\beta_4}\left(1+\frac{\beta_4}{\beta_3}\left(1+\frac{\beta_3}{\beta_2}\left(1+\frac{\lambda+\beta_2}{\beta_1}\right)\right)\right)\right)\right)\right)}. \quad (2)$$

Получив значение вероятности воздействия, можно вычислить показатель (вероятность) защищенности VoIP сети ($P_{защ}$):

$$P_{защ} = 1 - P_в, \quad (3)$$

где $P_в$ — вероятность воздействия со стороны нарушителя на VoIP сеть.

Реализация моделей в виде программного обеспечения

Для оптимизации расчета воздействия на VoIP сети по выражению (2) и принятия оперативных мер по устранению нарушения целостности сети было принято решение разработать ПО, позволяющее упростить все расчеты и получить готовый результат.

Программное обеспечение было написано на языке Java ver.8. с применением платформы JavaFX (рис. 7).

С помощью ПО [21] на основе исходных данных из табл. 4, являющихся экспертными оценками, были проведены контрольные решения оценки вероятности защищенности VoIP сети в условиях реализации подбора пароля с различной интенсивностью от 3 до 9 мин (рис. 8, *а*), авторизации в системе администрирования роутера с интенсивностью от 0,2 до 0,6 мин (рис. 8, *б*) при MiTM, а также хищения данных для авторизации учетных SIP-записей с интенсивностью от 1 до 30 мин (рис. 8, *в*) и массового входа в систему с похищенных учетных SIP-записей с интенсивностью от 2 до 6 мин (рис. 8, *г*) при SPIT.

Анализ зависимостей на рис. 8, *а–г* позволяет сделать вывод о том, что увеличение времени реагирования СЗИ $t_{СЗИ}$ VoIP сети при атаках MiTM и SPIT понижает защищенность $P_{защ}$ ниже требуемого уровня 0,9. В связи с этим возможно определить требования к $t_{СЗИ}$ с учетом условий противоборства:

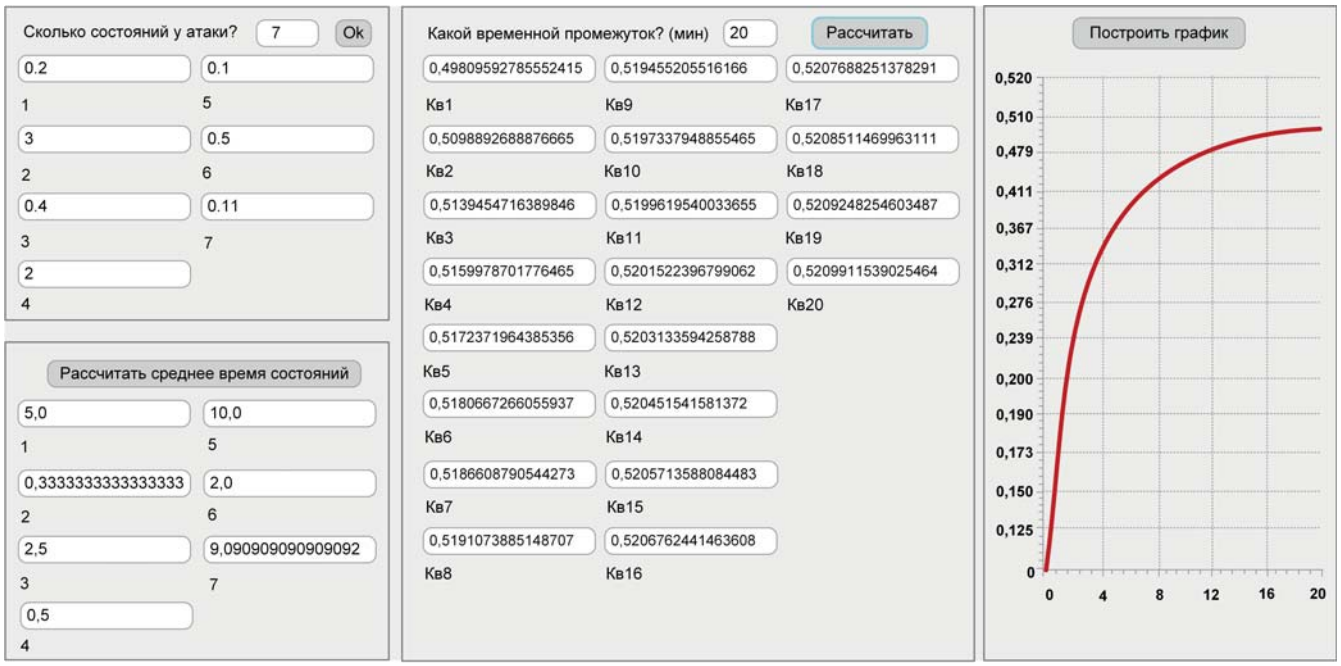
1) $t_{СЗИ} \le 0{,}0012$ мин в условиях реализации подбора пароля при MiTM (см. рис. 8, *а*);

2) $t_{СЗИ} \le 0{,}0014$ мин в условиях реализации авторизации в системе администрирования роутера при MiTM (см. рис. 8, *б*);

3) $t_{СЗИ} \le 0{,}046$ мин в условиях реализации получения из БД логинов и паролей от SIP учетных записей при SPIT (см. рис. 8, *в*);

4) $t_{СЗИ} \le 0{,}045$ мин в условиях реализации массовой авторизации учетных SIP-записей при SPIT (см. рис. 8, *г*).

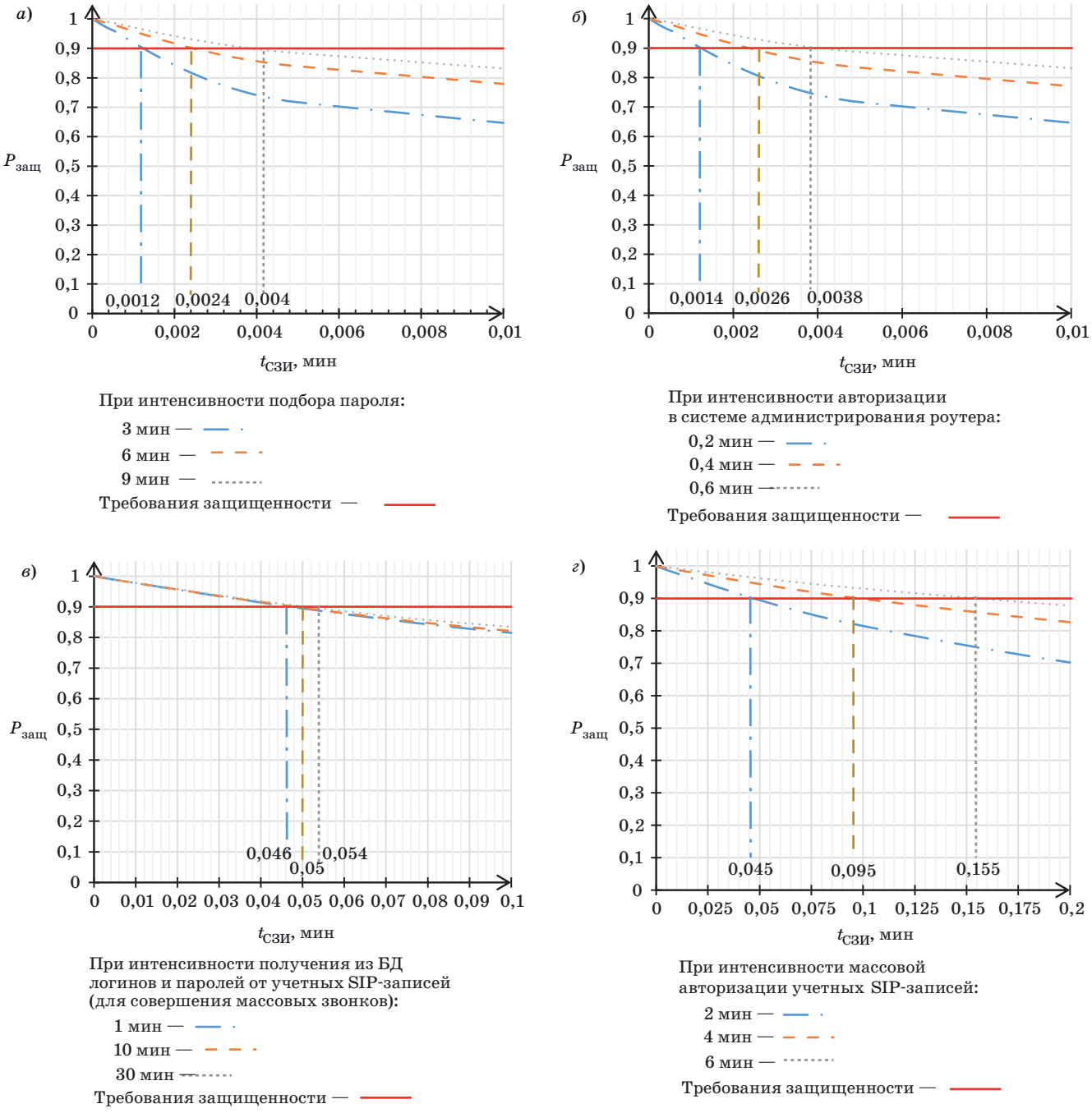
Также из графиков видно, что наибольшую угрозу для VoIP сети представляет MiTM-атака, так как вероятность защищенности резко падает в короткий промежуток времени. Следовательно, событие «реализация генерации пароля для входа в систему» будет более вероятным, в связи с этим вероятность того, что нарушитель этим воспользуется, высока. Поэтому администратору безопасности необходимо обратить внимание на устранение именно этой уязвимости [14].



■ ***Рис. 7.*** Интерфейс ПО для оперативного расчета вероятности воздействия на VoIP сети
■ ***Fig. 7.*** Software interface for on-line calculation of probability of impact on VoIP networks

■ ***Таблица 4.*** Исходные данные для контрольной оценки вероятности защищенности VoIP сети в условиях реализации MiTM и SPIT
■ ***Table 4.*** Initial data for the control assessment of the probability of VoIP network security in the context of MiTM and SPIT implementation

Событие	MiTM			SPIT		
	Описание	Параметр	Значение, мин	Описание	Параметр	Значение, мин
S_2	Генерация пароля (ГП) для входа в систему	$\beta_1 = \frac{1}{t_{ГП}}$	3 6 9	Генерация пароля для входа в систему	$\beta_1 = \frac{1}{t_{ГП}}$	10
S_3	Вход в систему (ВС) под учетной записью «администратор»	$\beta_2 = \frac{1}{t_{ВС}}$	0,2 0,4 0,6	Вход в систему под учетной записью «администратор»	$\beta_2 = \frac{1}{t_{ВС}}$	2
S_4	Просмотр пароля (ПП) и имени точки доступа на роутере для дальнейшего создания двойника на своем устройстве	$\beta_3 = \frac{1}{t_{ПП}}$	0,5	Поиск SIP-абонентов	$\beta_3 = \frac{1}{t_{SIP}}$	2
S_5	Имитация ложной точки доступа (ЛТД)	$\beta_4 = \frac{1}{t_{ЛТД}}$	0,6	Обнаружение (О) SIP-телефонов в сети и в режиме офлайн	$\beta_4 = \frac{1}{t_{О}}$	1
S_6	Обращение в Интернет (ОИ) через ложную точку доступа	$\beta_5 = \frac{1}{t_{ОИ}}$	0,3	Хищение данных (ХД) для авторизации учетных SIP-записей	$\beta_5 = \frac{1}{t_{ХД}}$	1 10 30
S_7	Вывод из строя роутера с помощью DDoS-атаки	$\beta_6 = \frac{1}{t_{DDoS}}$	1	Авторизация (А) в системе с похищенных учетных SIP-записей	$\beta_6 = \frac{1}{t_{А}}$	2 4 6
S_8	Подмена (П) атакуемого роутера ложной точкой доступа	$\beta_7 = \frac{1}{t_{П}}$	0,2	Запуск ПО Spitter	$\beta_7 = \frac{1}{t_{Spitter}}$	0,5



■ ***Рис. 8.*** Зависимость показателя защищенности VoIP сети от времени реагирования СЗИ в условиях: *а* — реализации подбора пароля при MiTM; *б* — реализации авторизации в системе администрирования роутера при MiTM; *в* — хищения данных для авторизации учетных SIP-записей при SPIT; *г* — реализации массового входа в систему с похищенных учетных SIP-записей при SPIT

■ ***Fig. 8.*** Dependence of the VoIP network security indicator on the response time of information security tools in conditions of: *а* — password matching in MiTM; *б* — authorization implementation in the router administration system with MiTM; *в* — data theft for authorization of SIP records during SPIT; *г* — a mass logon from stolen SIP accounts at SPIT

Заключение

Представлен анализ VoIP сети организации, алгоритм контроля ситуационных параметров при стохастической неопределенности, предложена архитектура прототипа VoIP сети, а также ПО, позволяющее оптимизировать расчеты для быстрого получения результатов оценки защищенности VoIP сети в целях последующего принятия решений по защите целостности сети.

Данный метод включает обнаружение, анализ действия нарушителя и прогноз реализации атак

на VoIP сеть с последующим блокированием нежелательной активности.

Научная новизна заключается в том, что в отличие от известных метод обеспечения ИБ сети VoIP-телефонии учитывает: выявление уязвимостей VoIP сети на основе тестирования реальной сети; выявление уязвимостей и пополнение БД угрозами НСД за счет анализа действий противника в ложной инфраструктуре VoIP сети; профили и виды атак, направленных на VoIP сеть и описанных в виде графов.

Теоретическая значимость заключается в разработке и усовершенствовании известных моделей, что позволяет определять вероятность воздействия, структуру и профиль атаки, а также способы защиты VoIP сети.

Практическая значимость определяется возможностью использовать метод управления обеспечения ИБ VoIP сети при разработке СУ ИБ.

Получены результаты аналитического моделирования, которые показали, что предложенный подход обеспечивает требуемый уровень достоверности принимаемых решений, что позволяет повысить вероятностно-временные характеристики работы VoIP сети.

В дальнейшем будут исследоваться возможности по реализации данного метода в автоматизированном виде с применением нейронной сети, позволяющей полностью на программном уровне принимать самостоятельные решения по предотвращению хищения информации, нарушения целостности и доступности сети.

Литература

1. **Маликов А. В., Авраменко В. С., Саенко И. Б.** Модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационных системах, основанные на глубоком машинном обучении. *Информационно-управляющие системы*, 2019, № 6, с. 32–42. doi:10.31799/1684-8853-2019-6-32-42
2. **Котлякова В. В., Кузьмина И. В.** Автоматизация процесса функционального тестирования распределенной информационной системы с использованием дистрибутива Docker. *Информационные системы и технологии ИСТ-2020: сб. матер. XXVI Междунар. науч.-техн. конф.*, Н. Новгород, 24–28 апреля 2020 г. Н. Новгород, 2020, с. 1247–1250.
3. **Котенко И. В., Хмыров С. С.** Анализ актуальных методик атрибуции нарушителей кибербезопасности при реализации целевых атак на объекты критической инфраструктуры. *Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021): сб. науч. ст. X Юбилейной Междунар. науч.-техн. и науч.-метод. конф.*, Санкт-Петербург, 24–25 февраля 2021 г. СПб., 2021, т. 4, с. 536–541.
4. Пат. 2705773 РФ, C1 G 06 F 12/14. *Способ защиты информационно-вычислительной сети от вторжений*, В. А. Липатников (РФ), К. В. Чепелев (РФ), А. А. Шевченко (РФ). № 2019100252; заявл. 09.01.2019; опубл. 11.11.2019, Бюл. № 32, 19 с.
5. **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.
6. **Котенко И. В., Ушаков И. А., Пелевин Д. В., Преображенский А. И., Овраменко А. Ю.** Выявление инсайдеров в корпоративной сети: подход на базе UBA и UEBA. *Защита информации. Инсайд*, 2019, № 5 (89), с. 26–35.
7. **Костарев С. В., Карганов В. В., Липатников В. А.** *Технологии защиты информации в условиях кибернетического противоборства*. Санкт-Петербург, ВАС им. Буденного, 2020. 716 с.
8. **Chandra K. P. B., Gu D.** *Nonlinear Filtering: Methods and Applications*. Springer, 2019. 197 p.
9. **Федорченко А. В., Дойникова Е. В., Котенко И. В.** Автоматизированное определение активов и оценка их критичности для анализа защищенности информационных систем. *Тр. СПИИРАН*, 2019, т. 18, № 5, с. 1182–1211.
10. **Ярушева С. А., Аверкина А. Н., Федотова А. В.** Модулярная модель прогнозирования временных рядов на основе нейро-нечетких сетей и когнитивного моделирования. *Нечеткие системы и мягкие вычисления*, 2017, т. 12, № 2, с. 159–168. doi:10.26456/fssc31
11. **Guay M., Adetola V., DeHaan D.** *Robust and Adaptive Model Predictive Control of Nonlinear Systems*. The Institution of Engineering and Technology, 2016. 253 p. doi:10.1049/PBCE083E
12. **Rezaee Z., Dorestani A., Aliabadi S.** Application of time series analyses in big data: Practical, research, and education implications. *Journal of Emerging Technologies in Accounting*, 2018, vol. 15, iss. 1, pp. 183–197.
13. **Липатников В. А., Колмыков Д. В., Косолапов В. С.** Способ управления информационной безопасностью информационно-вычислительной сети при вторжениях типа распределенного отказа в обслуживании. *Состояние и перспективы развития современной науки по направлению «Информационная безопасность»: сб. ст. III Всерос. науч.-техн. конф.*, Анапа, 2021, с. 643–654.
14. **Сорокин М. А., Стародубцев Ю. И.** Методика обоснования количества и мест размещения средств сетевого контроля информационного обмена меж-

ду элементами корпоративной системы управления. *Вопросы оборонной техники. Сер. 16. Технические средства противодействия терроризму*, 2021, № 3-4 (153-154), с. 65–74.
15. **Липатников В. А., Сокол Д. С.** Модель нарушителя безопасной передачи информации в сетях VoIP-телефонии. *Транспорт России: проблемы и перспективы — 2020: матер. Юбилейной междунар. науч.-практ. конф.*, Санкт-Петербург, 10–11 ноября 2020 г. СПб., Институт проблем транспорта им. Н. С. Соломенко РАН, 2020, с. 187–192.
16. **Pallaprolu S. C., Sankineni R., Thevar M., Karabatis G., Wang J.** Zero-day attack identification in streaming data using semantics and spark. *Proc. of the IEEE Intern. Congress on Big Data (BigData Congress)*, Honolulu, HI, USA, 2017, 25–30 June, pp. 121–128.
17. **Peters M. D., Wieder B., Sutton S. G., Wakefield J.** Business intelligence systems use in performance capabilities: Implications for enhanced competitive advantage. *International Journal of Accounting Information Systems*, 2021, no. 21, pp. 1–17.
18. **Borthick A. F., Schneider G. P., Viscelli T. R.** Analyzing data for decision making: Integrating spreadsheet modeling and database querying. *Issues in Accounting Education*, 2017, vol. 32, iss. 1, pp. 59–66. doi:10.2308/iace-51385
19. **Xi X., Zhang T., Ye W., Wen Z., Zhang S., Du D., Gao Q.** An ensemble approach for detecting anomalous user behaviors. *International Journal of Software Engineering and Knowledge Engineering*, 2018, vol. 28, no. 11-12, pp. 1637–1656. doi:10.1142/S0218194018400211
20. **Kawamura H.** *Advanced Process Control*. https://blog.yokogawa.com/ru-advanced-solutions-blog/-ru-advanced-process-control (дата обращения: 16.10.2019).
21. **Сокол Д. С., Косолапов В. С., Липатников В. А., Парфиров В. А., Шевченко А. А.** *Расчет коэффициентов воздействия атак на программно-аппаратное оборудование*. Свидетельство о регистрации программы для ЭВМ 2021616926, 29.04.2021. Заявка № 2021612805 от 05.03.2021.

UDC 004; 621.398
doi:10.31799/1684-8853-2022-1-54-67

Method for ensuring information security of a VoIP telephony network with a forecast of an intruder's intrusion strategy

V. A. Lipatnikov[a], Dr. Sc., Tech., Professor, orcid.org/0000-0002-3736-4743, lipatnikovanl@mail.ru
A. A. Shevchenko[a], Research Fellow, orcid.org/0000-0001-9113-1089
V. S. Kosolapov[a], Post-Graduate Student, orcid.org/0000-0001-8464-779X
D. S. Sokol[a], Science Company Operator, orcid.org/0000-0002-1532-8872
[a]S. M. Budenny Military Academy of Communication, 3, Tikhoretskii Pr., 190064, Saint-Petersburg, Russian Federation

Introduction: The development of technologies in the field of information and telecommunications, as well as the unification of networks, and in particular the construction of distributed VoIP telephony networks, allow us to formulate the problem that the known methods of managing the protection of VoIP networks are not effective enough in modern conditions, since they take into account only one side of the information confrontation. **Purpose:** To develop a method for ensuring the information security of a VoIP telephony network, which allows to increase the probability of VoIP network security by reducing the time required for analyzing the actions of the violator, analyzing and processing risks under the influence of the violator. **Results:** Based on the proposed structure of an information security management system integrated into a VoIP network, a method for ensuring the information security of a VoIP telephony network under the influence of an intruder has been developed by introducing decision-making support processes in the VoIP network information security management system using intelligent intrusion detection tools distributed across segments. This method allows you to build a graph of events of the intruder's actions, on the basis of which mathematical modeling of MiTM and SPIT attacks on the VoIP telephony network is carried out. As a result of the simulation, the dependence of the successful impact on the internal and external characteristics of attacks is obtained, which is the main one of the developed software, which allows to obtain the values of the probability of security of the VoIP network from the parameters of the intruder's impact for further selection of adequate measures for managing the information security of the VoIP telephony network. The method includes the processes of analyzing the digital stream and determining the parameters of protocols and profiles of intruder attacks. **Practical relevance:** The developed method provides an opportunity to study issues aimed at the security of the VoIP-telephony network, which is affected by violators.

Keywords — VoIP networks, information security, MiTM, SPIT, Markov random process, attack model.

For citation: 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

References

1. Malikov A. V., Avramenko V. S., Saenko I. B. Model and method for diagnosing computer incidents in information and communication systems based on deep machine learning. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 6, pp. 32–42 (In Russian). doi:10.31799/1684-8853-2019-6-32-42
2. Kotlyakova V. V., Kuzmina I. V. Automation of the functional testing process of a distributed information system using the docker distribution. *Materialy XXVI Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii "Informatsionnyye sistemy i tekhnologii" IST-2020* [Materials of the XXVI Intern. Sci. and Techn. Conf. "Information Systems and

Technologies" IST-2020]. N. Novgorod, 2020, pp. 1247–1250 (In Russian).
3. Kotenko I., Khmyrov S. Analysis of current methods of attributing cyber security offensers in the implementation of targeted attacks on objects of critical infrastructure. *10th Intern. Conf. on Advanced Infotelecommunications (ICAIT 2021)*, Saint-Petersburg, 2021, vol. 4, pp. 536–541 (In Russian).
4. Lipatnikov V. A., Chepelev K. V., Shevchenko A. A. *Sposob zashchity informacionno-vychislitel'noj seti ot vtorzhenij* [Method of protecting an information network from intrusions]. Patent RF, no. 2705773, 2019.
5. 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. *8th Intern. Conf. on Advanced Infotelecommunications (ICAIT 2019)*, Saint-Petersburg, 2019, vol. 4, pp. 659–664 (In Russian).
6. Kotenko I. V., Ushakov I. A., Pelevin D. V., Preobrazhenskiy A. I., Ovramenko A. U. Identification of insiders in the corporate network: UBA and UEBA based approach. *Zaśita Informacii. Inside*, 2019, no. 5 (89), pp. 26–35 (In Russian).
7. Kostarev S. V., Karganov V. V., Lipatnikov V. A. *Tekhnologii zashchity informatsii v usloviyakh kiberneticheskogo protivoborstva* [Technologies of information protection in the conditions of cybernetic confrontation]. Saint-Petersburg, VAS im. Budennogo Publ., 2020. 716 p. (In Russian).
8. Chandra K. P. B., Gu D. *Nonlinear Filtering: Methods and Applications*. Springer, 2019. 197 p.
9. Fedorchenko A. V., Doynikova E. V., Kotenko I. V. Automated detection of assets and calculation of their criticality for the analysis of information system security. *SPIIRAS Proc.*, 2019, vol. 18, no. 5, pp. 1182–1211 (In Russian). doi:10.15622/sp.2019.18.5.1182-1211
10. Yarusheva S. A., Averkina A. N., Fedotova A. V. Modular model for time series forecasting based on neuro-fuzzy nets and cognitive modelling. *Nechetkie sistemy i myagkie vychisleniya*, 2017, vol. 12, no. 2, pp. 159–168 (In Russian). doi:10.26456/fssc31
11. Guay M., Adetola V., DeHaan D. *Robust and Adaptive Model Predictive Control of Nonlinear Systems*. The Institution of Engineering and Technology, 2016. 253 p. doi:10.1049/PBCE083E
12. Rezaee Z., Dorestani A., Aliabadi S. Application of time series analyses in big data: Practical, research, and education implications. *Journal of Emerging Technologies in Accounting*, 2018, vol. 15, iss. 1, pp. 183–197.
13. Lipatnikov V. A., Kolmykov D. V., Kosolapov V. S. Sposob upravleniya informatsionnoy bezopasnost'yu informatsionno-vychislitel'noy seti pri vtorzheniyakh tipa raspredelennogo otkaza v obsluzhivanii. *Sbornik statey III Vserossiyskoy nauchno-tekhnicheskoy konferentsii "Sostoyaniye i perspektivy razvitiya sovremennoy nauki po napravleniyu "Informatsionnaya bezopasnost'"* [Collection of articles of the III All-Russian Scient. and Techn. Conf. "The state and prospects for the development of modern science in the direction of "Information security"]. Anapa, 2021, pp. 643–654 (In Russian).
14. Sorokin M. A., Starodubcev J. I. Methodology for substantiating the number and locations of network control facilities for information exchange between elements of the corporate management system. *Military Enginery. Scientific and Technical Journal. Counter-terrorism technical devices. Issue 16*, 2021, no. 3-4 (153-154), pp. 65–74 (In Russian).
15. Lipatnikov V. A., Sokol D. S. Intruder model for secure data transmission in VoIP telephony networks. *Mezhdunarodnaya nauchno-prakticheskaya konferentsiya "Transport Rossii: problemy i perspektivy — 2020"* [Intern. Scient. and Pract. Conf. "Transport of Russia: Problems and prospects — 2020"]. Saint-Petersburg, 2020, pp. 187–192 (In Russian).
16. Pallaprolu S. C., Sankineni R., Thevar M., Karabatis G., Wang J. Zero-day attack identification in streaming data using semantics and spark. *Proc. of the IEEE Intern. Congress on Big Data (BigData Congress)*, Honolulu, HI, USA, 2017, 25–30 June, pp. 121–128.
17. Peters M. D., Wieder B., Sutton S. G., Wakefield J. Business intelligence systems use in performance capabilities: Implications for enhanced competitive advantage. *International Journal of Accounting Information Systems*, 2021, no. 21, pp. 1–17.
18. Borthick A. F., Schneider G. P., Viscelli T. R. Analyzing data for decision making: Integrating spreadsheet modeling and database querying. *Issues in Accounting Education*, 2017, vol. 32, iss. 1, pp. 59–66. doi:10.2308/iace-51385
19. Xi X., Zhang T., Ye W., Wen Z., Zhang S., Du D., Gao Q. An ensemble approach for detecting anomalous user behaviors. *International Journal of Software Engineering and Knowledge Engineering*, 2018, vol. 28, no. 11-12, pp. 1637–1656. doi:10.1142/S0218194018400211
20. *Advanced Process Control*. Available at: https://blog.yokogawa.com/ru-advanced-solutions-blog/-ru-advanced-process-control (accessed 24 August 2019).
21. Sokol D. S., Kosolapov V. S., Lipatnikov V. A., Parfirov V. A., Shevchenko A. A. *Raschet koeffitsiyentov vozdeystviya atak na programmno-apparatnoye oborudovaniye* [Calculation of attack impact coefficients on software and hardware equipment]. Certificate of registration of the computer program 2021616926, 2021.