**ФГБОУ ВО**
**«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**РЕГИОНАЛЬНЫЙ УЧЕБНО-НАУЧНЫЙ ЦЕНТР**
**ПО ПРОБЛЕМАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

# ИНФОРМАЦИЯ И БЕЗОПАСНОСТЬ

**Том 28, Выпуск 3, 2025**

**Воронеж**

# ИНФОРМАЦИЯ И БЕЗОПАСНОСТЬ

*Том 28, Выпуск 3* *2025*



Журнал выходит четыре раза в год
Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций
Рег. номер ПИ №ФС77-74426 от 23 ноября 2018 г.

Подписной индекс в Объединенном каталоге «Пресса России» – 41255
Оформить подписку на журналы ВГТУ на 2025 год можно на сайте https://www.pressa-rf.ru/

Журнал входит в перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук

АДРЕС РЕДАКЦИИ:
394049, г. Воронеж, ул. Ватутина, д. 1
тел./факс: (473) 252-34-20

e-mail: alexanderostapenkoias@gmail.com

12+

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ:
ФГБОУ ВО «Воронежский государственный технический университет»

АДРЕС УЧРЕДИТЕЛЯ И ИЗДАТЕЛЯ:
394006, г. Воронеж, ул. 20-летия Октября, 84

# INFORMATION & SECURITY

*Vol 28, Part 3* *2025*



The magazine is published four times a year
The journal is registered in the Federal service for supervision of communications,
information technology and mass communications
Reg. number of PI No. FS77-74426 dated November 23, 2018

Subscription index in the United Catalogue "Press of Russia" – 41255
You can subscribe to VSTU journals for 2025 on the website https://www.pressa-rf.ru/

The journal is included in the list of peer-reviewed scientific publications in which the main scientific results of dissertations should be published for the degree of candidate of science, for the degree of doctor of science

ADDRESS EDITORIAL:
394049, Voronezh, ul. Vatutina, 1
tel./fax: (473) 252-34-20

e-mail: alexanderostapenkoias@gmail.com

FOUNDER AND PUBLISHER:
Federal State State-Financed Comprehensive Institution
of High Education «Voronezh State Technical University»

ADRESS FOUNDER AND PUBLISHER:
394006, Voronezh, 20-letiya Oktyabrya str., 84

12+

**СОДЕРЖАНИЕ**

**CONTENS**

**DOI 10.36622/1682-7813.2025.28.3.001**
**УДК 004.588**

# МОДЕЛИРОВАНИЕ СЦЕНАРИЕВ АТАК КЛАССОВ «ПЕРЕПОЛНЕНИЕ БУФЕРА» И «ЗЛОУПОТРЕБЛЕНИЕ ПРИВИЛЕГИЯМИ» В КОРПОРАТИВНОЙ СЕТИ

**В.П. Лось, Р.С. Лопатин, Е.С. Петрова, Д.А. Щеглова, А.М. Лебедев, Д.С. Покудин**

Рассматриваются основные этапы построения сценариев на основе комбинации векторов атак и уязвимостей, связанных с типами ошибок CWE. Представляется методология этапов моделирования сценариев эксплуатации уязвимостей в корпоративных сетях для противодействия современным кибератакам. Применение классификаций CAPEC и баз данных, таких как БДУ ФСТЭК России, позволило систематизировать информацию о киберугрозах. Предложены примеры сценариев атак, включая «переполнение буфера» и «злоупотребление привилегиями», построенные в соответствии с MITRE ATT&CK. Данный подход позволяет спрогнозировать действия злоумышленников от возможных атак, обеспечивая при этом устойчивую работу корпоративных сетей.

Ключевые слова: переполнение буфера, злоупотребление привилегиями, тактики, техники, моделирование, сценарий.

## Введение

Проблема защиты корпоративных сетей от компьютерных атак приобретает сегодня все большее значение [1], ибо современные организации сталкиваются регулярно с масштабными кибератаками, которые нацелены на их информационные ресурсы. Это объективно требует внедрения комплексных мер технической и организационно-правовой защиты для автоматизированных информационных систем (АИС) и телекоммуникационных сетей (ТКС). Где нужно учитывать сочетание различных векторов атак и уязвимостей в этих системах, которые злоумышленники могут использовать для их компрометации [2].

В связи с этим, специалистам, отвечающим за защиту АИС и ТКС, необходимо управлять сотнями известных злоумышленных сценариев и тысячами выявленных уязвимостей, что приводит к появлению десятков тысяч возможных комбинаций угроз. Каждая такая комбинация требует индивидуального подхода и специфического реагирования со стороны средств и органов защиты, что значительно усложняет процесс обеспечения безопасности [2]. Наиболее эффективным средством в этом случае является превентивное моделирование сценариев кибератак, подкрепленное адекватным риск-анализом.

## Исходные данные, необходимые и достаточные, для моделирования сценариев эксплуатации уязвимостей

Для моделирования сценариев необходимо сформировать пару «техника – уязвимость».

В качестве задающего вектора атаки выступает CAPEC-шаблон. CAPEC (Common Attack Pattern Enumeration and Classification) – это общедоступный справочник, содержащий классификацию и описание распространенных паттернов атак, предназначенный для анализа и понимания типичных методов эксплуатации уязвимостей в приложениях. Этот ресурс помогает специалистам по информационной безопасности эффективно выявлять угрозы и разрабатывать меры защиты, изучая способы, которые используют злоумышленники для реализации кибератак [3, 4].

CAPEC-шаблон представляет собой описание общих методов и средств, которые злоумышленники применяют для эксплуатации известных уязвимостей в корпоративных системах [4].

Использование нормативных возможностей ресурса CAPEC позволяет от заданного вектора атаки перейти к

рассмотрению используемых ею типов ошибок CWE к соответствующим им уязвимостям CVE/BDU [4].

Существенным недостатком системы CAPEC можно выделить тот факт, что информационные блоки о векторе атаке перегружены «водой», поэтому следует отфильтровать информацию и занести ее в шаблонизированную описательную структуру (табл.1), позволяющую получить исчерпывающее представление об атаке и связанных с ней слабых мест и уязвимостей аппаратного и программного обеспечения.

Таблица 1

Шаблон паспорта вектора атаки

| **Наименование поля** | **Пояснение к полю** | |
|---|---|---|
| Идентификатор системы CAPEC | В данное поле заносится условный идентификатор CAPEC и переведенное название атаки.<br>**(Примечание**: перевод должен быть технически верным, грубый машинный перевод недопустим) | |
| Описание вектора атаки | В данное поле отражается необходимая и достаточная информация о векторе атаке. | |
| Тип атаки | В данном поле указывается к какому классу атаки относится вектор атаки | |
| Соотношение типа ошибки CWE и статуса типа ошибки CWE | В данную ячейку следует заносить CWE относящиеся к данному вектору атаки | В данную ячейку заносится статус CWE, который отображается на сайте CWE.org в поле «Vulnerability Mapping», а именно:<br>- разрешен для использования в реальных уязвимостях (ALLOWED);<br>- не рекомендован для использования в реальных уязвимостях (DISCOURAGED);<br>- запрещен для использования в реальных уязвимостях (PROHIBITED). |

В качестве связующего звена, позволяющего сопоставить связанные с вектором атаки уязвимости, выступает тип ошибки CWE [4]. Дающей возможность на первичном этапе получить выборку всех уязвимостей.

Выбор Банка данных угроз безопасности информации ФСТЭК России (далее – БДУ ФСТЭК России) в качестве основного датасета аргументируется содержанием в нем сведений как об отечественном, так и западном ПО. Дополнительно стоит отметить, что в БДУ ФСТЭК России приведены детально описанные паспорта уязвимостей, чем не могут похвастаться западные аналоги (такие как NIST NVD) [4, 5].

Детальность записей об уязвимостях дают возможным выбрать в качестве эталонной структуры паспорта уязвимости структурное описание приведенное ФСТЭК России [5].

Отечественная база уязвимостей включает в себя не только сведения об уязвимостях ПО, но и описание угроз безопасности информации [5].

Для дальнейшего исследования были выбраны следующие структурные поля, которые достаточны и необходимы: идентификатор типа ошибки, метрики оценки критичности, степень подтверждения существования уязвимости, наличие эксплойта, участие в инцидентах и способ устранения.

Паспорт уязвимости, исходя из вышеописанного, имеет вид (табл. 2).

Таблица 2

Шаблон паспорта уязвимости

| **Наименование поля** | **Пояснение к полю** |
|---|---|
| Идентификатор уязвимости | CVE: ****-*****:<br>Уязвимость ***, позволяющая *** |
| Идентификатор типа ошибки | CWE-*** |
| Базовый вектор уязвимости | CVSS 3.0: AV:*/AC:*/PR:*/UI:*/S:*/C:*/I:*/A:* |

Продолжение табл. 2

| Наименование поля | Пояснение к полю |
|---|---|
| Уровень опасности уязвимости | Низкий/ Средний/Высокий/Критический уровень опасности (базовая оценка CVSS 3.0 составляет ***) |
| Статус уязвимости | Подтверждена производителем/ Подтверждена в ходе исследований/ Потенциальная уязвимость |
| Наличие эксплойта | Существует/ Существует в открытом доступе/ Данные уточняются |
| Способ устранения | *** |
| Участие в инцидентах | Да/Нет |

**Методика моделирования сценариев эксплуатации уязвимостей компьютерными атаками**

Имея необходимые исходные данные, можно приступить к моделированию сценария. Для этого следует, опираясь на шаблон атаки, выделить наиболее характерные техники MITR ATT&CK и соотнеся с уязвимостями выстроить предположительную цепочку действий злоумышленника в рамках заданного шаблона CAPEC.

Суть заключается в том, что имеется множество уязвимостей, эксплуатация которых приводит к использованию той или иной техники, в результате чего формируется множество путей реализации атаки (рис. 1).

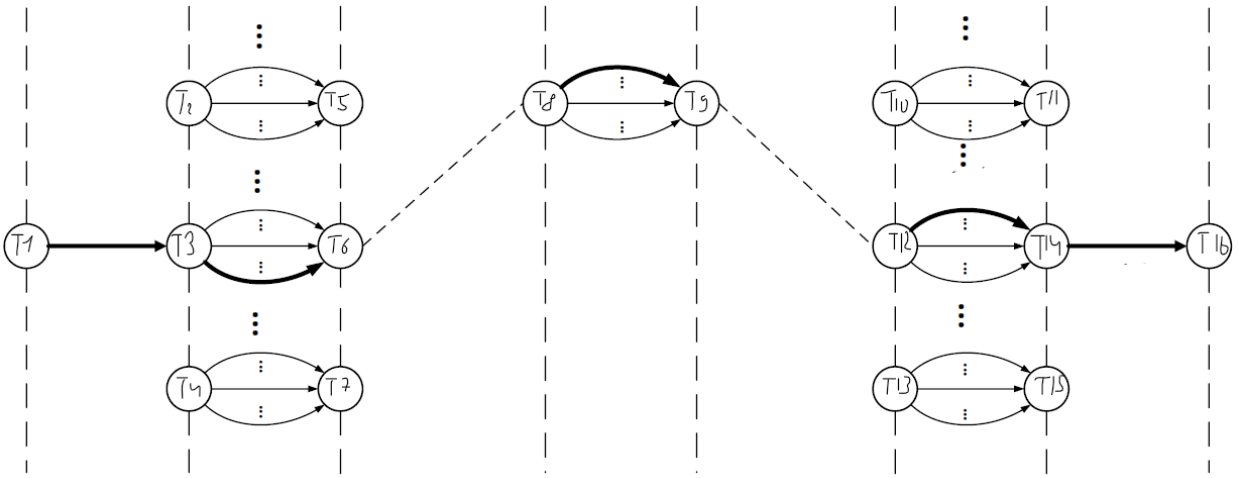


Рис. 1. Тактики реализации атаки

Для дальнейшего риск-анализа имеется возможным произвести отбор атак исходя из следующих критериев:

- максимальная вероятность (наиболее ожидаемый вариант);
- максимум ущерба (наихудший вариант);
- максимальный риск (рабочий вариант).

В результате может быть выделен один путь реализации атаки, с которым в дальнейшем и следует работать.

**Моделирование сценариев атак класса «Переполнение буфера»**

Переполнение буфера один из наиболее часто используемых векторов эксплуатации уязвимостей. Последствия встречи злоумышленника с уязвимым к переполнению буфера кодом могут варьироваться от раскрытия конфиденциальных данных до полного захвата системы.

Подобные атаки, а также растущее число зарегистрированных уязвимостей в базах данных показывают необходимость изучать данные уязвимости и способы защиты от них.

В качестве представителя класса «Переполнение буфера» выступит CAPEC-540 «Избыточное чтение буфера», так как согласно материалам CQR (представляющей комплексные услуги по обеспечению ИТ-безопасности) данный тип переполнения

буфера является наиболее часто встречающимся [7].

Паспорт CAPEC-540 имеет следующий вид (табл. 3) [3].

Таблица 3

Паспорт вектора атаки CAPEC-540

| | | |
|---|---|---|
| Идентификатор системы CAPEC | CAPEC-540<br>Избыточное чтение буфера | |
| Описание вектора атаки | Злоумышленник атакует цель, предоставляя входные данные, которые заставляют приложение выполнять чтение за пределами допустимой области памяти буфера. | |
| Тип атаки | Переполнение буфера | |
| Соотношение типа ошибки CWE и статуса типа ошибки CWE | CWE-125:<br>Чтение за границами буфера | Разрешен для использования в реальных уязвимостях |

Далее необходимо выделить связанные с CAPEC-540 через CWE-125 уязвимости (рис. 2).

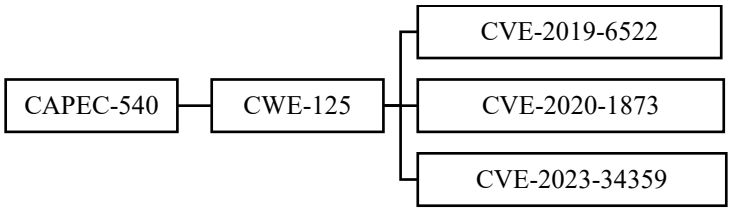



Рис. 2. Связанные с CAPEC – 540 уязвимости

Среднеквадратичная оценка критичности уязвимостей представлена в табл. 4.

Таблица 4

Среднеквадратичная оценка критичности уязвимостей для CAPEC-540

| **Уязвимость** | **Значение критичности** |
|---|---|
| CVE-2019-6522 | 0.65 |
| CVE-2020-1873 | 0.75 |
| CVE-2023-34359 | 0.73 |

Получив среднеквадратичные оценки критичности уязвимостей, можно приступить к моделированию сценария атаки, где следует соотнести техники и тактики с уязвимостями для CAPEC-540 (табл. 5).

Таблица 5

Соотнесение техник и тактик с уязвимостями для CAPEC-540

| **Техника** | **Тактика** | **Уязвимости, эксплуатация которых приводит к технике** |
|---|---|---|
| T1659: Content Injection | Первоначальный доступ | CVE-2019-6522 |
| T1059: Command and Scripting Interpreter | Выполнение | CVE-2020-1873<br>CVE-2019-6522 |
| T1203: Exploitation for Client Execution | | CVE-2020-1873<br>CVE-2019-6522 |
| T1562: Impair Defenses | Предотвращение обнаружения | CVE-2023-34359<br>CVE-2020-1873 |
| T1003: OS Credential Dumping | Получение учетных данных | CVE-2023-34359 |
| T1040: Network Sniffing | Изучение | CVE-2019-6522<br>CVE-2020-1873 |
| T1113: Screen Capture | Сбор данных | CVE-2023-34359 |
| T1056: Input Capture | Сбор данных | CVE-2019-6522 |

Продолжение табл. 5

| **Техника** | **Тактика** | **Уязвимости, эксплуатация которых приводит к технике** |
|---|---|---|
| T1048: Exfiltration Over Alternative Protocol | Эксфильтрация данных | CVE-2020-1873<br>CVE-2023-34359 |
| T1020: Automated Exfiltration | | CVE-2019-6522<br>CVE-2023-34359 |
| T1495: Firmware Corruption | Деструктивное воздействие | CVE-2019-6522 |
| T1491: Defacement | | CVE-2023-34359<br>CVE-2019-6522<br>CVE-2020-1873 |

Для наглядности визуализации на рис. 3-5 будет представлен сценарий атаки для CAPEC-540, где цифрами 1 – 20 обозначены уязвимости:

1) CVE-2019-6522;
2) CVE-2020-1873;
3) CVE-2019-6522;
4) CVE-2020-1873;
5) CVE-2019-6522;
6) CVE-2023-34359;
7) CVE-2020-1873;
8) CVE-2023-34359;
9) CVE-2019-6522;
10) CVE-2020-1873;
11) CVE-2023-34359;
12) CVE-2019-6522;
13) CVE-2020-1873;
14) CVE-2023-34359;
15) CVE-2019-6522;
16) CVE-2023-34359;
17) CVE-2019-6522;
18) CVE-2023-34359;
19) CVE-2019-6522;
20) CVE-2023-34359.

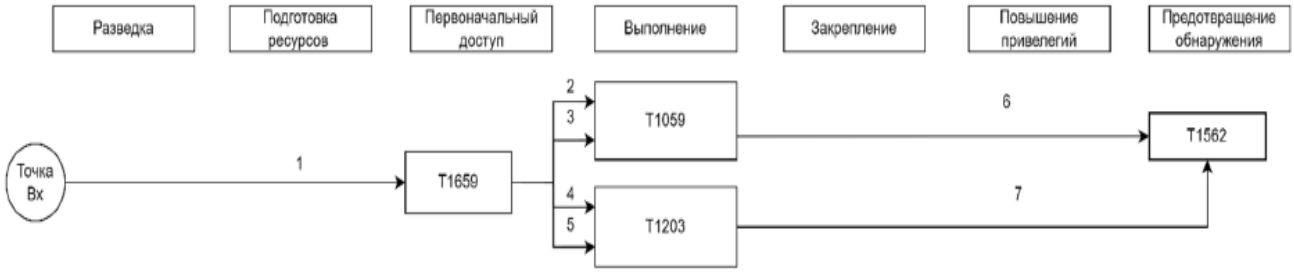



Рис. 3. Сценарий атаки CAPEC-540


Рис. 4. Сценарий атаки CAPEC-540 (продолжение)

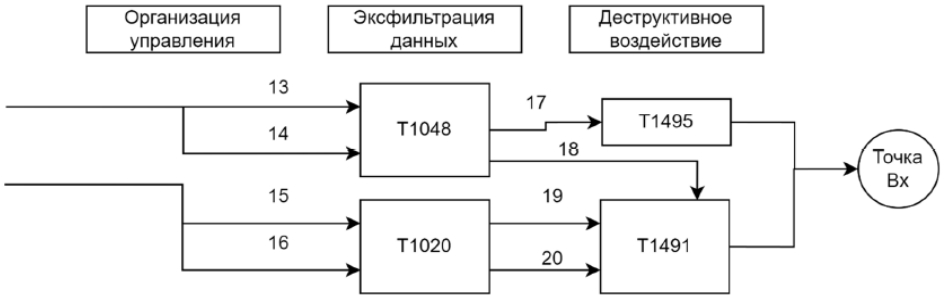



Рис. 5. Сценарий атаки CAPEC-540 (продолжение)

Для дальнейшего риск-анализа следует произвести выборку варианта реализации атаки по следующему критерию: максимальный риск.

Произведя выборку, получим путь реализации атаки с максимальным риском, с которым в дальнейшем и будем работать.

У каждого из сценариев имеются разветвления, поэтому разобьем каждый сценарий на несколько подсценариев по количеству имеющихся веток. Каждый подсценарий разобьем на микромодели. Для каждой микромодели отметим вероятность уязвимости, которая будет проэксплуатирована для перехода к следующей технике, и укажем ущерб, наносимый системе.

Расчет вероятности успеха единичной атаки вычисляется по следующей формуле (1):

$$P_i = \frac{\overline{K_i}}{\sum_i \overline{K_i}}, \qquad (1)$$

где $K_i$ - критичной *i*-той уязвимости.

Ущерб единичной атаки вычисляется следующим образом (2):

$$U = 1 - (1-U_к)(1-U_д)(1-U_ц), \qquad (2)$$

где Uк – ущерб конфиденциальности,
Uд – ущерб доступности,
Uц – ущерб целостности.

Формула (3), позволяет произвести оценку риска возникающего при реализации избранного сценария атаки CAPEC-540:

$$Risk = \prod_i p_i \times \sum_j U_j, \qquad (3)$$

где $p_i$ – вероятность эксплуатации *j*-ой уязвимости посредством реализации техники $T_i$;

$U$ – ущерб, наносимый атакуемой системе в результате эксплуатации уязвимости $CVE_j$ в ходе реализации техники $T_i$.

Для начала разобьем сценарий атаки для CAPEC-540 на микромодели (табл. 6-19, рис. 6-19).

Разбиение на микромодели дает произвести более внимательную оценка вероятности успеха и ущерба уязвимостей на конкретном участке проведения общей атаки.

Таблица 6

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели № 1

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 1 | CVE-2019-6522 | 1 | 0,75 |


Рис. 6. Микромодель № 1 для CAPEC-540

Таблица 7

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели № 2

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 2 | CVE-2020-1873 | 0,54 | 0,5 |
| 3 | CVE-2019-6522 | 0,46 | 0,75 |

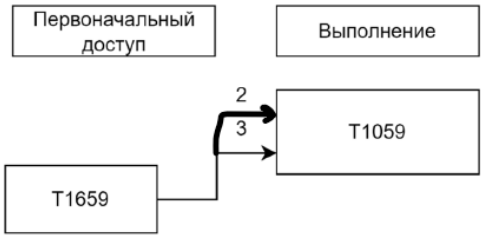



Рис. 7. Микромодель № 2 для CAPEC-540

Таблица 8

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели № 3

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 4 | CVE-2020-1873 | 0,54 | 0,5 |
| 5 | CVE-2019-6522 | 0,46 | 0,75 |

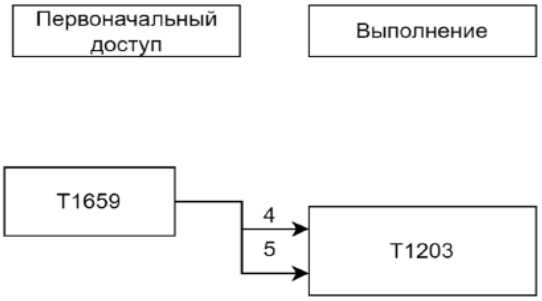



Рис. 8. Микромодель № 3 для CAPEC-540

Таблица 9

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели № 4

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 6 | CVE-2023-34359 | 1 | 0,5 |

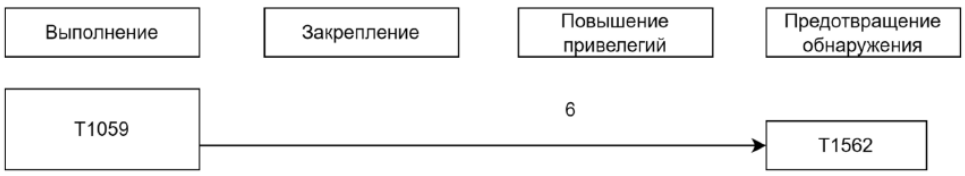



Рис. 9. Микромодель № 4 для CAPEC-540

Таблица 10

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели № 5

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 7 | CVE-2020-1873 | 1 | 0,5 |

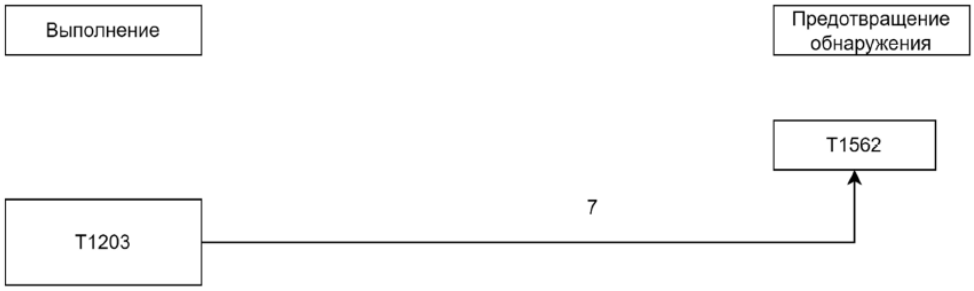



Рис. 10. Микромодель № 5 для CAPEC-540

Таблица 11

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели № 6

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 8 | CVE-2023-34359 | 1 | 0,5 |

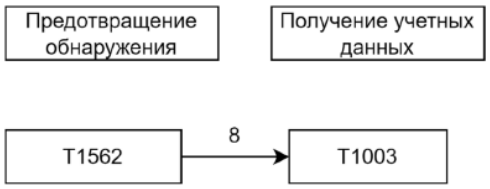



Рис. 11. Микромодель № 6 для CAPEC-540

Таблица 12

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели № 7

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 9 | CVE-2019-6522 | 0,47 | 0,75 |
| 10 | CVE-2020-1873 | 0,53 | 0,5 |

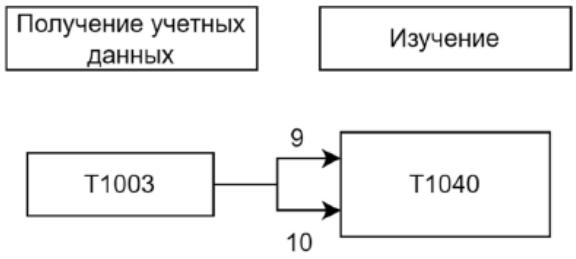



Рис. 12. Микромодель № 7 для CAPEC-540

Таблица 13

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели № 8

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 11 | CVE-2023-34359 | 1 | 0,5 |


Рис. 13. Микромодель № 8 для CAPEC-540

Таблица 14

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели № 9

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 12 | CVE-2019-6522 | 1 | 0,75 |


Рис. 14. Микромодель № 9 для CAPEC-540

Таблица 15

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели № 10

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 13 | CVE-2020-1873 | 0,51 | 0,5 |
| 14 | CVE-2023-34359 | 0,49 | 0,5 |

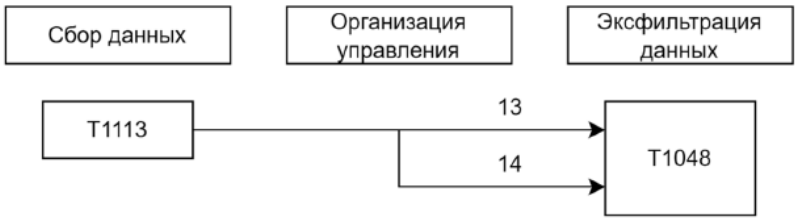



Рис. 15. Микромодель № 10 для CAPEC-540

Таблица 16

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели № 11

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 15 | CVE-2019-6522 | 0,47 | 0,75 |
| 16 | CVE-2023-34359 | 0,53 | 0,5 |

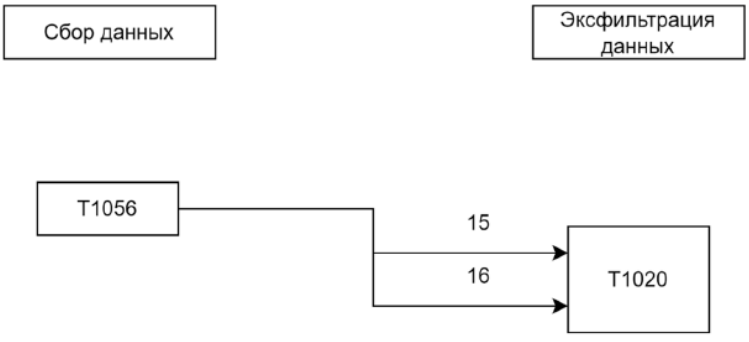



Рис. 16. Микромодель № 11 для CAPEC-540

Таблица 17

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели № 12

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 17 | CVE-2019-6522 | 1 | 0,75 |

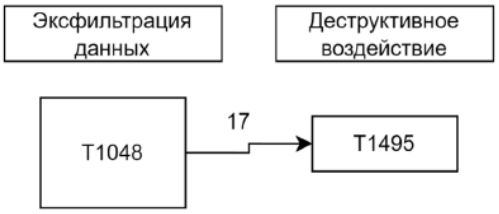



Рис. 17. Микромодель № 12 для CAPEC-540

Таблица 18

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели № 13

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 18 | CVE-2023-34359 | 1 | 0,5 |

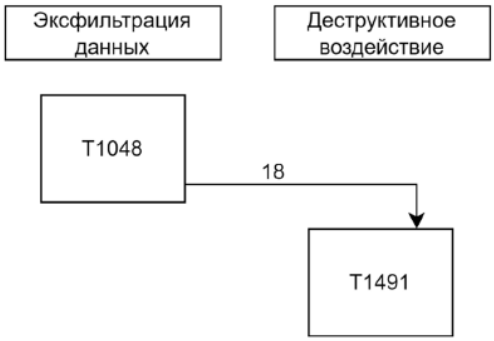



Рис. 18. Микромодель № 13 для CAPEC-540

Таблица 19

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели № 14

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 19 | CVE-2019-6522 | 0,47 | 0,75 |
| 20 | CVE-2023-34359 | 0,53 | 0,5 |

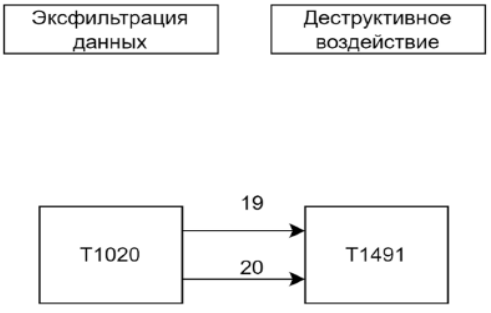



Рис. 19. Микромодель № 14 для CAPEC-540

Как видно из приведенного выше дробления общего сценария на 6 более мелких подсценариев, на каждом подсценарии выделяются значительные риски, а затем среди них находится максимальный и он непосредственно наносится на общий сценарий и впоследствии регламентация защиты будет производиться для этого выделенного пути.

Самый больший риск из всех возможных имеет путь: T1659 (CVE-2019-6522) -> T1203 (CVE-2020-1873) -> T1562 (CVE-2020-1873) -> T1003 (CVE-2023-34359) -> T1040 (CVE-2020-1873) -> T1113 (CVE-2023-34359) -> T1048 (CVE-2020-1873) -> T1495 (CVE-2019-6522) (Risk: 0.6568).

Отобразим этот путь на общем сценарии (рис. 20, 21).


Рис. 20. Сценарий атаки CAPEC-540 с выделенным путем по максимальному значению риска


Рис. 21. Сценарий атаки CAPEC-540 с выделенным путем по максимальному значению риска (продолжение)

Приведенный выше риск-анализ показал, что, своевременно рассчитывая риски реализации обнаруженных угроз можно спрогнозировать и адаптировать стратегию защиты организации, в условиях стремительно меняющегося ландшафта угроз, что позволяет ликвидировать или минимизировать «внезапный удар» злоумышленника и нивелировать дополнительные затраты, в случае успешности атаки если же не был проведен качественный и своевременный риск-анализ.

Описанное выше показывает, что Нарушение информационной безопасности может привести к многочисленным и серьезным последствиям, затрагивающим как организации, так и отдельных пользователей. При утечке конфиденциальной информации возможны финансовые потери, связанные с восстановлением утраченных данных и репутационными рисками. Ущерб для репутации может означать потерю доверия со стороны клиентов и партнеров, что в свою очередь усложняет привлечение новых пользователей и может привести к снижению доходов.

Кроме того, атаки киберпреступников могут вызвать сбои в работе систем, что затрудняет выполнение бизнес-процессов и может привести к задержкам в производстве или оказании услуг. Также существует риск юридических последствий, если произошедшее нарушение повлечет за собой несоответствие требованиям законодательства по защите данных.

В отличие от аналогов, впервые аккумулированы экспертные и статистические метрики частот реализации атак класса «Переполнение буфера» и критичности уязвимостей защищаемых корпоративных систем, что позволяет создать база данных метрик атак класса «Переполнение буфера» и уязвимостей защищаемых корпоративных систем

являющихся практической основой для риск-калькуляции единичных вторжений, а также сформированная база метрик открыта для ее расширения на другие атакуемые объекты и для многовариантного анализа корреляций входящих в нее данных.

**Моделирование сценариев атак класса «Злоупотребление привилегиями»**

«Злоупотребление привилегиями» можно описать следующим образом: злоумышленник может использовать функции цели, которые должны быть зарезервированы для привилегированных пользователей или администраторов, но доступны для использования учетными записями с более низкими или непривилегированными правами. Доступ к конфиденциальной информации и функциям должен контролироваться, чтобы гарантировать, что только авторизованные пользователи смогут получить доступ к этим ресурсам.

Наиболее «ярко» класс «Злоупотребление привилегиями» характеризует CAPEC-650 «Загрузка веб-оболочки на веб-сервер», это подтверждают материалы CQR [8].

Паспорт CAPEC-650 имеет следующий вид (табл. 20) [3].

Таблица 20

Паспорт вектора атаки CAPEC-650

| | | |
|---|---|---|
| Идентификатор системы CAPEC | CAPEC-650<br>Загрузка веб-оболочки на веб-сервер | |
| Описание вектора атаки | Используя недостаточные расширения, злоумышленник может загрузить веб-оболочку на веб-сервер таким образом, чтобы она могла выполняться удаленно. Эта оболочка может обладать различными возможностями, выступая в качестве «шлюза» к базовому веб-серверу. | |
| Тип атаки | Злоупотребление привилегиями | |
| Соотношение типа ошибки CWE и статуса типа ошибки CWE | CWE-287:<br>Неправильная аутентификация | Не рекомендован для использования в реальных уязвимостях |

Посредством типа ошибки CWE-287 с CAPEC-650 связаны следующие уязвимости (рис. 22).

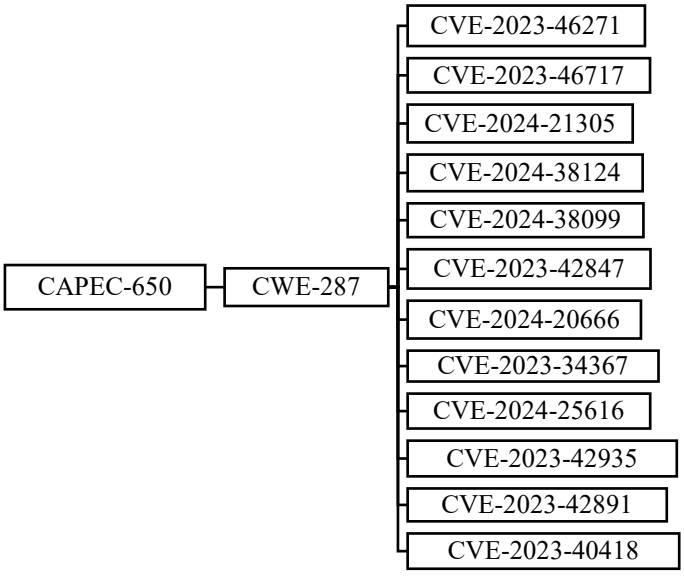



Рис. 22. Связанные с CAPEC-650 уязвимости

Среднеквадратичная оценка критичности уязвимостей представлена в табл. 21.

Таблица 21

Среднеквадратичная оценка критичности уязвимостей для CAPEC-650

| **Уязвимость** | **Значение критичности** |
|---|---|
| CVE-2024-38124 | 0.72457 |
| CVE-2024-38099 | 0.65611 |
| CVE-2023-46271 | 0.75778 |
| CVE-2023-46717 | 0.56332 |
| CVE-2024-25616 | 0.41062 |
| CVE-2023-42935 | 0.60546 |
| CVE-2022-48618 | 0.72006 |
| CVE-2024-22394 | 0.78129 |
| CVE-2024-20666 | 0.62562 |
| CVE-2024-21305 | 0.47236 |
| CVE-2023-42891 | 0.54932 |
| CVE-2023-42847 | 0.73349 |
| CVE-2023-40418 | 0.56104 |
| CVE-2023-34367 | 0.53881 |
| CVE-2023-28963 | 0.57828 |

Получив среднеквадратичные оценки критичности уязвимостей, можно приступить к моделированию сценария атаки. Перед моделированием следует соотнести техники и тактики с уязвимостями для CAPEC-650 (табл. 22).

Таблица 22

Соотнесение техник и тактик с уязвимостями для CAPEC-650

| **Тактика** | **Техника** | **Уязвимости, эксплуатация которых приводит к технике** |
|---|---|---|
| Первоначальный доступ | Exploit Public-Facing Application (T1190) | CVE-2024-38124<br>CVE-2023-46271 |
| Выполнение | Command and Scripting Interpreter: PHP (T1059.005) | CVE-2024-25616 |
| | Shared Modules (T1072) | CVE-2024-21305 |
| | Exploitation for Execution (T1203) | CVE-2024-22394 |
| Закрепление | Web Shell (T1505.003) | CVE-2023-42847<br>CVE-2023-42891 |
| Обнаружение | File and Directory Discovery (T1083) | CVE-2023-34367 |
| Предотвращение обнаружения | Modify Registry (T1112) | CVE-2023-40418 |
| Сбор данных | Data from Local System (T1005) | CVE-2023-34367 |
| Деструктивное воздействие | Data Destruction (T1485) | CVE-2024-22394<br>CVE-2024-38124 |

Для наглядности и визуализации на рис. 23 представлен сценарий атаки для CAPEC-650.

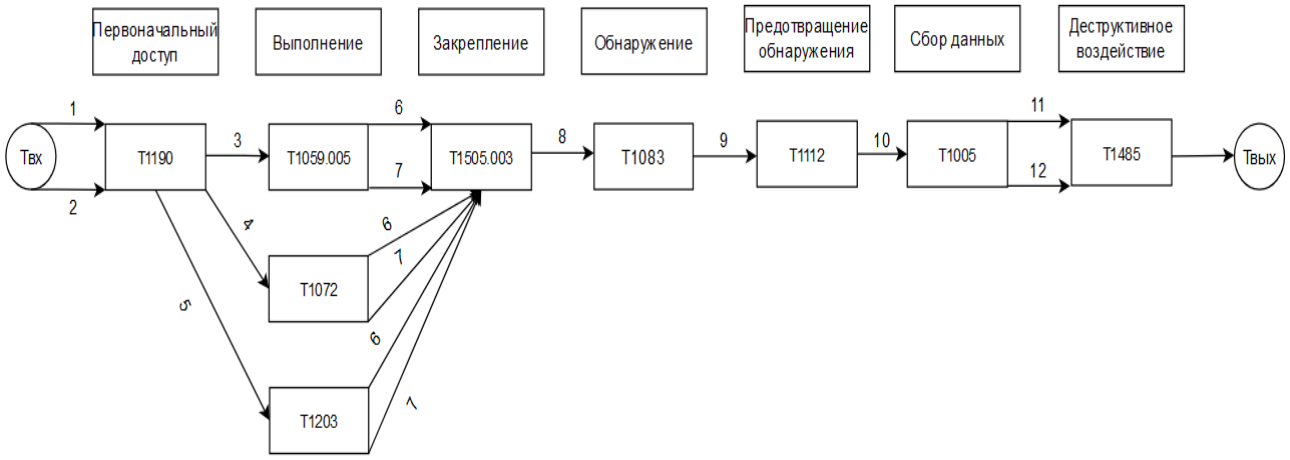



Рис. 23. Сценарий атаки CAPEC – 650

Для обозначения уязвимостей используем следующие сокращения:

1) CVE-2024-38124;
2) CVE-2023-46271;
3) CVE-2024-25616;
4) CVE-2024-21305;
5) CVE-2024-22394;
6) CVE-2023-42847;
7) CVE-2023-42891;
8) CVE-2023-34367;
9) CVE-2023-40418;
10) CVE-2023-34367;
11) CVE-2024-22394;
12) CVE-2024-38124.

Разобьем сценарий атаки для CAPEC-650 на микромодели (табл. 23-31, рис. 24-34).

Разбиение на микромодели дает произвести более внимательную оценка вероятности успеха и ущерба уязвимостей на конкретном участке проведения общей атаки.

Таблица 23

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели 1 для сценария CAPEC-58

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 1 | CVE-2024-38124 | 0.48 | 0.875 |
| 2 | CVE-2023-46271 | 0.52 | 0.875 |

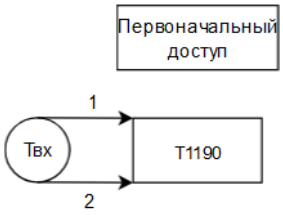



Рис. 24. Микромодель 1 для CAPEC-650

Таблица 24

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели 2 для сценария CAPEC-58

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 1 | CVE-2024-25616 | 1 | 0.2 |

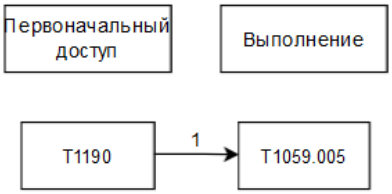



Рис. 25. Микромодель 2 для CAPEC-650

Таблица 25

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели 3 для сценария CAPEC-650

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 1 | CVE-2024-21305 | 1 | 0.5 |

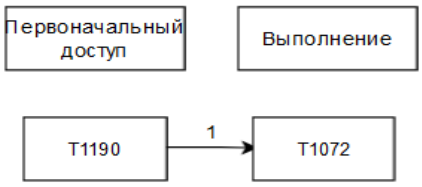



Рис. 26. Микромодель 3 для CAPEC-650

Таблица 26

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели 4 для сценария CAPEC-650

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 1 | CVE-2024-22394 | 1 | 0.5 |

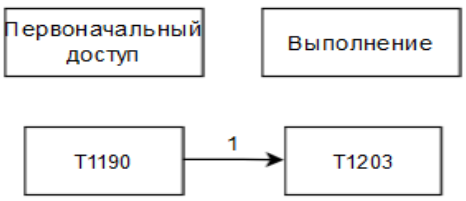



Рис. 27. Микромодель 4 для CAPEC-650

Таблица 27

Вероятность эксплуатации единичной уязвимости и ущерб для микромоделей 5, 6 и 7 для сценария CAPEC-650

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 1 | CVE-2023-42847 | 0.50447 | 0.5 |
| 2 | CVE-2023-42891 | 0.49553 | 0.5 |


Рис. 28. Микромодель 5 для CAPEC-650


Рис. 29. Микромодель 6 для CAPEC-650

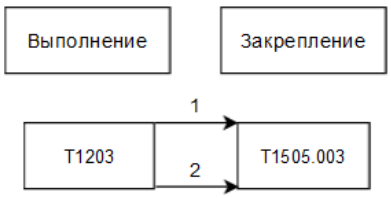



Рис. 30. Микромодель 7 для CAPEC-650

Таблица 28

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели 8 для сценария CAPEC-650

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 1 | CVE-2023-34367 | 1 | 0.36 |


Рис. 31. Микромодель 8 для CAPEC-650

Таблица 29

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели 9 для сценария CAPEC-650

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 1 | CVE-2023-40418 | 1 | 0.5 |

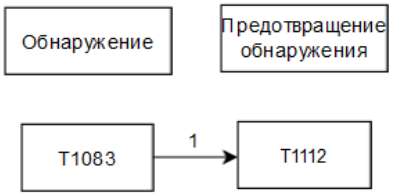



Рис. 32. Микромодель 9 для CAPEC-650

Таблица 30

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели 10 для сценария CAPEC-650

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 1 | CVE-2023-34367 | 1 | 0.36 |

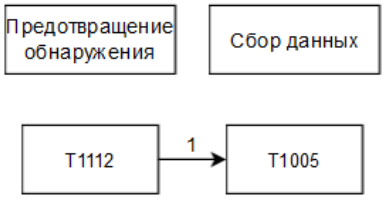



Рис. 33. Микромодель 10 для CAPEC-650

Таблица 31

Вероятность эксплуатации единичной уязвимости и ущерб для микромодели 11 для сценария CAPEC-650

| № | Уязвимость | Вероятность успеха | Ущерб |
|---|---|---|---|
| 1 | CVE-2024-22394 | 0.49 | 0.5 |
| 2 | CVE-2024-38124 | 0.51 | 0.875 |

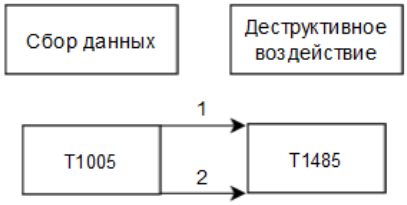



Рис. 34. Микромодель 11 для CAPEC-650

Для данного сценария атаки получилось 3 подсценария.

Наибольший риск: T1190 (CVE-2023-46271) -> T1203 (CVE-2024-22394) -> T1505.003 (CVE-2023-42847) -> T1083 (CVE-2023-34367) -> T1112 (CVE-2023-40418) -> T1005 (CVE-2023-34367) -> T1485 (CVE-2024-38124) (Risk: 0.5310).

Отобразим этот путь на общем сценарии (рис. 35).

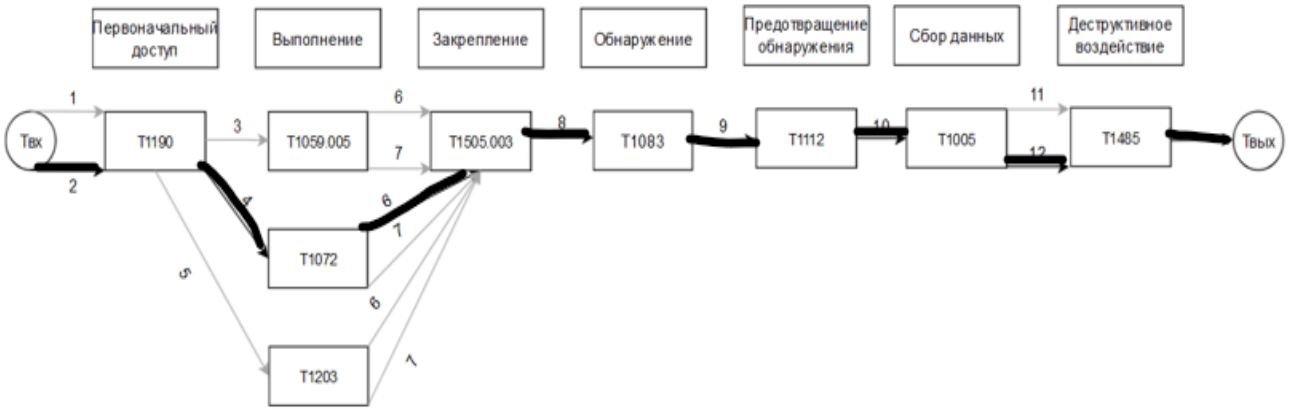



Рис. 35. Сценарий атаки CAPEC-650 с выделенным путем по максимальному значению риска

Проведённое исследование демонстрирует, что улучшение безопасности корпоративных сетей от кибератак типа «злоупотребление привилегиями» требует комплексного подхода, включающего оценку и управление рисками успешности атак. Представленная в статье методология оценки рисков даёт возможность количественно определить вероятность и потенциальный ущерб от таких атак, а также выбрать наиболее эффективные способы их предотвращения.

Предложенная методология оценки и управления рисками успешности кибератак типа «злоупотребление привилегиями» является действенным инструментом для обеспечения безопасности корпоративных сетей. Внедрение предложенных мер защиты способствует повышению устойчивости сетей к таким атакам и снижению связанных с ними рисков.

В дальнейшем исследования в этой области могут быть направлены на разработку более совершенствованных методов оценки и управления рисками, а также на изучение новых типов кибератак и разработку соответствующих мер защиты.

**Заключение**

Проведенное исследование подтвердило высокую значимость моделирования сценариев эксплуатации уязвимостей для обеспечения информационной безопасности корпоративных сетей. Анализ показал, что использование пар «вектор атаки – уязвимость» в сочетании с классификациями CAPEC и CWE позволяет эффективно выявлять критически опасные уязвимости, а также разрабатывать регламентированные меры противодействия кибератакам на основе сценариев.

Новизна заключается в том, что исключительно для атак класса «переполнение буфера» и «злоупотребление привилегиями» впервые предложена графовая локализация, иллюстрирующая корреляцию их с уязвимостями защищаемых корпоративных систем.

Практическая ценность видится в том, что роща графов-деревьев, практически отражает географию причинно-следственных связей пар «атака-уязвимость» в проектной деятельности защиты корпоративных систем от атак класса «переполнение буфера» и «злоупотребление привилегиями».

Методика построения сценариев, основанная на последовательности этапов MITRE ATT&CK, обеспечивает структурированность подхода, что способствует улучшению прогнозирования и минимизации последствий атак. Примеры сценариев эксплуатации, такие как атаки на основе «переполнения буфера» и «злоупотребления привилегиями», наглядно демонстрируют важность комплексного анализа угроз для создания устойчивой системы защиты.

На основе методологии оценки рисков разработана система регулирования рисков, которая включает в себя технические, организационные меры безопасности. Технические меры включают использование безопасных языков программирования, средств контроля потока данных, а также внедрение межсетевых экранов и систем обнаружения вторжений. Организационные меры предусматривают обучение персонала мерам безопасной работы.

Таким образом, использованная в данной работе методология оценки и регулирования рисков успешности кибератак класса «Переполнение буфера» является эффективным инструментом обеспечения безопасности корпоративных сетей. Реализация предложенных мер безопасности позволяет повысить устойчивость сетей к подобным атакам и минимизировать связанные с ними риски.

Дальнейшие исследования в этой области могут быть сосредоточены на разработке более совершенных методов оценки и регулирования рисков, а также на изучении новых типов кибератак и разработке соответствующих мер противодействия, а также расширить применение предложенных подходов на автоматизированные системы управления корпоративных сетей. Такой подход позволит усилить защиту информационного пространства и минимизировать риски, связанные с эксплуатацией уязвимостей.

## Список литературы

1 Моделирование компьютерных атак на распределенную информационную систему / А. А. Корниенко, А. Б. Никитин, С. В. Диасамидзе, Е. Ю. Кузьменкова // Известия ПГУПС, 2018. В. № 4. С. 613-615.

2 Организационно-правовая защита сетей / Г. А. Остапенко, Д. В. Щербакова, А. О. Калашников и др.; под ред. Академика РАН Д. А. Новикова. М.: Горячая линия Телеком, 2023. 228с.

3 The Common Attack Pattern Enumeration and Classification (CAPEC). URL: https://capec.mitre.org (дата обращения: 10.07.2025).

4 Остапенко Г.А. Формализация знаний и данных кибератак и уязвимостей / Г.А. Остапенко, А.П. Васильченко, А.А. Остапенко, Д.С. Покудин [и другие] // Информация и безопасность. 2024. Т. 27. Вып. 2. С. 231-238.

5 Банк данных угроз безопасности информации ФСТЭК. URL: https: bdu.fstec.ru/threat (дата обращения: 10.07.25).

6 MITRE ATT&CK. URL: https://attack.mitre.org/matrices/enterprise (дата обращения: 10.07.2025).

7 Переполнение буфера. URL: https://cqr.company/ru/web-vulnerabilities/file-upload-vulnerabilities (дата обращения: 10.07.2025).

8 Уязвимости при загрузке файлов. URL: https://cqr.company/ru/web-vulnerabilities/file-upload-vulnerabilities (дата обращения: 10.07.2025)

Российский государственный гуманитарный университет
Russian State University for the Humanities

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 17.07.2025

**Информация об авторах**

**Лось Владимир Павлович** – д-р воен. наук, профессор, Российский государственный гуманитарный университет, e-mail: los.vp@rea.ru

**Лопатин Роман Сергеевич** – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: lopatinr@mail.ru

**Петрова Елена Сергеевна** – старший преподаватель, Воронежский государственный технический университет, e-mail: lenoks.sokolova@mail.ru

**Щеглова Дарья Александровна** – студент, Воронежский государственный технический университет, e-mail: dasha.shcheglova.00@mail.ru

**Лебедев Антон Михайлович** – студент, Воронежский государственный технический университет, e-mail: anton05102001@mail.ru

**Покудин Данила Сергеевич** – аспирант, Воронежский государственный технический университет, e-mail: danila.pokudin@inbox.ru

# MODELING CLASS ATTACK SCENARIOS "BUFFER OVERFLOW" AND "ABUSE OF PRIVILEGES" IN THE CORPORATE NETWORK

**V.P. Los, R.S. Lopatin, E.S. Petrova, D.A. Shcheglova, A.M. Lebedev, D.S. Pokudin**

The main stages of building scenarios based on a combination of attack vectors and vulnerabilities related to CWE error types are considered. The methodology of the stages of modeling scenarios for exploiting vulnerabilities in corporate networks to counter modern cyber-attacks is presented. The use of CAPEC classifications and databases, such as the database of the FSTEC of Russia, made it possible to systematize information about cyber threats. Examples of attack scenarios are proposed, including "buffer overflow" and "privilege abuse", built in accordance with MITRE ATT&CK. This approach allows you to predict the actions of intruders from possible attacks, while ensuring the stable operation of corporate networks.

Keywords: attack vector, vulnerability, scenario, cyberattack, corporate network.

Submitted 17.07.2025

**Information about the authors**

**Vladimir P. Los** – Dr. Sc. (Military), Professor, Russian State University for the Humanities, e-mail: los.vp@rea.ru
**Roman S. Lopatin** – Cand. Sc. (Technical), Associate Professor, Voronezh State Technical University, e-mail: lopatinr@mail.ru
**Elena S. Petrova –** senior lecturer, Voronezh State Technical University, e-mail: lenoks.sokolova@mail.ru
**Daria A. Shcheglova** – student, Voronezh State Technical University, e-mail: dasha.shcheglova.00@mail.ru
**Anton M. Lebedev –** student, Voronezh State Technical University, e-mail: anton05102001@mail.ru
**Danila S. Pokudin** – postgraduate student, Voronezh State Technical University, e-mail: danila.pokudin@inbox.ru

**DOI 10.36622/1682-7813.2025.28.3.002**
**УДК 621.372.004**

# АВТОМАТИЗАЦИЯ ОЦЕНКИ И РЕГУЛИРОВАНИЯ РИСКОВ РЕАЛИЗАЦИИ КИБЕРАТАК: МОТИВАЦИЯ И ЦЕЛЕПОЛАГАНИЕ СОЗДАНИЯ ПРОГРАММНО-ТЕХНИЧЕСКОГО КОМПЛЕКСА

**Г.А. Остапенко, А.А. Остапенко, М.В. Кондратьев, А.С. Кривошеин, Д.С. Печкин**

Обосновывается целесообразность разработки программно-технического комплекса, обеспечивающего оценку и регулирование рисков реализации кибератак за счет создания модулей: сбора, обработки и хранения данных о них; генерации сценариев и мер противодействия им. Предлагается целеполагание исследования, базирующееся на анализе актуальности киберзащиты автоматизированных систем в контексте роста количества и изощренности компьютерных атак, констатации противоречий в подходах к обеспечению информационной безопасности, а также недостатках современных средств противодействия. Оцениваются ожидаемые новизна, практическая ценность и теоретическая значимость реализуемой разработки.

Ключевые слова: кибербезопасность, программно-технический комплекс, оценка рисков, кибератаки, автоматизированные системы, генерация сценариев, машинное обучение.

## Введение

Революционная цифровая трансформация мира превратила киберугрозы в настоящее оружие массового поражения для государственных и коммерческих структур. Это подтверждается тем, что с каждым годом инвестиции в кибербезопасность увеличиваются на миллиардные суммы, так в России в 2024 году вложения в средства защиты данных достигли 23 миллиардов рублей [1]. Но все же, несмотря на мировые инвестиции в повышение уровня информационной безопасности, тренд роста масштаба угроз для современного киберпространства укрепляется с каждым годом все сильнее.

В свете стремительного развития цифровых технологий привычные популярные средства обеспечения информационной безопасности теряют свою эффективность и устаревают, что нельзя сказать об изощренности атак злоумышленников, которые все чаще используют нейросетевой инструментарий в ходе своих вторжений. К тому же в настоящее время Россия держит оборону против самого настоящего цифрового терроризма, который совершает попытки нападений, парализующие отечественную инфраструктуру, такую как государственные структуры, банки, промышленность и многие другие секторы, тесно связанные с информатизацией.

В таких условиях сохранение безопасного и эффективного киберпространства требует развития средств обеспечения информационной безопасности и разработки решений, способных быстро адаптироваться к новым вызовам, что несомненно должно включать в себя этапы реализации через такие современные технологии, как машинное обучение (для быстрого и адаптивного анализа киберугроз) и использование новых средств разработки (для создания высокопроизводительных систем с максимальной точностью работы реализуемого программного обеспечения). Решения, направленные на обеспечение безопасности информации, должны предоставлять комплекс мер снижающих потенциальный ущерб от атак, предотвращая их еще на ранних стадиях вторжений, что является приоритетной задачей, так как восстановление инфраструктуры обходится организациям намного дороже мер по защите от таких инцидентов.

**Объектом исследования** выступают автоматизированные системы и сети, подвергающиеся кибератакам.

**Предметом исследования** являются методики и алгоритмы обеспечения автоматизированной генерации мер и сценариев противодействия кибератакам.

**Актуальность исследования** обусловлена наличием ряда противоречий, выявленных в ходе анализа аналогов, между:

1) необходимостью учета современных тенденций развития киберугроз для разработки эффективных и долгосрочных решений для защиты информации и отсутствием этого в методах большинства существующих аналогов;

2) потребностью учета взаимосвязей между компонентами кибератак для обеспечения комплексной безопасности информации и узконаправленным подходом большинства аналогов, ориентированных на локальное устранение конкретных уязвимостей;

3) необходимостью в обеспечении высокой информативности и адаптивности методов генерации сценариев кибератак и применением большинством аналогов моделей с линейным развитием атак, ограничивающих учет множества возможных путей реализации атак;

4) потребностью в формировании универсальных мер противодействия, направленных как на устранение самих угроз, так и их причин, и практикой аналогов в создании узконаправленных мер, не учитывающих высокую адаптивность современных атак.

**Цель работы** состоит в повышении киберустойчивости автоматизированных систем за счет разработки алгоритмического и программного обеспечения для автоматизированной генерации мер и сценариев противодействия кибератакам.

**Задачи работы**:

1) провести анализ современных проблем обеспечения киберустойчивости автоматизированных систем и сформулировать требования к алгоритмическому обеспечению, необходимые для эффективной и долгосрочной работы в условиях быстроразвивающихся угроз информационной безопасности;

2) разработать алгоритмическое и программное обеспечение модуля централизованного сбора, обработки и хранения информации о компонентах кибератак, который должен обеспечивать возможность автоматизированной интеграции данных из внешних источников, а также поддерживать структурированное хранение этих данных о компонентах кибератак с учетом взаимосвязей между ними;

3) создать алгоритмическое и программное обеспечение модуля генерации и анализа сценариев кибератак, который должен обеспечивать возможность построения нелинейных путей реализации кибератак, учитывая вероятные варианты развития событий в ходе атаки, альтернативные пути проникновения в атакуемую систему и завершения атаки, а также взаимосвязь между различными этапами жизненного цикла атаки, где необходимо реализовать методы анализа сценариев, которые обеспечат информацию о вероятности его реализации, потенциальном ущербе и рисках информационной безопасности;

4) разработать алгоритмическое и программное обеспечение модуля генерации мер противодействия кибератакам, который должен обеспечивать генерацию эффективных мер, обеспечивающих комплексное решение для защиты от конкретных угроз информационной безопасности, генерируя меры противодействия даже для новых уязвимостей.

**Новизна полученных результатов** видится в следующем:

1) комплекс требований к алгоритмическому обеспечению, выполнение которого позволит обеспечить эффективное и долгосрочное функционирование в условиях стремительно развивающегося множества киберугроз, в отличие от аналогов учитывают ограничения современных подходов к

обеспечению киберустойчивости автоматизированных систем, что позволяет повысить адаптивность разрабатываемых систем безопасности;

2) модуль централизованного сбора, обработки и хранения информации о компонентах кибератак, в отличие от аналогов обеспечит гибкую интеграцию данных об уязвимостях, слабостях, техниках и шаблонах кибератак из разнородных источников, а также поддержку хранения и генерации семантических связей между различными компонентами кибератак;

3) модуль для нелинейной генерации сценариев кибератак, в отличие от аналогов учитывает множественность путей проникновения и завершения атаки, а также взаимосвязи между последовательностью тактик злоумышленника на всех этапах жизненного цикла атаки, что существенно расширяет возможности прогнозирования и анализа угроз;

4) модуль для адаптивной генерации мер противодействия кибератакам, в отличие от аналогов позволит формировать комплексные меры обнаружения, реагирования и ликвидации последствий как для известных, так и для потенциально новых угроз информационной безопасности. Такой подход основан на кластерном анализе семантических векторов уязвимостей для их категорирования по мерам противодействия, что позволяет реагировать на угрозы даже если отсутствуют готовые меры в доступных базах уязвимостей.

**Теоретическая значимость** полученных результатов видится в том, что:

1) выявленные ограничения современных подходов к обеспечению киберустойчивости автоматизированных систем и обосновывают комплекс требований к алгоритмическому обеспечению, ориентированный на повышение адаптивности разрабатываемых систем безопасности к развивающимся кибератакам;

2) создаваемое алгоритмическое обеспечение для интеграции и хранения данных о компонентах кибератак, обеспечивающее семантическое моделирование взаимосвязей между ними, будет способствовать развитию подходов, заключающихся в структурном представлении кибератак;

3) предлагаемое алгоритмическое обеспечение для нелинейной генерации сценариев кибератак углубит понимание сложных многоэтапных кибератак и предоставляет новые возможности для изучения методов прогнозирования атак на основе графовых и вероятностных моделей;

4) создаваемое алгоритмическое обеспечение автоматизированной генерации мер противодействия кибератакам позволит выявлять скрытые закономерности в структуре угроз и формировать типовые модели реагирования, что вносит вклад в развитие теории адаптивной кибербезопасности.

**Практическая ценность** полученных результатов видится в том, что:

1) сформулированные требования могут применяться при разработке или обновлении систем кибербезопасности, что позволит повысить устойчивость к современным киберугрозам;

2) модуль централизованного сбора, обработки и хранения информации может быть интегрирован в системы управления инцидентами информационной безопасности или в платформы управления уязвимостями для повышения скорости и точности анализа угроз;

3) модуль генерации сценариев кибератак может быть интегрирован в системы проактивной защиты информации или тестирования защищенности. Также данное решение может использоваться для обучения специалистов по информационной безопасности;

4) модуль генерации мер противодействия кибератакам обеспечивает автоматизированную генерацию рекомендаций по обнаружению, реагированию и ликвидации последствий угроз информационной безопасности, поэтому данный модуль может быть объединен в системы с современными сканерами уязвимостей, что позволит

значительно сократить время реакции на инциденты информационной безопасности за счёт комплексного подхода.

**Современные проблемы обеспечения кибербезопасности**

Обеспечение киберустойчивости автоматизированных систем является одной из важнейших задач в области информационной безопасности в силу того, что цифровые технологии все больше интегрируются в повседневную жизнь людей, в том числе в государственные сферы, такие как: управление, здравоохранение и экономика. Это происходит из-за высокой зависимости общества от автоматизированных систем, ведь для него критически необходима устойчивая и безопасная работа информационной инфраструктуры, требующейся для таких важных систем, как: банки, энергетика, больницы и другие государственные учреждения, с которыми общество сталкивается ежедневно. Но рост интеграции автоматизированных систем расширяет и поле взаимодействия злоумышленников с этими системами, что порождает множество рисков [2-4].

Хотя методы обеспечения информационной безопасности непрерывно совершенствуются, все же эволюция киберугрозы от этого не замедляется - атаки становятся более сложными, масштабными и целенаправленными. Среди примеров современных кибератак уже встречаются настолько опасные, что представляют собой многоэтапные скоординированные операции, в которых используются передовые достижения информационных технологий, включая, в том числе и нейросетевые разработки. Ущерб от настолько подготовленных атак может выражаться не только в финансовых потерях организаций, но и в нарушении жизненно важных информационных процессов в автоматизированных системах, что приводит к проблемам начиная от потери доверия к системам и заканчивая угрозами национальной безопасности [5-6].

В связи с этим высокую значимость в процессе обеспечения киберустойчивости автоматизированных систем приобретает разработка более эффективных методов моделирования кибератак, а также формирование подходящего комплекса мер противодействия им. Исходя из этого, настоящая работа направлена на всесторонний анализ кибербезопасности автоматизированных систем, включая современное состояние информационной среды, тенденции развития киберугроз и анализ существующих подходов к моделированию кибератак и противодействию им, что позволит сформировать необходимые требования к разрабатываемому алгоритмическому обеспечению.

**Уровень информатизации государственных и коммерческих структур**

Цифровизация в государственных и коммерческих информационных структурах России находится на высоком уровне. Так еще в 2022 году, после публикации Всемирным банком результатов, связанных с международным рейтингом GTMI (GovTech Maturity Index), стало известно, что России заняла место среди стран-лидеров, чья цифровая трансформация правительства и цифровизация государственного сектора услуг имеет внушительные результаты. Кроме того, Россия, по данным исследования ООН за 2024 год, входит в рейтинг стран, лидирующих в развитии электронного правительства, занимая 43 место в мире по индексу EDGI (E-Government Development Index), который относит страну к категории «очень высоких», тем самым подтверждая высокую степень информатизации государственных структур [7].

В конце декабря 2024 была завершена национальная программа «Цифровая экономика Российской Федерации», у которой были такие важные цели, как внедрение цифровых технологий в экономике и социальной сфере страны, а также создание благоприятных условий для успешного функционирования высокотехнологичного бизнеса, что несомненно приведет к повышению конкурентоспособности страны во всем мире, укрепив национальную безопасность и повысив общее качество

жизни граждан. Уровень достижения реализации данной программы составил 99,97 % [8]. В электронный формат было переведено более 200 услуг, важных для социальной сферы государства. Также важным достижением за последние годы является то, что к единой сети электросвязи страны был присоединен Чукотский автономный округ. В ходе данной программы были полностью выполнены следующие инициативы социально-экономического развития Российской Федерации [9]:

1) “Доступ в Интернет”;
2) “Цифровой профиль гражданина”;
3) “Госуслуги онлайн”;
4) “Электронный документооборот”;
5) “Подготовка кадров для ИТ”.

Что же касается коммерческих структур, то к началу 2025 года, удалось провести исследование, по результатам которого удалось выяснить, что большинство российских организаций имеют продвинутый уровень внутренней цифровизации. Данное исследование было проведено аналитический цен-тр ООО "На-цио-наль-ное агентство фи-нан-со-вых ис-сле-дова-ний", в ходе которого были проведены опросы организаций из различных отраслей экономики. Также на высокую цифровизацию указывают и данные ассоциации компаний интернет-торговли (АКИТ), которые помогли выявить значительный рост электронной коммерции, произошедший в 1 квартале 2024 года. В этих данных указано, что объём продаж, совершенных через интернет, вырос на 39% по сравнению с аналогичным периодом предыдущего года и составил 1,9 трлн рублей, что, несомненно, указывает на то, что потребители активно используют цифровых каналы [10].

Таким образом, цифровизация в России находится на достойном уровне, демонстрируя высокие показатели как в государственных, так и в коммерческих структурах, что, несомненно, повышает рост зависимости от автоматизированных систем.

**Рост цифровой зависимости**

Повышение зависимости России от автоматизированных систем связано со значительным ростом цифровой трансформации всех секторов страны, а также, в последнее время, еще и с возникшими внешними ограничениями, в условиях которых важно поддерживать на высоком уровне эффективность и устойчивость государства и бизнеса, что сопряжено с использованием автоматизированных систем. Особенно значительно это отобразилось на таких важных секторах страны как государственные структуры, промышленность и сфера услуг, где роль информации приобрела высокую значимость во внутренних процессах.

Наиболее важным из показателей роста автоматизированных систем является исследование группы, состоящей из таких авторитетных организаций, как: группа компаний «УльтимаТек», Positive Technologies и «Аквариус» при поддержке особо значимых структур, а именно: Министерства промышленности и торговли Российской Федерации и Ассоциации предприятий компьютерных и информационных технологий. Результатами данного исследования является подведение итогов 2024 года в контексте АСУ ТП на российском рынке. Показатели практически достигли 125 миллиардов рублей, тем самым установив значительный рост в 50 % за год [11]. Основой такого роста послужили проекты по реорганизации крупных предприятий и рост доли комплексных услуг. Все это подчеркивает то, что внедрение автоматизированных систем среди предприятий происходит все активнее.

Но кроме реорганизации предприятий немаловажным фактором послужило и стремление компаний значительно увеличить производительность, тем самым решив главную проблему современности, а именно дефицит квалифицированных специалистов. В данном стремлении роботизация и искусственный интеллект имеют наиболее перспективные направления, которые практически стали стратегическими.

В результате становится очевидным, что при устойчивой тенденции увеличения зависимости от автоматизированных систем, при всем множестве изменений, включающих рост рынка АСУ ТП, внедрение

искусственного интеллекта и массовой роботизации, порождается большое количество рисков нарушения информационной безопасности, что требует обеспечения надежности, безопасности и гибкости таких систем, ведь информация становится уже не просто инструментов, а стратегическим ресурсом, который важно защитить.

**Эволюция роли информации как стратегического ресурса**

Переход информации в России от обычного вспомогательного инструмента к одному из самых важных элементов национальной безопасности страны является важным указанием стремительной эволюции роли информации как стратегического ресурса, от которого зависит множество секторов страны, включая экономику и государственное управление.

Информация все больше рассматривается как полноценный ресурс, наряду с финансовым, материальным и человеческим капиталом, что отражает нарастающую важность информации. Стратегическая значимость подтверждается тем, что информация все чаще становится основой для управленческих решений на всех уровнях государства, начиная от малого бизнеса и заканчивая принятием решений на уровне государства, что несомненно определяет конкурентоспособность страны в условиях информационного противодействия [12-16].

Кроме того, экономика страны все больше переходит в сторону цифровизации всевозможных структур, тем самым создавая такое явление, при котором недооценка роли информации как стратегического ресурса или же игнорирование ее влияния, приводит к тому, что происходит критическое замедление социального и экономического развития страны в целом.

Также немаловажной является и позиция государства, которая формирует внутреннее цифровое пространство так, чтобы развитие цифровых технологий обеспечивало такие серьезные задачи, как обеспечение суверенитета, повышения качества жизни граждан, а также обеспечения национальной безопасности страны.

В результате, становится очевидным то, что за последние годы информационное развитие в России совершило стремительный рывок. Информатизация проникла во все структуры государства, автоматизированные системы оказывают все большее влияние на экономику страны, ее развитие, а также национальную безопасность, в связи с чем растет и роль информации как стратегического ресурса страны. Вследствие повышения важности информации, постоянно появляются и новые угрозы для нее, что несет в себе большие риски для безопасности государства, поэтому важной задачей является обеспечение информационной безопасности информации, циркулирующей во всем множестве автоматизированных систем, покрывающих киберпространство страны. Поэтому важно отслеживать тенденции развития киберугроз в стране для своевременного реагирования и подготовки к возникающим атакам [17-18].

**Рост количества кибератак**

Динамика киберугроз, а соответственно и инцидентов в области информационной безопасности за последнее время показывает значительный рост, как в численности атак, так и в их сложности. Наиболее же заметным стало увеличение 2022 года, что связано не только со стремительной цифровизацией в государстве, но и усиленным вниманием хакерских групп к российским организациям в силу изменений геополитической обстановки в мире.

Количество кибератак растет высокими темпами, так с 2021 года, в течение 2 лет, их число увеличилось в 3-3,5 раза, о чем говорит исследование лидера в области аудита, налогообложения, права, стратегии, сделок и консультирования группы компаний Б1 [19]. Данный скачок в количестве кибератак можно объяснить следующими факторами:

- расширение поверхности возможных атак из-за глобальной цифровизации во всех секторах государства;

- повышение ценности информации, циркулирующей в автоматизированных системах;

- переход многих организаций на удаленную работу;

- быстрое развитие информационных технологий, что также сказывается и на развитии атакующей стороны.

Но за это время произошел не просто рост числа атак, но и значительное увеличение доли критических инцидентов, которые являются большой угрозой, в особенности, в государственном секторе.

Несмотря на скачок количества кибератак в 2022 и 2023 году, на следующий год увеличение числа инцидентов все же продолжилось, из-за чего были достигнуты новые исторические максимумы. Так можно выделить следующие события:

- по сравнению с предыдущими годами, в 2024 году общее число инцидентов информационной безопасности выросло на 64 % и достигло отметки в 1,5 миллиона событий;

- доля критических инцидентов снизилась, что в корреляции с общим ростом указывает на то, что злоумышленники начали атаковать малозащищенные цели вследствие того, что в более крупных организациях сформировался высокий уровень защиты.

Также стоит обратить внимание и на рост инцидентов связанных с утечками персональных данных, так их число увеличилось на 30 % по сравнению с 2023 годом, что подтверждает исследование экспертно-аналитического центра ГК InfoWatch, что еще больше усиливает тенденцию роста кибератак [20].

Данная тенденция к росту сохраняется и в 2025 году, так с 2024 года и по начало 2025 года количество кибератак на российские компании увеличилось в 2,5 раза, что говорит о высокой напряженности в киберпространстве, так как основными целями атак были такие важные структуры, как организации энергетического, финансового и телекоммуникационного секторов. К тому же по информации ГК «Солар», специализирующейся на кибербезопасности, только за 1 квартал текущего года уже было зафиксировано более 800 миллионов кибератак, направленных на сетевую инфраструктуру организаций, что еще раз подтверждает масштабность угрозы [21].

Становится очевидным, что несмотря на укрепление систем обеспечения информационной безопасности, уровень киберугроз все же остается высоким и имеет следующие тенденции:

- непрерывный рост числа кибератак, где пик приходится на 2024 и 2025 года;

- доля критических инцидентов стала снижаться, что говорит о повышении защищенности крупных организаций, и смене злоумышленником целей на менее развитые объекты;

- несмотря на уменьшение критических инцидентов, количество атак на государственные структуры, включая энергетику и финансы, продолжает быть опасно высоким из-за ценности информации, циркулирующей в данных автоматизированных системах.

Но угроза от кибератак заключается не только в повышении их числа. Большое количество похожих атак можно предотвратить комплексом типовых мер противодействия, из-за чего злоумышленники часто меняют количественный подход на качественный, усложняя свои атаки, чтобы превзойти защитные меры своих целей.

**Повышение уровня сложности кибератак**

В современном киберпространстве наблюдается значительное повышение уровня сложности кибератак, в том числе методов и инструментов, которые использует злоумышленник. Такие атаки приобретают множество качеств, отличных от обычных кибератак, а именно:

- становятся более целенаправленными, тем самым повышая потенциальный ущерб от успешной атаки, за счет предварительной разведки и подготовки заранее выделенной цели;

- приобретают многоуровневость, из-за чего вероятность успеха атаки повышается, ведь в ней сочетается множество различных техник и векторов воздействия на цель злоумышленника;

- используют уязвимости в новых технологиях, что усложняет выработку подходящих мер противодействия.

Также ключевой тенденцией за последний год является применение искусственного интеллекта и средств автоматизации эксплуатации уязвимостей, что значительно усложняет выработку эффективных мер противодействия атакам злоумышленника, ведь атаки становятся более разнообразными, адаптируясь под существующие известные системы обеспечения информационной безопасности [22].

Основой повышения сложности кибератак стал переход атак от простых к многоэтапным, что произошло из-за активного развития средств защиты информации для того, чтобы повысить эффективность атак, намного увеличивая шанс достижения цели. Еще несколько лет назад сценарии атак были сравнительно простыми, ограничиваясь простым фишингом или DDoS - атаками, но за последние годы реализация таких атак перестала приносить успех злоумышленнику, вследствие разработки эффективных мер обнаружения и реагирования на инциденты информационной безопасности, что повлекло за собой переход атакующих к более совершенным и продуманным методам атаки. Такие многоэтапные атаки позволяют злоумышленникам достигать своей цели с наибольшей вероятностью успеха, ведь появляется строгий сценарий кибератаки, который позволяет совершать последовательные продуманные действия начиная от разведки и проникновения в сеть и заканчивая хищением данных и уничтожением атакуемой системы.

Атаки, основанные на таком подходе, являются скрытными и адаптивными, так как допускают изменения атакующих техник злоумышленника в реальном времени, в зависимости от реакции систем обеспечения информационной безопасности и применяемых мер противодействия.

Еще одним из главных факторов усложнения атак является развитие искусственного интеллекта и машинного обучения, что позволяет злоумышленникам автоматизировать рутинные действия, которые занимают слишком много времени, а также разрабатывать новые методы атак, тем самым повышая их эффективность, скрытность и масштабируемость, что значительно увеличивает уровень угрозы, как для обычных пользователей, так и для крупных организаций. Наиболее важными и популярными являются следующие направления применения искусственного интеллекта в проведении кибератак [23]:

- фишинг - наиболее распространенное направления применения искусственного интеллекта, подразумевающее автоматическую генерацию и рассылку фишинговых писем всем организациям, которые являются целью злоумышленника;

- вредоносное ПО - направление использования машинного обучения, которое направлено на создание и модификация вредоносного программного обеспечения так, чтобы системы обнаружения не смогли противостоять такому программному обеспечению, что достигается применением алгоритмов, способных генерировать новые версии кода так, чтобы сохранялся прежний функционал, но сигнатурные методы, активно используемые современными антивирусами, не смогли отличить этот код от легитимного;

- целенаправленность атаки - при помощи искусственного интеллекта злоумышленники все чаще подготавливаются к атакам на конкретные организации, что достигается путем нейросетевого анализа большого объема открытых данных об организации, выявляя уязвимых сотрудников, их интересы, круг общения и остальную важную информацию, которая позже будет применена для атаки на организацию;

- эксплуатация уязвимостей - с помощью машинного обучения для злоумышленника раскрываются большие возможности в области анализа программного обеспечения атакуемых организаций с целью выявления уязвимостей для последующей эксплуатации незащищенных мест системы в ходе атаки;

- адаптивность атаки - искусственный интеллект, имея информацию о текущем ходе

выполнения сценария и реакции систем безопасности организации, имеет возможность к быстрому анализу ситуации и принятию верных решений, который приведут атакующего к наиболее эффективному пути атаки, а соответственно и наибольшей вероятности успеха.

В результате, обобщая выявленную информацию о тенденциях повышения уровня сложности кибератак, становится очевидным, что основными факторами, из-за которых это случилось, являются повышение целенаправленности и многоуровневости атак, а также использование таких современных технологий, как искусственный интеллект и машинное обучение. Данное разнообразие подходов к атаке образовалось за счет активного развития систем защиты информации, что позволяет сделать выводы в скором устаревании защиты и необходимости вести постоянное улучшение мер обеспечения информационной безопасности.

**Системы сбора, обработки и хранения информации о кибератаках**

Современные системы обеспечения информационной безопасности включают множество средств, которые требуют большого количества информации о кибератаках, чтобы в полной мере анализировать угрозы и вычислять правильные оценки риска. Однако, на практике, большинство таких баз данных о киберугрозах являются узконаправленными и созданы для выполнения той или иной функции, не учитывая при этом адаптивность к новым угрозам. Наиболее совершенными и популярными являются следующие платформы сбора, обработки и хранения информации о киберугрозах:

1) CVE (Common Vulnerabilities and Exposures) - открытая база уязвимостей программного обеспечения и оборудования, в которой каждой уязвимости присвоены уникальные идентификаторы, позволяющие правильно реагировать на конкретные инциденты. В большинстве случаев данная платформа применяется для интеграции уязвимостей в системы мониторинга и управлениями патами в автоматизированных системах [24]. Можно выделить следующие положительные стороны данной базы данных:

- универсальность применения - данная платформа широко используется во всем мире в различных системах обеспечения информационной безопасности;
- интеграция с другими инструментами обеспечения безопасности - поддерживается большинством сканеров уязвимостей и систем управления обновлениями;
- поддержание актуальности - новые уязвимости отслеживаются и добавляются в базу данных после их обнаружения и исследования.

Но, несмотря на все преимущества, CVE все же имеет такой важный недостаток, как пассивность, вследствие того, что платформа не описывает методы, с помощью которых эксплуатируются уязвимости, а позволяет отследить только факт существования уязвимости.

2) CWE (Common Weakness Enumeration) - платформа представляет собой классификацию уязвимостей в архитектуре информационных систем [25]. В базе содержатся слабости программного обеспечения, которые являются источниками CVE. Можно выделить следующие преимущества этой базы данных:

- фокус на причины уязвимостей - использование данных CWE позволяет устранять причины уязвимостей еще до их появления;

- поддержка реализации проактивной защиты - используется при аудите кода программного обеспечения системы, для выявления слабых мест, тем самым устраняя потенциальные уязвимости.

Основным же минусом данной платформы является высокий уровень абстракции данных, так как их не всегда возможно применить к конкретным инцидентам.

3) MITRE ATT&CK - детализированная матрица тактик и техник, которые применяются злоумышленником на различных этапах жизненного цикла

кибератаки, начиная от получения начального доступа и заканчивая деструктивным воздействием. В большинстве случаев база данных применяется для создания систем обнаружения вторжений и оценки защищенности [26].

К преимуществам такой базы данных можно отнести:

- практическая направленность - данные основаны на реальных многоуровневых атаках;

- детализация действий - тактики и техники позволяют моделировать полный жизненный цикл атаки;

- простая структура - благодаря матричной структуре, появляется возможность быстрого нахождения необходимых тактик и техник.

Главным недостатком является сложность интерпретации данных, что требует квалифицированных специалистов и методы принятия решений, так как пути защиты могут быть разнообразными из-за высокой абстрактности данных.

4) CAPEC (Common Attack Pattern Enumeration and Classification) - является каталогом, в котором рассмотрены типовые шаблоны атак, основанным на анализе реальных сценариев кибератак злоумышленников [27]. Данная база данных дает описание того, как злоумышленники реализуют те или иные атаки для достижения своей цели, и дает возможность моделировать сложные атаки.

Можно выделить следующие плюсы от использования данного каталога:

- реалистичность данных описывает поведение злоумышленников в ходе реальных атак;

- проактивность: база данных дает возможность заранее готовиться к возможным сценариям атак;

- гибкость: каталог может применяться в широком спектре действий по обеспечению информационной безопасности, начиная от обучения персонала и заканчивая разработкой политик безопасности в организациях.

Главными же недостатками CAPEC является сложность восприятия, требующего понимания процессов атаки и защиты, за счет чего проявляется и ограниченная автоматизация, так как немногие разработчики систем обеспечения информационной безопасности способны интегрировать каталог в функционал своих систем.

В результате, после анализа наиболее популярных современных систем сбора, обработки и хранения информации о киберугрозах, становятся очевидными следующие ключевые проблемы:

- фрагментированность данных: информация о компонентах киберугроз распределена по различным источникам, что значительно затрудняет моделирование кибератак и их последующий анализ, ведь для этого необходим подход, учитывающий кибератаку не только как единое целое, но и как систему, где каждая часть вносит свой определенный вклад;

- отсутствие централизованного подхода к хранению информации. В некоторых случаях системы хранения требует взаимодействия между собой, но из-за того, что данные находятся в разных базах данных, получение информации происходит с задержками, а в некоторых случаях используется ручная обработка, для получения качественных результатов, что недопустимо в условиях автоматизированных атак, действия в которых развиваются с высокой скоростью.

Из проанализированной информации можно сделать вывод, что существующие методы сбора, обработки и хранения информации о киберугрозах недостаточно адаптированы к современным вызовам, что способны бросить злоумышленники в ответ на активно развивающиеся методы защиты информации. Так, для повышения эффективности существующих систем защиты информации от кибератак, становится необходимой алгоритмическая и программная разработка модуля

централизованного сбора, обработки и хранения информации о киберугрозах которая будет устранять недостатки аналогов, а именно:

- объединять наиболее полезные данные из различных источников;

- применять машинное обучение для качественной и быстрой обработки поступающей в систему информации;

- обеспечивать централизованное место для хранения информации о различных компонентах киберугроз для быстрого обмена между модулями систем защиты информации.

**Методы генерации сценариев кибератак**

В современных условиях, когда кибератаки становятся многоуровневыми в ответ на большое количество мер противодействия, генерация возможных сценариев кибератак становится важной задачей для обеспечения эффективной защиты, поскольку это позволяет моделировать логику злоумышленника, включая: пути проникновения, наиболее вероятные методы распространения и закрепления, а также сбора данных и деструктивного воздействия на систему. На практике применяются следующие наиболее популярные подходы к генерации сценариев кибератак:

1) линейная модель атаки - данный метод заключается в представление атаки как последовательности строго определенных этапов, где каждый из этих этапов идет после успешного завершения предыдущего. Наиболее распространенным примером такой модели является матрица MITRE ATT&CK, в которой последовательность тактик строго зафиксирована. Данные модели представляют интерес в базовом анализе и обучении специалистов, но для противодействия сложным современным кибератакам, данный метод не подходит, так как не учитывает возможность нелинейного развития сценариев [28];

2) генерация сценариев на основе шаблонов и правил - метод, использующий заранее разработанные шаблоны типовых атак и правила, которыми руководствуется злоумышленник во время таких атак. В большинстве случаев такие методы применяются в симуляции атак, что позволяет проводить успешные тренировки специалистов по информационной безопасности, но несмотря на высокую степень автоматизации, данные методы недостаточно гибкие из-за чего нет возможности создать на их основе системы, способные адаптироваться к быстро изменяющейся обстановке в киберпространстве [29];

3) составление сценариев на основе логических выводов и экспертных знаний - формальный метод, основанный на логическом анализе атак, а также на экспертном мнении в контексте определенного типа атаки. Такие подходы являются наиболее точными и подробными, но значительным недостатком является потребность в высококвалифицированных экспертах и большом количестве времени и ресурсов для поддержания актуальности баз знаний, составленных таким методом, сценариев [30].

Несмотря на разнообразие подходов, у наиболее популярных из них присутствует ряд недостатков, из-за которых меры противодействия многоэтапным атакам становятся неэффективными:

- ограниченное множество генерируемых сценариев - подходы охватывают лишь часть от возможных сценариев кибератак, из-за чего опасные сценарии могут быть не учтены и меры противодействия будут неполными, что наиболее критично для систем, в которых необходим анализ сложных многоэтапных кибератак;

- неспособность учитывать обратные связи - подходы основаны на статических методах моделирования атак, не учитывая при этом возможность корректировки этапов атаки злоумышленником в зависимости от множества факторов, влияющих на исход атаки;

- низкая адаптивность к новым типам угроз – системы, основанные на шаблонах и

правилах атак, применявшихся в прошлом, не способны генерировать сценарии новых атак, информации о которых еще не было в киберпространстве, особенно при применении атакующими искусственного интеллекта.

На основе проведенного анализа популярных подходов к генерации сценариев кибератак, явно выделяются серьезные ограничения, связанные с недостаточной гибкостью и адаптивностью. Для преодоления ограничений требуется разработка инструмента, учитывающего в себе как большинство положительных качеств предыдущих подходов, так и новые возможности, основными из которых будут использование нелинейных моделей кибератак и способность адаптироваться к изменениям подхода злоумышленников в киберпространстве.

**Подходы к формированию мер противодействия кибератакам**

В обеспечении информационной безопасности автоматизированных систем одним из наиболее важных направлений является формирование мер противодействия кибератакам, так можно выделить популярные подходы:

- шаблонные меры противодействия кибератакам. Это наиболее распространенный подход, основанный на использовании шаблонов, разработанных на основе типовых кибератак. Включает в себя такие основные меры, как обнаружение, реагирование и ликвидацию последствий угроз. Основным недостатком такого подхода является отсутствие адаптивности к быстро развивающимся угрозам информационной безопасности из-за сложного формирования шаблонов для мер противодействия [31];

- базы знаний и стандарты – подход, основанный на генерации мер противодействия при помощи экспертов. Наиболее авторитетным примером такого метода является руководство по обработке инцидентов компьютерной безопасности NIST SP 800-61 [32]. В данном руководстве описаны основные этапы реагирования: подготовка системы к возможной атаке, обнаружение атаки, ее сдерживание и ликвидацию, а также восстановление и анализ после защиты. Однако, несмотря на внушительную подробность мер противодействия, данные рекомендации все же носят общий характер и не учитывают конкретные виды атак.

В результате можно выделить следующие общие недостатки популярных подходов к формированию мер противодействия кибератакам:

- низкая степень автоматизации – подавляющее большинство подходов, требуют ручного анализа и обработки мер противодействия определенным атакам, что значительно снижает эффективность защиты против новых атак;

- отсутствие русскоязычной локализации – большинство подходов основаны на иностранных стандартах и рекомендациях, что значительно затрудняет их применение в российских организациях.

Для устранения ограничений, выявленных в результате анализа популярных подходов к формированию мер противодействия кибератакам, представляется целесообразной разработка модуля автоматизированной генерации регламентов реагирования, у которого будут отсутствовать выявленные недостатки.

Обобщая промежуточные выводы, сделанные во время анализа существующих подходов к противодействию кибератакам, можно выделить основные недостатки, которые необходимо устранить при разработке системы автоматизированной генерации мер и сценариев противодействия кибератакам, а именно:

- фрагментированность данных;
- ограниченная адаптивность моделей;
- задержки при реагировании на новые угрозы;
- отсутствие русскоязычной локализации.

Такова мотивация создания программно-технических модулей противодействия кибератакам, обеспечивающих:

1) централизованный сбор, обработку и хранение информации о компонентах кибератак - данный модуль должен

предоставить доступ к единой базе знаний о компонентах кибератак, гарантируя при этом качество данных и точность взаимосвязей между этими компонентами., что значительно повысит эффективность анализа киберпространства;

2) генерацию и анализ сценариев кибератак - модуль должен генерировать сценарии сложных многоэтапных кибератак, с поддержкой адаптивности к динамично развивающимся методам, используемым в современных атаках, а также иметь методы анализа сгенерированных сценариев, позволяющие точность оценивать вероятность, потенциальный ущерб и риски информационной безопасности;

3) генерацию мер противодействия кибератакам - этот модуль должен обеспечивать оперативное формирование мер по обнаружению, реагированию и ликвидации последствий кибератак, ориентированных на русскоязычное киберпространство. Перечисленные модули составят основу разрабатываемой системы автоматизированной генерации мер и сценариев противодействия кибератакам. Решения, позволяющие преодолеть ограничения, которые присутствуют в аналогах, выявленные в ходе анализа современных проблем обеспечения киберустойчивости автоматизированных систем, будут подробно рассмотрены в дальнейших работах.

**Заключение**

В ходе выполнения данной работы была поставлена цель повышения киберустойчивости автоматизированных систем за счет разработки алгоритмического и программного обеспечения для автоматизированной генерации мер и сценариев противодействия кибератакам.

В качестве перспектив развития следований предлагается далее внедрение средств искусственного интеллекта для:

1) прогнозирования тенденций развития киберугроз и формирования на их основе актуальных требований к системам обеспечения безопасности информации, что поможет автоматизировать поддержание высокой адаптивности разрабатываемых систем к новым типам атак,

2) семантической интерпретации неструктурированных данных о кибератаках для выявления новых компонентов кибератак и их описаний, что обеспечит более высокое значение актуальности базы данных о компонентах кибератак, а следовательно, повысит эффективность работы взаимосвязанных модулей,

3) прогнозирования сценариев кибератак в различных типах автоматизированных систем, что позволит динамически обновлять взаимосвязи в графе сценариев кибератак в зависимости от параметров системы,

4) построения временных последовательностей мер противодействия кибератакам, учитывающих динамику развития кибератак и этапы сценариев в момент генерации мер, что значительно повысит эффективность противодействия кибератакам за счет снижения возможного ущерба от кибератак.

В этом случае разрабатываемый программно-технический комплекс для автоматизированной генерации мер и сценариев противодействия кибератакам демонстрирует значительную практическую ценность, а также высокий потенциал к улучшению показателей эффективности в обеспечении безопасности информации и киберустойчивости защищаемых автоматизированных систем.

**Список литературы**

1. Российский рынок средств защиты данных в 2024 году. URL: https://www.computerra.ru/309167/rossijskij-rynok-sredstv-dlya-zashhity-dannyh-v-2024-godu-dostig-23-mlrd-rub/ (дата обращения 21.08.2025).

2. Остапенко Г.А. Модернизация методического обеспечения автоматизированного сервиса агрегации данных и риск-анализа уязвимостей / Г.А. Остапенко, А.П. Васильченко, А.А. Остапенко, Н.Н. Корвяков, Д.С. Покудин, А.А. Ноздрюхин // Информация и безопасность. 2024. Т. 27. Вып. 2. С. 219-230.

3. Александров А.Г. Анализ угроз информационной безопасности при использовании облачных сервисов / А.Г. Александров, А.Ю. Петухов, М.Ю. Рытов // Информация и безопасность. 2024. Т. 27. Вып. 1. С. 143-151.

4. Картография защищаемого киберпространства / Остапенко [и др.]; [под ред. чл.-корр. РАН Д.А. Новикова]. М: Горячая линия – Телеком, 2022. 372 с. (Серия «Теория сетевых войн»; вып. 7).

5. Социальные сети и риск-мониторинг / Остапенко [и др.]; [под ред. чл.-корр. РАН Д.А. Новикова]. М: Горячая линия – Телеком, 2019. 284 с. (Серия «Теория сетевых войн»; вып. 4).

6. Организационно-правовая защита сетей / Остапенко [и др.]; [под ред. чл.-корр. РАН Д.А. Новикова]. М: Горячая линия – Телеком, 2023. 228 с. (Серия «Теория сетевых войн»; вып. 8).

7. Исследование ООН “Электронное правительство 2024” URL: https://desapublications.un.org/sites/default/files/publications/2025-01/E-Government%20Survey%202024%20RUS-compressed.pdf (дата обращения 21.08.2025).

8. Национальная программа «Цифровая экономика Российской Федерации». URL: https://digital.gov.ru/target/naczionalnaya-programma-czifrovaya-ekonomika-rossijskoj-federaczii (дата обращения 21.08.2025).

9. Распоряжение Правительства Российской федерации от 6 октября 2021 г. № 2816-р “Об утверждении перечня инициатив социально-экономического развития Российской Федерации до 2030 года” URL: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=0&nd=602471593&intelsearch=&firstDoc=1 (дата обращения 21.08.2025).

10. Объём интернет-торговли в первом квартале 2024 года. URL: https://akit.ru/news/obyom-rossijskoj-internet-torgovli-v-pervom-kvartale-vyros-na-39 (дата обращения 21.08.2025).

11. Исследование рынка АСУ ТП в России. URL: https://ptsecurity.com/ru-ru/research/analytics/issledovanie-rynka-asu-tp-v-rossii/ (дата обращения 21.08.2025).

12. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL: http://www.consultant.ru/document/cons doc LAW_61798/ (дата обращения 21.08.2025).

13. Овчинский А.С. Информационное противоборство с деструктивными сетевыми сообществами / А.С. Овчинский, К.К. Борзунов // Информация и безопасность. 2024. Т. 27. Вып. 2. С. 159-168.

14. ГОСТ Р ИСО/МЭК 27001:2021. Информационная технология. Системы менеджмента информационной безопасности. Требования. URL: https://docs.cntd.ru/document/1200181890 (дата обращения 21.08.2025).

15. ГОСТ Р ИСО/МЭК 27002:2021. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. URL: https://docs.cntd.ru/document/1200179669 (дата обращения 21.08.2025).

16. ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. URL: https://docs.cntd.ru/document/1200179612 (дата обращения 21.08.2025).

17. ГОСТ Р ИСО/МЭК 27005-2010. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. URL: https://docs.cntd.ru/document/1200084141 (дата обращения 21.08.2025).

18. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) (утв. ФСТЭК России 15 февраля 2008 г.). URL: https://docs.cntd.ru/document/902330983 (дата обращения 21.08.2025).

19. Рынок информационной безопасности России URL: https://b1.ru/local/assets/surveys/russian-information-security-market-survey-2025.pdf?ysclid=mbopnq5sur876913517 (дата обращения 21.08.2025).

20. Количество скомпрометированных персональных данных в 2024 году URL: https://www.infowatch.ru/company/presscenter/

news/kolichestvo-slitykh-personalnykh-dannykh-v-dve-tysyachi-dvadtsat-chetvertom-godu-vyroslo-na-tret (дата обращения 21.08.2025).

21. ГК «Солар»: число веб-атак на сайты российских компаний за год выросло в 2 раза URL: https://rt-solar.ru/events/news/5498/?ysclid=mborttqfcc529597068 (дата обращения 21.08.2025).

22. Искусственный интеллект: инструмент или угроза информационной безопасности. URL: https://articles.moluch.ru/archive/550/121036 (дата обращения 21.08.2025).

23. Искусственный интеллект в кибератаках URL: https://ptsecurity.com/ru-ru/research/analytics/iskusstvennyj-intellekt-v-kiberatakah/ (дата обращения 21.08.2025).

24. CVE: Common Vulnerabilities and Exposures URL: https://www.cve.org/ (дата обращения 21.08.2025).

25. CWE – Common Weakness Enumeration URL: https://cwe.mitre.org/ (дата обращения 21.08.2025).

26. MITRE ATT&CK® URL: https://attack.mitre.org/ (дата обращения 21.08.2025).

27. CAPEC – Common Attack Pattern Enumeration and Classification (CAPEC™) URL: https://capec.mitre.org/ (дата обращения 21.08.2025).

28. Автоматизация безопасности с разнообразием матриц MITRE URL: https://habr.com/ru/companies/securityvison/articles/763218/ (дата обращения 21.08.2025).

29. Моделирование угроз на основе сценариев URL: https://safe-surf.ru/specialists/article/5247/626649/ (дата обращения 21.08.2025).

30. Формальные методы экспертных оценок. URL: https://cyberleninka.ru/article/n/formalnye-metody-ekspertnyh-otsenok/viewer/ (дата обращения 21.08.2025).

31. ГОСТ Р ИСО/МЭК 15408-2-2013.Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. URL: https://docs.cntd.ru/document/1200105710 (дата обращения 21.08.2025).

32. SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC. URL: https://csrc.nist.gov/pubs/sp/800/61/r2/final (дата обращения 21.08.2025).

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 25.08.2025

**Информация об авторах**

**Остапенко Григорий Александрович** – д-р техн. наук, профессор, Финансовый университет при Правительстве Российской Федерации, e-mail: ost@fa.ru

**Остапенко Александр Алексеевич** – аспирант, Воронежский государственный технический университет, e-mail: alexostap123@gmail.com

**Кондратьев Максим Витальевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Кривошеин Александр Сергеевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Печкин Дмитрий Сергеевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

# AUTOMATION OF ASSESSMENT AND REGULATION OF RISKS OF IMPLEMENTATION OF CYBER-ATTACKS: MOTIVATION AND GOAL-SETTING OF CREATION OF SOFTWARE AND HARDWARE COMPLEX

**G.A. Ostapenko, A.A. Ostapenko, M.V. Kondratyev, A.S. Krivoshein, D.S. Pechkin**

The article substantiates the feasibility of developing a software and hardware complex that ensures the assessment and regulation of risks of cyber attacks by creating modules: collecting, processing and storing data on them; generating scenarios and countermeasures. The proposed goal-setting of the study is based on: an analysis of the relevance of cyber protection of automated systems in the context of the growth in the number and sophistication of computer attacks, the identification of contradictions in approaches to ensuring information security, as well as the shortcomings of modern countermeasures. The expected: novelty, practical value and theoretical significance of the implemented development are assessed.

Keywords: cybersecurity, software and hardware complex, risk assessment, cyberattacks, automated systems, scenario generation, machine learning.

Submitted 25.08.2025

**Information about the authors**

**Gregory A. Ostapenko** – Dr. Sc. (Technical), Professor, Financial University under the Government of the Russian Federation, e-mail: ost@fa.ru

**Alexander A. Ostapenko** – graduate student, Voronezh State Technical University, e-mail: alexostap123@gmail.com

**Maksim V. Kondratyev** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Alexander S. Krivoshein** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Dmitriy S. Pechkin** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**DOI 10.36622/1682-7813.2025.28.3.003**
**УДК 378:811**

# МОДЕЛИРОВАНИЕ И ПРОГНОЗИРОВАНИЕ ФИШИНГОВЫХ АТАК

**В.А. Минаев**, **А.О. Фаддеев**, **Ю.В. Броненкова**

В статье рассматриваются вопросы моделирования динамики фишинговых атак в киберпространстве Российской Федерации на основе рекуррентной нейронной сети. Поставлена и решена задача получения прогнозной информации о количестве атак подобного вида. Проведено исследование структуры динамического ряда фишинговых атак на предмет выявления в нём трендовой, сезонной и случайной составляющих. Рассмотрены два вида моделей, использованных при проведении прогностических оценок фишинговых атак – *LSTM*-модель и *Auto ARIMA*. Анализ результатов прогностических оценок убедительно свидетельствует о значительном преимуществе *LSTM*-модели. Точность прогноза, полученного с ее помощью, в среднем не более 6%. Делается вывод, что представляемый на данном этапе прогноз, основываясь на реально существующих, но пока не объясненных закономерностях реализации фишинговых атак, требует для своего уточнения более сложных математических моделей, учитывающих многих факторов, определяющих это новое криминальное явление. Рекуррентные нейронные сети при этом могут весьма полезными на первом этапе исследований и других видов киберпреступлений.

Ключевые слова: фишинговая атака, моделирование, прогнозирование, рекуррентная нейронная сеть, LSTM-модель.

## Введение

Преступность является одной из острейших проблем современности, оказывающей существенное негативное влияние на многие сферы жизнедеятельности современного общества. Достаточно указать на такие серьёзные угрозы и тяжёлые последствия для него, как разрушение социальных связей, ухудшение общественного климата, формирование обстановки страха и неуверенности, снижение безопасности граждан, экономический ущерб, потеря доверия к государственным институтам [1].

В то же время, повсеместное внедрение новых информационных технологий и

стремительная цифровизация общества создают благоприятные обстоятельства для дополнительного осложнения обстановки в связи с развитием киберпреступности [2].

Растёт число кибератак, цель которых – не только получить конфиденциальную информацию или дестабилизировать работу того или иного предприятия, но и расшатать сами устои современного российского государства [3].

Спектр кибератак включает фишинговые атаки, методы социальной инженерии, использование вредоносного программного обеспечения, атаки, базирующиеся на эксплуатации уязвимостей программного

обеспечения (ПО), а также другие криминальные способы применения информационно-телекоммуникационных технологий [3]. Поэтому защита информационных систем, баз и банков данных, персональной информации выступают приоритетными задачами в контексте обеспечения безопасности как государства и общества, так и каждого его гражданина [4, 5].

Рассмотреть в одной статье вопросы, связанные с оценками всего спектра киберугроз нереально, поэтому уделим внимание только фишинговым атакам, являющимися доминирующим видом киберпреступлений в России [3].

Фишинг (от англ. fishing – выуживать) определяется как вид кибератаки, используемой членами криминальной среды для организации доступа к информации конфиденциального характера юридического или физического лица, с целью получения данных о логине или пароле электронной почты, о закрытых финансовых атрибутах (счета, номера банковских карт,

осуществленные транзакции), промышленной тайне или персональной информации.

При этом злоумышленники активно манипулируют такими эмоциями человека, как страх и любопытство, используя открытые источники для сбора информации о том или ином индивиде. Именно человеческий фактор становится доминирующим в цепочке «приманка – забрасывание удочки – подсечка» в фишинговых атаках, доводя в утечке данных ее успешность до 90%.

Конечно, организации и конкретные пользователи могут распознавать и блокировать фишинговые атаки с помощью различных программ, фильтров спама и других современных инструментов. Но фишинг-технологии стремительно развиваются, интегрируясь с социальной инженерией, и это требует более глубоких научных исследований явления, разработки более эффективных способов практического противодействия электронному криминалу.

Весьма перспективным направлением в этом отношении выступают программы-имитаторы фишинговых атак, позволяющие воспроизводить разные сценарии их реализации и дающие возможность повышать осведомленность пользователей, выявлять среди них наиболее уязвимых, нуждающихся в дополнительном индивидуальном обучении.

Среди таких программ-имитаторов известны Phished AI, Gophish, SafeTitan, Phishing box и ряд других. Это автоматизированные программные системы моделирования, которое обеспечивают оценку риска поведения сотрудников, целенаправленно обучать наиболее уязвимых из них определению вредоносных файлов и ссылок. Некоторые из программ-имитаторов, например, Phished AI, используют технологии искусственного интеллекта для разработки персонализированных тренингов.

Однако, несмотря на появление инструментов подобного рода, необходимо существенно углублять осведомленность пользователей о безопасности в борьбе с фишингом. Одним из способов предотвращения угроз и рисков фишинга выступает их моделирование с учетом интенсивно развивающихся факторов, определяющих это опасное социально-экономическое явление.

**Постановка задачи**

Одним из важных аспектов превентивной оценки фишинговых атак является получение данных о том, каков характер её динамики применительно к киберпространству России. Для оценки к динамическому ряду, отражающему количественные значения фишинговых атак в стране, следует применить довольно развитый аппарат статистического анализа [6].

В таком случае задача прогнозирования представляет собой получение на основе имеющихся последовательных данных о фишинговых атаках в прошлом, прогнозной информации об их количестве на заранее определённом временном интервале упреждения.

В качестве такого интервала выбран первый квартал 2025 года. Этот выбор обусловлен тем, что на момент проведения исследований уже имелась необходимая информация для подтверждения точности прогнозирования о количестве фишинговых атак, произошедших в указанный период времени.

Первой процедурой, которая произведена с динамическим рядом фишинговых атак, является выявление в нём случайной и детерминированной компонент [7].

После определения структуры динамического ряда, необходимо определиться с видом моделей, которые следует использовать для получения прогнозной информации [8].

Далее следует этап непосредственных прогностических оценок по отобранным моделям количества фишинговых атак на определённом временном интервале.

Наконец, на заключительном этапе необходимо произвести сравнительный анализ прогнозной информации, полученной на основе различных моделей.

Согласно представленной краткой методике, решим задачу прогнозирования на реальных данных количества фишинговых атак в киберпространстве страны.

**Теоретические модели**

При оценке структуры динамического ряда фишинговых атак использована модель, в которой значение $Y(t_i)$ предопределяется значениями $Y(t)$ в предыдущие моменты времени [9]:

$$Y(t_i) = f\left[Y(t_{i-1}), Y(t_{i-2}), \ldots\right] + \varepsilon(t_i),$$

где $\varepsilon(t_i)$ – случайная составляющая.

Степень статистической связи между последовательностями $Y(t_1)$, $Y(t_2)$, …, $Y(t_n)$ и $Y(t_{1+l})$, $Y(t_{2+l})$, …, $Y(t_{n+l})$ (сдвинутых относительно друг друга на $l$ моментов времени, или, как говорят, с лагом $l$) может быть определена с помощью коэффициента автокорреляции. Для этого необходимо вычислить значения автокорреляционной функции ряда по формуле [9, 10]:

$$r(l) = \frac{(n-l)\sum_{i=1}^{n-l} y_i y_{i+l} - \left(\sum_{i=1}^{n-l} y_i\right)\cdot\left(\sum_{i=1}^{n-l} y_{i+l}\right)}{\sqrt{(n-l)\sum_{i=1}^{n-l} y_i^2 - \left(\sum_{i=1}^{n-l} y_i\right)^2}\cdot\sqrt{(n-l)\sum_{i=1}^{n-l} y_{i+l}^2 - \left(\sum_{i=1}^{n-l} y_{i+l}\right)^2}}$$

где $l$ – величина лага,

$n$ – длина динамического ряда.

Требуется проверить значимость отдельно взятых коэффициентов и всей их совокупности [6]. Значимость отдельного коэффициента определим по формуле [10]:

$$-1.96\cdot\frac{1}{\sqrt{n}} \le r_l \le 1.96\cdot\frac{1}{\sqrt{n}} \qquad (1)$$

Значимость всей совокупности коэффициентов автокорреляции конкретного динамического ряда проверяется по $Q$-критерию Бокса-Пирса [6]:

$$Q = n\cdot\sum_{i=1}^{m} r_i^2 \approx \chi^2(m), \qquad (2)$$

где $m$ – максимальный рассматриваемый лаг.

Статистика (2) имеет распределение $\chi^2$ с $m$ степенями свободы, и поэтому в случае, когда расчетное значение $Q$ превосходит критическое значение $\chi^2$, то вся группа коэффициентов для лагов, не превосходящих $m$, считается значимой [11].

Для анализа структуры динамического ряда применялась аддитивная модель вида [6, 9]:

$$Y(t_i) = q(t_i) + \varepsilon(t_i),\ i = 1, 2, \ldots, n, \qquad (3)$$

где $q(t_i)$ детерминированная составляющая включает трендовую и сезонную компоненты.

С целью прогнозирования фишинговых атак использована рекуррентная нейронная сеть *LSTM* (*Long Short-Term Memory*) [12], специально разработанная для обработки длинных динамических последовательностей данных. *LSTM* отличается от классических рекуррентных нейронных сетей использованием управляющих механизмов – ворот забывания (*forget gate*), входных ворот (*input gate*) и выходных ворот (*output gate*) [13]. Управляющие механизмы описываются уравнениями, регулирующими поток информации о прошлом и выводящими ее из обработки по мере старения.

Теперь охарактеризуем модели, которые использовались для сравнения результатов получения прогнозной информации.

В первую очередь, выбрана модель прогнозирования *ARIMA*, представляющая собой комбинацию двух моделей, используемых для анализа динамических рядов: авторегрессионную модель (*AR*-модель) и модель скользящего среднего (*MA*-модель) [14].

Помимо классической модели *ARIMA* рассмотрены две её модификации – *SARIMA* и *Auto ARIMA* [14]. Важной особенностью модели *SARIMA* является то, что она учитывает сезонность, что делает её особенно эффективной при анализе последовательных данных с выраженной периодичностью.

В отношении модификации *Auto ARIMA* отметим, что она обеспечивает автоматизацию подбора параметров, позволяющую избежать их ручного перебора при выполнении прогностических оценок, что значительно сокращает временные затраты при расчетах.

Отметим такие важные элементы, необходимые для обучения нейронной сети, как функцию потерь и метод оптимизации. В

качестве функции потерь использована среднеквадратическая ошибка:

$$MSE = \frac{1}{m}\sum_{i=1}^{m}(y_i - \hat{y}_i)^2,$$

где $y_i$ и $\hat{y}_i$ – истинное и предсказанное значения;

$m$ – число точек сравнения на интервале прогноза.

Для оптимизации выбран метод *Adam*, сочетающий преимущества методов *AdaGrad* и *RMSProp*.

**Экспериментальные результаты**

На первом этапе экспериментальных исследований поквартального количества фишинговых атак в России за период 2019 – 2024 гг. (рис. 1), выполнен расчёт значений автокорреляционной функции (рис. 2) и произведена оценка значимостей коэффициентов автокорреляции на основании выражений (1) и (2).

Количество значимых коэффициентов – два из восемнадцати, при этом значение максимального коэффициента из них составляет 0.704.

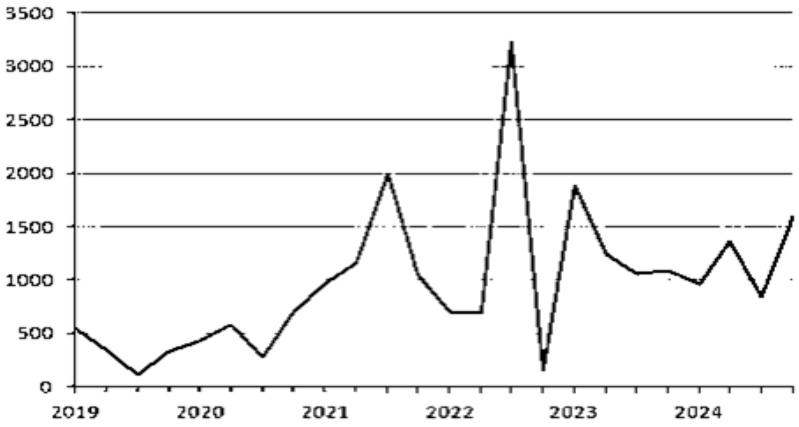



Рис. 1. Исходный динамический ряд количества фишинговых атак

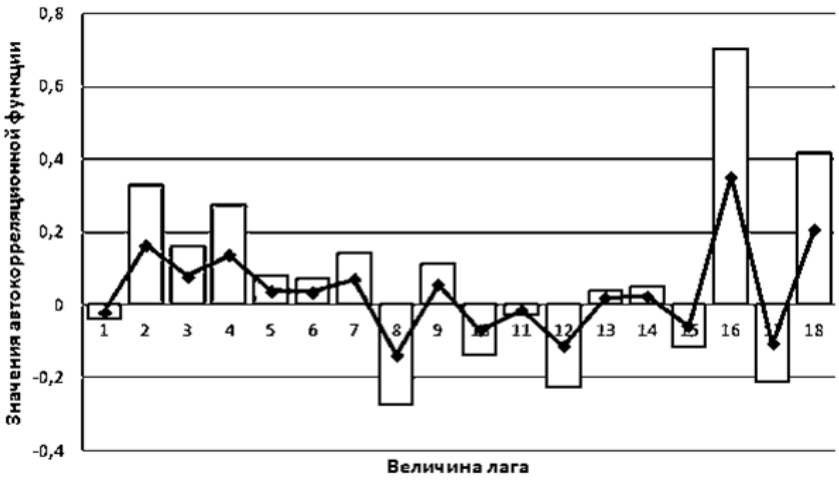



Рис. 2. Коррелограмма распределения фишинговых атак. Ломаной линией обозначены средние значения автокорреляционной функции

Из теории динамических рядов следует, что наличие хотя бы одного значимого коэффициента свидетельствует о существовании циклической компоненты, а также о возможности выделения сезонной и трендовой компонент.

Далее проведено выравнивание исходного динамического ряда фишинговых атак методом скользящей средней. Затем оценены значения сезонной компоненты как разность между фактическими уровнями ряда и центрированными скользящими средними (табл. 1).

В моделях с сезонной компонентой при проведении расчетов, как правило, предполагается взаимопогашение сезонных колебаний в течение оцениваемого периода. В аддитивной модели (3) это выразилось в том, что сумма значений сезонной компоненты по всем кварталам принималась равной нулю после применения корректирующего коэффициента (табл. 2).

Таблица 1

Значения сезонной компоненты для динамического ряда фишинговых атак

| Год | Номер квартала | | | |
|---|---|---|---|---|
| | I | II | III | IV |
| 2019 | 0 | 0 | -208,75 | -5,88 |
| 2020 | 49,13 | 133,88 | -288,13 | -8,63 |
| 2021 | -24 | -86,25 | 737 | -123 |
| 2022 | -555,63 | -620,63 | 1891,75 | -1412,38 |
| 2023 | 533,13 | 39,25 | -141 | -12,5 |
| 2024 | -131,5 | 237,25 | 0 | 0 |

Таблица 2

Скорректированные значения сезонной компоненты

| Квартал | I | II | III | IV |
|---|---|---|---|---|
| Скоррект. оценка | -10,8 | -24,8 | 165,9 | -130,3 |
| Итоговая сумма | 0 | | | |

График сезонных колебаний фишинговых атак на временно́м интервале 2023-2024 гг. приведён на рис. 3.

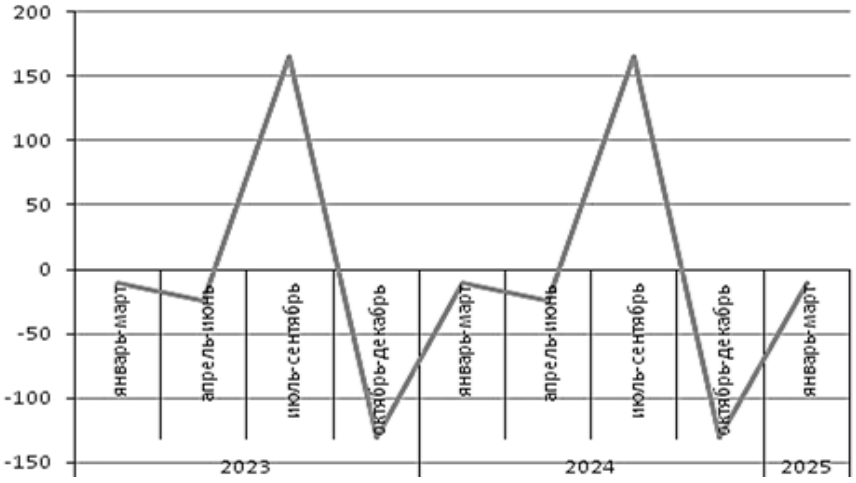



Рис. 3. Сезонная компонента для фишинговых атак

Исходя из графика, представленного на рис. 3, можно заключить, что максимальная активность фишинговых атак приходится на июль-сентябрь. С чем это связано?

Можно предположить, что фишинговые атаки наиболее интенсивны в период отпусков наибольшего количества россиян, когда они получили отпускные, накопили

перед отпуском больше средств, планируя различные туристские, развлекательные и иные поездки, отложенные дела – ремонт квартир, дач, автотранспорта и т.д.

Но это, заметим, только предположения, требующие своего исследования и фактического подтверждения. В этой связи подчеркнем, что представляемый в статье прогноз на данном этапе основывается на внутренних, реально существующих, но пока не объясненных закономерностях реализации фишинговых атак. Которые определяются целым комплексом факторов, требующих своего учета в специальных, довольно сложных математических моделях. Как, впрочем, и другие виды киберпреступлений, возникшие в качестве новых явлений в современном криминальном мире.

Далее, элиминируя влияние сезонной компоненты, посредством вычитания её значений из исходного динамического ряда, получим в каждый момент времени данные, содержащие для этого ряда трендовую (рис. 4) и случайную компоненты (рис.5).

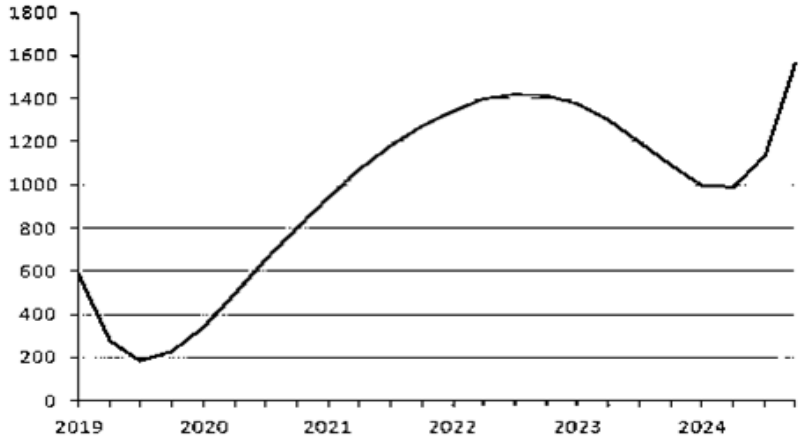



Рис. 4. Трендовая компонента динамического ряда фишинговых атак

Судя по трендовой компоненте на рис. 4., взлёт числа фишинговых атак наблюдался в 2024 году при общей тенденции роста их количества на протяжении 2020-2022 гг. Вопрос о том, произойдёт ли значительный рост количества этих инцидентов в 2025 или в 2026 годах, остаётся пока открытым.

Для этого необходимы дальнейшие исследования динамики этого вида кибератак. Обратимся к результатам моделирования динамики фишинговых атак на основе использования рекуррентной нейронной сети *LSTM*.

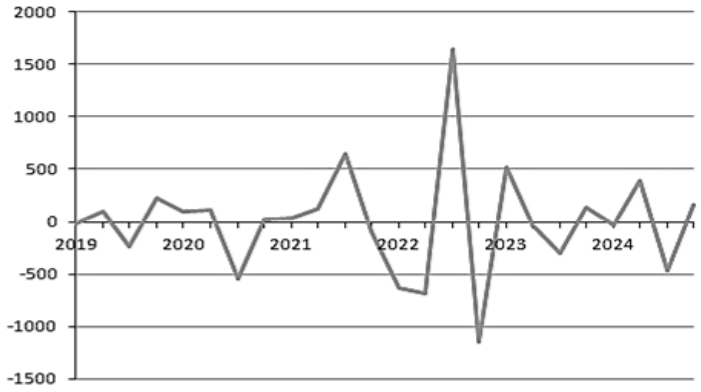



Рис. 5. Случайная компонента динамического ряда фишинговых атак

Программное исполнение модели выполнено на языке *Python*. При этом для выполнения прогностических оценок применен ряд стандартных библиотек. Результаты прогнозных оценок представлены на рис. 6. Линией синего цвета на рис. 6 обозначены фактические данные исходного динамического ряда фишинговых атак за первые три месяца 2025 года, линией красного цвета – значения количества фишинговых атак, полученные на основании прогнозных оценок по *LSTM*-модели.

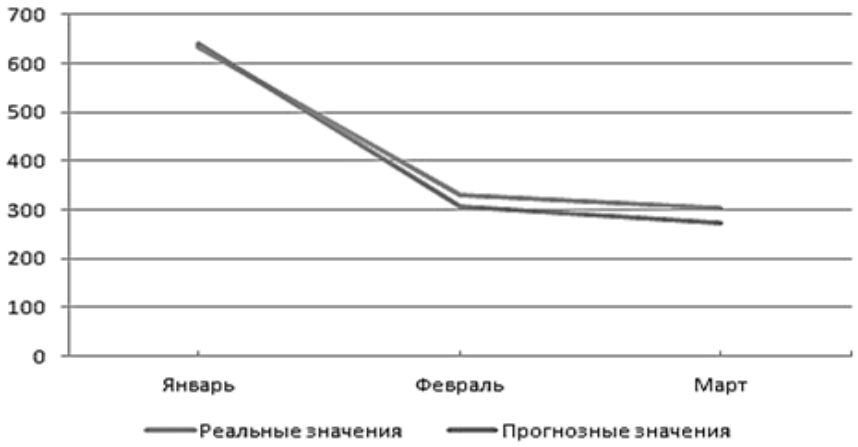



Рис. 6. Реальная динамика и прогноз фишинговых атак в первом квартале 2025

Точность прогноза в среднем составляет 5.95%, то есть прогнозные и реальные данные о количестве фишинговых атак в первый квартал 2025 года весьма близки между собой. Отметим при этом, что прогноз фишинговых атак, выполненный на основании *LSTM*-модели значительно превышает точность модели *Auto ARIMA* и моделей, базирующихся на аппарате обычной экстраполяции.

**Выводы и обсуждение**

В статье поставлена и решена задача прогнозирования фишинговых атак в киберпространстве Российской Федерации. Для этого проведено исследование структуры динамического ряда фишинговых атак, показано, что он четко подразделяется на трендовую, сезонную и случайную компоненты.

При проведении прогностических оценок фишинговых атак использовалась рекуррентная нейронная сеть *LSTM,* обладающая развитыми механизмами постепенного забывания прошлой информации и замещения ее актуальной.

Это дало возможность с высокой точностью (5.95%) по сравнению с моделью *ARIMA* и моделями аппроксимационного характера осуществлять краткосрочные прогнозы фишинговых атак.

**Заключение**

Развиваемые в статье подходы ориентированы на построение системы моделей прогнозирования кибератак, позволяющих на первом этапе использовать нейросетевые модели типа *LSTM* для формирования рабочих гипотез относительно факторного комплекса, определяющего сложные взаимодействия при реализации криминальных явлений в современном информационно-телекоммуникационном пространстве, позволяя затем перейти ко второму этапу – аналитического и имитационного моделирования в сфере противодействия компьютерным атакам в Российской Федерации.

При этом надо понимать, что сегодня отмечается существенное усложнение кибератак, как инструментальное, так и сценарное с появлением множества новых качеств стратегического и тактического характера, а именно:

- за счет предварительной интеллектуальной разведки вторжения

становятся подготовленными, тем самым повышая вероятность успеха и потенциальный ущерб от реализации атаки;

- сочетание множества техник и векторов вторжения атаки становятся многоуровневыми и используют искусственный интеллект;

- машинное обучение не успевает за темпом появления уязвимостей нулевого дня, особенно в части средств искусственного интеллекта.

К тому же, интенсивное применение в противоборстве искусственного интеллекта и средств автоматизации эксплуатации уязвимостей значительно усложняет выработку эффективных мер противодействия атакам злоумышленника, которые становятся все более разнообразными, адаптируясь под известные системы обеспечения информационной безопасности.

Переход сценариев атак от простых к многоэтапным произошел из-за активного развития средств защиты информации, дабы повысить эффективность вторжения намного увеличивая шанс достижения цели. Буквально несколько лет назад сценарии атак ограничивались простым фишингом или DDoS, но за последние годы реализация таких атак перестала приносить успех вследствие разработки эффективных мер обнаружения и реагирования на инциденты информационной безопасности. Это повлекло за собой переход атакующих к более совершенным и продуманным методам атаки, которые позволяют злоумышленникам достигать своей цели с наибольшей вероятностью успеха, так как искусственный интеллект генерирует сценарии кибератаки, который позволяет совершать последовательные продуманные действия, начиная от разведки и проникновения в сеть и заканчивая хищением данных и даже уничтожением системы.

Атаки, основанные на искусственном интеллекте, являются скрытными и адаптивными, так как допускают изменения атакующих техник злоумышленника в реальном времени, в зависимости от реакции систем обеспечения информационной безопасности и применяемых мер противодействия.

Здесь одним из главных факторов усложнения атак является развитие искусственного интеллекта и машинного обучения, что позволяет злоумышленникам автоматизировать рутинные процедуры и также разрабатывать новые методы, тем самым повышая их эффективность, скрытность и масштабируемость, что значительно увеличивает уровень угрозы, как для обычных пользователей, так и для крупных организаций. Наиболее важными и популярными являются следующие направления применения искусственного интеллекта в проведении кибератак:

- целенаправленность атаки: при помощи искусственного интеллекта злоумышленники все чаще подготавливаются к атакам на конкретные организации, что достигается путем нейросетевого анализа большого объема открытых данных об объекте, выявляя уязвимых сотрудников, их интересы, круг общения и другую важную информацию, которая позже будет применена для атаки средствами социнженерии;

- эксплуатация уязвимостей: с помощью машинного обучения для злоумышленника раскрываются большие возможности в области анализа программного обеспечения атакуемых организаций с целью выявления уязвимостей для последующей эксплуатации слабостей системы в ходе атаки;

- адаптивность атаки: искусственный интеллект, обрабатывая информация о текущем ходе выполнения сценария и реакции систем безопасности организации, имеет возможность быстрого анализа ситуации и принятию верных решений, которые приведут атакующего к наибольшей вероятности успеха.

Обобщая вышеизложенное, можно утверждать, что противодействие современным кибератакам, в том числе и фишинговым, не представляется возможным без активного и всестороннего внедрения искусственного интеллекта и машинного обучения.

## Список литературы

1. Лунеев, В. В. Преступность XX века: мировые, региональные и российские тенденции: Монография / В. В. Лунеев. 2-е

изд., переработанное и дополненное. М.: Норма, 2021. 912 с.

2. Авсентьев А.О., Винокуров С.А., Минаев В.А. и др. Основы кибербезопасности: Учебник. М.: ГУРЛС МВД России, 2024. 408 с.

3. Минаев В. А., Бондарь К. М., Андреев А.А. Терроризм и экстремизм: моделирование информационного противодействия: Монография. Хабаровск: РИО ДВЮИ МВД России, 2020. 248 с.

4. О Стратегии национальной безопасности Российской Федерации / Указ Президента Российской Федерации от 02.07.2021 № 400. Доступ из справочной правовой системы «КонсультантПлюс».

5. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы / Указ Президента Российской Федерации от 09.05.2017 № 203. Доступ из справочной правовой системы «КонсультантПлюс».

6. Кильдишев Г.С., Френкель А.А. Анализ временных рядов и прогнозирование. Издание 2-е. M. URSS, 2021. 101 с.

7. Бриллинджер Д. Р. Временные ряды: обработка данных и теория / Пер. с англ. А. В. Булинского, И. Г. Журбенко. М.: Мир, 1980. 536 с.

8. Нильсен Эйлин. Практический анализ временных рядов: прогнозирование со статистикой и машинное обучение. М., СПб.: Диалектика, 2021. 538 с.

9. Shumway R.H., Stoffer D.S. Time Series Analysis and Its Applications. With Examples. Second edition. New York: Springer, 2006. 576 p.

10. Плотников А.Н. Элементарная теория анализа и статистическое моделирование временных рядов. 2-е изд., исправленное и дополненное. СПб.: Лань, 2021. 212 с.

11. Гмурман В.Е. Теория вероятностей и математическая статистика: Учебник для вузов. 12-е издание. М.: Издательство Юрайт, 2024. 479 с.

12. Brownlee J. Time Series Prediction with LSTM Recurrent Neural Networks in Python with Keras. Machine Learning Mastery. 2016. URL: https://machinelearning mastery.com/ time-series-prediction-lstm-recurrent-neural-net works-python-keras (дата обращения 21.09.2025).

13. Deep Learning Memory Option by Alex Nguyen. URL: https://dev.to/alex-nguyen-duyanh/deep-learning-memory-option-by-alexnguyen-2ha6 (дата обращения 21.09.2025).

14. Кратович П.В. Нейронные сети и модели ARIMA для прогнозирования котировок // Программные продукты и системы. 2011. №1. С. 95-98.

Московский университет МВД РФ им. В.Я. Кикотя
Moscow University of the Ministry of Internal Affairs of Russia

Академия управления МВД России
The Academy of Management of the Ministry of Internal Affairs of Russia

Поступила в редакцию 10.09.25

**Информация об авторах**

**Минаев Владимир Александрович** – д-р техн. наук, профессор, профессор кафедры специальных информационных технологий, Московский университет МВД РФ им. В.Я. Кикотя, Москва, e-mail: m1va@yandex.ru

**Фаддеев Александр Олегович** – д-р техн. наук, доцент, профессор кафедры экономической безопасности Рязанского филиала, Московский университет МВД РФ им. В.Я. Кикотя, Москва, e-mail: fao1@mail.ru

**Броненкова Юлия Васильевна** – заместитель начальника кафедры информационных технологий Академии управления МВД России, e-mail: bronenkova87@mail.ru

# MODELING AND FORECASTING PHISHING ATTACKS

**V.A. Minaev, A.O. Faddeev, Yu.V. Bronenkova**

The article discusses the issues of modeling the phishing attacks dynamics in the cyberspace of the Russian Federation based on a recurrent neural network. The task of obtaining predictive information about the number of attacks of this type has been set and solved. A study of the dynamic series structure of a phishing attacks has been conducted to identify its trending, seasonal and random components. Two types of models used in predictive assessments of phishing attacks are considered: the LSTM model and Auto ARIMA. The analysis of the predictive assessments results strongly indicates the significant advantage of the LSTM model. The accuracy of the forecast obtained with its help is on average no more than 6 %. It is concluded that the forecast presented at this stage, based on the actual, but not yet explained patterns of phishing attacks, requires more complex mathematical models for its refinement, taking into account many factors determining this new criminal phenomenon. Recurrent neural networks can be very useful on the first stage of research on other types of cybercrime.

Keywords: phishing attack, modeling, forecasting, recurrent neural network, LSTM model.

Submitted 10.09.25

**Information about the authors**

**Vladimir A. Minaev** – Dr. Sc. (Technical), Professor, Professor of the Special Information Technologies Department, V. Ya. Kikot Moscow University of the Ministry of Internal Affairs of Russia, Moscow, e-mail: m1va@yandex.ru

**Alexander O. Faddeev –** Dr. Sc. (Technical), Associate Professor, Professor of the Economic Security Department of the Ryazan Branch, V. Ya. Kikot Moscow University of the Ministry of Internal Affairs of Russia, Moscow, e-mail: fao1@mail.ru

**Julia V. Bronenkova –** Deputy Head of the Information Technology Department of the Academy of Management of the Ministry of Internal Affairs of Russia, Moscow, e-mail: bronenkova87@mail.ru

**DOI 10.36622/1682-7813.2025.28.3.004**
**УДК 621.372.004**

# АВТОМАТИЗАЦИЯ ОЦЕНКИ И РЕГУЛИРОВАНИЯ РИСКОВ РЕАЛИЗАЦИИ КИБЕРАТАК: ПРОЦЕДУРЫ СБОРА, ОБРАБОТКИ И ХРАНЕНИЯ ДАННЫХ

**Г.А. Остапенко, А.А. Остапенко, М.В. Кондратьев, А.С. Кривошеин, Ю.В. Макаров**

Работа посвящена формализации модуля централизованного сбора, обработки и хранения информации о компонентах графовой модели кибератак. Целью настоящей работы является постановка задач, которые должны решаться внедрением модуля в систему, а также реализации самих алгоритмов, которые должны обеспечивать автоматизированный сбор данных о компонентах графа кибератак, их обработку и обогащение, связанное с повышением целостности и качества данных.

**Ключевые слова:** кибербезопасность, уязвимость, техники атак, шаблоны атак, оценка рисков, машинное обучение, CVSS, EPSS, MITRE ATT&CK.

## Введение

В контексте создания модуля централизованного сбора, обработки и хранения информации о компонентах кибератак, основными задачами являются:

1) формирование модели компонентов кибератак,
2) обработка данных графа компонентов кибератак,
3) генерация ребер графа компонентов кибератак.

Формирование модели компонентов кибератак, которая представляет собой ориентированный мультиграф G=(N, E), где множество узлов N включает следующие элементы:

- шаблоны кибератак;
- техники кибератак;
- слабости, из-за которых возможна реализация атаки;
- уязвимости атакуемых систем,

а множество ребер E включает взаимосвязи между следующими парами узлов:

- шаблоны и техники;
- техники и слабости;
- слабости и уязвимости.

1) Обработка данных графа компонентов кибератак, для чего необходимо назначить веса компонентам графа. У ребер весом является вероятность перехода от родительского узла к конкретному дочернему узлу, что характеризует поведение злоумышленника в выборе того или иного компонента кибератаки для его последующей реализации:

$$W_{\text{узел}\to\text{дочерний узел}} = \frac{P_{\text{дочерний узел}}}{\sum_{j=1}^{N} \text{P}_{\text{дочерний узел } jj}},$$

где $N$ – количество дочерних узлов для материнского узла.

Весом узла является вероятность реализации атаки через данный узел и потенциальный ущерб системе в результате успеха кибератаки. Для узлов уязвимостей вероятность рассчитывается на основе статистических калькуляторов, например, EPSS для CVE. Для остальных типов узлов вероятность рассчитывается с помощью дочерних узлов графовой модели по следующей формуле:

$$P_{\text{узел}} = \sum_{i=1}^{n}\left(P_{\text{дочерний узел } i} \times \prod_{j=1, j!=i}^{n}\left[1 - -P_{\text{дочерний узел } j}\right]\right),$$

где $n$ – номер дочернего узла в графе для материнского узла;

$P_{\text{дочерний узел}}$ – вероятность реализации атаки через дочерний узел.

Риск в данной модели рассчитывается по следующим формулам:

а) для уязвимостей:

$$\overline{Risk_{CVE_j}^{К,Ц,Д}} = P_{CVE_j} * \overline{U}_{CVE_j},$$

где К, Ц, Д – означают влияние на конфиденциальность, целостность или доступность информации;

Р – вероятность эксплуатации уязвимости;

$\overline{U}$- нормированный ущерб, который будет нанесен системе в случае успешной эксплуатации уязвимости.

б) для остальных узлов графа компонентов кибератак:

$$\overline{Risk_{\text{узел}}^{К,Ц,Д}} = \sum_{i=1}^{N} \overline{Risk_{\text{дочерний узел}}^{К,Ц,Д}} * W_{\text{узел}\rightarrow\text{дочерний узел}}.$$

Нормированный ущерб эксплуатации какой-либо из уязвимостей, в контексте данной реализации модуля, рассчитывается по следующей формуле:

$$\overline{U_{К,Ц,Д}} = \frac{CVSS_{CVE_j}^{К,Ц,Д}}{10},$$

где $CVSS_{CVE_j}^{К,Ц,Д}$ – CVSS-оценка по уровню влияния на конфиденциальность, целостность и доступность информации [1];

10 – коэффициент нормировки с учетом максимального значения CVSS.

Для разделения CVSS по уровню влияния на конфиденциальность, целостность и доступность информации используется метод Шепли, который позволяет распределить вклад каждой компоненты безопасности в базовую оценку CVSS [2]. Данный метод реализуется комплексом следующих формул:

$$\phi\Phi_i(v) = \frac{1}{n!} \sum_{p \in (\text{перестановки } N)} \left[v\left(S_p(i) \cup \{i\}\right) - v\left(S_p(i)\right)\right],$$

где $\phi\Phi_i(v)$ – вклад метрики $i \in \{К, Ц, Д\}$ в CVSS Base Score;

$S_p(i)$ – множество метрик, добавленных до i в перестановке p;

$v(S)$ – функция расчета базовой CVSS-оценки при наличии только метрик из S.

После расчета маргинальных вкладов для каждой метрики требуется нормализация, что реализует следующая формула:

$$W_{К,Ц,Д} = \frac{\Phi_{к,ц,д}}{\Phi_к + \Phi_ц + \Phi_д}.$$

И результирующей является формула, которая позволяет рассчитать CVSS для каждой отдельной метрики безопасности информации:

$$CVSS_{CVE_j}^{К,Ц,Д} = CVSS_{CVE_j}^{Base\ Score} \times W_{К,Ц,Д},$$

где $CVSS_{CVE_j}^{Base\ Score}$ – базовая CVSS-оценка критичности уязвимости.

Данные метрики важны для качественного моделирования кибератак с помощью графа и предоставляют достаточный объем информации для последующего анализа.

Генерация ребер графа компонентов кибератак - данная задача является одной из наиболее важных в данном модуле в силу того, что полнота взаимосвязей между узлами графа влияет на качество анализа рисков. Для генерации ребер в данном модуле необходимо реализовать нейросетевую модель обработки естественного языка, которая даст возможность выявлять семантические связи между описаниями конкретных пар узлов, тем самым указывая на возможные связи между анализируемыми парами узлов. Нейросетевая модель основана на

объединении семантических векторов BERT (Bidirectional Encoder Representations from Transformers) и векторов ключевых слов TF-IDF (Term Frequency-Inverse Document Frequency), связка которых позволяет в полной мере обнаруживать взаимосвязи между узлами графа [3, 4].

Необходимо сформировать следующие дополнительные требования к алгоритмическому обеспечению. Данные требования подробно описывают варианты решения существующих проблем обеспечения киберустойчивости автоматизированных систем, учитывая динамику растущего числа угроз и их опасность. Далее приведены задачи, которые относятся к разработке алгоритмического обеспечению данного модуля:

- интеграция разнородных источников данных – ключевое требование, обеспечивающее поддержку различных источников данных о кибератаках, что должно достигаться стандартизацией формата загружаемых данных, а также автоматизированной установкой связей между новыми компонентами;

- работа в режиме реального времени - от алгоритмов модуля требуется поддержка постоянной эффективной работы в условиях, когда влияние киберугроз на информационное пространство быстро увеличивается. Данное требование позволит поддерживать данные в актуальном состоянии, обеспечивая эффективную работу остальных модулей системы;

- автоматизация – от модуля требуется высокий уровень автоматизации всех этапов его работы, сводя к минимуму ручную обработку данных, и тем самым ускоряя общее время реагирования на возникающие угрозы;

- поддержка графовой модели кибератак – алгоритмы должны поддерживать обработку и хранение данных в виде графа, где узлами являются компоненты кибератак, а ребра характеризуют взаимосвязи между этими компонентами, что обеспечивает наглядность модели угроз, поддержку анализа нелинейных сложных атак и быстрый поиск новых угроз;

- поддержка интеграции с другими модулями – от алгоритмов требуется такая структура, которая обеспечит быструю интеграцию с другими модулями системы, что требует использования протоколов обмена данными и возможности расширения функциональности без значительных изменений в существующих алгоритмах;

- точность и полнота информации – ключевое требование к алгоритмам модуля, гарантирующее отсутствие пропусков новых угроз, а также детализированную информацию о кибератаках, что критически необходимо для качественного проведения анализа.

Перечисленные требования важны для преодоления существующих ограничений противодействию новым угрозам кибербезопасности.

**Структура алгоритмического обеспечения**

Модуль централизованного сбора, обработки и хранения информации о компонентах кибератак представляет собой автоматизированное решение, которое дает возможность рассмотреть кибератаки на всех уровнях абстракции. Он обрабатывает следующие компоненты, которые содержит в себе атака:

- шаблоны сценариев атак;

- техники, применяемые в атаках;

- слабости архитектуры атакуемых систем;

- уязвимости атакуемых систем.

Данные компоненты дают достаточное количество информации о современной кибератаке, чтобы эффективно провести анализ рисков и выработать подходящие меры противодействия, даже если злоумышленник совершает многоэтапное нападение.

Главными задачами модуля являются сбор и обработка данных о компонентах кибератак, а также их хранение в графовой базе данных. Схематичное представление взаимосвязей между компонентами можно наблюдать на рис. 1.

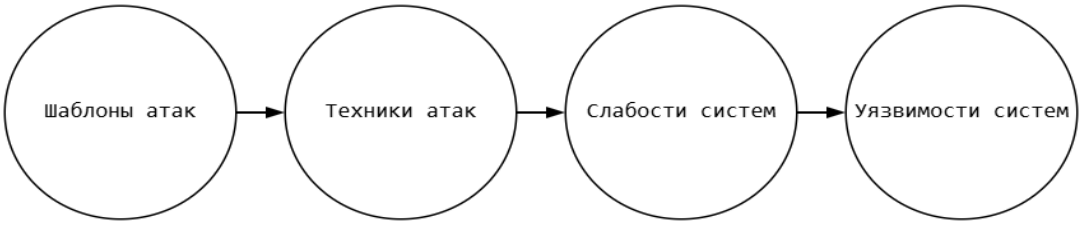



Рис. 1. Схема причинно-следственных связей между компонентами кибератаки

Данная модель кибератаки выделяет такую важную информацию, как:

- планы злоумышленника, которые отображены в шаблонах атак;
- набор техник злоумышленника, с помощью которых возможно выполнение его плана;
- слабости в системе, которые дают возможность атакующему применять определенные техники;
- конкретные уязвимости, которые порождаются слабостями в системе.

В результате, модуль централизованного сбора, обработки и хранения информации о компонентах кибератак, можно разделить на:

- алгоритмы сбора данных – алгоритмы должны обеспечить надежный и расширяемый функционал загрузки данных, необходимых для качественной работы, как настоящего модуля, так и других модулей, интегрированных в систему. Они должны поддерживать разные источники и давать возможность обеспечить полностью автоматизированный сбор данных о компонентах кибератак, что очень важно в условиях быстро развивающихся киберугроз;
- алгоритмы обработки данных – алгоритмы должны в полном объеме обрабатывать информацию, которая хранится в базе данных, с целью обогащения данных о киберугрозах, что обеспечит взаимодействующие модули качественной и полной информацией о кибератаках, что должно повысить их эффективность. В этом контексте алгоритмы должны с высокой точностью вычислять такие метрики, как нормированный ущерб, вероятность эксплуатации узлов, вероятность перехода от родительского узла к конкретному его дочернему узлу, а также риски реализации кибератак. Алгоритмы также должны обладать математической обоснованностью, тем самым подтверждая корректность используемых в расчетах формул;
- алгоритм генерации ребер графа кибератак – алгоритм должен обеспечить быстрое и безошибочное сопоставление узлов графа между собой, тем самым связывая компоненты кибератак с разными типами, так как это напрямую влияет на полноту и эффективность обработки данных настоящим модулем и последующий анализ взаимодействующих модулей.

**Процедуры сбора данных**

1. Загрузка данных через JSON-файл – данный алгоритм необходим для универсальной загрузки данных из любого доступного источника. Формат JSON (JavaScript Object Notation) был выбран для загрузки данных из-за следующих его преимуществ [5]:

- кроссплатформенность – JSON поддерживается большинством наиболее популярных языков программирования, таких как Python, JavaScript, Java и C#, что дает возможность интегрировать модуль в различные системы;
- поддержка API – большинство современных API применяют JSON как основной метод передачи данных между клиентом и сервером;
- простота парсинга и сериализации данных – в большинстве популярных языков программирования есть встроенные, либо библиотечные средства для работы с JSON файлами.

Для успешной загрузки информации в грузовую базу данных требуется собрать необходимые данные и преобразовать их в JSON-файл по заданным шаблонам, в которых для всех типов данных необходимы уникальные идентификаторы и описание. Дополнительно для техник необходимы тактики, которым они соответствуют, а для

уязвимостей важными данными является вероятность эксплуатации и нормированный ущерб. Блок-схема данного алгоритма представлена на рис. 2:

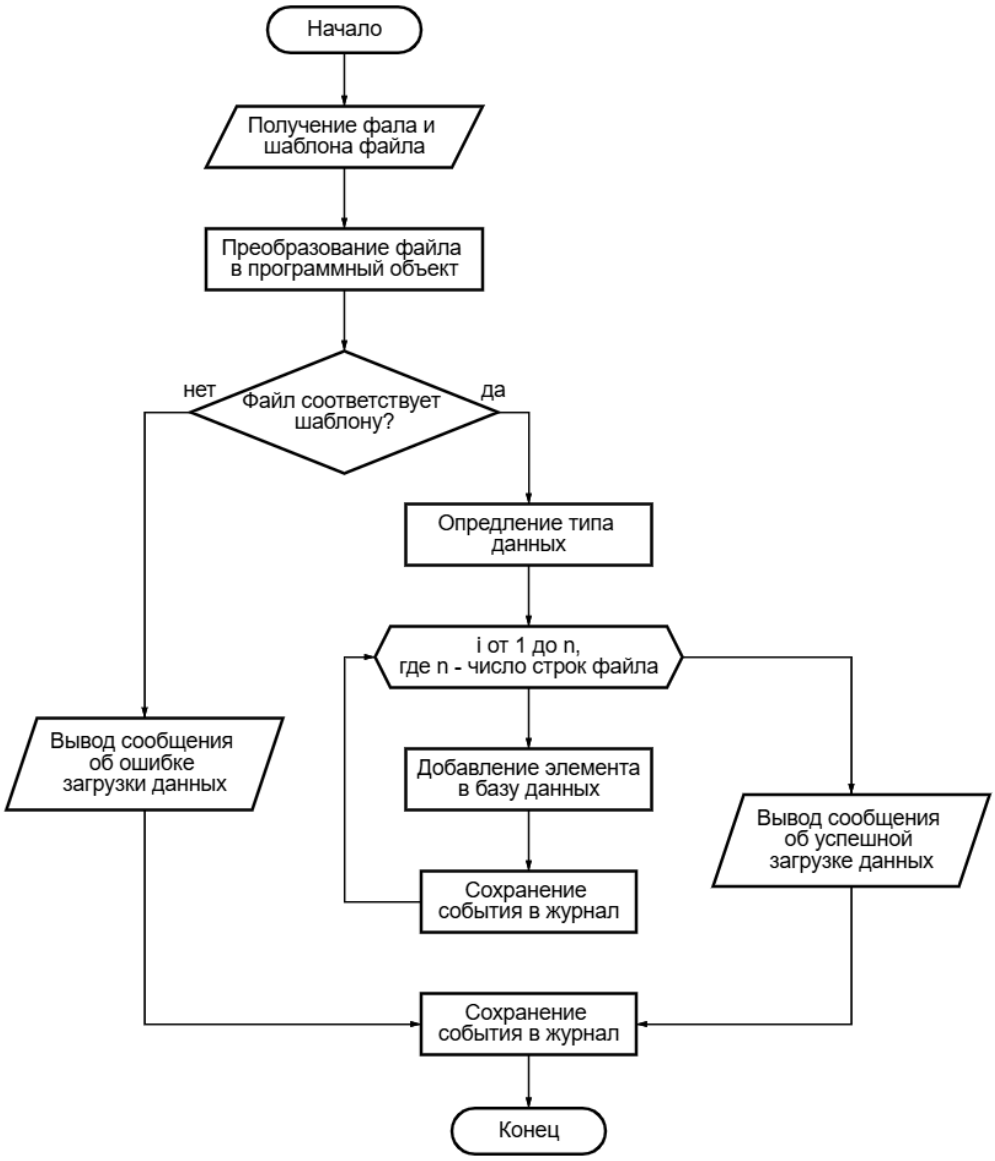



Рис. 2. Блок-схема алгоритма загрузки данных через JSON файл

Данный алгоритм полностью автоматизирует загрузку данных в хранилище информации о компонентах кибератак, предварительно проверяя структуру получаемого файла на соответствие шаблонам, а также сохранение всех событий, которые происходят во время работы в журнал, что гарантирует контроль за работой модуля.

2. Автоматизированная загрузка данных из внешних источников – источниками данных были выбраны такие наиболее популярные и авторитетные ресурсы, как: NVD и MITRE:

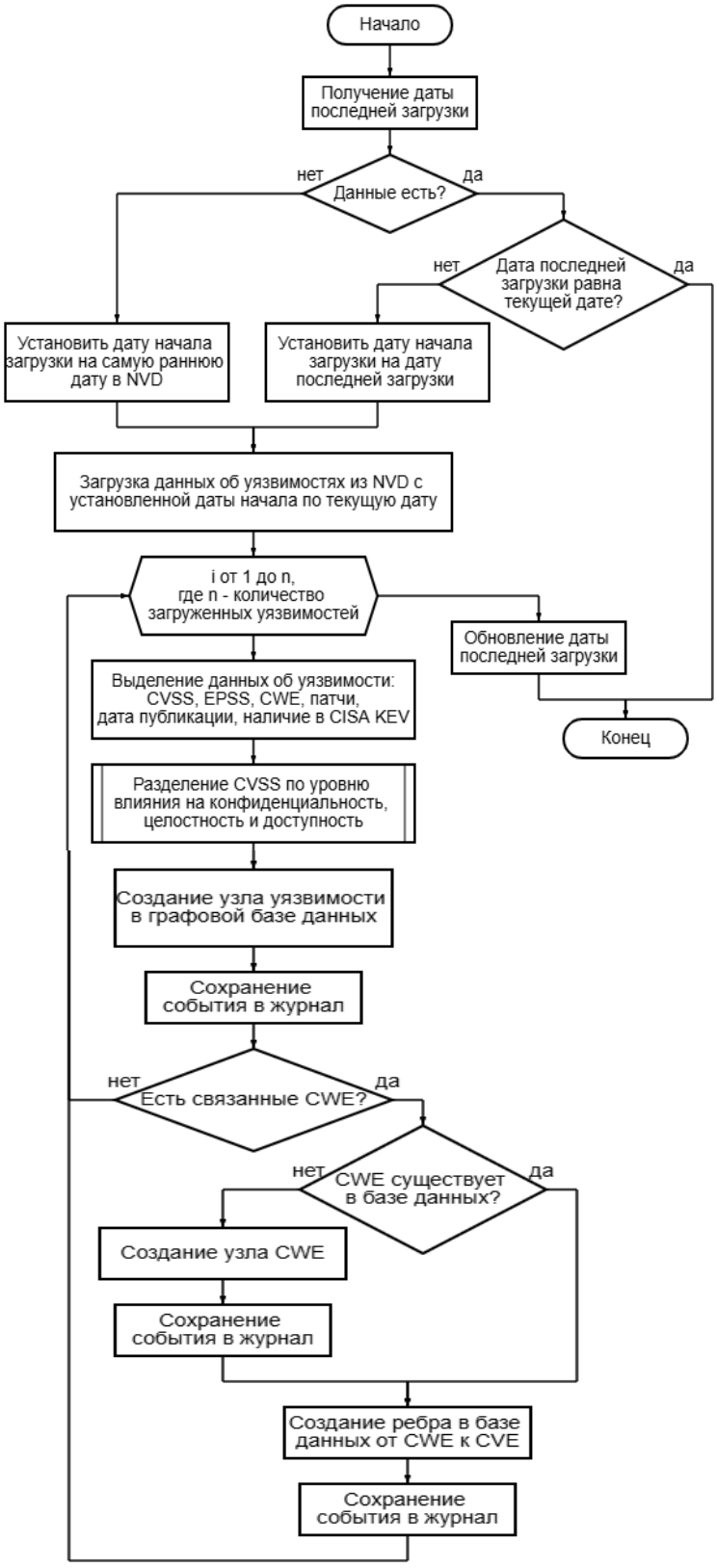



Рис. 3. Блок-схема алгоритма автоматизированной загрузки CVE из базы NVD

а) загрузка уязвимостей из базы данных NVD – NVD (National Vulnerability Database – база данных уязвимостей, которая содержит информацию о большинстве известных уязвимостей программного обеспечения. В этой базе данных каждой уязвимости присваивается свой уникальный идентификатор CVE (Common Vulnerabilities and Exposures) [6]. Также для уязвимостей составляется список данных, в который включены: описание, уровень опасности (CVSS), дата обнаружения и публикации и

рекомендации по устранению. Еще одним наиболее важным для автоматизации преимуществом NVD является наличие открытого API, что значительно упрощает алгоритм и ускоряет процесс загрузки и обновления данных.

В начале работы алгоритм должен проверять актуальность существующих данных об уязвимостях, что выполняется путем сверки последней даты загрузки. После чего из NVD загружается информация о новых уязвимостях, которая накапливается в массивы данных, включая в себя такие важные составляющие CVE, как: уникальный идентификатор, описание уязвимости, дату ее публикации, оценку CVSS и существующие исправления. Кроме того, происходит обогащение данных о CVE ее оценкой EPSS, характеризующей вероятность эксплуатации уязвимости за ближайшие 30 дней, а также наличие уязвимости в списке CISA KEV (Cybersecurity and Infrastructure Security Agency Known Exploited Vulnerabilities), что позволяет выявить наиболее популярные в эксплуатации уязвимости [7, 8].

Одним из этапов является алгоритм разделения CVSS по уровню влияния на конфиденциальность, целостность и доступность, что дает возможность проводить не только общую оценку критичности атаки, но и ее угрозу основным свойствам безопасности информации. Представление алгоритма в виде блок-схемы изображено на рис. 3

Также важным достоинством алгоритма является то, что из NVD загружаются данные о взаимосвязях уязвимостей со слабостями CWE, которые эксперты выявили в ходе исследований. После любого действия, связанного с изменением информации в базе данных, информация о нем обязательно сохраняется в журнал, что значительно повышает безопасность.

б) загрузка слабостей из MITRE CWE - CWE (Common Weakness Enumeration) - система классификации слабостей программного обеспечения, представленная в виде списка типовых слабых мест архитектуры. В этой базе данных каждому типу уязвимости присваивается уникальный идентификатор CWE с ее подробным описанием, распространенностью, а также рекомендациями по предотвращению появления таких слабостей в программном обеспечении.

Наиболее важными достоинствами CWE является структурированность и широкая применимость, что предоставляет такие возможности в обеспечении безопасности информации, как использование на этапах: разработки, тестирования и анализа программного обеспечения. Главным преимуществом CWE в модели кибератак принято считать, что слабости в программном обеспечении помогают выявлять не только конкретные инциденты безопасности, как это делает CVE, но и понимать причины, из-за которых данные уязвимости возникли.

В начале работы алгоритм осуществляет проверку актуальности данных. Так как MITRE публикует наиболее актуальные данные в виде файлов на своем сайте, то проверка на обновление информации должна проводиться путем сопоставления хэша файлов (уникальных строк символов, являющихся цифровыми отпечатками содержимого файлов). Если хэш последней загрузки совпадает, то из этого следует, что содержимое файла CWE MITRE не менялось, и обновление слабостей графовой базы данных не требуется.

В случае же, когда файла предыдущей загрузки нет (загрузка слабостей в графовую базу данных происходит впервые) или когда хэш файлов не совпал, происходит загрузка данных и парсинг (сбор и структурирование информации, содержащейся в файле), при котором формируются такие поля слабости, как: уникальный идентификатор CWE, описание слабости и распространенность. Кроме обработки этой информации происходит и обновление связей между CWE и CVE или техниками MITRE ATT&CK. В конце успешной загрузки данных хэш файла последней загрузки обновляется. Блок-схема данного алгоритма изображена на рис. 4.

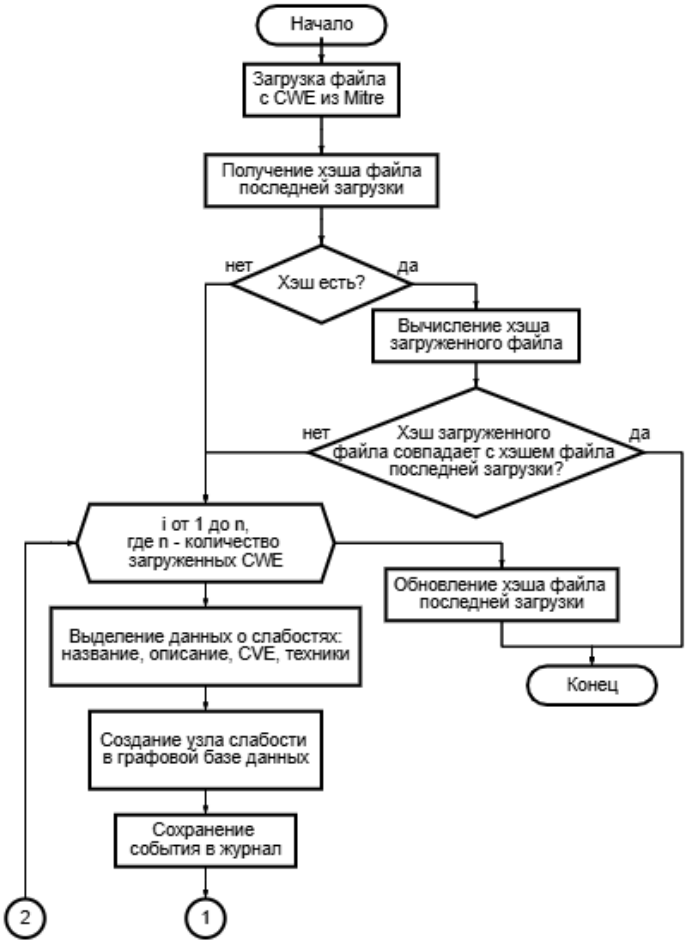



Рис. 4. Блок-схема алгоритма автоматизированной загрузки слабостей из MITRE CWE

в) загрузка техник из MITRE ATT&CK - MITRE ATT&CK – это база данных включающая в себя информацию о тактиках и техниках, которые злоумышленник использует на различных этапах кибератаки. В информацию о техниках входят такие данные, как: уникальный идентификатор, подробное описание, связанные тактики, а также методы обнаружения и меры защиты, которые помогают предотвратить или ослабить воздействие кибератаки на систему.

Важным преимуществом использования техник данной базы знаний является высокие структурированность и степень детализации, так как описываются все этапы кибератак, начиная от разведки и первоначального доступа и заканчивая эксфильтрацией данных и деструктивным воздействием на систему. Наличие информации о связанных тактиках позволяет в будущем сформировать граф сценариев кибератак, который сможет моделировать реалистичное и точное поведение злоумышленников, в отличие от современных популярных методов, что подходят к этому избыточно линейно. Такие важные достоинства делают MITRE ATT&CK наиболее приоритетным инструментом для моделирования и анализа кибератак.

Из-за того, что данной базой данных владеет MITRE, то актуальность загруженной информации о техниках, подобно предыдущему алгоритму, проверяется при помощи сверки хэшей загруженного ранее файла и файла с последней информацией на сайте MITRE. Процесс обновления или же первоначальной загрузки данных схож с загрузкой CWE, но важным отличием является создание взаимосвязей, которые выявили эксперты MITRE, между обновляемой техникой и шаблонами сценариев CAPEC или слабостями CWE.

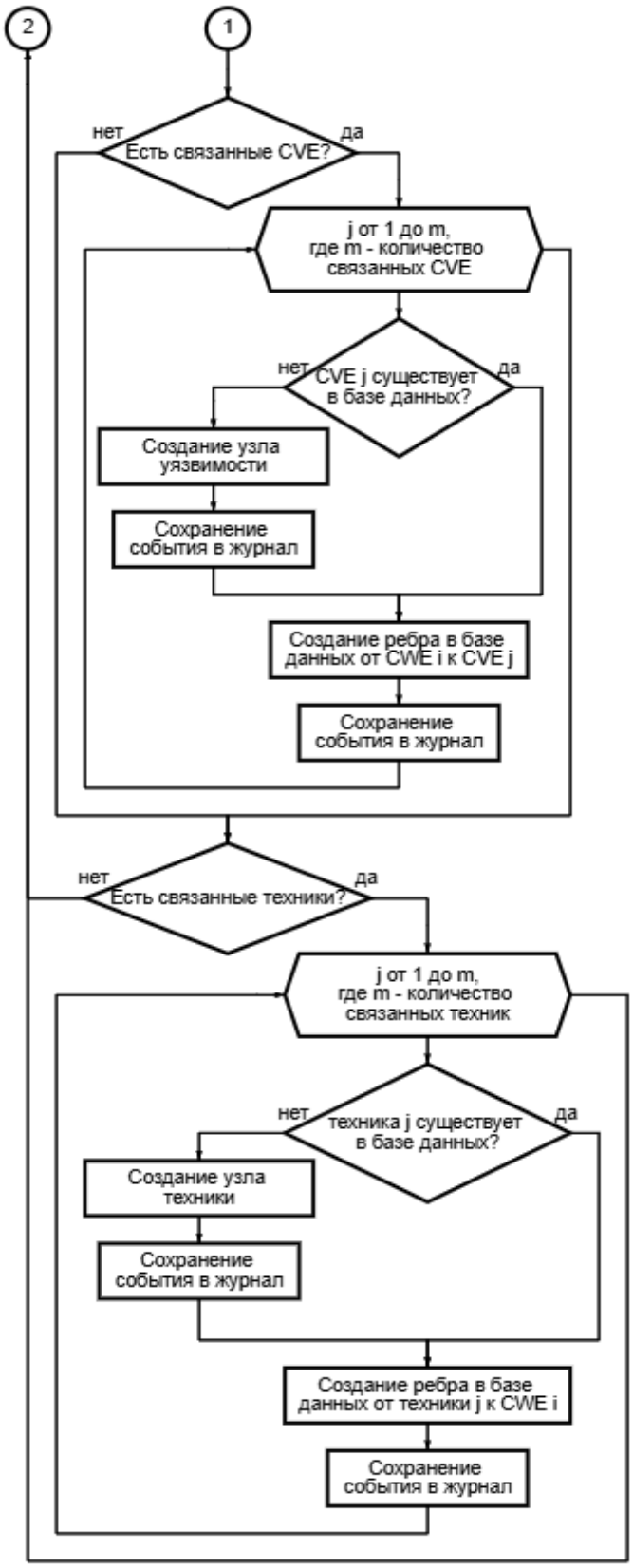



Рис. 4. Продолжение

В конце успешного завершения обеспечения корректную проверку формирования новых данных хэш актуальности при следующем запуске загружаемого файла сохраняется с целью

алгоритма. Блок-схема алгоритма представлена на рис. 5.

г) загрузка шаблонов сценариев из MITRE CAPEC – CAPEC (Common Attack Pattern Enumeration and Classification) - база знаний, созданная для классификации атак на основе реальных угроз. В CAPEC для каждого отдельного шаблона сценариев атаки описываются такие данные, как его уникальный идентификатор, описание целей атакующего, последовательности его действий и предпосылок для их реализации.

Главным преимуществом этой базы данных является то, что она фокусируется на сценариях атак, применяемых против различных систем и технологий. Это позволяет использовать CAPEC для объединения различных техник кибератак, что были интегрированы в данный модуль ранее, тем самым моделируя множества сценариев атак, реализуемых злоумышленниками, основываясь на их поведении и целях.

Включение шаблонов сценариев кибератак из базы знаний CAPEC обеспечивает следующие возможности:

- моделирование поведения злоумышленника на основе сценариев кибератак;
- связь между тактиками злоумышленника, а соответственно, и его техниками;
- поддержка анализа современных сложных многоэтапных атак, включая нелинейные сценарии развития.

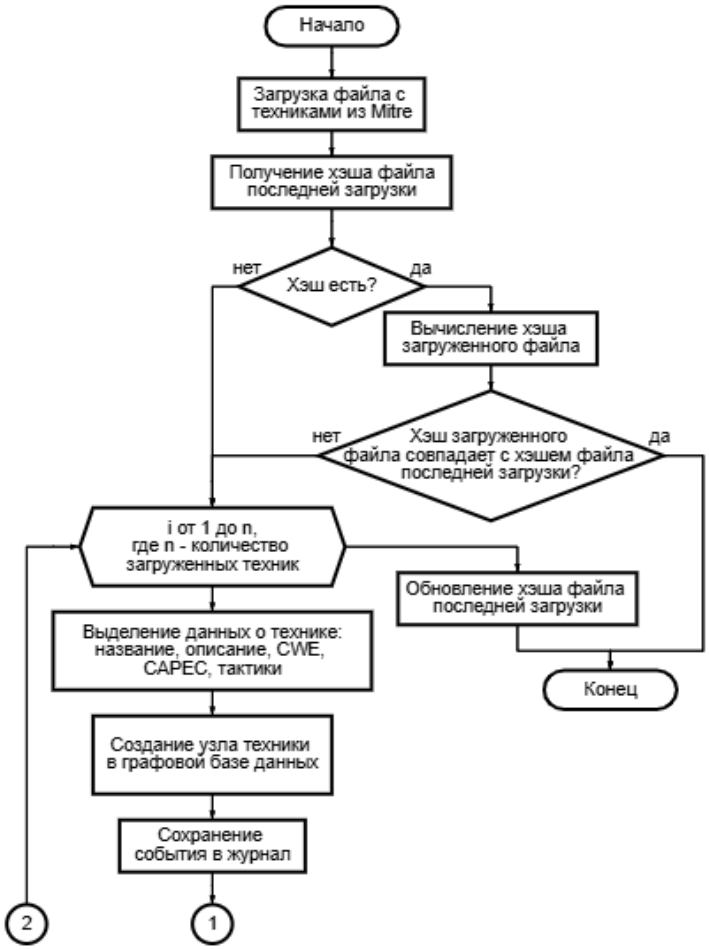



Рис. 5. Блок-схема алгоритма автоматизированной загрузки техник из MITRE ATT&CK

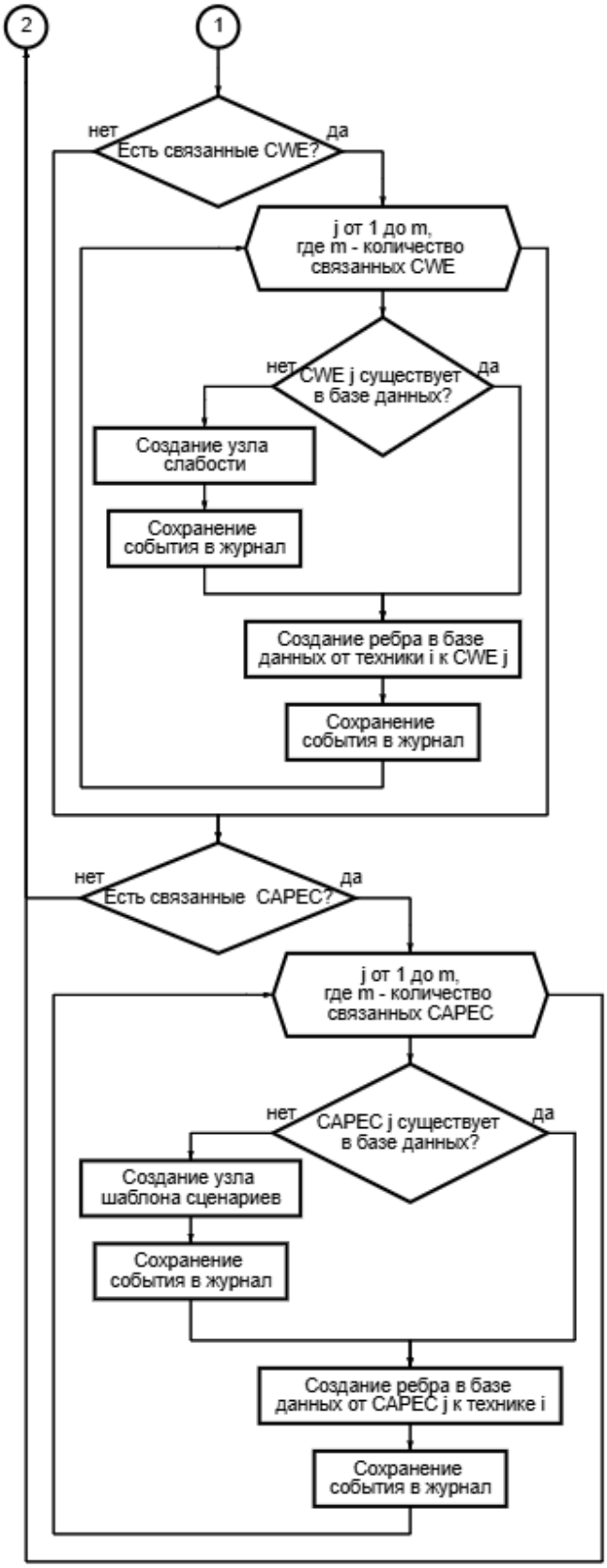



Рис. 5. Продолжение

Для автоматизированной загрузки информации о шаблонах сценариев кибератак из MITRE CAPEC используется аналогичный подход, как и при работе с CWE и техниками ATT&CK. Алгоритм начинает работу с проверки актуальности

существующих данных, сравнивая хэш ранее загруженного файла с хэшем последней версии, что доступна на официальном сайте MITRE CAPEC. В случае, если текущие данные устарели или же загрузка выполняется впервые, запускается процесс загрузки и парсинга файла, предоставляемого MITRE, в результате чего формируются такие поля о шаблонах сценариев кибератак, как: уникальный идентификатор CAPEC, название и подробное описание шаблона, а также взаимосвязи с соответствующими техниками MITRE ATT&CK.

После успешного завершения загрузки и обработки данных, хэш нового файла сохраняется в локальное хранилище. Блок-схема алгоритма представлена на рис. 6.

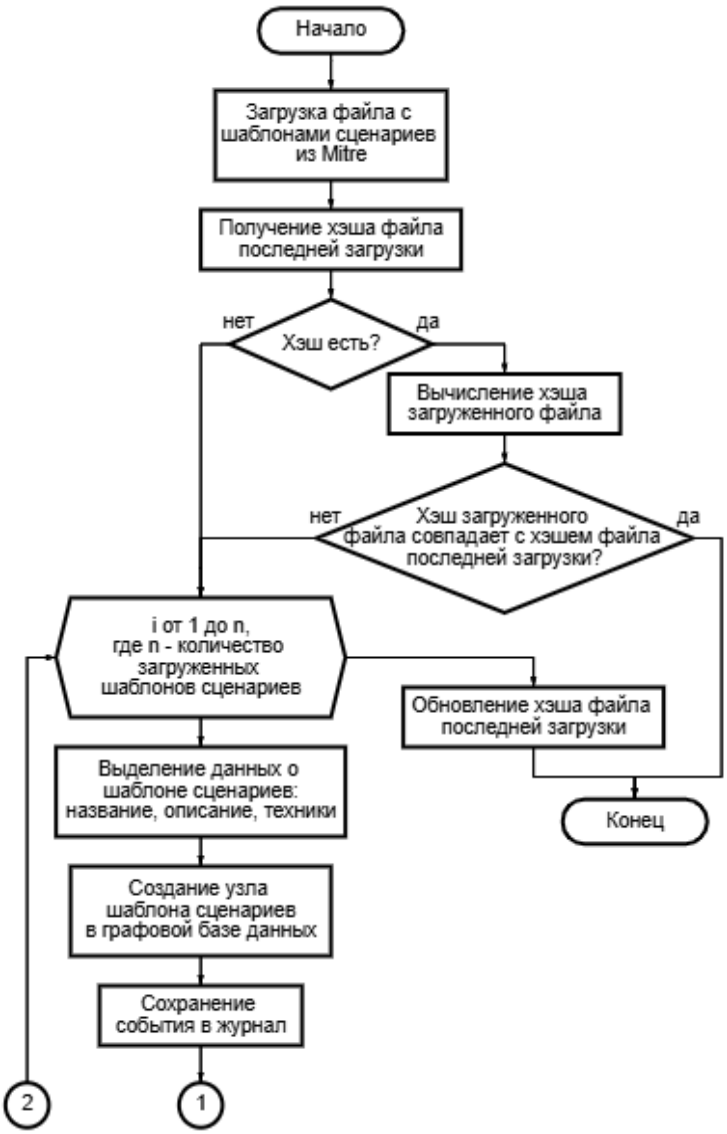



Рис. 6. Блок-схема алгоритма автоматизированной загрузки шаблонов сценариев из MITRE CAPEC

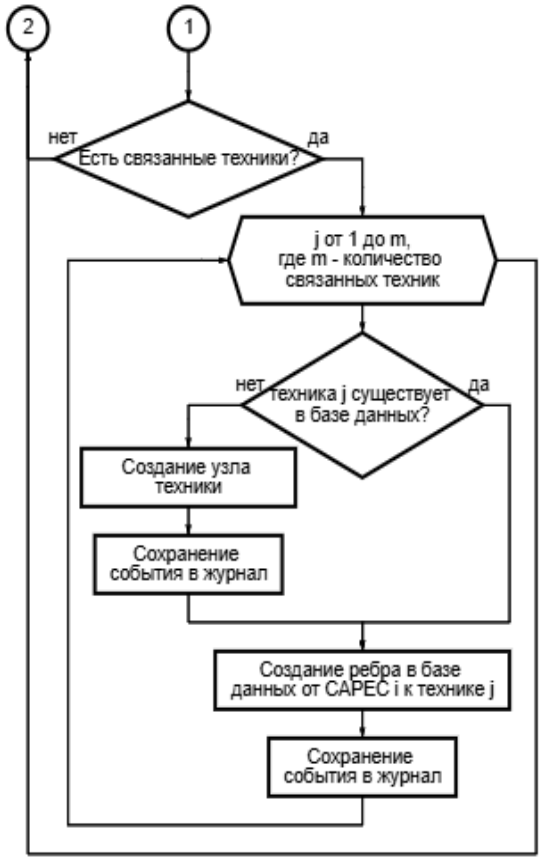



Рис. 6. Продолжение

е) автоматическое обновление графовой базы данных – алгоритм автоматического обновления графовой базы данных необходим для обеспечения актуальности информации о компонентах кибератак. Он играет ключевую роль в выполнении одного из самых важных требований к алгоритмическому обеспечению, а именно работы системы в режиме реального времени.

Данный алгоритм отвечает за периодический запуск комплекса алгоритмов загрузки данных из внешних источников, которые были приведены ранее, тем самым обеспечивая постоянное обновление актуальных данных о кибератаках без необходимости ручного вмешательства со стороны пользователя. Выполнение таких задач позволяет системе оперативно реагировать на новые кибератаки, своевременно дополняя появившиеся данные.

Данный алгоритм имеет гибкую структуру, так как дает возможность пользователю самому выбрать временной интервал, с периодичностью которого будет происходить обновление базы данных. Данный интервал задается в минутах, обеспечивая возможность выбора большого спектра частот проверки обновлений. После ввода значения интервала и между обновлениями алгоритм находится в режиме ожидания.

По истечении заданного временного интервала алгоритм активирует ранее разработанные алгоритмы:

- автоматизированной загрузки уязвимостей из NVD;
- автоматизированной загрузки слабостей из MITRE CWE;
- автоматизированной загрузки техник из MITRE ATT&CK;
- автоматизированной загрузки шаблонов сценариев из MITRE CAPEC.

Из-за того, что в каждом из этих алгоритмов заложен функционал проверки актуальности уже имеющихся данных, данный подход в алгоритме является наиболее эффективным. При выявлении обновлений алгоритмами производится загрузка этих данных, их парсинг и обогащение, а также обновление связей между различными компонентами кибератак. Таким образом, алгоритм автоматического обновления графовой базы данных позволяет поддерживать модель кибератак в актуальном состоянии, что особенно важно в условиях быстро меняющихся угроз.

После завершения цикла обновления алгоритм снова переходит в режим ожидания, тем самым начиная новый отсчёт времени. Таким образом, процесс обновления данных является бесконечным и выполняется пока общая система находится в рабочем состоянии. Блок-схема алгоритма представлена на рис. 7.

В результате построены алгоритмы сбора данных, которые реализуют надежную, автоматизированную и гибкую систему загрузки и обновления информации о компонентах кибератак в графовой базе данных. Эти алгоритмы позволяют:

- поддерживать актуальность информации в режиме реального времени;
- интегрировать разнородные источники данных;

- обеспечивать полноту и точность модели кибератак;
- поддерживать дальнейший анализ рисков и построение защитных мер на основе качественной и структурированной информации.

Алгоритмы сбора данных являются основополагающей частью функциональности настоящего модуля и системы в целом.

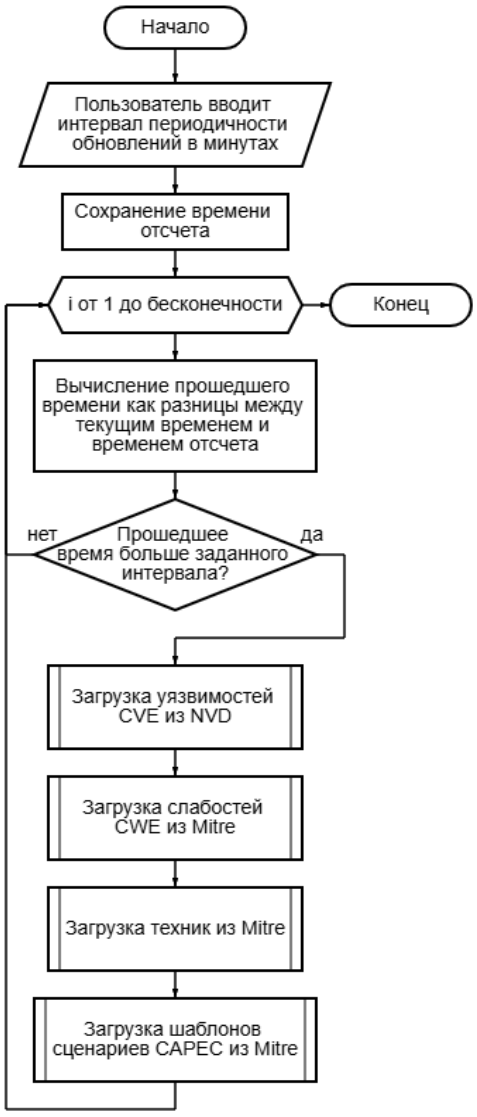



Рис. 7. Блок-схема алгоритма автоматического обновления графовой базы данных

**Процедуры обработки данных**

Алгоритмы обработки данных в модуле централизованного сбора, обработки и хранения информации о компонентах кибератак представляют высокую значимость. Данные, которые загружаются из внешних источников, имеют обобщенный вид и предназначены больше для обзора, чем для полноценного управления рисками, а их обработка и вычисление дополнительных метрик безопасности информации значительно обогащают базу данных. Далее будут рассмотрены алгоритмы, необходимые для полноценного функционирования модуля.

1. Алгоритм разделения CVSS по уровню влияния на конфиденциальность, целостность и доступность информации - в данном алгоритме реализован метод Шепли в контексте распределения вклада каждой метрики безопасности информации в базовую оценку CVSS, что существенно расширяет возможности анализа рисков кибератак, позволяя выявлять только самые важные объекты для защиты.

Алгоритм получает на вход версию и вектор CVSS, после чего происходит цикл со всевозможными перестановками метрик конфиденциальности, целостности и доступности информации. Для каждой такой коалиции происходит расчет базовой оценки CVSS с конкретной метрикой и ее отсутствием в коалиции, и наконец вычисляется маргинальный вклад данной метрики, как разница между базовыми оценками CVSS, рассчитанными до и после добавления этой метрики в коалицию.

После того, как для каждой метрики и перестановки рассчитан свой вклад, происходит усреднение этого вклада в контексте каждой из трех метрик: конфиденциальности, целостности и доступности, путем деления этого вклада на количество перестановок.

И в результате отнормирования вклада каждой метрики делением на сумму вкладов всех метрик, появляется возможность найти значение CVSS, которое влияет на определенную метрику безопасности информации, путем умножения базового значения CVSS, рассчитанного по начальному вектору CVSS, на нормированный вклад метрики в это самое базовое значение.

Наглядное отображение данного алгоритма изображено в виде блок-схемы на рис. 8.


Рис. 8. Блок-схема алгоритма разделения CVSS по уровню влияния на конфиденциальность, целостность и доступность информации

2. Алгоритм расчета вероятности успешной эксплуатации узла в ходе атаки. Вероятность успешной эксплуатации узла в ходе атаки является важным значением для анализа рисков, так как именно она позволяет определить наиболее вероятные направления кибератак.

У уязвимостей CVE, как наименее абстрактных и наиболее распространенных по количеству успешной эксплуатации элементов рассматриваемой модели кибератак, имеется возможность статистического расчета вероятности эксплуатации. Так, из большого количества обнаруженных эксплуатаций уязвимостей в различных системах, а также информации о наличии в них эксплойтов, возможно определение статистической вероятности эксплуатации той или иной уязвимости, что и было реализовано для CVE системой EPSS, которая позволяет оценить вероятность эксплуатации уязвимости в ближайшие 30 дней.

Зная вероятность эксплуатации уязвимостей, которые являются фундаментальными элементами графовой модели кибератак, можно осуществить агрегирование данных вероятностей на более абстрактные уровни модели. Таким образом, данный алгоритм решает задачу расчета вероятностей эксплуатации слабостей и техник, а вероятности реализации шаблонов атак не представляют интереса в силу того, что модуль генерации сценариев кибератак рассматривает данные шаблоны более подробно и с высокой точностью.

Работа алгоритма начинается с получения конкретного родительского узла и всех его дочерних узлов, у которых уже имеются вычисленные вероятности, что гарантируется шаблонами загружаемых файлов в алгоритмах сбора данных рассматриваемого модуля.

После получения всех необходимых данных выполняется этап вычисления вероятности эксплуатации узла, результатом которого должна быть вероятность того, что какой-либо один из дочерних узлов будет проэксплуатирован в ходе атаки. Алгоритм совершает перебор дочерних узлов и для каждого вычисляет вероятность, что именно этот узел будет проэксплуатирован, а все

остальные нет. Результат полученных вероятностей суммируется и тем самым рассчитывает вероятность, что только один из дочерних узлов будет проэксплуатирован. Блок-схема алгоритма расчета вероятности успешной эксплуатации узла в ходе атаки изображена на рис. 9.

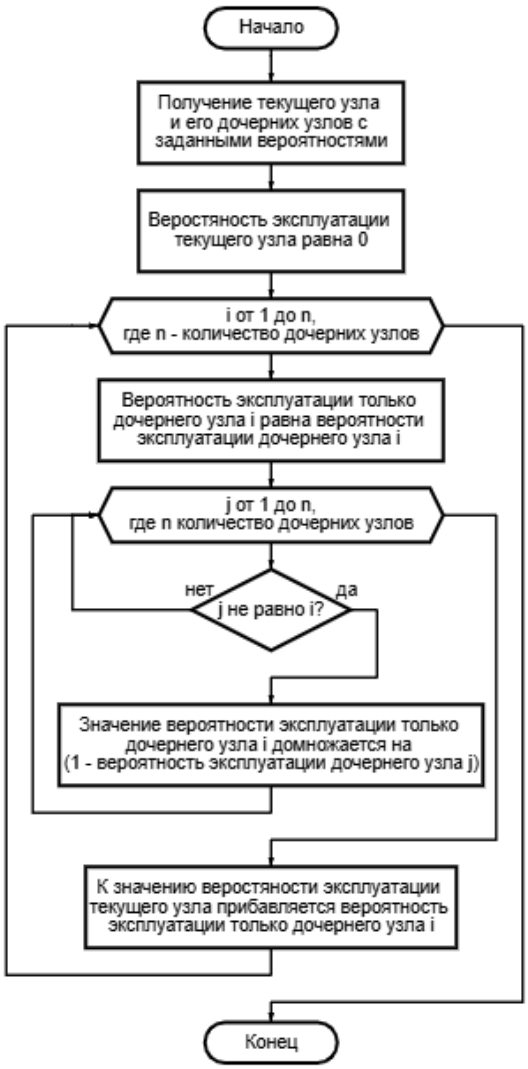



Рис. 9. Блок-схема алгоритма расчета вероятности успешной эксплуатации узла графа в ходе атаки

3. Алгоритм расчета вероятности выбора злоумышленником следующего дочернего узла. Расчет вероятности применения дочернего узла в контексте конкретного узла следующего уровня абстракции в модели кибератак одно из самых важных требований информационного обеспечения. Это значение описывает логику злоумышленника в том, что он будет использовать только те техники и уязвимости, которые с наибольшей вероятностью смогут обеспечить успех атаки и достижение поставленной цели атакующим. В конкретной атаке от любого узла вероятность перехода к какому-либо дочернему узлу равна 100%, поэтому алгоритм реализует расчет вероятности как пропорцию вероятности конкретного дочернего узла к сумме вероятностей всех дочерних узлов.

Алгоритм начинает работу с получения родительского узла в контексте кибератаки, целевого дочернего узла, вероятность перехода к которому нужно рассчитать, а также остальных дочерних узлов с вероятностями их эксплуатации. Далее происходит расчет суммарной вероятности эксплуатации всех дочерних узлов, данное значение может принимать значение больше 1, так как оно используется только для определения пропорции вероятности эксплуатации целевого дочернего узла к сумме всех дочерних узлов.

Заключительным этапом алгоритма является нахождение частного вероятности эксплуатации целевого дочернего узла к сумме вероятностей эксплуатации остальных дочерних узлов, что и является вероятностью применения дочернего узла в ходе реализации атаки. Визуально данный алгоритм изображен в виде блок-схемы на рис. 10.

4. Алгоритм расчета рисков является одним из фундаментальных алгоритмов в контексте обеспечения информационной безопасности, поскольку дает возможность осуществлять количественную оценку элементов графа кибератак, учитывая при этом вероятности возникновения инцидента и ущерб, который он может причинить системе. При этом, не учитывая риск, невозможно точно ранжировать угрозы и тем самым вырабатывать эффективные меры противодействия и обоснованные решения по обеспечению безопасности информации.


Рис. 10. Блок-схема алгоритма расчета вероятности перехода к дочернему узлу графа

Так как данный алгоритм расчёта рисков применяется не только к конкретным уязвимостям, но также и к слабостям, техникам и шаблонам атак, то он обеспечивает возможность проводить анализ не только с технической стороны реализации кибератаки, но и с организационной стороны, учитывая условия, при которых атака может быть совершена злоумышленником. Данный подход позволяет сосредоточить внимание на наиболее опасных угрозах безопасности информации, что повышает эффективность организационно-правового управления рисками информационной безопасности.

Данный алгоритм рассчитывает риски для следующих узлов:

- уязвимости – значения риска рассчитывается как произведение вероятности эксплуатации и нормированного ущерба. В рассматриваемой графовой модели риск уязвимости является фундаментальным значением и все остальные риски графа зависят от него;

- слабости и техники - для узла риск рассчитывается как взвешенная сумма рисков дочерних узлов, то есть суммируются произведения риска дочерних узлов на вероятности выбора злоумышленником этих узлов. Таким образом происходит агрегация рисков к более абстрактным уровням модели.

- шаблоны атак - так как шаблоны описывают возможные сценарии кибератак, то риск такого узла рассчитывается на основе рисков сценариев. Алгоритм генерирует сценарии шаблона, а также рассчитывает их риски при помощи модуля генерации сценариев кибератак. После получения необходимых данных, алгоритм суммирует риски каждого из сценариев атаки, тем самым получая риск шаблона атаки.

Результатом работы алгоритма является рассчитанный риск для каждого из доступных типов узлов графовой модели кибератак. Полученные данные важны для взаимосвязанных алгоритмов и модулей разрабатываемой системы, ведь они позволяют ранжировать узлы по уровню их опасности.

Блок-схема алгоритма расчета рисков изображена на рис. 11.

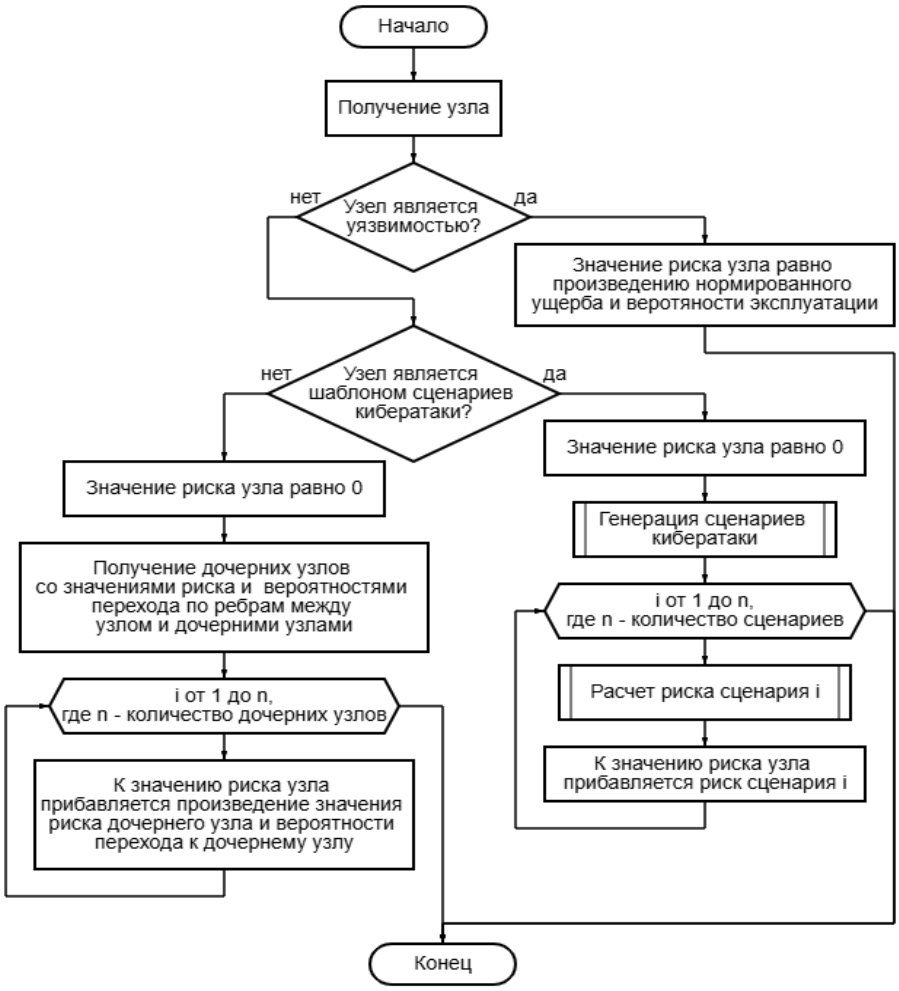



Рис. 11. Блок-схема алгоритма расчета рисков

**Процедуры генерации ребер графа кибератак**

Полнота компонентов графа кибератак является неотъемлемым условием для получения точных результатов анализа рисков, а также для промежуточных вычислений, производимых другими алгоритмами системы. Обеспечение полноты данных в графовой базе данных является одной из основных задач информационного обеспечения, разработанного для данной системы автоматизированной генерации мер и сценариев противодействия кибератакам.

Алгоритм генерации ребер графа кибератак в своей работе использует подход оценки ансамблированного сходства между векторами BERT, которые указывают на семантические данные об узле, а также векторами TF-IDF, описывающие ключевые термины, применяемые в

При работе алгоритм обеспечивает генерацию ребер графа кибератак между следующими парами узлов:

- между слабостями и уязвимостями;
- между техниками и слабостями;
- между шаблонами атак и техниками.

Для каждой из пар узлов происходит перебор узлов для всякой пары, тем самым внутри пары объединяются новые пары, но уже между узлами, а не между типами узлов. Для каждой пары узлов происходит расчет смысловых векторов BERT и векторов ключевых слов TF-IDF. Эти векторы сравниваются между собой и вычисляется косинусное сходство, после чего данные объединяются в ансамбль, где сходство векторов BERT имеет 70 % от объединенного значения, а остальные 30 % имеет сходство векторов TF-IDF. Данное соотношение подобрано так, чтобы семантика в контексте сравнения описаний имела доминирующую роль, но ключевые

слова, применяемые в описаниях, все же учитывались в конечном результате. Также точность таких пропорций между косинусным сходством векторов подтверждается в ходе множества разработок систем анализа естественного языка.

После вычисления ансамблированного сходства алгоритм совершает проверку на условие, превышает ли оно порог в 80 процентов. Если значение выше порогового, то происходит создание нового ребра в графе между парой рассматриваемых узлов и внесение данных о созданном ребре в журнал. Если же значение вычисленного сходства меньше порогового значения, то алгоритм пропускает данную пару. Пороговое значение было подобрано экспериментально, ибо в случаях, когда значение было выше 80 процентов происходил пропуск важных связей между узлами графа кибератак, в свою же очередь значение ниже 80 процентов генерировало большое количество ребер для пар узлов, связь между которыми слабо обоснована и тем самым снижает целостность модели.

Алгоритм обеспечивает полноту графа кибератак, тем самым гарантируя наиболее эффективный процесс анализа рисков и точность сформированной модели кибератак. Наглядное представление данного алгоритма изображено в виде блок-схемы на рис. 12.

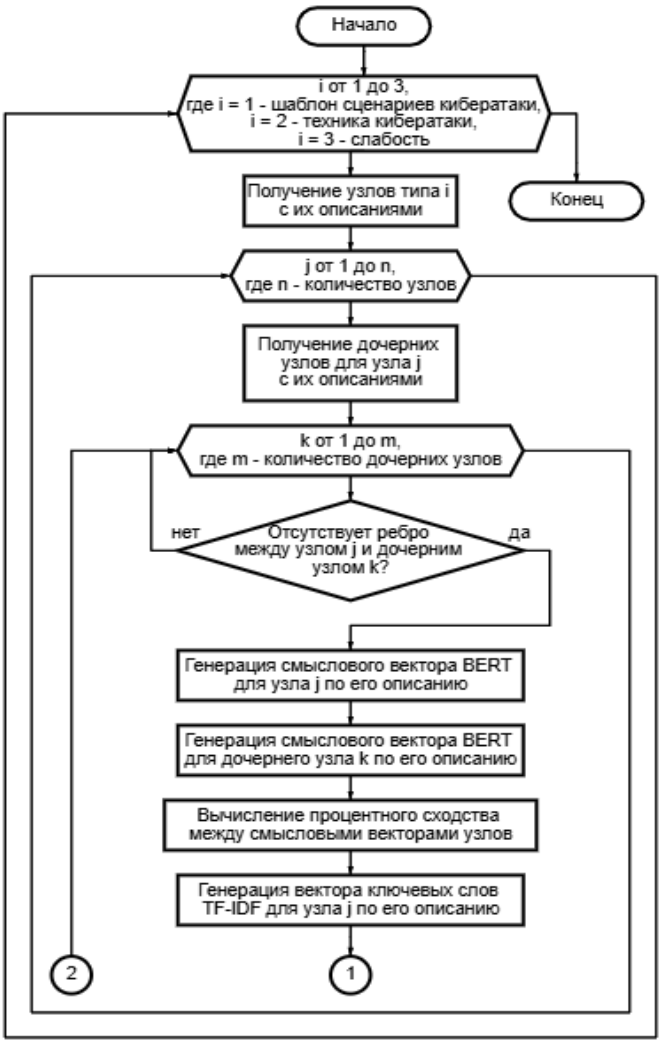



Рис. 12. Блок-схема алгоритма генерации ребер графа кибератак

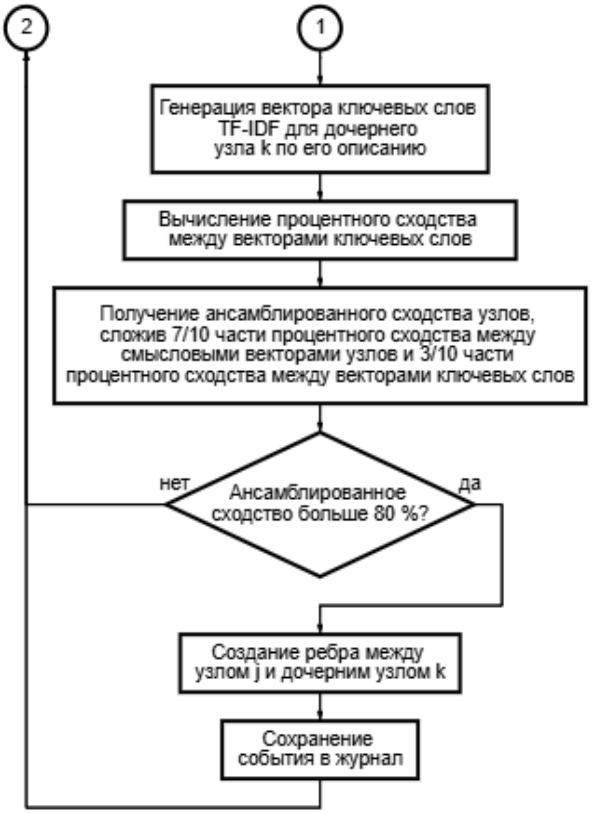



Рис. 12. Продолжение

**Заключение**

В результате были сформированы ключевые требования к алгоритмическому обеспечению модуля централизованного сбора, обработки и хранения информации о компонентах кибератак, а также рассмотрены требования методического обеспечения для автоматизированной генерации мер и сценариев противодействия кибератакам. Во исполнение этих требований методического обеспечения были сформулированы и решены следующие задачи:

- формирование графовой модели кибератак - для решения данной задачи был разработан как универсальный алгоритм для загрузки данных через JSON файл на основе разработанных шаблонов, так и узконаправленные алгоритмы агрегации данных из таких внешних источников как: NVD для загрузки уязвимостей CVE, MITRE для загрузки слабостей программного обеспечения CWE, техник MITRE ATT&CK и шаблонов атак CAPEC;

- обработка данных графовой модели - задача была решена разработкой комплекса алгоритмов, позволяющих рассчитать такие веса узлов, как нормированный ущерб, вероятность эксплуатации и риск информационной безопасности. Для ребер графа был разработан алгоритм расчета вероятности перехода от узла более высокого уровня иерархии к конкретному дочернему узлу;

- генерация связей между различными типами узлов графа - задачу решает алгоритм, подразумевающий в своей реализации нейросетевую модель, которая будет на основе анализа семантической взаимосвязи и ключевых слов между описаниями узлов выбирать наиболее релевантные связи, обеспечивая точность и полноту графовой модели.

Дополнительные требования к алгоритмическому обеспечению были сформированы на основе проведенного исследования современных киберугроз и недостатков существующих средств противодействия им. Они включают в себя следующие пункты:

- интеграция разнородных источников данных;

- поддержка работы в режиме реального времени;

- высокий уровень автоматизации;

- возможность интеграции с другими модулями системы;

- обеспечение точности и полноты информации.

Предъявленные к алгоритмам требования были полностью реализованы, что обеспечило модулю высокую функциональную целостность, а также адаптивность к стремительно развивающемуся киберпространству и угрозам, циркулирующим в нем.

В ходе работы была полностью сформирована разработанная структура модуля, которая включает в себя такие части как:

- алгоритмы сбора данных, позволяющие загружать информацию в графовую базу данных как в ручном, так и в автоматическом режиме, обеспечивая тем самым актуальность и полноту данных;

- алгоритмы обработки данных, реализующие вычисления важных метрик графа;

- алгоритм генерации ребер графа, использующий методы машинного обучения (BERT + TF-IDF) для установления новых взаимосвязей между компонентами графа кибератак, что значительно повышает полноту модели и её аналитическую ценность.

Таким образом, было разработано алгоритмическое обеспечение, которое доведенот до программной реализации, объединяющей в себе автоматизированный сбор, анализ, обогащение и хранение информации о компонентах модели кибератак. Благодаря этому возникнет такие важные преимущества как: оперативное реагирование на новые угрозы и анализ рисков, необходимый для последующей генерации эффективных мер противодействия.

В результате разработанный модуль централизованного сбора, обработки и хранения информации о компонентах модели кибератак обеспечивает основу для последующей автоматизированной генерации мер и сценариев противодействия кибератакам.

## Список литературы

1. CVSS v4.0 Документация. URL: https://www.first.org/cvss/specification-document (дата обращения 20.08.2025).

2. Теория игр: Модель Шепли. URL: https://chiefauto.ru/blog/teoriya-igr-model-shepli-i-ee-primenenie-v-marketinge (дата обращения 20.08.2025).

3. BERT (языковая модель). URL: https://neerc.ifmo.ru/wiki/index.php?title=BERT_(%D1%8F%D0%B7%D1%8B%D0%BA%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C) (дата обращения 20.08.2025).

4. TF-IDF (Term Frequency-Inverse Document Frequency). URL: https://www.geeksforgeeks.org/understanding-tf-idf-term-frequency-inverse-document-frequency/?ysclid=mcmzciujto168940424 (дата обращения 20.08.2025).

5. Понятие JSON и работа с форматом данных JSON. URL: https://ru.hexlet.io/blog/posts/ponyatie-json-i-rabota-s-formatom-dannyh-json?ysclid=mcmzfdngmu860802487 (дата обращения 20.08.2025).

6. NVD – Vulnerabilities. URL: https://nvd.nist.gov/vuln (дата обращения 20.08.2025).

7. Exploit Prediction Scoring System (EPSS). URL: https://www.first.org/epss/

8. The KEV Catalog | CISA. URL: https://www.cisa.gov/resources-tools/resources/kev-catalog (дата обращения 20.08.2025).

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 23.08.2025

**Информация об авторах**

**Остапенко Григорий Александрович** – д-р техн. наук, профессор, Финансовый университет при Правительстве Российской Федерации, e-mail: ost@fa.ru

**Остапенко Александр Алексеевич** – аспирант, Воронежский государственный технический университет, e-mail: alexostap123@gmail.com

**Кондратьев Максим Витальевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Кривошеин Александр Сергеевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Макаров Юрий Вадимович** – студент, Воронежский государственный технический университет, e-mail: makarov0130@gmail.com

# AUTOMATION OF ASSESSMENT AND REGULATION OF RISKS OF IMPLEMENTATION OF CYBER-ATTACKS: PROCEDURES FOR COLLECTING, PROCESSING AND STORING DATA

**G.A. Ostapenko, A.A. Ostapenko, M.V. Kondratyev, A.S. Krivoshein, Yu.V. Makarov**

The work is devoted to the formalization of a module for centralized collection, processing and storage of information about the components of a graph model of cyber attacks. The purpose of this work is to formulate the tasks that should be solved by implementing the module into the system, as well as implementing the algorithms themselves, which should provide automated collection of data about the components of the graph of cyber attacks, their processing and enrichment associated with increasing the integrity and quality of the data.

**Keywords:** cybersecurity, vulnerability, attack techniques, attack patterns, risk assessment, machine learning, CVSS, EPSS, MITRE ATT&CK.

Submitted 23.08.2025

**Information about the authors**

**Gregory A. Ostapenko** – Dr. Sc. (Technical), Professor, Financial University under the Government of the Russian Federation, e-mail: ost@fa.ru

**Alexander A. Ostapenko** – graduate student, Voronezh State Technical University, e-mail: alexostap123@gmail.com

**Maksim V. Kondratyev** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Alexander S. Krivoshein** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Yuriy V. Makarov** – student, Voronezh State Technical University, e-mail: makarov0130@gmail.com

**DOI 10.36622/1682-7813.2025.28.3.005**
**УДК 004.056**

# УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДЕСТРУКТИВНЫХ ИДЕОЛОГЕМАХ

**А.С. Овчинский, К.К. Борзунов**

Исследование смыслового содержания детской литературы высветило угрозы информационной безопасности, которые возникают на ранних этапах жизни людей. В более 60% просмотренных детских книжек был выявлен вредоносный контент. Основные деструктивные темы включали: предательство, неопределенность или смену половой принадлежности, сочетание несовместимого, неестественное изменение социальных ролей, отклонение от нормы, безразличие к будущему, вариации в подходах к смерти «живи быстро, умри молодым». Издание книг с «творческими находками» зарубежных авторов щедро финансируется известными западными фондами, деятельность которых направлена на распространение нужных им смыслов. Делается акцент на том, что на фоне цифровой трансформации, открывающиеся «удобства» оставляют без внимания задачи обеспечения информационной безопасности образовательной сферы. Речь идет не только о защите сознания от вредоносной информации, но и о необходимости с детства развивать способности мыслить и усваивать знания. Отмечаются угрозы клипового, кнопочного, навигационного мышления. Порожденные цифровизацией уязвимости сознания создают пространство и непосредственно для идеологической деструкции. В условиях нарастающего противостояния России со странами Западной Европы все большее значение приобретает защита исторического наследия, традиционных культурных и духовных ценностей. Отмечается, что хотя пока не сложилось консолидированное мнение о необходимости иметь государственную идеологию, понятие “деструктивная идеология” уже вошло в правовое поле. Обсуждаются возможности применения самообучающихся нейронных сетей для контроля смыслового наполнения издаваемых книг, а также использование систем генеративного искусственного интеллекта в противоборстве идеологической деструкции.

Ключевые слова: информационная безопасность, детская литература, вредоносный контент, защита сознания, образовательная сфера, идеологическая деструкция, искусственный интеллект.

## Актуальность гуманитарного направления информационной безопасности

То обстоятельство, что информационная безопасность является весьма емким понятием уже вполне очевидно. На начальном этапе, с появлением электронно-вычислительных машин оно формировалось вокруг задач, связанных непосредственно с необходимостью обеспечить безопасность информации на электронных носителях и, естественно, с защитой автоматизированных систем обработки данных.

Однако с течением времени акценты неудержимо смещались. С развитием электронных коммуникаций и с расширяющимся доступом к глобальной сети все более явно на первый план выдвигались проблемы не столько защиты информации, сколько защиты сознания людей и целых народов от целенаправленно распространяемой вредоносной информации.

Так, наряду с необходимостью решения технических проблем, задачи обеспечения информационной безопасности все в большей мере охватывали и гуманитарные сферы. Этот «охват» расширяется с цифровой трансформацией, качественно меняющей не только характер деятельности, но и образ жизни людей. Заметим, что согласно Доктрины информационной безопасности РФ (2016) – это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз.

Драматичные события отечественной истории наглядно свидетельствуют о том, что в условиях обостряющейся конфронтации с западным миром наибольшего внимания требуют угрозы информационной безопасности именно в

социальной, культурной и духовной сферах жизни современного общества.

**Актуальность** исследований гуманитарных аспектов информационной безопасности обусловлена и тем, что в ментально-когнитивной войне деструктивные воздействия на сознание принимают все более изощренный характер. От откровенной антироссийской пропаганды они переходят в область скрытого внедрения в сознание деструктивных идеологем, направленных на деформирование мировоззрения, в первую очередь, подрастающего поколения.

При этом анализ многочисленных акций пролонгированной информационной войны, которая ведется против России, вскрывает такие угрозы, которые возникают не только в неожиданных сферах, но и в жизни россиян на самых разных ее этапах, включая детские годы.

**Неожиданные ракурсы информационной безопасности**

Так, учрежденный в декабре 2022 года Союзом писателей России (СПР) Совет по детской книге провел необычное исследование, которое, как оказалось, было напрямую направлено на выявление угроз информационной безопасности. Стояли задачи выяснить, как функционирует современная издательская деятельность и что, собственно, транслирует детская книжка юным читателям. Были отобраны более тысячи книг от около двухсот издательств.

Изучение оформления, тиражей и непосредственно содержания показало, что более 60% книг для детей оказались вредоносными и вообще деструктивными [1]. Можно сказать, открылся такой фронт глубинной информационной войны, результаты стратегических операций на котором ожидаются через 20-30 лет. Непосредственно в сегодняшних детских книжках было выявлено пять основных деструктивных тем, которые могли между собой переплетаться.

**Основные деструктивные темы в детских книжках**

Первое направление – ***предательство***. Эта тема тонко встраивается в повествование. Ее, как правило, сложно заметить и осознать сразу. Например, утка нашла яйцо и высидела его. Вылупился крокодил, утка его воспитала, и он пошел и убил всех других крокодилов. Это не известный «гадкий утенок», который вырос, оказался лебедем, нашел своих и был ими принят. В «новом варианте»: тебя воспитали, ты вырос, ты должен пойти и убить.

В другой книжке. «Солдатик снял мундир, и никто не обвинил его в том, что он – дезертир. При этом есть строчки, в которых заключена главная мысль: «От солдата ничего не зависит». Эти книжки рекомендуется прочитать детям до трех лет. Их воздействие вполне ощутимо. На вопрос о том, кем хочешь стать, когда вырастешь, находятся мальчики, которые отвечают: «Хочу стать дезертиром».

Второе деструктивное направление, которое прослеживается в детских книгах сегодня, включает темы: ***человек – это животное, неопределенность или смена половой принадлежности, сочетание несовместимого***. Например, у голубой коалы есть друг – птичка. Понять, кто это девочки или мальчики невозможно. Мечта коалы – надеть платье. Но почему-то она этого желания стесняется, а ей говорят, что стесняться нельзя, не надо. Все построено на полутонах. Все герои этих книжек – это сегодня они мальчики, завтра – девочки, послезавтра – непонятно кто.

В другой книге крольчиха, которая живет и одевается как человек, ищет свою любовь. Но она не может найти кролика, она может связать свою жизнь только с лисой. То есть фактически крольчиха начинает жить с тем, кто в реальности охотился бы за ней и, поймав бы, просто убил и съел. Так, весьма изощренно запутывают и, можно сказать, разрушают сознание детей.

Третья деструктивная тема – ***изменение социальных ролей***, в том числе отвержение «традиционных гендерных ролей» мужчины и женщины. Мальчикам не обязательно быть защитниками и героями, а девочкам – стремиться к семейным ценностям. Семья

вообще перестает быть важной ценностью и всячески дискредитируется. Например, на обложке одной из таких книжек изображен ребенок, у которого рвотный рефлекс, его тошнит. На развороте родители разрезают торт из «детей». Из другой иллюстрации видно, что зачать ребенка можно только на ложе смерти.

Но недостаточно опорочить родителей. В книжке, посвященной матери, изображена женщина вся в татуировках. Дочка поясняет: «Любовь моей мамы – как роза с шипами. Она капризнее цветущего сада. В мамином сердце свернулась клубочком волчица». Так в детском сознании формируется, мягко говоря, нетрадиционный образ матери. Но этого недостаточно. Самое главное – чего маму страшит и чего она не боится. «Мама не боится темноты, ее страшит свет!». Это уже подход непосредственно к сатанизму.

Четвертая деструктивная тема – ***отклонение от нормы***. Книжки весьма образно показывают, что не нужно следить за собой, выглядеть определенным образом, вести себя соответственно ситуации. Из них следует, что это неправильно, потому что не надо чему-то соответствовать, надо просто быть таким, каким хочешь. Будь собой и абсолютно неважно каким! В таких книжках через иллюстрации, дающие уродливые образы, ребенку, говорится: норм нет, не имеет значения, как ты себя проявляешь в мире, тебя все равно примут любым. В финале, как правило, намечаются и «перспективы». Читателю сообщают: если вдруг ты захочешь пойти еще дальше, то ничего страшного не будет, даже если ты станешь, например, вампиром или оборотнем, это также нормально.

В другой массе книг встроена подмена смыслов и ролей, Например, бабушка теперь – Пират, а дедушка – Фей. Что может поведать бабушка о приключениях на корабле под черным флагом, как грабить и убивать? Видимо это единственное, что хочет передать бабушка своим внукам. Они приезжают к ней гостить и начинают «зажигать».

Пятая, условно завершающая, вредоносная и, пожалуй, наиболее деструктивная тема – ***безразличие к будущему***. Это книги, которые внушают идею о том, что не нужно задумываться о том, что ждет впереди. Все построено так, чтобы привести ребенка к мысли, что жизнь не самоценна. При этом жить, дружить, общаться, встречаться, решать какие-то задачи и проблемы, к чему-то стремиться, чего-либо достигать – все это глупость, это не является важным. Взамен внимание ребенка фокусируется на том, что у него есть лучший друг – это смерть. Смерть становится ориентиром во множестве детских книг. Постепенно ребенка приводят к мысли о том, что если вдруг у тебя есть какая-то проблема или трудность, если с тобой что-то произошло – ничего страшного, у тебя же есть смерть! Так, в одной из книг персонаж Смертиус изображен настолько харизматичным, он обладает такими качествами, что хочется быть на него похожим.

На книжных страницах в разных вариациях звучит популярный лозунг части представителей рок-н-ролл и панк субкультуры: «Live fast, die young» – «Живи быстро, умри молодым» Подобные призывы можно обнаружить не только в детской литературе. Танатизация сознания (Танатос – бог смерти в греческой мифологии), депрессия и суициды – это целое направление в русле деградирующей либеральной идеологии, которое проникло в российскую молодежную среду как трудно истребимый сорняк, укоренилось и дает всходы в самых разных сферах жизни.

## Западные фонды в стратегических операциях глубинной информационной войны

Проведенное исследование показало, что подавляющая часть книг с деструктивным содержанием – это «творческие находки» зарубежных авторов. Авторами книжек для российских детей они оказались благодаря деятельности многочисленных западных фондов. На основе этих фондов в России сложилась и внедрена стройная и весьма эффективная система по распространению нужных им смыслов. Изданная книжка – носитель мировоззрения, мина замедленного действия ментальной войны. Система построена так, что издатель не должен касаться смыслов.

Они заложены, табуированы и, главное, хорошо оплачены. Связь между выпуском вредоносных книг и «помощью» зарубежных фондов не скрывается. Соответствующие отметки есть в самих книгах. В ряду таких фондов наиболее часто встречаются: Институт Гете, Фонд Фридриха Наумана, Фонд Noria (Norwegian literature abroad), Французский институт в Москве при посольстве Франции.

В свое время один из представителей фонда Noria заметил: «Для нас важно, чтобы вот этот рассказ попал к ребенку в 8 лет». Почему? «Все просто: через 30 лет ему будет 38, и тогда, возможно, он придет в политику, во власть». Так, вскрываются механизмы глобальной информационной войны против России. Это не фейки и дипфейки, не провокации и вбросы, которые требуют адекватных реакций «здесь и сейчас». В книжных изданиях, наполненных морально-психологической и скрытой идеологической деструкцией, мы имеем дело со стратегическими операциями глубинной информационной войны. Сейчас, на фоне продвижения российских войск в специальной военной операции, начавшихся контактов с администрацией США, растерянности западноевропейских политиков возникает впечатление, что враг отступает и на «информационных фронтах». Но важно представлять, что отступление – это один из самых сложных маневров в любой войне. Враги России «играют в долгую». Они сражаются хитро и с нарастающим упорством. Их цель, чтобы в России, скажем, лет через 30, пришли к власти люди, вскормленные на их установках.

Сегодняшние детские, да и юношеские книги – это опасная, но одновременно и относительно небольшая платформа заражения сознания подрастающего поколения россиян деструктивными жизненными смыслами. Гораздо большие угрозы накапливает электронная образовательная среда.

**Информационная безопасность сферы образования**

Обратим внимание на то, что на фоне цифровой трансформации учебного процесса и непосредственно преподавания самых разнообразных дисциплин, открывающиеся «удобства» оставляют без внимания задачи обеспечения информационной безопасности образовательной сферы.

Речь идет не только о защите сознания от вредоносной информации, но, главное, о необходимости формирования у граждан страны способностей мыслить самостоятельно, усваивать фундаментальные знания, критически анализировать совокупность поступающих сведений. Не раз отмечалось, как цифровизация гуманитарных сфер порождает и последовательно укореняет «клиповое», «кнопочное», «навигационное» мышление, при котором информация воспринимается все меньшими дозами, знания не становятся объектом усвоения, жизненные смыслы задаются извне. Эти уязвимости сознания новых поколений «цифрового мира» создают пространство и непосредственно для идеологической деструкции.

Так, ярким примером одной из характерных акций ментально-когнитивной войны является учебный курс ***«Россия и деколонизация»***, который уже более года находится в открытом доступе в электронной образовательной среде [2].

В этой акции информационной войны известные русофобы, обосновавшиеся за рубежами нашей страны, преподносят историю развития Российского государства как последовательную насильственную колонизацию многочисленных народов с их эксплуатацией и ограблением. Многочисленные темы онлайн курса посвящены самым разным регионам, входивших и входящих в состав России в различные исторические эпохи.

Уже на этапе анонсированного анализа представленных тем выявляется предельно циничная попытка обратить против России наиболее неприглядные эпизоды истории западной цивилизации. Именно экономическому подъему европейских стран предшествовали грабительские крестовые походы, а начиная с эпохи географических открытий, их «расцвет» происходил за счет использования ресурсов и безжалостной эксплуатации колонизируемых народов.

Творческий подход в очередной деструкции российской истории заключался в обещании щедрой оплаты разрабатываемых проектов – сочинений по многочисленным темам курса. Более того, предполагается на их основе создать учебные материалы и методические пособия по «практике» деколонизации для учителей школ и преподавателей вузов.

Если совсем недавно возможность распада России выглядела некой конспирологической теорией, то с определенного момента план раздела страны был представлен в англо-американском проекте «деколонизация» открыто. Он включает создание в разных регионах страны сепаратистских движений. разжигание экстремистских настроений. Организаторы, по-видимому, не рассчитывают на быстрый успех затеи с расчленением России на отдельные анклавы. Они опять же ориентируются на перспективы подготовить необходимые ресурсы разрушительных идей и заразить ими подрастающее поколение.

**Необходимость «идеологических фильтров» в обеспечении информационной безопасности**

В условиях нарастающего военного, политического и идеологического противостояния России со странами Западной Европы в обеспечении информационной безопасности все большее значение приобретает антропоцентричный подход, предполагающий, в первую очередь, защиту сознания людей, традиционных, культурных и духовных ценностей. В этом направлении принимаются правовые и организационные меры: выявляются иностранные агенты, блокируются нежелательные источники информации, вводятся запреты на пропаганду деструктивных идей, вносятся изменения в школьные и университетские программы обучения.

Так, Министерство юстиции с 2015 года активно закрывает враждебные иностранные и международные неправительственные организации. С их перечнем можно ознакомиться на сайте Минюста. К настоящему времени он содержит 194 позиции. Но до сих пор иностранные фонды, спонсирующие выпуск детских книг, не воспринимались как враждебные; эта тема не считалась значимой. Деятельность этих фондов не рассматривалась в качестве системы влияния, определяющей поведение и формирование мировоззрения детей, которые через 30-40 лет станут не только взрослыми, но и будут определять политику государства.

В значительной мере это связано не только с отсутствием четко оформленной и закрепленной в правовом поле конструктивной идеологии, но и с недостаточным осознанием сущности собственно идеологии и ее роли в жизни людей, развитии социума, перспективами государственного строительства и, в целом, с обеспечением информационной и национальной безопасности.

Заметим, то, что принято понимать под идеологией, а именно некую обобщенную систему (можно сказать, матрицу) взглядов, которые отражают отношение к прошлому, происходящему сейчас, ожидаемому будущему, представляет только одну из ее функций, условно – отражательную. Важно представлять и другую, значительно более значимую роль идеологии, которая заключается в обосновании права на те или иные поступки, на принимаемые решения, последующие действия, даже на образ жизни. Так, выкристаллизовывается наряду с принятой – отражательной функцией идеологии ее более важная – обосновывающая роль.

Несмотря на то, что понятие «идеология» вошло в оборот только в 19 веке, на протяжении всей истории человечества и захватнические войны, и освободительные движения требовали идеологического обоснования.

Идеологическое разнообразие, признаваемое и зафиксированное Конституцией Российской Федерации, в обстановке жесткого информационного противостояния ни коим образом не исключает необходимость иметь четкие ориентиры в виде государственной идеологии.

Положения о разнообразии и необязательности, естественно, призваны

оградить граждан страны от идеологического насилия. Однако сложно представить эффективное управление великой державой, обеспечение ее безопасности и суверенитета, политическую деятельность и военную службу людьми, не спаянными общими целями, зафиксированными ясной, позитивной государственной идеологией.

Хотя в современном российском обществе пока не сложилось консолидированное мнение о необходимости документально зафиксировать конструктивную идеологию, в правовое поле уже прочно вошло понятие “деструктивная идеология”.

В Основах государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей (2022 г.) **деструктивная идеология** предстает как в содержательном, так и в смысловом и даже в целевом ракурсе.

Отмечается, что она представляет собой чуждую российскому народу и разрушительную для российского общества систему идей и ценностей. Ее содержание включает в себя культивирование эгоизма, вседозволенности, безнравственности.

Она направлена на дискредитацию ценности крепкой семьи, брака, многодетности. Ее цель – разрушение традиционной семьи, вплоть до отрицания естественного продолжения жизни с помощью пропаганды нетрадиционных сексуальных отношений.

Эта идеология исключает патриотизм, служение Отечеству, отрицает идеи созидательного труда. Ее важнейшим элементом является непризнание позитивного вклада России в мировую историю и культуру.

История становления и кризисных ситуаций в развитии российской государственности убедительно свидетельствует, насколько опасна идеологическая деструкция. В условиях пролонгированной ментально-когнитивной войны и цифровой трансформации, охватывающей все этапы жизни человека, она становится всё более значимой угрозой социальной стабильности не только на данном этапе, но и в обозримом будущем. Анализ литературы, издающейся для детей, показывает, как глубоко деструктивные идеи и деформация жизненных смыслов проникают в те сферы, в которых формируются личностные качества человека и его гражданская позиция.

**Криминальные идеологические течения**

Значительные вредоносные воздействия на формирование мировоззрения детей и подростков оказывают и откровенно криминальные идеологии. Здесь речь идет уже о внедрении в неокрепшее сознание понятий и представлений, непосредственно ориентирующих на противоправное поведение и преступную деятельность. Завуалированные криминальные мотивы звучат и на страницах книг, ориентированных на подрастающее поколение. Можно выделить определенные направления таких идеологических течений, которые детерминируют в правовом поле общественно опасные и, в целом, недопустимые в цивилизованном мире деяния.

Например, ***идеология «Колумбайн»*** (название школы в США, где были убиты 12 учеников и учитель) породила вал инцидентов с массовыми расстрелами учащихся в самых разных странах. Убийства безоружных людей обосновывались идеей о «никчемности» человеческой жизни, «задушенной» обязанностью работать и учиться. При этом именно школа играет особую роль в «укрощении и истощении» природных качеств человека, учащиеся, «не понимающие своей никчемности, достойны смерти». Они и становились в первую очередь жертвами этой криминальной идеологии уже и городах России.

В информационном поле России проявляют себя и криминальные идеологические течения, зародившиеся на отечественной почве. Среди них набольшее распространение получила ***идеология АУЕ*** (арестантское уголовное единство). Оправдание преступного образа жизни составляет ядро этой идеологии. Ее цель построение «правильного криминального мира» Утверждая неизбежность пребывания в местах лишения свободы, она призывает к

материальной поддержке лиц, отбывающих наказание в местах лишения свободы. Криминальная идеология направлена на молодежь, требуя с детства изучать традиции, нормы, обычаи арестантского сообщества и вести соответствующий образ жизни.

Уже в начале XXI века на мировую арену вышла ***идеология педофилии***. Ключевую роль в оформлении и распространении этой криминальной идеологии сыграли сетевые ресурсы Интернета, в основном – тематические форумы. Получили развитие представления о конструктивности сексуальных отношений между взрослым и ребенком.

Непосредственные угрозы жизни людей и, в первую очередь, подростков несет ***идеология криминального суицида***.

Здесь на первый план выходят представления о смерти как о высшем проявлении протеста и, главное, свободы. Например, многократно воспроизводятся такие образы: «молодые люди подобно китам, которые выбрасываются на берег, совершают самоубийство в стремлении к свободе и в знак протеста «угнетающим» их социальным институтам». Идеология внедрялась через подобные интернет-мемы. Она приводила к трагическим последствиям в суицидально ориентированных играх («тихий дом», «синий кит», «тихое место»). Более того, создавались «группы смерти», в которых коммуникационная практика между участниками, оправдывала и поощряла суицидальные намерения.

## Перспективные технологии идеологического противоборства

В комплексе применения правовых и организационных мер современные технологии открывают возможность создать и непосредственно технические барьеры на пути идеологической деструкции.

Речь может идти о тех возможностях, которые открываются с применением самообучающихся нейронных сетей, скажем, для контроля издательской деятельности. Заметим, что некий прообраз такого контроля уже существует. Так, статьи, подготовленные для публикации, во многих научных журналах проходят проверку на наличие плагиата. Широко известный программный комплекс «Антиплагиат» быстро и весьма эффективно просматривает огромные объемы научной, околонаучной, учебной продукции и выявляет заимствования. При этом применение современных искусственных нейросетей открывает перспективы не только «вылавливать повторы». Определенным образом настроенная и на соответствующих массивах обученная сеть сможет автоматически оценивать степень новизны, актуальности, оригинальности представляемых текстов и многое другое. Заметим, что генеративный искусственный интеллект уже сам создает и научные, и художественные произведения, выдает курсовые и дипломные работы.

Открывающиеся возможности как уже применяемых, так и создаваемых систем искусственного интеллекта могут составить технологическую базу информационного противоборства в гуманитарных сферах. Так, первейшая задача в борьбе с идеологической деструкцией состоит в том, чтобы научить нейросеть распознавать скрытые смыслы, выявлять те темы, мотивы, намеки, полутона, которые составляют вредоносную информацию. Для этого потребуется создать ресурсы определенных блоков такой условно вредоносной «идеологической» информации, которая необходима в специфической настройке нейросетей.

Нейросети, распознающие вредоносный контент, позволят создать те фильтры, пропуская через которые, скажем, огромные массивы художественной, научной, учебной литературы и, в первую очередь, издания для детей и подростков, удастся технологически оздоровить информационный фон, формирующий сознание граждан страны.

Применение систем генеративного искусственного интеллекта открывает и более широкие возможности противоборства идеологической деструкции. Речь может идти о формировании уже и таких информационных ресурсов, которые будут содержать необходимые контраргументы.

Сделать это вполне реально, поскольку несмотря на то, что пока отсутствует утвержденная государственная идеология, многие выступления патриотично

ориентированных философов и политологов содержат весьма весомые объемы таких идеологем, которые смогут автоматически находить предельно убедительные аргументы для «лечения» поврежденного сознания, будь то дети, подростки или взрослые. Исследования, проводимые в этом направлении, дают обнадеживающие результаты.

**Список литературы**

1. Дипстейт воюет с Россией и на страницах детских книг / Газета "Завтра" / Дзен. URL: https://dzen.ru/a/Z2sJ62DPwEvKhVr5.

2. Россия и деколонизация: введение. URL: https://youtube.com › channel/UC99wm7n_xH6OGXH_9S1c_OA.

Московский университет МВД РФ им. В.Я. Кикотя
Moscow University of the Internal Affairs Ministry of Russia

Поступила в редакцию 15.07.25

**Информация об авторах**

**Овчинский Анатолий Семенович** – д-р техн. наук, профессор, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя, e-mail: o4506179@yandex.ru

**Борзунов Константин Константинович** – канд. техн. наук, ст. науч. сотр., доцент кафедры информационной безопасности учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя, e-mail: sunobor@yandex.ru

## INFORMATION SECURITY THREATS IN DESTRUCTIVE IDEOLOGIES

**A.S. Ovchinsky, K.K. Borzunov**

A study of the semantic content of children's literature highlighted the information security threats that arise in the early stages of people's lives. Malicious content was detected in more than 60% of the children's books viewed. The main destructive themes included betrayal, uncertainty or gender reassignment, a combination of the incompatible, an unnatural change in social roles, deviation from the norm, indifference to the future, variations in approaches to death "live fast, die young". The publication of books with "creative finds" by foreign authors is generously funded by well-known Western foundations, whose activities are aimed at spreading the meanings they need. The emphasis is placed on the fact that against the background of digital transformation, the emerging "amenities" ignore the tasks of ensuring the information security of the educational sphere. It is not only about protecting the mind from harmful information, but also about the need to develop the ability to think and assimilate knowledge from childhood. The threats of clip-based, push-button, and navigational thinking are noted. The vulnerabilities of consciousness generated by digitalization create a space for ideological destruction. In the context of the growing confrontation between Russia and the countries of Western Europe, the protection of historical heritage, traditional cultural and spiritual values is becoming increasingly important. It is noted that although there has not yet been a consolidated opinion on the need to have a state ideology, the concept of “destructive ideology” has already entered the legal field. The possibilities of using self-learning neural networks to control the semantic content of published books, as well as the use of generative artificial intelligence systems in the confrontation of ideological destruction are discussed.

Keywords: information security, children's literature, malicious content, protection of consciousness, educational sphere, ideological destruction, artificial intelligence.

Submitted 15.07.25

**Information about the authors**

**Anatoly S. Ovchinsky** – Dr. Sc. (Technical), Professor, Professor of the Department of Information Security of the educational and scientific complex of information Technologies of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot, e-mail: o4506179@yandex.ru

**Konstantin K. Borzunov** – Cand. Sc. (Technical), Senior Researcher, Associate Professor of the Department of Information Security of the educational and scientific complex of information Technologies of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot, e-mail: sunobor@yandex.ru

**DOI 10.36622/1682-7813.2025.28.3.006**
**УДК 621.372.004**

# АВТОМАТИЗАЦИЯ ОЦЕНКИ И РЕГУЛИРОВАНИЯ РИСКОВ РЕАЛИЗАЦИИ КИБЕРАТАК: ПРОЦЕДУРЫ ГЕНЕРАЦИИ СЦЕНАРИЕВ

**Г.А. Остапенко, А.А. Остапенко, М.В. Кондратьев, А.С. Кривошеин, М.Д. Неменущий**

Модуль дополняет функциональные возможности моделирования и анализа атак, что подтверждает исследования современного киберпространства, в ходе которого были выявлены существующие недостатки аналогов, заключающиеся в слабой автоматизации сценарного моделирования таких атак и оценки их опасности. Целью работы является описание структуры алгоритмического обеспечения; задач, выполняемых модулем; разработка алгоритмов, необходимых для моделирования многоэтапных атак и генерации множества их сценариев с последующим анализом рисков нарушения информационной безопасности.

Ключевые слова: кибербезопасность, моделирование атак, генерация сценариев, оценка рисков, многоэтапные кибератаки, алгоритм поиска в ширину, MITRE ATT&CK.

**Введение**

Прежде всего необходимо определить требования к алгоритмическому обеспечению модуля генерации сценариев кибератак, которые включают следующее.

1. Построение графа сценариев кибератак, который представляет собой узлы техник, которые использует злоумышленник на различных этапах жизненного цикла кибератак и ребра, описывающие взаимосвязи между этими техниками. Техники объединяются между собой соответствующими им тактиками на основе разработанного словаря, где ключами являются тактики текущего этапа кибератаки, а значениями – возможные тактики, которые с определенной вероятностью будет использовать злоумышленник на следующем этапе своей атаки.

Таким образом, словарь образует тактическую модель кибератак, которая изображена в виде графа на рис.1.

Задачей модуля является сортировка техник по соответствующим им тактикам и формирование на основе получившегося словаря графа сценариев кибератак на основе техник, применяемых злоумышленником на различных этапах жизненного цикла атаки.

2. Генерация сценариев кибератак. Так как граф сценариев кибератак реализует модель, которая допускает нелинейное развитие атаки, то для выявления большинства таких сценариев кибератак требуются надежные алгоритмы. Поэтому для данной задачи необходимо реализовать алгоритм обхода графа и поиска всех возможных путей от начального узла (СТАРТ) до конечного узла (СТОП). Для такой задачи больше всего подходит алгоритм поиска в ширину в графе, который позволяет исследовать все достижимые вершины графа, начиная с начальной заданной точки и распространяя поиск по всем соседним узлам [41]. Данное преимущество алгоритма гарантирует, что будут найдены все возможные пути. Однако, в графе сценариев кибератак возможны циклы, что необходимо обрабатывать установкой ограничений на минимальную вероятность реализации того или иного сценария, и если вероятность сценария становится ниже порогового значения, то поиск в ширину в данном разветвлении возможных путей прекращается.

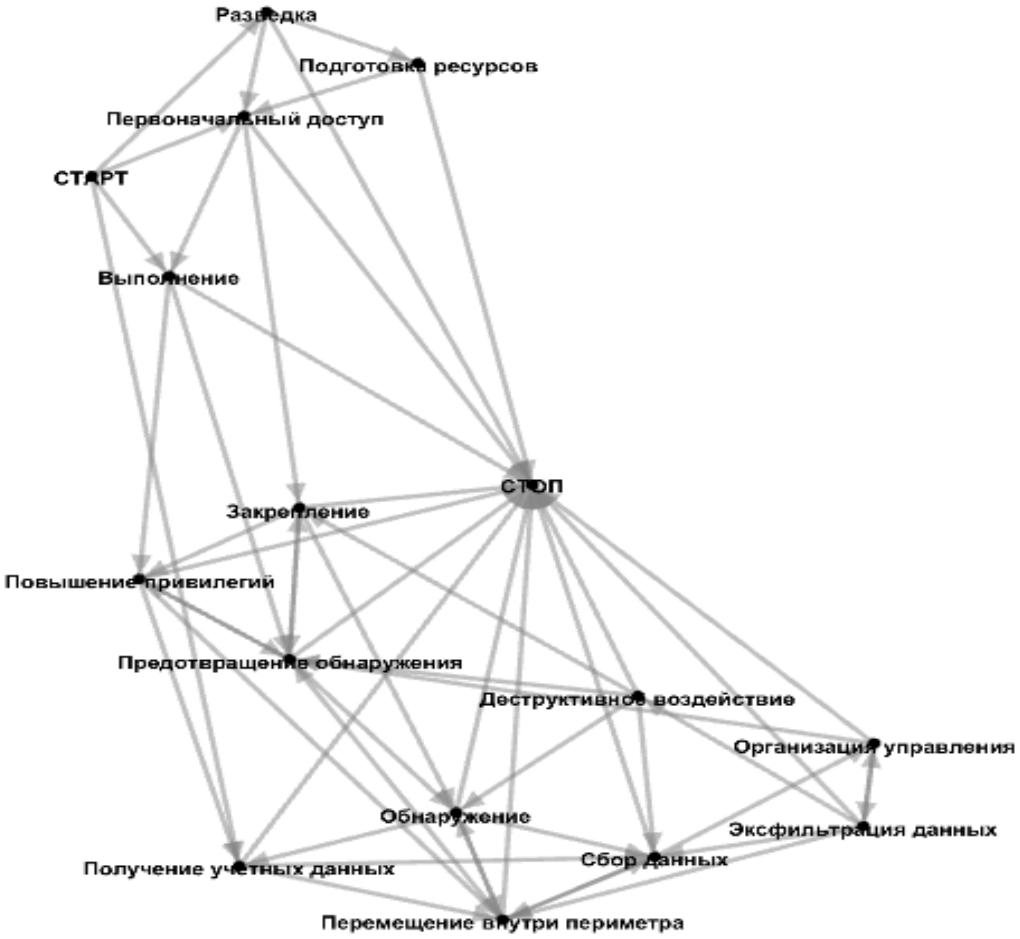



Рис. 1. Граф тактической модели кибератак

3) Анализ сценариев кибератак позволяет выявить наиболее опасные пути реализации кибератаки злоумышленником. Алгоритм анализа должен рассчитывать точное значение риска каждого сценария, учитывая совокупность всех использующихся в нем техник, что достигается использованием следующей формулы:

$$Risk_{\text{сценарий}} = \frac{\sum_{i=1}^{n}(\prod_{j=1}^{i}[P_{\text{техника } j-1 \to \text{техника } j}] \times Risk_{\text{техника } i})}{n}, \quad (1)$$

где $n$ - количество техник в сценарии,

$\prod_{j=1}^{i} P_{\text{техника } j-1 \to \text{техника } j}$ – вероятность применения злоумышленником техники i в контексте сценария кибератаки.

Вычисляемый по этой формуле риск характеризует значение потенциального ущерба, который может быть нанесен атакуемой системе, но данного значения недостаточно для эффективной оценки опасности сценария. Поэтому дополнительной задачей является разработка алгоритма позволяющего вычислять распределение вероятности нанесения ущерба определенной величины, что даст визуальное понимание опасности сценариев, а также конкретные значения, где тот или иной сценарий наиболее опасен и с какой вероятностью он несет эту угрозу системе.

Также, на основе исследования были выявлены недостатки современных подходов к генерации сценариев кибератак, которые важно устранить в разрабатываемом алгоритмическом обеспечении:

- ограниченное множество генерируемых сценариев: алгоритмы должны определять всевозможные пути реализации кибератак, учитывая вероятностные подходы к определению

техник в сценарии кибератак, а также обратные связи в графе, что учитывает возможную корректировку действий злоумышленника в ходе атаки;

- граф сценариев должен быть адаптивным к новым кибератакам: алгоритмы должны учитывать возможность появления новых техник, которыми злоумышленник сможет усилить атакующие возможности и нанести большей ущерба системе;

- недостаточная гибкость: алгоритмы должны поддерживать изменение установленных порогов и структуры графа сценариев кибератак под задачи отдельных систем обеспечения информационной безопасности.

**Структура алгоритмического обеспечения**

Разрабатываемый модуль представляет собой комплекс алгоритмов, направленных на выполнение задач, определенных в требованиях к алгоритмическому обеспечению. Таким образом структура алгоритмического обеспечения модуля генерации сценариев кибератак делится на 3 основные части:

1) алгоритм формирования графа сценариев кибератак - данный алгоритм является фундаментальным для данного модуля, так как другие алгоритмы модуля будут функционировать на основе формируемого графа сценариев кибератак. Графовая модель сценариев, в которой узлами являются техники атак, а ребра - тактическими переходами между ними, позволит моделировать возможные пути реализации кибератак.

2) алгоритм генерации сценариев кибератак - сформированный граф сценариев кибератак представляет общую модель многоэтапных кибератак, но все же для выделения сценариев кибератак требуется разработка отдельного алгоритма, который смог бы выделить техники, относящиеся к определенным шаблонам кибератак, и на основе них осуществить поиск всевозможных путей реализации этой атаки злоумышленником.

3) алгоритмы анализа сценариев кибератак - в результате работы алгоритма генерации сценариев кибератак формируется множество уникальных сценариев кибератак различного уровня опасности. При этом выделение наиболее опасных из которых требует анализа этого множества сценариев, что включает в себя следующие ключевые алгоритмы:

- алгоритм расчета риска сценариев кибератак: данный алгоритм рассчитывает потенциальный ущерб, который может быть нанесен системе, что важно для выделения наиболее опасных сценариев;

- алгоритм построения распределения вероятности нанесения ущерба реализованным сценарием кибератаки: после формирования количественной оценки риска сценариев кибератаки и выделения тем самым множества наиболее опасных сценариев. Для более детальной оценки опасности этих сценариев данный алгоритм строит распределения вероятностей ущерба заданной величины.

Таким образом, структура алгоритмического обеспечения модуля генерации сценариев кибератак позволяет сформировать комплекс алгоритмов, способных обеспечить полноту моделирования многоэтапных кибератак, повысить точность оценки их рисков, что значительно увеличивает показатели эффективности разрабатываемой программы автоматизированной генерации мер и сценариев противодействия кибератакам.

**Построение графа сценариев кибератак**

Алгоритм работает на основе словаря, который состоит из следующих тактик [2, 3]:

- разведка – одна из начальных тактик в сценариях атак, описывающая методы злоумышленника для сбора информации, которую он может использовать для планирования будущих кибератак. В случае ее успешного выполнения злоумышленник может перейти к таким тактикам как: подготовка ресурсов, первоначальный доступ или закончить атаку;

- подготовка ресурсов, данная тактика также является начальной и описывает методы злоумышленника для создания ресурсов, которые он может использовать в своей кибератаке. В кибератаках после нее,

как правило, следует первоначальный доступ, но злоумышленник также может и отменить атаку;

- первоначальный доступ использует методы злоумышленника, которые позволят проникнуть в атакуемую систему. После успешного доступа могут быть реализованы такие тактики, как: выполнение, закрепление или завершение атаки;

- выполнение – тактика, которая может быть начальной в сценариях атак и описывающая методы по запуску вредоносного кода в атакуемой системе. После успешного запуска вредоносного кода в атакуемой системе злоумышленник может перейти к следующим этапам: повышение привилегий, предотвращение обнаружения или завершить атаку;

- закрепление – этап, который включает в себя методы злоумышленника, позволяющие ему сохранить доступ к атакуемой системе. После успешного закрепления злоумышленник может выбрать одну из следующих тактик: повышение привилегий, перемещение внутри периметра или завершение атаки;

- повышение привилегий. Тактика реализует попытки злоумышленника получить в системе возможности более высокого уровня доступа. При успешном повышении привилегий атака может перейти к таким тактикам, как: предотвращение обнаружения, получение учетных данных, перемещение внутри периметра или завершение атаки;

- предотвращение обнаружения. Данный этап использует методы злоумышленника для предотвращения его обнаружения средствами защиты атакуемой системы. После применения методов предотвращения обнаружения происходит переход к следующим тактикам: выполнение, обнаружение или завершение атаки;

- получение учетных данных. Тактика использует методы злоумышленника, направленные на получение учетных данных, которые, как правило, включают в себя логины и пароли пользователей системы. После получения данных злоумышленник использует такие тактики, как: сбор данных, перемещение внутри периметра или завершение атаки;

- обнаружение использует методы злоумышленника внутри системы, направленные на обнаружение сведений об окружении. После успешного выполнения тактики, злоумышленник переходит к: получению учетных данных, сбору данных или завершению атаки;

- перемещение внутри периметра – тактика использует методы злоумышленника, с помощью которых он совершает попытки перемещения по атакуемой системе. После перемещения по системе используются такие тактики, как: предотвращение обнаружения, сбор данных, обнаружение или завершение атаки;

- сбор данных. Этап использует методы злоумышленника, с помощью которых он совершает попытки собрать данные, представляющие для него интерес. После успешной попытки сбора данных происходит переход на следующие техники атаки: перемещение внутри периметра, организация управления или завершение атаки;

- организация управления. Тактика использует методы злоумышленника, направленные на управление атакуемой системой. После успешной организации управления происходят попытки предотвращения обнаружения, деструктивного воздействия, эксфильтрации данных или завершения атаки;

- эксфильтрация данных. Этап использует методы, применяемые злоумышленником для кражи данных из системы. В результате успешной кражи данных атака переходит на такие этапы, как: сбор данных, организация управления, деструктивное воздействие или завершение атаки;

- деструктивное воздействие – тактика, использующая методы, которым злоумышленник может нарушить целостность и доступность данных системы или же само функционирование системы. После деструктивного воздействия на атакуемую систему злоумышленник может перейти к следующим тактикам: закрепление, обнаружение, предотвращение обнаружения, сбор данных или завершение атаки.

Словарь описывает множество вариантов развития путей в развитии кибератак, включая и нелинейные, что важно в моделировании многоэтапных атак. После формирования данного словаря с тактиками злоумышленника, а также взаимосвязями между ними, алгоритм переходит к получению связанных с шаблоном атаки техник и соответствующих им тактик в графовой базе данных.

Когда алгоритм получил все необходимые данные для формирования графа сценариев кибератак, он проводит сортировку и распределение техник в соответствии со словарем тактик и взаимосвязей между ними. После успешной сортировки происходит перебор начальных техник, которые являются ключами нового словаря и для каждой такой техники так же совершается перебор соответствующих им техник.

Итогом работы алгоритма является проверка на наличие ребра между техниками:

- если ребро в графе сценариев кибератак между техниками уже существует, то алгоритм пропускает такую пару;
- если ребра в графе сценариев кибератак нет, то алгоритм создает его в базе данных и сохраняет это событие в журнал.

Наглядно данный алгоритм изображен в виде блок-схемы на рис. 2.

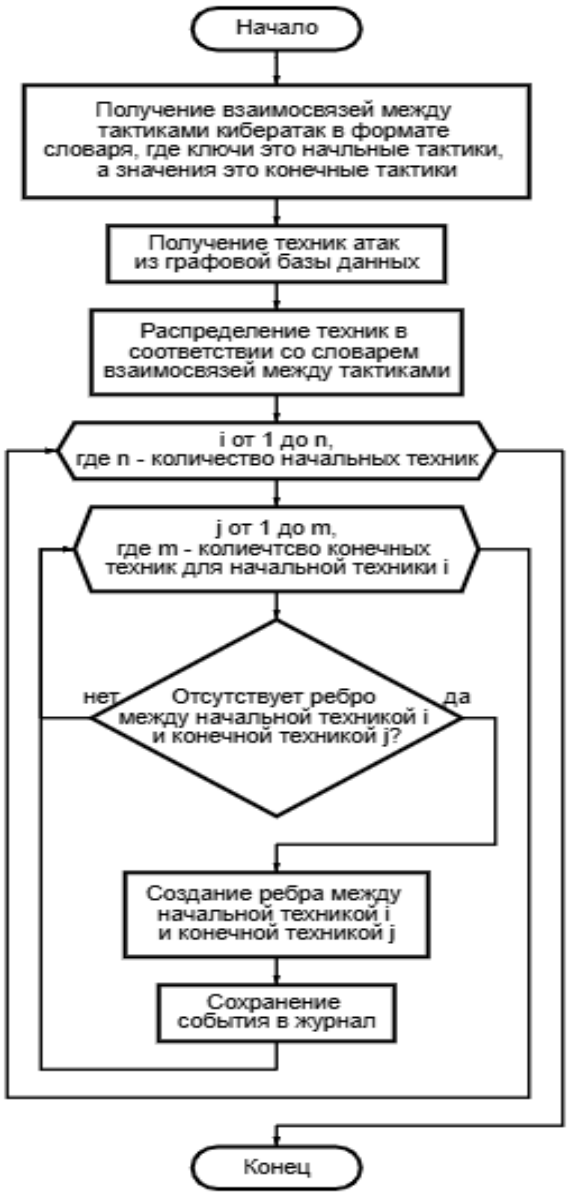



Рис. 2. Блок-схема алгоритма построения графа сценариев кибератак

**Генерация сценариев кибератак**

Граф сценариев кибератак, сформированный одноименным алгоритмом, уже представляет собой подробную графовую модель многоэтапных кибератак, но все же из-за большого числа существующих техник и взаимосвязей между ними, а именно 825 узлов и 236449 ребер, анализ сценариев в контексте определенных атак становится затруднительным, что еще раз подтверждает важность разработки алгоритма генерации сценариев кибератак, способного работать с данным графом.

Так как алгоритм генерации сценариев кибератак выполняет свои задачи на основе данных графа и должен находить всевозможные пути реализации атаки, было принято решение разработки на основе алгоритма поиска в ширину, который предназначен для совершения обхода или поиска в графе. Данный алгоритм выполняет последовательное исследование графа от заданного узла, рассматривая все его дочерние узлы прежде, чем перейти на уровень ниже рассматривая уже дочерние узлы предыдущего уровня, то есть дочерних к начальному узлу, тем самым равномерно расширяя область поиска путей во все стороны от начальной вершины.

В данном случае важен порядок обхода начиная от узла “СТАРТ”, обозначающего начало сценариев, а также учет всех возможных сценариев. Далее будет рассмотрена более подробная реализация алгоритма генерации сценариев кибератака.

Для начала работы алгоритму требуется передать вводные данные, такие как шаблон атаки и пороговое значение вероятности реализации сценариев данной атаки, необходимое для решения проблемы с бесконечными циклами. После этого алгоритм получает из графовой базы данных все техники, которые соответствуют введенному шаблону атаки, и из них формирует подграф с добавлением к нему узлов “старт” и “стоп”.

Следующим этапом работы алгоритма является поиск в ширину всех путей от узла “старт” до узла “стоп” в сформированном подграфе, для этого создается очередь, в которую помещается начальный путь, имеющий единственную вершину “старт”. Организовав очередь, алгоритм запускает цикл, который остановится лишь тогда, когда очередь станет пуста.

В каждом цикле вначале из очереди извлекается первый путь и происходит проверка на условие, является ли он сценарием кибератаки. Если последний узел является узлом “стоп”, то это означает, что найден сценарий кибератаки, и данный путь вместе вероятностью его реализации помещается в массив хранения сценариев кибератаки. В обратном же случае для последнего узла пути в подграфе сценариев кибератаки находятся все дочерние техники и происходит их последовательный перебор.

Для каждого нового пути, где последним узлом теперь является дочерняя техника, вычисляется новая вероятность прохождения такого пути. Если последний узел нового пути является узлом “стоп”, то вероятность реализации нового пути остается прежней, иначе вероятность будет равна произведению вероятности прохождения пути до добавления дочерней техники на вероятность перехода к текущей дочерней технике.

После расчета вероятности реализации нового пути происходит проверка, больше ли это значение порогового значения вероятности. Если вероятность прохождения нового пути меньше порога, то данный новый путь пропускается и данное разветвление графа больше не будет рассматриваться алгоритмом в будущем. В случае же, если вероятность реализации нового пути больше порога, то данный путь добавляется в конец очереди и будет обработан в новом цикле алгоритма в порядке очереди.

Таким образом происходит необходимое исследование подграфа поиском в ширину на наличие всевозможных сценариев кибератак с расчетом вероятности достижения конца такого сценария в ходе реализации кибератаки. Блок-схема данного алгоритма изображена на рис. 3.

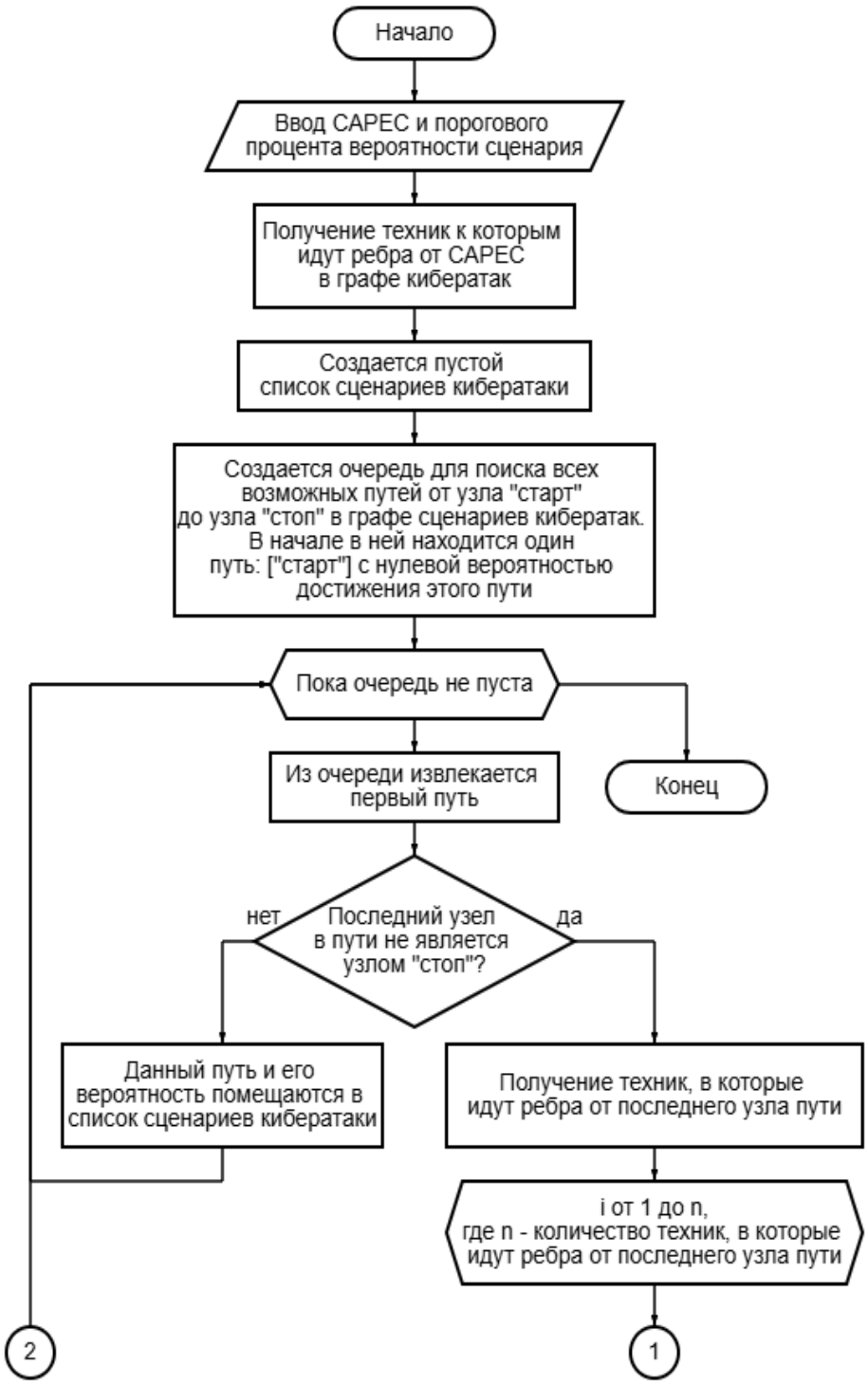



Рис. 3. Блок-схема алгоритма генерации сценариев кибератаки

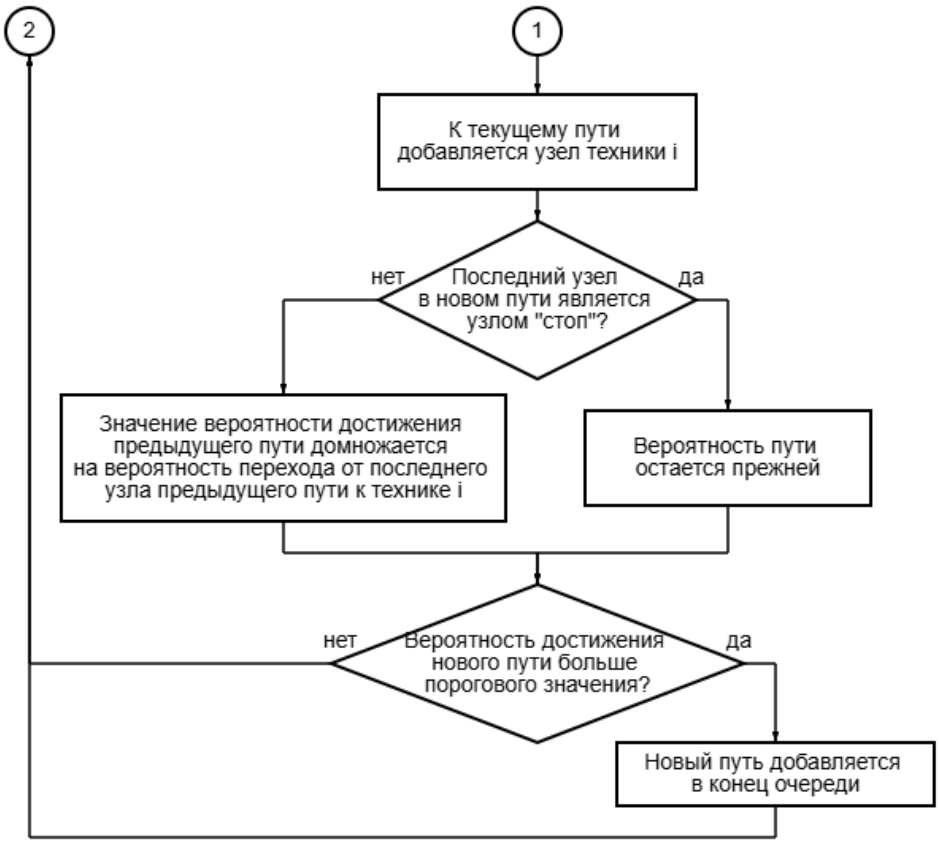



Рис. 3. Продолжение

**Анализ сценариев кибератак**

С возможностью использовать сформированный граф сценариев кибератак, а также генерировать множества возможных сценариев для заданного шаблона атаки, возникает необходимость в анализе этих сценариев с целью их ранжирования по опасности. Она играет ключевую роль в обнаружении критических для защищаемых систем путей развития многоэтапных кибератак.

На данном этапе алгоритмического обеспечения решаются такие важные задачи, как: количественная оценка рисков сценариев кибератак и построение распределений вероятностей нанесения ущерба различной величины в ходе реализации какого-либо сценария. Решение этих задач разработкой соответствующих алгоритмов позволит значительно повысить точность прогнозирования угроз безопасности информации и обеспечить взаимодействующие модули ценной информацией для эффективного формирования мер противодействия кибератакам. К ним относятся следующие.

1. Алгоритм расчета риска сценария кибератаки - так как риск уже определен для каждой техники и характеризует потенциальный ущерб, наносимый системе в ходе атаки этим методом, то риск сценария определяется как нормированная взвешенная сумма рисков последовательности техник, из которых он состоит.

Работа алгоритма начинается с получения сценария кибератаки, в том числе рисков отдельных техник и вероятности перехода между ними в контексте сценария. После этого алгоритмом осуществляется перебор последовательности всех техник сценария. Для каждой конкретной техники происходит расчет вероятности достижения этой техники в сценарии, что достигается произведением всех ребер пути графа, ведущих от начального узла до текущей техники, для которой рассчитывается вероятность ее реализации.

После расчета таковой в сценарии происходит ее умножение на риск этой

техники и полученное произведение суммируется к риску сценария, тем самым получая взвешенную сумму рисков техник, составляющих сценарий. И результирующим действием алгоритма является нормировка значения риска сценария в пределах от 0 до 1 его делением на количество техник в сценарии.

Наглядно алгоритм расчета риска сценария кибератаки изображен на рис. 4.

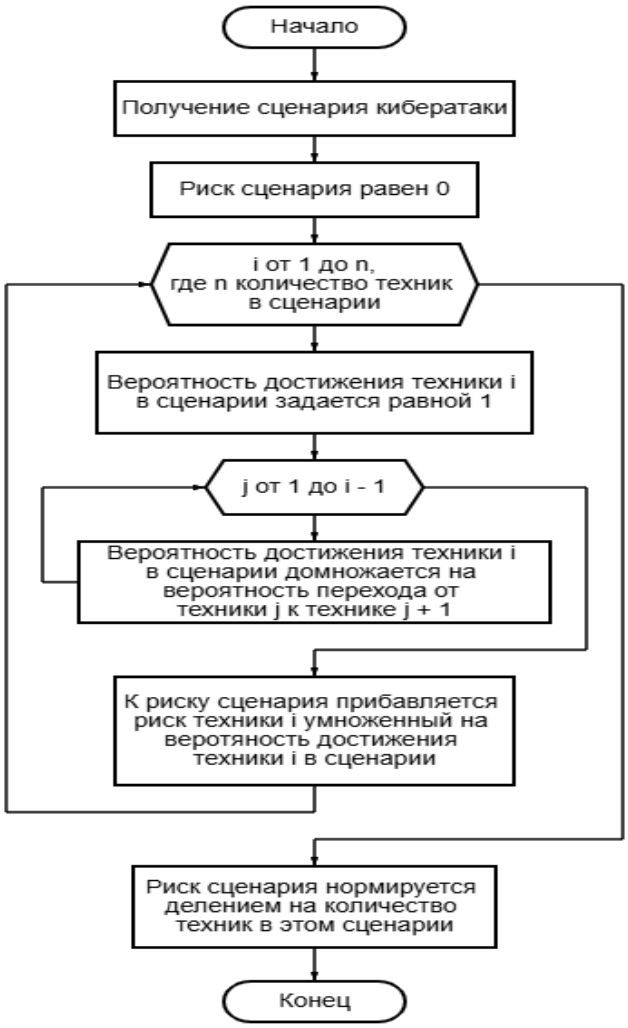



Рис. 4. Блок-схема алгоритма расчета риска для сценария

2. Алгоритм построения распределения вероятности нанесения ущерба в результате реализации сценария кибератаки - данный алгоритм значительно повышает эффективность анализа сценариев кибератак, поскольку позволяет не только оценить уровень потенциального ущерба в результате атаки, но и детально рассмотреть с какой вероятностью системе может быть нанесет ущерб определенной величины. То есть, в отличие от стандартной количественной оценки общего риска сценария, алгоритм обеспечивает дополнительный более тонкий и информативный анализ, что делает возможным выявление наиболее опасных множеств уязвимостей, а соответственно и принятие более обоснованных мер противодействия многоэтапным атакам.

Кроме того, данное распределение представляет возможность для проведения сравнительного анализа между сценариями, так как существуют сценарии с одинаковым потенциальным ущербом, но все же разным характером распределения ущерба, что позволяет определить какой сценарий является более предсказуемым и реализуется уязвимостями с высокой вероятностью и небольшим ущербом системе, а какой

является более опасным при маловероятных, но в то же время критических для системы исходах от реализации атаки.

Работа алгоритма начинается с этапа получения сценария атаки, после чего начинается перебор последовательности техник этого сценария. Для каждой техники из графа причинно-следственных связей компонентов кибератак алгоритм получает соответствующие уязвимости, и для каждой из них сохраняет данные о вероятности эксплуатации и нормированном ущербе от эксплуатации этой уязвимости.

После того, как все необходимые данные получены, происходит расчет параметров распределения для каждого набора уязвимостей. В случае, если для набора уязвимостей какой-либо техники рассчитать параметры распределения не удалось, алгоритм выводит сообщение о невозможности построения распределения для текущей техники и переходит к обработке следующей. Если же параметры распределения для техники успешно рассчитаны, то алгоритмом происходит перебор всех возможных значений ущерба с шагом в 0.01, где для каждого такого значения рассчитывается и сохраняется плотность вероятности нанесения такого ущерба.

После обработки всех техник сценария происходит повторный перебор всех возможных значений ущерба с шагом в 0.01, но уже для объединения плотностей вероятности ущерба всех техник, для построения общего распределения вероятности нанесения ущерба реализацией сценария. Далее алгоритм строит график распределения и выводит его для пользователя. Блок-схема данного алгоритма изображена на рис. 5.

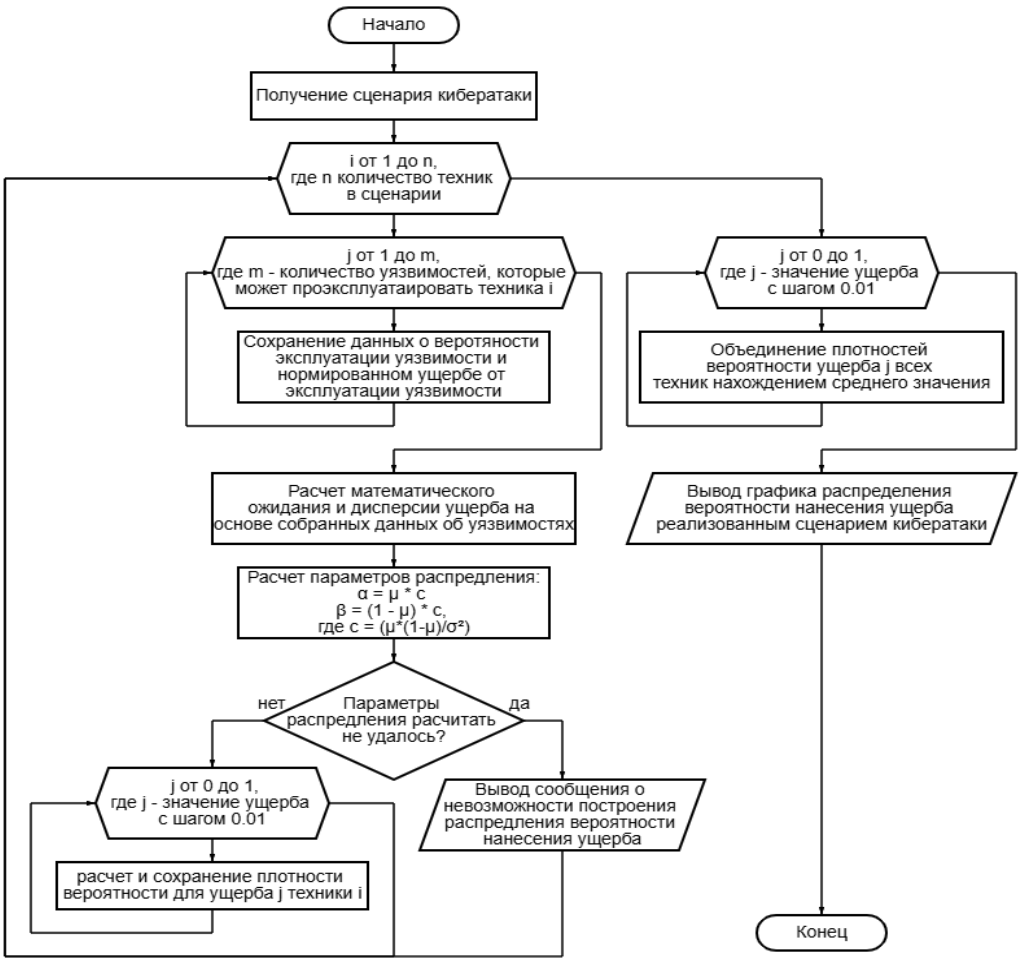



Рис. 5. Блок-схема алгоритма построения распределения вероятности нанесения ущерба в результате реализации сценария кибератаки

**Заключение**

В результате были определены основные требования и задачи к алгоритмическому обеспечению модуля генерации сценариев кибератак и решены следующие задачи:

- построение графа сценариев кибератак - для решения этой задачи был разработан алгоритм, который выполняет формирование графовой модели многоэтапных атак на основе словаря тактик и техник, где узлы представляют техники, а рёбра - взаимосвязи между ними;

- генерация сценариев кибератак - разработан алгоритм на основе поиска путей графа в ширину для обхода подграфа сценариев атак и выявления всех возможных путей от начального узла до конечного. Проблема бесконечных циклов в подграфе была решена введением ограничения на минимальную вероятность реализации сценария;

- анализ сценариев кибератак - для решения задачи были разработаны алгоритмы, дающие возможность оценивать риск сценария на основе соответствующих ему техник и вероятностей их реализации в контексте этого сценария. Также был реализован алгоритм построения распределения вероятности нанесения ущерба определенной величины в результате реализации сценария атаки, который позволяет более подробно анализировать риски сценариев кибератак.

Также в разработанных алгоритмах были устранены следующие недостатки, выявленные в аналогах генерации сценариев кибератак:

- ограниченное множество генерируемых сценариев - данное ограничение было преодолено использованием вероятностного подхода при формировании путей в графе сценариев кибератак, а также включением обратных связей при формировании этого графа;

- недостаточная адаптивность к новым кибератакам - данный недостаток был устранен благодаря возможности динамического добавления новых техник и тактик в графовую модель, что дает возможность оперативного обновления графовой базы данных без вмешательства в алгоритмическое обеспечение;

- недостаточная гибкость генерации сценариев - недостаток устранен за счёт возможности изменения параметров алгоритмов, таких как пороговые значения вероятностей сценариев, а также структура графа в словаре тактик и техник.

В итоге, разработанные алгоритмы обеспечивают такие возможности, как:

- моделирование многоэтапных кибератак;

- генерация возможных сценариев кибератак;

- детальный анализ сценариев кибератак.

Полученное алгоритмическое обеспечение модуля реализовано программно для автоматизированной генерации мер и сценариев противодействия кибератакам, что позволит совершать подробный анализ такой активно растущей угрозы информационной безопасности, как многоэтапные кибератаки.

**Список литературы**

1. Поиск в ширину - Алгоритмика URL: https://ru.algorithmica.org/cs/shortest-paths/bfs/?ysclid=mcmzp7t04682391094 (дата обращения: 10.07.25).

2. Tactics | MITRE ATT&CK® URL: https://attack.mitre.org/tactics/enterprise/ (дата обращения: 10.07.25).

3. Матрица MITRE ATT&CK - URL: https://mitre.ptsecurity.com/ru-RU?amp=&amp= (дата обращения: 10.07.25).

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 15.07.2025

**Информация об авторах**

**Остапенко Григорий Александрович** – д-р техн. наук, профессор, Финансовый университет при Правительстве Российской Федерации, e-mail: ost@fa.ru

**Остапенко Александр Алексеевич** – аспирант, Воронежский государственный технический университет, e-mail: alexostap123@gmail.com

**Кондратьев Максим Витальевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Кривошеин Александр Сергеевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Неменущий Максим Дмитриевич** – студент, Воронежский государственный технический университет e-mail: alexanderostapenkoias@gmail.com

# AUTOMATION OF ASSESSMENT AND REGULATION OF RISKS OF IMPLEMENTATION OF CYBER-ATTACKS: PROCEDURES FOR GENERATION OF SCENARIOS

**G.A. Ostapenko, A.A. Ostapenko, M.V. Kondratyev, A.S. Krivoshein, M.D. Nemenushchiy**

The module complements the functionality of attack modeling and analysis, which confirms the research of modern cyberspace, during which the existing shortcomings of analogs were identified, consisting in weak automation of scenario modeling of such attacks and assessment of their danger.

The purpose of the work is to describe the structure of algorithmic support; tasks performed by the module; development of algorithms necessary for modeling multi-stage attacks and generating a set of their scenarios with subsequent analysis of the risks of information security violation.

**Keywords:** cybersecurity, attack modeling, scenario generation, risk assessment, multi-stage cyberattacks, breadth-first search algorithm, MITRE ATT&CK.

Submitted 15.07.2025

**Information about the authors**

**Gregory A. Ostapenko** – Dr. Sc. (Technical), Professor, Financial University under the Government of the Russian Federation, e-mail: ost@fa.ru

**Alexander A. Ostapenko** – graduate student, Voronezh State Technical University, e-mail: alexostap123@gmail.com

**Maksim V. Kondratyev** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Alexander S. Krivoshein** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Maksim D. Nemenushchiy** – student Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**DOI 10.36622/1682-7813.2025.28.3.007**
**УДК 004.056.5**

# НОРМАТИВНО-АНАЛИТИЧЕСКАЯ МОДЕЛЬ И МЕТОДИКА ОЦЕНКИ ШТАТНОЙ ЧИСЛЕННОСТИ ПОДРАЗДЕЛЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**В.В. Грызунов, Ю.А. Лысенко, А.В. Шестаков**

Несмотря на законодательное требование к корпоративным структурам создавать подразделения информационной безопасности научно обоснованная методология определения их штатной численности отсутствует. Разработана нормативно-аналитическая модель, формально связывающая требуемую численность персонала с количественными параметрами защищаемой корпоративной IT-инфраструктуры и трудоемкостью работ согласно утвержденным федеральным нормам. Выявлена диагностическая функция модели: прямое применение норматива на консультирование пользователей привело к аномально высокому результату, что продемонстрировало способность модели выявлять процессы с необоснованной трудоемкостью, требующие оптимизации или автоматизации. Определена область применения модели, разграничивающая повседневную (нормированную) деятельность от экстремальной (реагирование на инциденты) и научно-исследовательской, для которых требуются иные подходы к нормированию. Перспективными направлениями развития модели являются ее интеграция с методами расчета дежурных смен и введение коэффициентов, учитывающих уровень квалификации персонала, либо дополнительных ролей согласно квалификационной решётке.

Ключевые слова: информационная безопасность, ресурсы информационной безопасности, нормативно-аналитическая модель.

## Введение

Стремительная цифровизация всех сфер деятельности в условиях роста интенсивности и сложности киберугроз, направленных на критическую информационную инфраструктуру Российской Федерации, порождают проблему обеспечения информационной безопасности (ИБ) корпоративных информационных инфраструктур (КИИ). Указ Президента РФ от 1 мая 2022 г. № 250 и Приказ ФСТЭК России от 11.02.2013 г. № 17 (пункт 9) прямо указывают на необходимость создания специализированных ИБ-подразделений по обеспечению КИИ и возлагают на руководителей персональную ответственность за ее состояние.

Сложившаяся практика формирования штатов по остаточному принципу или на основе экспертных оценок приводит к хроническому кадровому дефициту, перегрузке ИБ-специалистов и, как следствие, к повышению рисков реализации угроз безопасности информации. Реализация требований сталкивается с серьезной методологической проблемой: отсутствием научно обоснованных подходов к определению необходимой штатной численности ИБ-подразделений.

## Анализ проблемной области

В современных исследованиях все больше внимания уделяется человеческому фактору в обеспечении информационной безопасности. Например, в статье [1] авторы показывают, что ключевым элементом является культура ИБ внутри подразделений, и одним из важнейших компонентов этой культуры – наличие у сотрудников достаточных профессиональных навыков (IS skill). Авторы констатируют, что зачастую задачи по защите информации поручаются персоналу, не обладающему необходимой квалификацией, что ведет к снижению общего уровня защищенности КИИ.

Однако, признавая важность «мягких» факторов, таких как культура и мотивация, существующие исследования оставляют без ответа ключевой управленческий вопрос: какое количество квалифицированных специалистов необходимо для выполнения всего комплекса задач по ИБ?

В систематическом обзоре 58 научных статей за 10 лет [2] убедительно

доказывается, что ключевыми факторами формирования культуры ИБ являются поддержка руководства, наличие четких политик, а также постоянное обучение и повышение осведомленности персонала. Вместе с тем практическая реализация мероприятий требует значительных трудовых ресурсов (ИБ-специалистов). Вопрос количественной оценки трудозатрат и определения необходимой штатной численности для их выполнения остается за рамками значительной части исследований в данной области.

Автор работы [3] справедливо отмечает, что традиционные методы нормирования для оценки интеллектуального и аналитического труда сотрудников служб безопасности неэффективны, и указывает на необходимость разработки новых подходов. Автор доказывает актуальность проблемы, однако исследование носит постановочный характер, конкретный инструмент для решения заявленной задачи не указан.

Исследование [4] фокусируется на функциях центров мониторинга и реагирования на инциденты (SOC). В исследовании предложена модель, основанная на оценке производительности аналитиков по обработке потока событий безопасности. Такой инцидентно-ориентированный подход, безусловно, актуален для организаций с высоким уровнем зрелости ИБ, создающих полноценные SOC. Однако он не охватывает весь спектр задач, возлагаемых на ИБ-подразделения в большинстве корпоративных структур. Вне рамок подобных моделей остается значительный объем плановых, превентивных и поддерживающих работ: администрирование средств защиты информации (СЗИ) и программного обеспечения (ПО) на конечных точках, управление криптосредствами, техническая поддержка пользователей, ведение эксплуатационной документации и др.

Существующие подходы к нормированию труда в смежных областях безопасности также подтверждают перспективность использования математических моделей. Так, в работе [5] приведена методика расчета численности дежурных смен пунктов управления комплексной безопасностью. Авторы используют модель, основанную на нормах времени и нормах выработки, для определения необходимого числа операторов, выполняющих задачи мониторинга. Представленная методика ориентирована на специфику непрерывного дежурства и обработку входящих информационных потоков, что не в полной мере отражает весь спектр задач ИБ-подразделений. Деятельность ИБ-специалистов включает в себя значительный объем плановых, регламентных и проектных работ (администрирование инфраструктуры, установка и обновление ПО, консультирование пользователей), трудоемкость которых зависит не столько от интенсивности потока инцидентов, сколько от масштаба и сложности защищаемой информационной системы.

За рубежом также предпринимаются попытки создания моделей для расчета численности ИТ-персонала.

Особого внимания заслуживает работа иранских исследователей [6], которые предложили предиктивную модель для больниц, основанную на методе Дельфи и многокритериальной оценке (MCDM). Сильной стороной предложенного подхода является формализованная процедура выявления и взвешивания показателей факторов, влияющих на рабочую нагрузку. К сожалению, используемая модель опирается на субъективные экспертные оценки как при определении весов показателей факторов, так и при калибровке итоговой расчетной формулы, что снижает объективность и воспроизводимость результатов.

Проблемы управления информационной безопасностью на стратегическом уровне подробно рассмотрены в работе [7]. Авторы предложили интегрированную концептуальную модель, которая систематизирует подход к ИБ через четыре ключевых аспекта: среду, цели, требования и оценку. Модель является ценным инструментом для руководителей при формировании общей стратегии. Однако, будучи высокоуровневой и качественной по своей природе, модель не затрагивает

операционные вопросы реализации этой стратегии и не дает инструментов для оценки необходимых для этого ресурсов. Образуется методологический разрыв между стратегическим пониманием «что делать» и операционным расчетом «какими силами это делать». Данный разрыв не позволяет полноценно реализовать обратную связь в иерархической информационной системе [8, 9], связывающую уровень персонала с обеспечивающим уровнем, уровнями аппаратного и программного обеспечения информационной системы (ИС).

Цель настоящего исследования – разработать математическую модель и методику расчета штатной численности ИБ-специалистов для операционного кадрового планирования, являющиеся связью между всеми уровнями ИС (КИИ).

**Формальная постановка задачи**

Дано: пусть защищаемая корпоративная информационная инфраструктура описывается вектором типов объектов

$$\Pi = <\pi_1, \pi_2, ..., \pi_m>,$$

где m – общее число типов объектов,

$\pi_j$ – конкретный тип объекта, например, АРМ, сервер, пользователь, аттестованная ИС, СЗИ) и вектором количества объектов

$$P = <p_1, p_2, ..., p_m>,$$

$p_j$ – числовое значение (количество) объектов $\pi_j$ типа.

Пусть S множество ролей (должностей)

$$S = \{s_1, s_2, ..., s_k\},$$

где k – число ролей в подразделении ИБ (например, $s_{tech}$ – техник, $s_{eng}$ – инженер, $s_{head}$ – руководитель), которые определены в соответствии с профессиональными стандартами.

Для каждой $s_i \in S$ роли определено множество регламентированных трудовых $F_i$ функций и множество всех уникальных функций в подразделении:

$$F_{total} = F_1 \cup F_2 \cup ... \cup F_k.$$

Для каждой $s_i$ роли множество функций $F_i$ разделяется на два непересекающихся подмножества:

$F_{ivar}$ – трудоемкость которых масштабируется в зависимости от количества объектов;

$F_{ifix}$ – с фиксированной годовой трудоемкостью, не зависящей от масштаба инфраструктуры (например, планирование, отчетность, разработка политик).

Нормативная база и параметры определены. Матрица релевантности R: бинарная матрица размерностью $|F_{total}| \times m$, где элемент $r_{fj} = 1$, если функция $f \in F_{total}$ применима к объектам $\pi_j$ типа, и $r_{fj} = 0$ в противном случае. Пусть нормативы времени заданы следующим образом:

для каждой функции $f \in F_{var}$ (где $F_{var} = \cup F_{ivar}$) и каждого типа объекта $\pi_j \in \Pi$ определен норматив $T_{norm}(f, \pi_j)$ – трудозатраты в человеко-часах на выполнение операции f над одной единицей $\pi_j$ объекта;

для каждой функции $f \in F_{fix}$ (где $F_{fix} = \cup F_{ifix}$) определена фиксированная годовая трудоемкость $T_{fix}(f)$ в человеко-часах.

Пусть задан эффективный годовой фонд рабочего времени. Вектор $T_{eff\ vec}$ эффективных фондов рабочего времени размерностью k (по числу ролей):

$$T_{eff\ vec} = <T_{eff}(s_1), T_{eff}(s_2), ..., T_{eff}(s_k)>,$$

где $T_{eff}(s_i)$ – скалярная величина, представляющая собой эффективный годовой фонд рабочего времени для одного сотрудника, занимающего $s_i$ роль ($s_i \in S$). Значение рассчитывается индивидуально для каждой роли с учетом специфики отпусков, служебной подготовки и прочих непроизводственных активностей, характерных для данной должности.

Требуется: разработать нормативно-аналитическую модель для расчета штатной численности $N_{unit}$, которая удовлетворяет ряду условий.

Во-первых, декомпозиция по ролям: модель должна позволять определять требуемую штатную численность $N_{req}(s_i)$ для каждой $s_i \in S$ роли.

Во-вторых, агрегация: общая штатная численность $N_{total\ unit}$ должна определяться как сумма численностей по всем S ролям.

В-третьих, полнота: модель должна учитывать как масштабируемые (переменные), так и не масштабируемые (фиксированные) трудозатраты.

В-четвертых, целочисленность: итоговая численность по каждой $s_i \in S$ роли должна быть целым числом, полученным с округлением в большую сторону для гарантированного выполнения всего объема работ.

Задача: определить на основе входных данных и разработанной модели:

а) годовую трудоемкость $W(s_i)$ для каждой $s_i \in S$ роли:

$$W(s_i) = W_{var}(s_i) + W_{fix}(s_i), \quad (1)$$

где:

$$\sum_{f \in Fvar} \sum_{j=1\ldots m} r(f, \pi_j)\, p_j\, T_{norm}(f, \pi_j), \quad (2)$$

$$W_{fix}(s_i) = \sum_{f \in Fifix} T_{fix}(f), \quad (3)$$

б) требуемую $N_{req}(s_i)$ штатную численность для каждой роли $s_i \in S$.

$$N_{req}(s_i) = \lceil W(s_i) / T_{eff}(s_i) \rceil, \quad (4)$$

где символы $\lceil x \rceil$ – обозначение для функции «потолок» (ceiling function), которая округляет число до целого в большую сторону, так как штатная единица является неделимой;

в) общую $N_{total\ unit}$ штатную численность подразделения:

$$N_{total\ unit} = \sum_{i=1\ldots k} N_{req}(s_i). \quad (5)$$

Примечание: нормативно-аналитическая модель должна обладать рядом ключевых свойств, отвечающих требованиям к современным инструментам кадрового планирования:

объективности: минимизирует влияние субъективных экспертных оценок, основывая расчет на измеряемых параметрах (P) инфраструктуры и утвержденной нормативной базе ($T_{norm}$, $T_{fix}$);

воспроизводимости: является полностью детерминированной. При одинаковом наборе входных данных результат расчета будет идентичным, что исключает разночтения, либо обновлять нормативы времени без изменения самой логики расчета путем или обновления нормативов времени без изменения самой логики расчета, изменения входного вектора P количества объектов, вектора П типов объектов, и S ($F_{total}$) множеств;

прозрачность: пошаговый алгоритм и однозначные математические формулы делают логику расчета понятной и доступной для проверки и аудита.

**Методика расчёта**

Расчёт выполняется посредством последовательного выполнения шагов.

Шаг 1. Инициализация входных данных

Определяются и собираются все необходимые входные параметры, формализованные в постановке задачи:

вектор П типов объектов и вектор P их количества, характеризующие масштаб защищаемой КИИ;

множество S ролей, формирующих структуру ИБ-подразделения;

множества $F_{ivar}$, $F_{ifix}$ трудовых функций для каждой $s_i$ роли, с разделением на масштабируемые и не масштабируемые.

Нормативная база:

матрица релевантности R, связывающая функции и объекты;

нормативы времени $T_{norm}(f, \pi_j)$ для масштабируемых функций;

годовая трудоемкость $T_{fix}(f)$ для не масштабируемых функций.

Вектор эффективных фондов рабочего времени $T_{eff\,vec} = \langle T_{eff}(s_1), \ldots, T_{eff}(s_k) \rangle$, где каждый компонент соответствует определенной $s_i$ роли.

Шаг 2. Расчет $W(s_i)$ суммарной годовой трудоемкости для каждой $s_i$ роли

Общая годовая трудоемкость $W(s_i)$, согласно выражению (1) для каждой $s_i \in S$ роли, рассчитывается как сумма переменной и фиксированной компонент.

2.1. Расчет $W_{var}(s_i)$ переменной (масштабируемой) трудоемкости

Компонента отражает объем работ, напрямую зависящий от размера и сложности инфраструктуры.

Расчет $W_{var}(s_i)$ осуществляется путем суммирования произведений количества объектов на соответствующие нормативы времени по всем релевантным функциям и объектам согласно выражению (2).

2.2. Расчет $W_{fix}(s_i)$ фиксированной трудоемкости

Компонента включает задачи с постоянными годовыми трудозатратами, такие как разработка регламентов, планирование, подготовка периодической отчетности и другие аналитические или управленческие функции и рассчитывается согласно выражению (3).

Шаг 3. Расчет требуемой штатной численности для каждой $s_i$ роли

Расчетная численность для каждой $s_i$ роли определяется согласно выражению (4) как отношение ее суммарной $W(s_i)$ годовой трудоемкости к эффективному фонду рабочего времени $T_{eff}(s_i)$, предусмотренному для данной $s_i$ роли.

Шаг 4. Расчет $N_{total\ unit}$ общей штатной численности подразделения

Итоговая штатная численность ИБ-подразделения $N_{total\ unit}$ определяется как сумма требуемых штатных единиц по всем $s_i$ ролям согласно выражению (5).

**Границы применения модели**

Корректная интерпретация результатов и эффективное практическое применение подразумевают следующее понимание концептуальных основ и границ применимости модели.

1. Фокус на повседневной (регламентной) деятельности. Деятельность по обеспечению ИБ условно разделяется на три типа:

повседневная (регламентная) деятельность: выполнение плановых и регулярных задач, таких как установка и обновление СЗИ, администрирование систем, управление доступом, техническая поддержка, ведение документации;

экстремальная деятельность (реагирование): отражение кибератак в режиме реального времени, локализация инцидентов и ликвидация их последствий;

научно-исследовательская и проактивная деятельность: анализ новых угроз, исследование уязвимостей, проактивный поиск угроз (Threat Hunting), разработка и тестирование перспективных методов защиты.

Разработанная модель предназначена для оценки трудозатрат исключительно на повседневную (регламентную) деятельность. Модель позволяет рассчитывать численность для поддержания «постоянной боевой готовности» (по аналогии с силовыми ведомствам), но не для ведения активных «боевых действий» в условиях высших степеней готовности, где должны применяться иные нормативы и ресурсы. Задачи экстремального реагирования в корпоративной структуре решает специализированное подразделение. Научно-исследовательская и проактивная работа централизованно поддерживается НКЦКИ, а также силами корпоративных вузов и научно-исследовательских организаций (при наличии). Модель расширяет существующую систему обеспечения ИБ, предоставляя инструмент для нормирования самого массового и рутинного компонента корпоративной ИС.

2. Принцип усреднения и работа с нормативами. Общий объем работ по обеспечению ИБ декомпозируется на дискретные трудовые функции, закрепленные за конкретными должностными ролями в соответствии с профессиональными стандартами. Если работа не может быть декомпозирована, для оценки её трудоёмкости необходим иной подход, либо работа должна учитываться как отдельная $F_i$ функция в модели.

Модель оперирует усредненными показателями трудоемкости, что является ее осознанным методологическим выбором. Действительно, на практике одна и та же задача, например, «установка СЗИ», может занимать как три минуты при

благоприятных условиях, так и трое суток при возникновении нештатных ситуаций.

Цель модели – не хронометрировать каждую отдельную операцию, а рассчитать совокупные трудозатраты на продолжительных временных интервалах (год) и для значительного количества объектов.

Важно подчеркнуть, что используемые усредненные значения не являются экспертной оценкой авторов. Они основаны на официально утвержденных документах – «Сборнике типовых норм времени...», разработанном ФГБУ «НИИ труда и социального страхования» Минтруда России. Таким образом, модель переносит вопрос о корректности конкретного норматива с уровня подразделения на уровень федерального регулятора, что является ее сильной стороной при обосновании штатной численности. Любая система имеет предел производительности, и данная модель позволяет оценить среднюю нагрузку, для обработки которой должна быть рассчитана емкость ИБ-подразделения корпоративной ИС.

3. Квалификация персонала как управленческий ресурс. Модель намеренно не делает различий между специалистами разной квалификации, оперируя понятием «усредненной штатной единицы». Это не недостаток, а отражение ее назначения как инструмента кадрового планирования, а не операционного управления. Модель отвечает на вопрос «сколько человеко-часов требуется для выполнения всего объема регламентных работ?». Задача руководителя – эффективно распределить этот рассчитанный объем работ между сотрудниками с учетом их реальной квалификации и производительности. Более того, такой подход формирует основу для прозрачной мотивационной системы: сотрудник, обладающий высокой квалификацией, способен выполнить свой нормированный объем задач быстрее, высвобождая время для более сложных и интересных проектов (например, участия в проактивной деятельности), профессионального развития или поддержания баланса между работой и личной жизнью.

4. Расчет численности для экстремальных режимов – отдельная задача. Определение необходимого количества сотрудников для эффективного реагирования на кибератаки (экстремальная деятельность) требует принципиально иного подхода, выходящего за рамки данной работы. Такой расчет должен базироваться на риск-ориентированной модели, включающей:

формирование актуальной модели нарушителя и сценариев кибератак;

оценку потенциального ущерба от реализации рисков;

анализ стоимости владения командой реагирования (cost of controls) в сравнении с возможными потерями.

На основе такого комплексного анализа можно обоснованно определять состав и численность дежурных смен SOC или групп реагирования на инциденты (CERT). Представленная модель служит отправной точкой для определения базового штата, который необходимо поддерживать в постоянной деятельности.

5. Линейность модели и допущение о независимости задач. Важной методологической особенностью, определяющей границы применимости модели, является ее строгая линейность. Суммарная годовая трудоемкость $W(s_i)$ рассчитывается согласно выражениям (1) и (2) как линейная комбинация количественных параметров $p_j$ инфраструктуры. Это означает, что модель базируется на двух ключевых допущениях:

во-первых, отсутствие эффекта «экономии на масштабе» или роста «издержек с ростом масштаба». В модели принято, что трудозатраты на обслуживание 2N объектов ровно в два раза больше, чем на обслуживание N объектов. На практике, при использовании современных средств автоматизации (например, систем централизованного развертывания ПО или управления конфигурациями), трудоемкость на единицу объекта обычно снижается по мере роста их числа, но может и увеличиваться [10]. Данный аспект требует отдельного изучения;

во-вторых, независимость и аддитивность трудозатрат. Модель не

учитывает сложность, порождаемую взаимосвязями между элементами системы. Предполагается, что задачи по администрированию разных объектов независимы, и общая трудоемкость является их простой суммой. В реальности, с ростом числа серверов и сетевых устройств сложность управления их взаимодействием (настройка правил доступа, диагностика сетевых проблем, управление зависимостями) может расти нелинейно.

Подход является осознанным методологическим упрощением, продиктованным основной целью – создать объективный и воспроизводимый инструмент на основе утвержденных нормативов, которые сами по себе являются линейными (т.е. даны в формате «человеко-часов на единицу объекта»). Таким образом, модель корректно оценивает базовую трудоемкость выполнения регламентных, повторяющихся операций в их «атомарном» виде.

Учет нелинейных факторов, связанных со сложностью архитектуры системы или, наоборот, с эффективностью ее автоматизации, выходит за рамки данной модели и остается в зоне ответственности руководителя. Результаты моделирования могут служить отправной точкой для обоснования проектов по внедрению средств автоматизации (чтобы снизить базовую трудоемкость) или для введения дополнительных «коэффициентов сложности» при планировании штата для особо крупных и гетерогенных инфраструктур.

**Контрольный пример**

Расчет штатной численности структурного ИБ-подразделения проведем для одного из сегментов корпоративной ИС в соответствии с методикой, описанной выше.

Шаг 1. Инициализация входных данных

На основе требований руководящих документов и практических данных о моделируемой ИС формализуем параметры.

1.1. Вектор П типов объектов и вектор Р их количества

Количественные параметры инфраструктуры (вектор Р) примем для одного из сегмента корпоративной ИС.

Параметры, отсутствующие в явном виде, введем как обоснованные допущения:

$p_{arm}$: автоматизированные рабочие места (АРМ) – не менее 2500 ед.;

$p_{arm\ rem}$: АРМ, требующие первоначальной установки или переустановки ПО (согласно «Сборнику….» Минтруда оценка: 10% от общего числа в год) – не менее 250 ед.;

$p_{servers\ core:}$ ключевые серверы – 7 ед. (первого типа – 2 ед.; второго типа – 2 ед.; третьего типа – 2 ед.; четвертого типа – 1 ед.);

$p_{mse}$: межсетевые экраны уровня ядра сети – 1 ед. (пятого типа – 1);

$p_{net\ devices}$: сетевые устройства (маршрутизаторы, коммутаторы) – не менее 400 ед.;

$p_{users}$: пользователи (операторы систем) – не менее 1900 чел.;

$p_{crypto\ total\ lic}$: общее число крипто-лицензий (первого типа, второго типа, третьего типа) – не менее 1900 ед.;

$p_{db\ backup}$: базы данных, подлежащие резервированию (допущение: по числу серверов + FTP) – не более 10 ед.;

$p_{arm\ incident}$: АРМ с инцидентами, требующими восстановления ПО (статистическая оценка, данные можно получить, например, из Service Desk или журнала учета инцидентов) – не более 1200 ед.

1.2. Ролевая структура (S) и распределение функций ($F_i$)

Руководящим документом [11] предусмотрены следующие обобщённые трудовые функции, возлагаемые на техников, инженеров и руководителей в ИБ сфере:

обслуживание систем защиты информации в ИС;

обеспечение защиты информации в ИС в процессе их эксплуатации;

внедрение и разработка систем защиты информации ИС;

формирование требований к защите информации в ИС.

В организационной структуре сегмента корпоративной ИС явно просматриваются

три роли: техник, инженер, руководитель. Использование модели в расчётах для других подразделений или организаций вне контрольного примера, где присутствуют дополнительные роли, множество ролей (должностей) S и множество всех уникальных функций в подразделении: $F_{total}$ будут другими.

Примем для контрольного примера три ключевые роли:

$s_{tech}$: техник по защите информации;

$s_{eng}$: инженер по защите информации;

$s_{head}$: руководитель ИБ-подразделения.

1.3. Матрица R релевантности, нормативная база ($T_{norm}$, $T_{fix}$) и ее практическая корректировка

Нормативы времени примем для контрольного примера из сборника [12].

Для наглядности и полного соответствия формальной постановке задачи, представим совокупность масштабируемых трудовых функций ($F_{var}$), их применимость к объектам (суть матрицы R релевантности) и соответствующие нормативы времени ($T_{norm}$) в виде сводной таблицы (табл. 1).

Корректировка норматива: норматив 12,0 чел.-час/пользователя (п. 3.15) для функции $f_{eng\ 11}$ (Консультирование), вероятно, предназначен для первичного обучения. Для расчета текущей поддержки принят скорректированный экспертный норматив $T_{norm\ adj}(f_{eng\ 11})$ = 1,0 чел.-час/год, что дает более адекватную модель.

Примем, что $T_{fix}$ фиксированная трудоемкость:

для инженера:

$$T_{fix}\ (f_{eng\ doc}) + T_{fix}\ (f_{eng\ training}) = 160 + 32 = 192\ (\text{чел.-часа/год});$$

для руководителя (сумма управленческих задач):

$$T_{fix}\ (f_{head\ total}) = 1140\ \text{чел.-часов/год}.$$

1.4. Эффективный годовой фонд $T_{eff}$ рабочего времени

В общем случае, $T_{eff}$ является вектором, но применительно к корпоративным ИС можно считать, что величина показателя одинакова для всех ролей.

Далее в расчётах $T_{eff}$ используется как скаляр:

$$T_{eff} = 1979 - (304 + 173 + 220 + 100) = 1182,$$

где $T_{год}$ – количество рабочих часов сотрудника в год составляет 1979 [13];

$T_{отпуск}$ – минимальная длительность отпуска сотрудника составляет 304 ч/год;

$T_{пп}$ – профессиональная переподготовка сотрудника составляет 173 ч/год (данные из корпоративных локальных правовых актов о порядке подготовки специалистов и программ профессиональной переподготовки специалистов);

$T_{сп}$ – самостоятельная подготовка сотрудника 220 ч/год;

$T_{фп}$ – минимальное количество часов на занятия по физической подготовке специалистов 100 ч/год (при наличии корпоративных требований).

Шаг 2. Расчет годовой трудоемкости

Расчеты проведены согласно выражениям (1) - (3) и данным из табл. 1.

2.1. Расчет $W(s_{tech})$ для роли «Техник по защите информации» часа (фиксированные затраты отсутствуют)

$$W_{var}(s_{tech}) = (250 * 2,4) + (2500 * 1,8) + (2500 * 0,5) + (435 * 2,4) + \\ + (1970 * 1,0) + +(1900 * 2,4) = 13\ 924\ (\text{чел.-часа}).$$

2.2. Расчет $W(s_{eng})$ для роли «Инженер по защите информации»

$$W\_var(s_{eng}) = (7 * 17,0) + (1970 * 0,5) + (1 * 1,5) + (7 * 126,0) + (2500 * 1,8) + (1 * 75,6) + \\ + (1900 * 1,0) + (9 * 100,8) + (1200 * 1,6) + (7 * 24,0) + (1900 * 1,0) = 192\ (\text{чел.-часа}).$$

2.3. Расчет $W(s_{head})$ для роли «Руководитель отдела»

$$W(s_{head}) = W_{fix}(s_{head}) = 1140 \text{ чел.-часов}$$

Шаг 3. Расчет требуемой штатной численности (ед.) согласно выражению (4):

$$N_{req}(s_i) = \lceil W(s_i)/ T_{eff} \rceil,$$

где $T_{eff} = 1182$.

Техники ($s_{tech}$):

$$N_{req}(s_{tech}) = \lceil 13924/1182 \rceil = \lceil 11{,}78 \rceil = 12.$$

Инженеры ($s_{eng}$):

$$N_{req}(s_{eng}) = \lceil 13550/1182 \rceil = \lceil 11{,}46 \rceil = 12.$$

Руководитель ($s_{head}$):

$$N_{req}(s_{head}) = \lceil 1140/1182 \rceil = \lceil 0{,}96 \rceil = 1.$$

Таблица 1

Матрица релевантности и нормативы для масштабируемых функций

| **Код функции (f)** | **Наименование трудовой функции** | **Применимый тип объекта ($\pi_j$)** | **Параметр количества ($p_j$)** | **Норматив $T_{norm}(f, \pi_j)$, чел.-час** |
|---|---|---|---|---|
| Техник | | | | |
| $f_{tech}$ 1 | Установка ПО на АРМ | АРМ (новые/ремонт) | $P_{arm\ rem}$ | 2,4 |
| $f_{tech}$ 2 | Контроль и поддержка АРМ | АРМ | $p_{arm}$ | 1,8 |
| $f_{tech}$ 3 | Конфигурация АРМ | АРМ | $p_{arm}$ | 0,5 |
| $f_{tech}$ 4 | Монтаж и диагностика сетей | Сетевые устройства | $p_{net\ devices}$ | 2,4 |
| $f_{tech}$ 5 | Установка криптосредств | Крипто-лицензии | $p_{crypto\ total\ lic}$ | 1,0 |
| $f_{tech}$ 6 | Информирование персонала | Пользователи | $p_{users}$ | 2,4 |
| Инженер | | | | |
| $f_{eng}$1 | Администрирование серверов | Серверы | $p_{servers\ core}$ | 17,0 |
| $f_{eng}$ 2 | Администрирование криптосредств | Крипто-лицензии | $p_{crypto\ total\ lic}$ | 0,5 |
| $f_{eng}$ 3 | Администрирование МСЭ | МСЭ | $p_{mse}$ | 1,5 |
| $f_{eng}$ 4 | Инструментальный контроль серверов | Серверы | $p_{servers\ core}$ | 126,0 |
| $f_{eng}$ 5 | Инструментальный контроль АРМ | АРМ | $p_{arm}$ | 1,8 |
| $f_{eng}$ 6 | Инструментальный контроль МСЭ | МСЭ | $p_{mse}$ | 75,6 |
| $f_{eng}$ 7 | Управление полномочиями | Пользователи | $p_{users}$ | 1,0 |
| $f_{eng}$ 8 | Резервное копирование БД | Базы данных | $p_{db\ backup}$ | 100,8 |
| $f_{eng}$ 9 | Восстановление ПО после сбоев | АРМ с инцидентами | $p_{arm\ incident}$ | 1,6 |
| $f_{eng}$ 10 | Обеспечение безопасности серверов | Серверы | $p_{servers\ core}$ | 24,0 |
| $f_{eng}$ 11 | Консультирование пользователей | Пользователи | $p_{users}$ | 1,0 (скорр.) |

Шаг 4. Расчет общей штатной численности согласно выражению (5):

$$N_{total\ unit} = N_{req}(s_{tech}) + N_{req}(s_{eng}) + N_{req}\ (s_{head})$$

$$N_{total\ unit} = 12 + 12 + 1 = 25 \text{ (ед.)}.$$

**Обсуждение результатов**

Требуемая численность ИБ-подразделения для выполнения повседневных регламентных задач в сегменте корпоративной ИС составляет 25 чел., в том числе: руководитель – 1 чел.; инженеры по защите информации – 12 чел.; техники по защите информации – 12 чел.

Ключевым моментом, влияющим на результат, является корректировка норматива на консультирование пользователей.

Прямое применение норматива (12,0 час/год) регламентирует объем нагрузки в

22,8 тыс. часов. Это требует привлечения 20 инженеров для решения только этой задачи, и итоговый результат в 43 потребных специалистов – практически нереализуемым и не обоснованным для изменения штатной численности ИБ-подразделения.

Разработанная модель является не просто «калькулятором», но и диагностическим инструментом. Модель позволяет выявлять задачи с аномально высокой или необоснованной трудоемкостью, которые являются главными кандидатами на оптимизацию, автоматизацию (например, через внедрение базы знаний или чат-ботов на базе искусственного интеллекта) или пересмотр действующих и принятых регламентных процедур. Модель дает руководителю объективные данные для принятия обоснованных управленческих решений в области кадровой политики и политики обеспечения информационной безопасности корпоративной информационной инфраструктуры.

**Заключение**

В настоящей работе решена актуальная научная задача по разработке и апробации нормативно-аналитической модели для объективного расчета штатной численности подразделений информационной безопасности в корпоративных структурах. Модель разработана для устранения методологического разрыва между требованием регуляторов о создании ИБ-подразделений в системах информационной безопасности корпоративных информационных инфраструктур, особенно относящихся к критическим и отсутствием формализованных инструментов для определения их необходимой численности, что на практике приводит к хроническому кадровому дефициту и повышению рисков.

Модель основывается на трех ключевых принципах: декомпозиции трудовых функций в соответствии с профессиональными стандартами, привязки трудозатрат к измеряемым параметрам защищаемой инфраструктуры и использования утвержденной на федеральном уровне нормативной базы. Позволяет перейти от субъективных экспертных оценок к воспроизводимому и прозрачному аналитическому расчету.

Апробация модели на примере сегмента корпоративной ИС продемонстрировала ее практическую применимость. Расчет показал, что для выполнения всего объема повседневных регламентных задач требуется подразделение в составе 25 человек (1 руководитель, 12 инженеров, 12 техников).

Важнейшим результатом апробации стала демонстрация диагностической функции модели: она позволила выявить задачу с аномально высокой нормативной трудоемкостью («Консультирование пользователей») и обосновать необходимость ее корректировки, что указывает на потенциал модели как инструмента для анализа и оптимизации бизнес-процессов в ИБ-сфере. Главная практическая ценность представленной работы заключается в том, что она предоставляет руководителям корпоративных структур мощный, основанный на доказательствах аргумент для диалога с кадровыми и финансовыми службами. Модель позволяет объективно обосновать потребность в персонале, привязав ее к масштабу IT-инфраструктуры и требованиям официальных нормативных документов.

Модель предназначена для расчета численности персонала, выполняющего повседневную (регламентную) деятельность. Расчет штата для экстремальной (реагирование на инциденты) и научно-исследовательской (проактивный поиск угроз, проектирование СЗИ) деятельности требует иных, как правило, риск-ориентированных подходов и является предметом отдельных исследований.

Направлениями для дальнейшего развития предложенной модели могут стать:

интеграция с моделями расчета численности дежурных смен SOC для создания комплексного подхода к формированию ИБ-подразделений;

введение в модель коэффициентов, которые учитывают уровень квалификации персонала, позволит перейти от расчета «усредненных штатных единиц» к планированию квалификационного состава команды либо введение разных $s_i$ ролей ($s_i \in$

S) согласно квалификационной решётке: техник I категории, II категории и далее с разными $T_{norm}(f, \pi_j)$ нормативами;

актуализация и расширение используемой нормативной базы для охвата новых технологий, таких как облачные вычисления, контейнеризация и микросервисные архитектуры.

Статья подготовлена в рамках выполнения НИР «Кибермониторинг» по государственному заданию МЧС России (ЕГИСУ НИОКТР №125031703734-4).

**Список литературы**

1. Dornheim, P., Zarnekow, R. Factors Shaping Information Security Culture in an Internal IT Department // In International Conference on Human-Computer Interaction. 2020. Lecture Notes in Computer Science. Vol. 12427. Pp. 507-521. Springer, Cham. DOI: 10.1007/978-3-030-60152-2_38.

2. Uchendu, B., Nurse, J.R.C., Bada, M., Furnell, S. Developing a Cyber Security Culture: Current Practices and Future Needs // Computers & Security. 2021. Vol.109(2), 102387. DOI: 10.1016/j.cose.2021.102387.

3. Копьев, И.Г. Проблема определения оптимального численного и профессионального состава служб (отделов) безопасности // Креативная экономика. 2021. Том 15. № 4. С. 1557-1568. DOI: 10.183334/ce.15.4.111968.

4. Кочин, В.П. Методика создания и структура корпоративного подразделения информационной безопасности / В.П. Кочин, А.В. Шанцов // Цифровая трансформация. 2022. Том 28. № 3. С. 65-72. DOI: 10.35596/2522-9613-2022-28-3-65-72.

5. Кондратьев, А.Ю. Методика определения штатной численности пунктов управления комплексной безопасностью / А.Ю. Кондратьев, И.Е. Новокшонов, А.В. Усов, С.С. Рогожин // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2021. № 5-6 (155-156). С. 85-90. EDN WKIRVL.

6. Jangi, M., Babokani, A.S., Rezaei, M., Nasab, S. K., Mirzaei, M., Kazemzadeh, M. Predicting the number of IT staff needed in hospitals of Isfahan University of Medical Sciences based on modeling in 2023: A descriptive-analytical study // Health Science Reports. 2024. Vol.7(7). e2230. DOI: 10.1002/hsr2.2230.

7. Alzahrani, L., Seth, K.P. The Impact of Organizational Practices on the Information Security Management Performance// Information. 2021. 12(10). 398. DOI: 10.3390/info12100398.

8. Грызунов, В.В. Модель системы адаптивного управления киберполигоном МЧС России на основе операторного уравнения / В.В. Грызунов, А.В. Шестаков // Вопросы кибербезопасности. 2024. № 6(64). С. 140-149. DOI: 10.21681/2311-3456-2024-6-140-149. EDN GSHMNZ.

9. Грызунов, В.В. Формирование условия гарантированного достижения цели деятельности информационной системой на базе операторного уравнения // Информатизация и связь. 2022. № 4. С. 67-74. DOI: 10.34219/2078-8320-2022-13-4-67-74. EDN NGLZEW.

10. Максимова, Е.А. Аксиоматика инфраструктурного деструктивизма субъекта критической информационной инфраструктуры // Информатизация и связь. 2022. № 1. С. 68-74. DOI: 10.34219/2078-8320-2022-13-1-68-74. EDN ZMOPQB.

11. Приказ Минтруда России «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах» от 15.09.2016 г. № 522н.

12. Раздел 14 «Работы, выполняемые руководителями, специалистами и служащими» в Сборнике типовых норм времени на техническое и сервисное обслуживание информационных ресурсов в государственных (муниципальных) учреждениях по Реестру сборников норм труда, разработанном Институтом труда и утвержден ФГБУ «Научно-исследовательский институт труда и социального страхования» Минтруда России от 07.03.2014 г. №012.

13. Производственный календарь 2024 года (составлен на основе Постановления Правительства РФ «О переносе выходных дней в 2024 году» от 10.08.2023 № 1314).

Санкт-Петербургский университет ГПС МЧС России
St. Petersburg University of the State Fire Service of the Ministry
of Emergency Situations of Russia

Главное Управление МЧС России Московской области
The Main Directorate of the Russian Ministry of Emergency Situations of the Moscow region

Поступила в редакцию 5.09.25

**Информация об авторах**

**Грызунов Виталий Владимирович** – д-р техн. наук, доцент, профессор кафедры прикладной математики и информационных технологий, Санкт-Петербургского университет ГПС МЧС России, e-mail: viv1313r@mail.ru. ORCID https://orcid.org/0000-0003-4866-217X.

**Лысенко Юрий Александрович** – начальник управления информационных технологий и связи Главного Управления МЧС России Московской области. e-mail: lualis@ya.ru. ORCID https://orcid.org/0009-0003-6384-5828.

**Шестаков Александр Викторович** – д-р техн. наук, старший науч. сотрудник, ведущий науч. сотрудник, Санкт-Петербургский университет ГПС МЧС России, e-mail: alexandr.shestakov01@yandex.ru. ORCID https://orcid.org/0000-0002-8462-6515.

# REGULATORY AND ANALYTICAL MODEL AND TECHNIQUE FOR ASSESSING THE STAFFING OF INFORMATION SECURITY DEPARTMENTS

**V.V. Gryzunov, Y.A. Lysenko, A.V. Shestakov**

Despite the legislative requirement for corporate structures to create information security units, there is no scientifically substantiated methodology for determining their staffing requirements. A regulatory and analytical model has been developed that formally links the required staffing requirements to the quantitative parameters of the protected corporate IT infrastructure and the complexity of routine work in accordance with approved federal standards. The diagnostic function of the model was identified: the direct application of the user consultation standard resulted in an abnormally high score, demonstrating the model's ability to identify processes with unjustified labor intensity that require optimization or automation. The model's application scope has been defined, distinguishing between everyday (calculation) activities and extreme (incident response) and research activities, which require different approaches to regulation. Promising areas for the model's development include its integration with methods for calculating on-duty shifts and the introduction of coefficients that take into account the level of personnel qualifications or additional roles based on the qualification grid.

Keywords: information security, information security resources, regulatory and analytical model.

Submitted 5.09.25

**Information about the authors**

**Vitaly V. Gryzunov** – Dr. Sc. (Technical), Associate Professor, Professor of the Department of Applied Mathematics and Information Technologies at the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia. e-mail is viv1313r@mail.ru. ORCID https://orcid.org/0000-0003-4866-217X.

**Yuri A. Lysenko** – Head of the Department of Information Technologies and Communications of the Main Department of the Russian Ministry of Emergency Situations in the Moscow Region. e-mail is lualis@ya.ru. ORCID https://orcid.org/0009-0003-6384-5828.

**Alexander V. Shestakov** – PhD, Senior Researcher, Leading Researcher of St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia, e-mail: alexandr.shestakov01@yandex.ru. ORCID https://orcid.org/0000-0002-8462-6515.

**DOI 10.36622/1682-7813.2025.28.3.008**
**УДК 621.372.004**

# АВТОМАТИЗАЦИЯ ОЦЕНКИ И РЕГУЛИРОВАНИЯ РИСКОВ РЕАЛИЗАЦИИ КИБЕРАТАК: ПРОЦЕДУРЫ ГЕНЕРАЦИИ МЕР ПРОТИВОДЕЙСТВИЯ

**Г.А. Остапенко, А.А. Остапенко, М.В. Кондратьев, А.С. Кривошеин, А.В. Ясенев**

Меры противодействия кибератакам являются фундаментальными средствами управления рисками организации защиты информации. Они позволяют заранее определить последовательность предпринимаемых действий, направленных на обнаружение атак, проводимых в защищаемой системе; реагирование на выявленные атаки для снижения максимального ущерба, который может нанести злоумышленник; а также ликвидацию последствий от таких атак, что важно для максимального быстрого восстановления атакуемой системы. Целью работы является формирование алгоритмического обеспечения модуля генерации мер противодействия кибератакам, алгоритмы которого должны соответствовать требованиям, сформированным в методическом обеспечении, а также исправлять ограничения существующих аналогов, выявленных в ходе исследования современных проблем обеспечения киберустойчивости автоматизированных систем.

Ключевые слова: кибербезопасность, кибератака, автоматизация, уязвимость, семантический анализ, машинное обучение, оценка рисков.

## Введение

Методическое обеспечение модуля генерации мер противодействия кибератакам включает ряд важных требований к алгоритмическому обеспечению в следующих аспектах:

1) генерация категорий уязвимостей по семантическому смыслу. Требуется реализовать алгоритмы для автоматического выявления и создания категорий уязвимостей на основе анализа их семантического смысла. Такой подход позволит выявлять категории уязвимостей, которые имеют одинаковые меры противодействия кибератакам, что позволит повысить адаптивность к новым уязвимостям и уменьшить время анализа и реагирования на угрозы нарушения информационной безопасности;

2) генерация мер противодействия для категорий уязвимостей - необходимо разработать алгоритм автоматизированной генерации мер противодействия, ориентированных на каждую выявленную категорию уязвимостей. Данный подход должен обеспечить быстрое реагирование за счет генерируемой базы знаний о мерах противодействия уязвимостям каждой категории. В случае появления уязвимости новой категории, данный алгоритм сможет за короткие сроки сгенерировать комплекс мер обнаружения, реагирования и ликвидации последствий для таких кибератак. Таким образом алгоритм обеспечит генерацию мер противодействия со следующими преимуществами:

- повышение целевой защиты обеспечивается выработкой мер противодействия, учитывающих специфику каждого кластера уязвимостей;
- автоматизация реакции на новые категории уязвимостей достигается за счет формирования базы знаний мер противодействия для категорий уязвимостей;

3) категорирование уязвимостей по семантическому смыслу. Для полноценной работы созданной предыдущими алгоритмами базы знаний о мерах противодействия категориям уязвимостей, необходимо разработать алгоритм, который позволит совершать категоризацию уязвимостей, на основе их подробного описания. В случае, если уязвимость относится к новой категории уязвимостей, которых еще не было выявлено ранее, алгоритм должен запустить обновление базы

знаний о категориях уязвимостей и противодействия им.

Кроме того, в ходе исследования современных проблем обеспечения киберустойчивости автоматизированных систем были выявлены существенные недостатки современных подходов к генерации мер противодействия кибератакам, поэтому разрабатываемое алгоритмическое обеспечение должно удовлетворять следующим требованиям:

- алгоритмы обязаны обеспечивать высокую степень автоматизации модуля - ручная подготовка и обработка мер противодействия в ходе генерации должны сводиться к минимуму;

- алгоритмы призваны генерировать меры противодействия для русскоязычных пользователей - данная проблема должна решаться разработкой подходов к обработке иностранных стандартов и рекомендаций, результатом которых должно быть преобразование к русскому языку иностранных текстов.

Таким образом, на основе сформулированных требований к алгоритмическому обеспечению модуля генерации мер противодействия кибератакам, становится очевидной необходимость в разработке комплекса алгоритмов, ориентированных на выполнение поставленных задач. Для наиболее эффективной работы модуля, алгоритмы должны быть правильно структурированы и иметь возможность взаимодействия между результатами своей работы. Далее будет рассмотрена структура разрабатываемого алгоритмического обеспечения модуля генерации мер противодействия.

**Структура алгоритмического обеспечения**

Модуль генерации мер противодействия кибератакам представляет собой комплекс алгоритмов, которые должны удовлетворять поставленным требованиям к алгоритмическому обеспечения путем самостоятельной работы или взаимодействия между друг другом. Таким образом структура алгоритмического обеспечения, в соответствии с основными требования должна состоять из 3 частей, которые описаны далее.

1. Алгоритм генерации категорий уязвимостей по семантическому смыслу - данный алгоритм играет ключевую роль в структуре алгоритмического обеспечения, так как генерирует массив данных, хранящий информацию об уязвимостях, объединенных семантическими связями. Данный алгоритм позволяет определять общие подходы к противодействию уязвимостям из каждой категории. После этого собранная информация передается в следующую структурную часть алгоритмического обеспечения, где происходит обогащение данных и формирование базы знаний о мерах противодействия категориям уязвимостей путем их автоматизированной генерации.

2. Алгоритм генерации мер противодействия для категорий уязвимостей - данный алгоритм является важной частью структурной организации модуля, так как генерирует базу знаний о мерах противодействия категориям уязвимостей. Данная база знаний необходима для дальнейшей работы модуля, так как именно на основе нее будут происходить такие важные процессы, связанные с уязвимостями, как выработка мер противодействия им или же решение о повторной генерации категорий уязвимостей, в случае выявления новой категории.

3. Алгоритм категорирования уязвимостей по семантическому смыслу - данный алгоритм является частью алгоритмического обеспечения и напрямую взаимодействует с конкретной уязвимостью и анализирует ее с целью определения ее в одну из категорий уязвимостей составленной ранее базы знаний. В случае же, если уязвимость не относится к имеющимся в базе категориям, то происходит взаимодействие с предыдущими структурными частями алгоритмического обеспечения, запуская повторную генерацию категорий уязвимостей и мер противодействия им.

В результате, становится возможным сформировать схему взаимодействия алгоритмов в разрабатываемом

алгоритмическом обеспечении модуля генерации мер противодействия кибератакам, которая изображена на рис. 1.

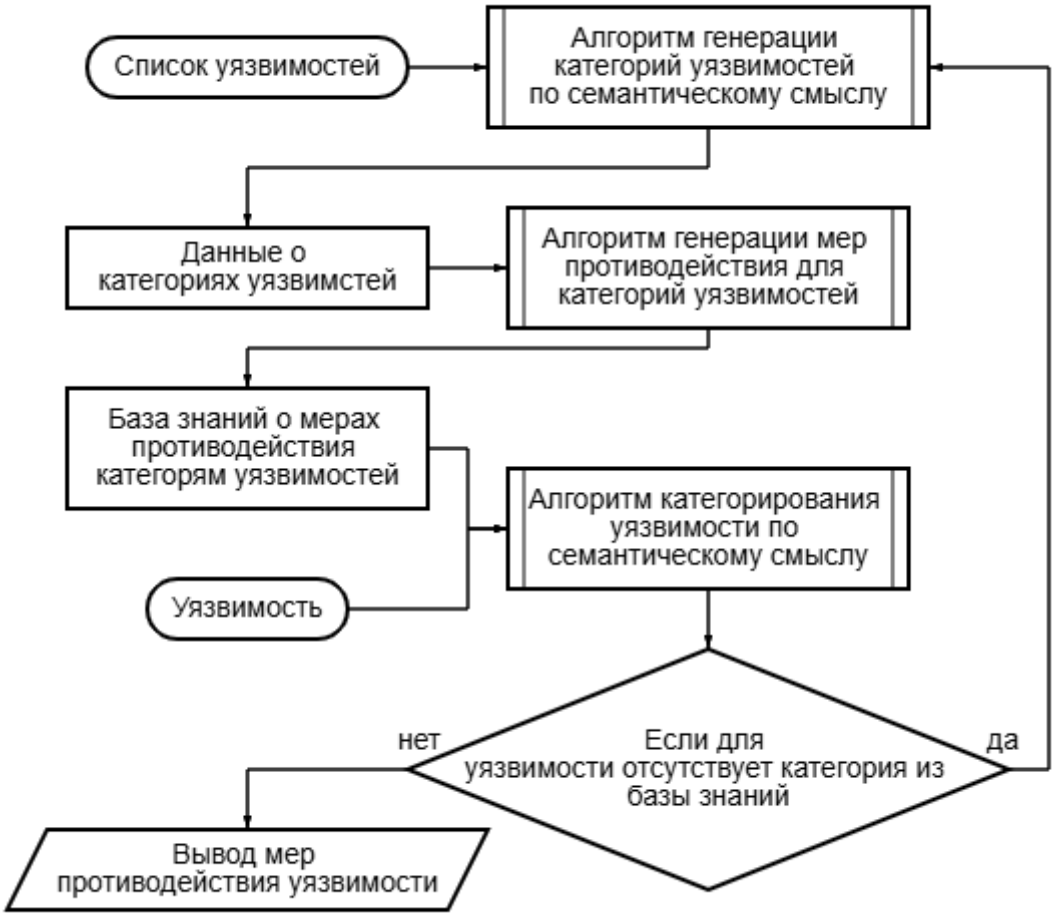



Рис.1. Структурная схема алгоритмического обеспечения модуля генерации мер противодействия кибератакам

Таким образом, полученная структура алгоритмического обеспечения позволяет сформировать комплекс алгоритмов, необходимых для выполнения всех сформулированных требований и формирования мер противодействия кибератакам, реализуемым через эксплуатацию любых уязвимостей, даже если ранее они были неизвестны.

**Процедуры генерации категорий уязвимостей по семантическому смыслу**

Алгоритм генерации категорий уязвимостей по семантическому смыслу позволяет сформировать группы уязвимостей, которые близки по своим семантическим характеристикам. Каждая группа объединяется таким образом, что меры обнаружения, реагирования и ликвидации последствий для уязвимостей являются одинаковыми, что существенно повышает адаптивность модуля и выработку эффективных мер противодействия кибератакам.

Работа алгоритма состоит из следующих процедур:

1) получение информации об уязвимостях из графовой базы данных. Требуется список идентификаторов уязвимостей и их подробных описаний,

2) инициализация массивов для векторов уязвимостей. Данный этап необходим для хранения смыслов векторов BERT и векторов ключевых слов TF-IDF,

3) цикл, реализующий перебор полученного списка уязвимостей, который включает в себя следующие фазы:

- предобработка описаний уязвимостей - для каждого текстового описания уязвимости происходят такие преобразования, как: удаление специальные символов, лемматизация слов (преобразование в основную форму), а также удаление стоп слов (слова которые встречаются часто, но не несут смысловой нагрузки на текст) [1];

- генерация и сохранение смысловых векторов BERT для уязвимостей - используется нейросетевая модель CySecBERT обученная на корпусе данных по информационной безопасности, которая выделяет связи в описаниях уязвимостей и генерирует смысловые векторы для них [2];

- генерация и сохранение векторов ключевых слов для уязвимостей - происходит процесс выделения важных слов в текстовых описаниях уязвимостей с помощью статистической модели TF-IDF, учитывающей частоту встречаемости и уникальности слов в описаниях,

4) кластеризация уязвимостей на основе смысловых векторов BERT. После перебора всех уязвимостей и формирования массивов для их хранения происходит процесс кластеризации смысловых векторов BERT на основе алгоритма кластеризации HDBSCAN (Hierarchical Density-Based Spatial Clustering of Applications with Noise), где каждый кластер является категорией уязвимостей с общими признаками [3],

5) цикл, реализующий перебор кластеров уязвимостей, который включает в себя следующие фазы:

- вычисление центроида кластера - вычисление центрального вектора для кластера, который является средним значением среди всех смысловых векторов BERT в кластере и характеризует семантический смысл всей категории уязвимостей;

- расчет сходства с центроидом для каждого смыслового вектора кластера и сохранение этого результата;

- для распределения сходства между смысловыми векторами вычисляется верхний и нижний квартили, а также межквартильный размах, на основании которых вычисляется порог допустимого сходства между векторами и кластером (центроидом кластера) [4],

6) анализ векторов ключевых слов TF-IDF кластера. Данный анализ необходим для выявления ключевых слов кластера, наиболее сильно характеризующих категорию уязвимостей, для генерации названия этой категории,

7) генерация названия категории уязвимостей. Данный реализуется с помощью нейросетевой модели T5, которая предназначена для преобразования векторов в осмысленный текст [5],

8) сохранение данных о категориях уязвимостей. Окончательный этап алгоритма, который сохраняет такие данные о кластерах уязвимостей, как: название категории, семантический вектор центроида кластера и порог допустимого сходства с центроидом кластера.

Блок-схема алгоритма изображена на рис. 2.

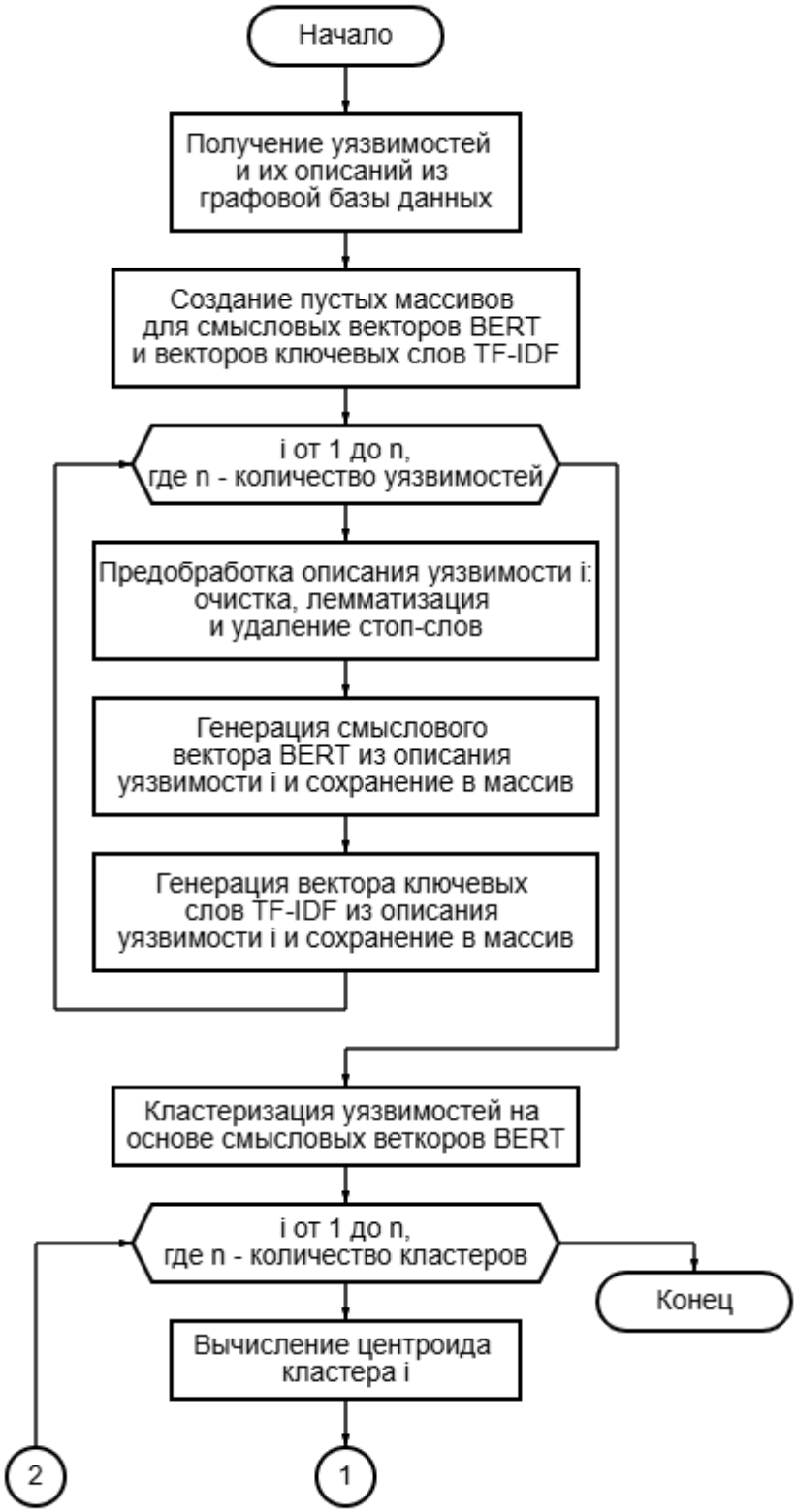



Рис. 2. Блок-схема алгоритма генерации категорий уязвимостей по семантическому смыслу

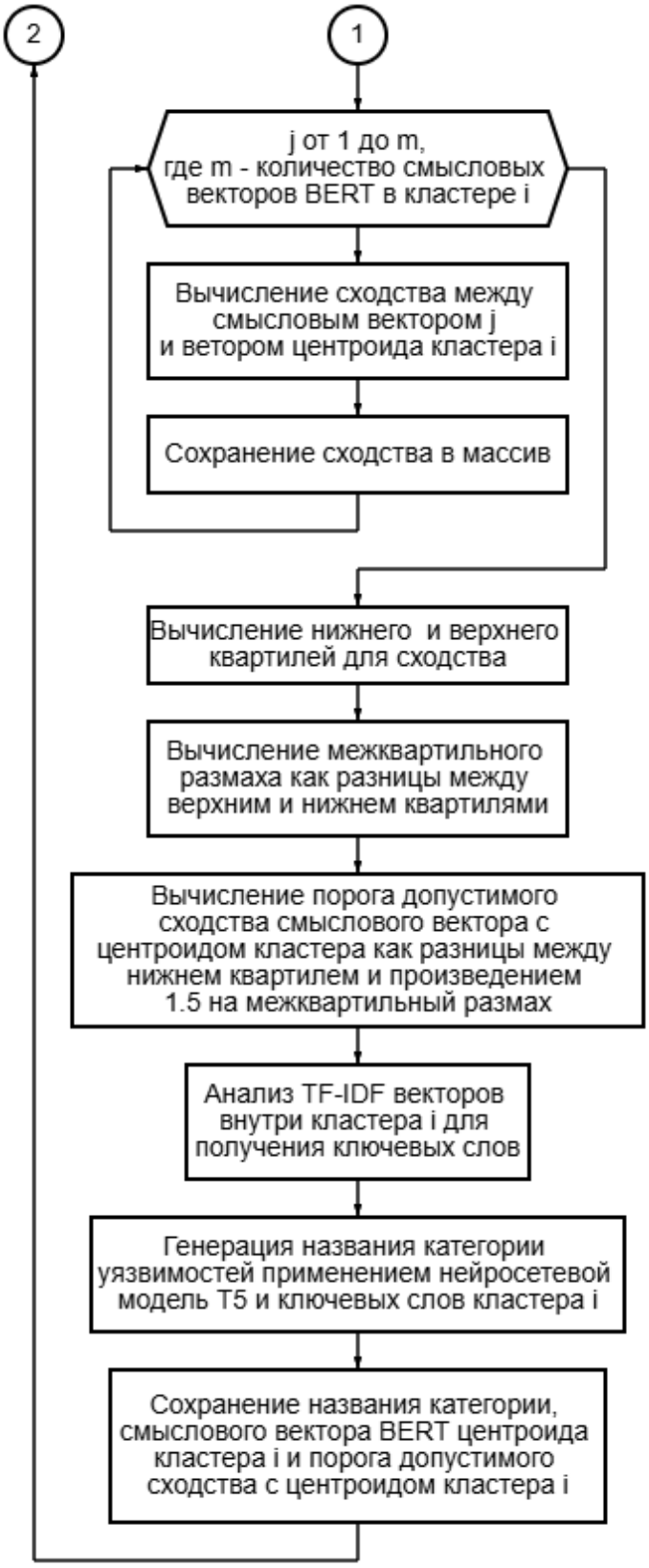



Рис. 2. Продолжение

**Процедуры генерации мер противодействия категориям уязвимостей**

Генерация мер противодействия является важной задаче модуля, так как именно он нее зависит насколько эффективно будет выстраиваться защита систем. Для начала работы данному алгоритму требуются два массива входных данных:

- данные о категориях уязвимостей - массив с данной информацией формируется алгоритмом генерации категорий уязвимостей по семантическому смыслу, который был разработан в предыдущем пункте текущей главы настоящей работы;

- список типовых мер противодействия - данный список включает в себя набор действий, которые могут быть применены к различным категориям уязвимостей с целью обеспечения информационной безопасности. Есть два варианта применения данного списка: пользовательский список типовых мер противодействия или список типовых мер противодействия по умолчанию.

Список типовых мер обнаружения, реагирования и ликвидации последствий по умолчанию был сформирован на основе авторитетных источников и мировых стандартов в области информационной безопасности, наиболее популярными из которых являются [6-8]:

- NIST SP 800-61 Rev. 2 - публикация национального института стандартов и технологий США (NIST), которая содержит рекомендации по подготовке, обнаружению, анализу, реагированию и ликвидации последствий инцидентов;

- ГОСТ Р ИСО/МЭК ТО 18044-2007 - российский национальный стандарт, который содержит информацию о менеджменте инцидентов информационной безопасности;

- CIS Controls (Center for Internet Security) - набор практических контрольных мероприятий для защиты систем, включающий в себя мер обнаружения аномалий, анализ и реагирование на них, а также ликвидацию последствий.

После загрузки необходимых данных алгоритм переходит к генерации смысловых векторов BERT для типовых мер противодействия, которые необходимы для сравнительного анализа между категориями уязвимостей.

После обработки векторов мер противодействия алгоритмом производится перебор всех категорий уязвимостей. В случае, если в базе знаний для категории уже сформированы меры противодействия, то она пропускается и алгоритм начинает обрабатывать следующую категорию. Если же меры противодействия для категории отсутствуют, то происходит перебор всех типовых мер противодействия с целью выявления подходящих категорий уязвимостей.

Между парой векторов категории уязвимостей и типовой меры противодействия вычисляется косинусное сходство и в случае, если сходство между векторами больше или равно 80 процентов, то мера противодействия вносится в базу знаний мер противодействия категориям уязвимостей и цикл продолжается дальше.

Таким образом, данный алгоритм обеспечивает непрерывную автоматизированную генерацию мер противодействия категориям уязвимостей, даже если данный тип уязвимостей является новым в информационном пространстве, что обеспечивает высокую адаптивность и динамичность алгоритма. А формируемая база знаний о мерах противодействия категориям уязвимостей обеспечивает основу для взаимодействующих алгоритмов данного модуля и других.

Наглядно алгоритм генерации мер противодействий категориям уязвимостей изображен на рис. 3.

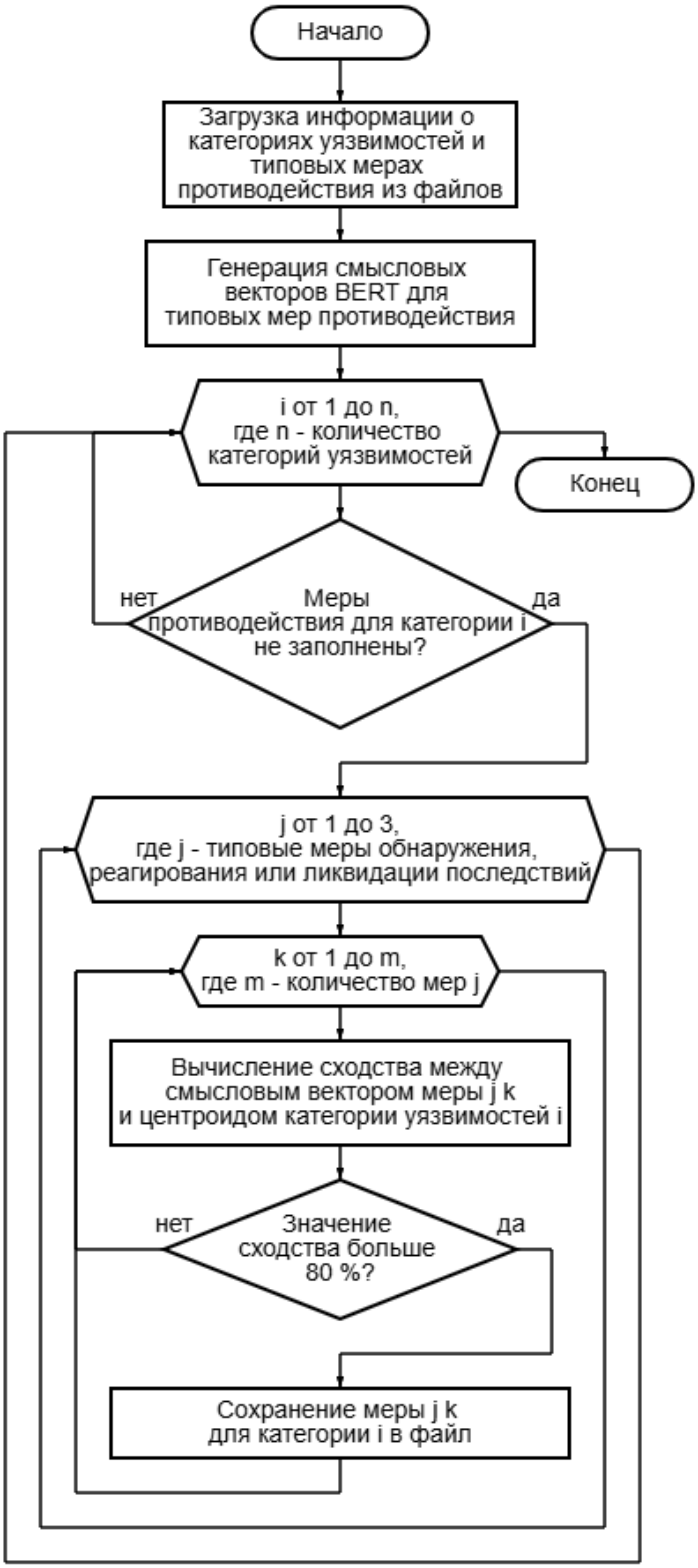



Рис 3. Блок-схема алгоритма генерации мер противодействия категориям уязвимостей

**Процедуры категорирования уязвимости по семантическому смыслу**

Категорирование уязвимостей по семантическому смыслу является итоговой частью алгоритмического обеспечения модуля, так как именно оно позволяет сопоставить конкретную уязвимость с мерами противодействия ей. Исходя из этого важно обеспечить алгоритм, осуществляющий это категорирование, высокой точностью, ведь именно от этого зависит генерация релевантных и эффективных мер противодействия кибератакам.

Алгоритм начинает работу с получения информации об уязвимости, для которой необходимо определить категорию. После происходит предобработка текстового описания полученной уязвимости, включающая в себя: очистку специальных знаков в тексте; лемматизацию слов; а также удаление стоп-слов, которые не несут никакой смысловой нагрузки на описание этой уязвимости. После предобработки текста алгоритм генерирует смысловой вектор BERT, который точно отражает семантический смысл описания уязвимости за счет того, что лишние данные были удалены из описания.

Следующим этапом алгоритма является загрузка данных о категориях уязвимостей, а именно: смысловые векторы BERT для центроидов кластеров каждой категории и пороги допустимого сходства уязвимостей с данными векторами центроидов. После того как алгоритм получил все необходимые данные для категорирования уязвимости, он переходит к этапу поиска категории с максимальным сходством ее центроида кластера с заданной уязвимостью.

На этапе поиска соответствующей категории уязвимости инициализируются переменные для хранения значения максимального сходства и, непосредственно, самой категории уязвимости, которая имеет это сходство. Далее происходит перебор всех центроидов кластеров загруженных категорий уязвимостей и последующее вычисление сходства между вектором центроида и вектором заданной уязвимости. Если вычисленное сходство меньше значения максимального сходства, которое хранится в соответствующей переменной алгоритма, то данная категория не относится к уязвимости и пропускается.

В случае же, если установленное сходство больше максимального сходства среди всех уже перечисленных категорий уязвимостей, то данное значение обновляет переменную с максимальным сходством. А в соответствующую переменную, где хранится информация о категории, фиксируется текущая категория, как потенциальная для рассматриваемой уязвимости.

Когда цикл перечисления категорий закончен и выявлена потенциальная категория уязвимости, наступает заключительный этап алгоритма, в ходе которого происходит проверка, входит ли смысловой вектор уязвимости в кластер выявленной категории с максимальным сходством. Если максимальное сходство выше порога допустимого сходства, то категория уязвимости найдена, и ее меры противодействия могут быть применены для рассматриваемой уязвимости. Если же максимальное сходство меньше порога, то уязвимость относится к неизвестной категории, и алгоритм выводит сообщение об этом с последующим сохранением события в журнал для того, чтобы можно было запустить повторный цикл генерации категорий уязвимостей.

Блок-схема алгоритма категорирования уязвимости по семантическому смыслу позволяет рассмотреть отдельные его этапы более наглядно и изображена на рис. 4.


Рис. 4. Блок-схема алгоритма категорирования уязвимости по семантическому смыслу

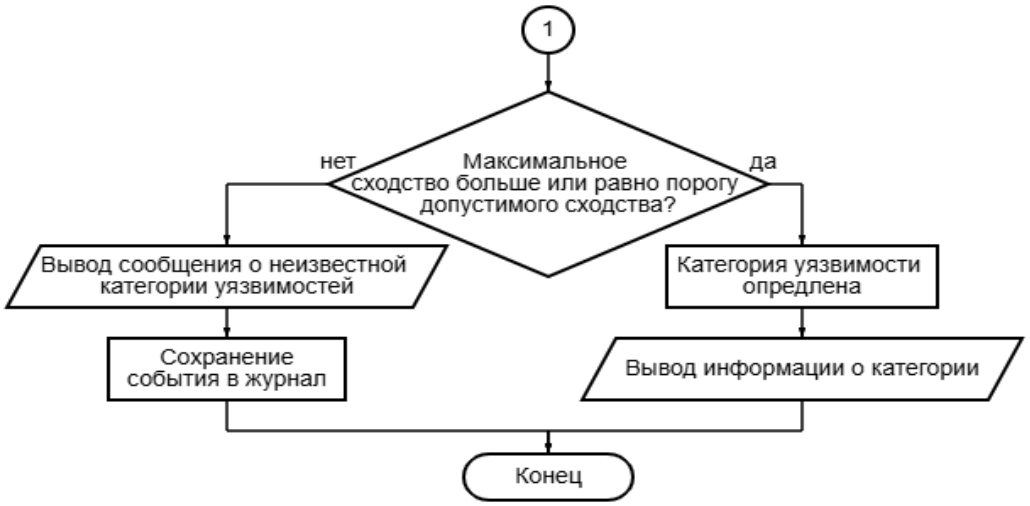



Рис. 4. Продолжение

**Заключение**

В результате было разработано алгоритмическое обеспечение, которое позволяет автоматизировать процесс генерации эффективных мер противодействия кибератакам. Структура обеспечения включает в себя ряд алгоритмов, обеспечивающих: генерацию категорий уязвимостей по семантическому смыслу, формирование мер противодействия для этих категорий, а также определение конкретных уязвимостей к сгенерированным категориям.

Разработанное алгоритмическое обеспечение вносит ряд преимуществ в программу для автоматизированной генерации мер и сценариев противодействия кибератакам, а именно: высокую степень автоматизации процессов генерации мер противодействия; повышение адаптивности к появлению новых уязвимостей; генерацию русскоязычных мер обнаружения, реагирования и ликвидации последствий. Реализация программного обеспечения данного модуля описана в соответствующем пункте приложения А настоящей работы.

Таким образом, представленные технические решения полностью соответствуют поставленным требованиям и позволяют в полной мере их реализовать в виде программы для автоматизированной генерации мер и сценариев противодействия кибератакам.

**Список литературы**

1. 4 главных метода предобработки текста в NLP с Python. URL: https://python-school.ru/blog/nlp/nlp-text-preprocessing/?ysclid=mcpb9cm3b214855573 (дата обращения: 1.07.2025).

2. markusbayer/CySecBERT Hugging Face. URL: https://huggingface.co/markusbayer/CySecBERT (дата обращения: 1.07.2025).

3. The hdbscan Clustering Library — hdbscan 0.8.1 documentation. URL: https://hdbscan.readthedocs.io/en/latest/index.html (дата обращения: 1.07.2025).

4. IQR в статистике: как использовать межквартильный размах данных. URL: https://sky.pro/wiki/analytics/iqr-v-statistike-kak-ispolzovat-mezhkvartilnyj-razmah-dannyh/?ysclid=mcpbgu0mwx702448219 (дата обращения: 1.07.2025).

5. Нейросетевая модель T5. URL: https://huggingface.co/docs/transformers/model_doc/t5 (дата обращения: 1.07.2025).

6. SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC. URL: https://csrc.nist.gov/pubs/sp/800/61/r2/final (дата обращения: 1.07.2025).

7. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности (Переиздание) - docs.cntd.ru URL: https://docs.cntd.ru/document/1200068822?yscl

id=mcpbv5nvnv746246472 (дата обращения: 1.07.2025).
8. CIS_Controls__v8.1_Guide__2024_06.pdf URL: https://etir.unb.br/wp-content/uploads/2024/10/CIS_Controls__v8.1_Guide__2024_06.pdf (дата обращения: 1.07.2025).

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 5.07.2025

**Информация об авторах**

**Остапенко Григорий Александрович** – д-р техн. наук, профессор, Финансовый университет при Правительстве Российской Федерации, e-mail: ost@fa.ru

**Остапенко Александр Алексеевич** – аспирант, Воронежский государственный технический университет, e-mail: alexostap123@gmail.com

**Кондратьев Максим Витальевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Кривошеин Александр Сергеевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Ясенев Александр Владимирович** – студент, Воронежский государственный технический университет, e-mail: shurat9@mail.ru

# AUTOMATION OF ASSESSMENT AND REGULATION OF RISKS OF IMPLEMENTATION OF CYBER-ATTACKS: PROCEDURES FOR GENERATION OF COUNTER-ACTION MEASURES

**G.A. Ostapenko, A.A. Ostapenko, M.V. Kondratyev, A.S. Krivoshein, A.V. Yasenev**

Countermeasures against cyberattacks are fundamental means of managing the risks of an information security organization. They allow you to determine in advance the sequence of actions taken to detect attacks carried out in the protected system; respond to identified attacks to reduce the maximum damage that an intruder can cause; as well as eliminate the consequences of such attacks, which is important for the fastest possible recovery of the attacked system. The purpose of the work is to form an algorithmic support for a module for generating countermeasures against cyberattacks, the algorithms of which must meet the requirements formed in the methodological support, as well as correct the limitations of existing analogs identified during the study of modern problems of ensuring cyberstability of automated systems.

Keywords: cybersecurity, cyberattack, automation, vulnerability, semantic analysis, machine learning, risk assessment.

Submitted 5.07.2025

**Information about the authors**

**Gregory A. Ostapenko** – Dr. Sc. (Technical), Professor, Financial University under the Government of the Russian Federation, e-mail: ost@fa.ru

**Alexander A. Ostapenko** – graduate student, Voronezh State Technical University, e-mail: alexostap123@gmail.com

**Maksim V. Kondratyev** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Alexander S. Krivoshein** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Alexander V. Yasenev** – student, Voronezh State Technical University, e-mail: shurat9@mail.ru

**DOI 10.36622/1682-7813.2025.28.3.009**
**УДК 004.056**

# ПОДХОДЫ К ПОСТРОЕНИЮ МОДЕЛИ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК НА ОСНОВЕ КОНВОЛЮЦИОННО-СПАЙКОВОЙ НЕЙРОННОЙ СЕТИ

**А.Г. Чурсин, С.А. Ермаков**

Статья посвящена освещению актуальной проблемы, которая связана с все возрастающими угрозами и рисками для безопасности информационных сетей и данных, которые через них передаются. Решить эту проблему можно благодаря разработке и усовершенствованию методов обнаружения атак на сети с применением передовых аналитических методов и средств искусственного интеллекта. В связи с этим цель статьи заключается в рассмотрении особенностей модели обнаружения сетевых атак на основе конволюционной нейронной сети. В процессе исследования формализованы этапы обнаружения атак. Также предложено использовать конволюционно-спайковую нейронную сеть, которая имеет ряд преимуществ по сравнению с обычными рекуррентными нейронными сетями. Отдельное внимание в статье уделено составлению карты активации и оценке вклада временных спаек.

Ключевые слова: сетевая атака, обнаружение, нейронная сеть, спайк, данные, обучение

## Введение

С быстрым развитием информационно-коммуникационных технологий объем данных, которые циркулируют в современном обществе растет стремительными темпами, а сетевые угрозы, в свою очередь, становятся все более серьезными [1].

По прогнозам Cybersecurity Ventures, ежегодные убытки от атак на различные сети в мире достигнут 9,5 трлн. дол. в 2024 г. и 10,5 трлн. дол. к 2025 г. Эксперты отмечают, что программы-вымогатели являются «самой непосредственной угрозой» в глобальном масштабе: к 2031 году ущерб от них будет стоить жертвам почти 265 млрд. дол. [2].

Очевидно, что в таких условиях особо актуальными становятся задачи разработки эффективных стратегий обнаружения и защиты от атак, а также выбора и обоснования методов поддержки безопасности сети. Кроме того, необходимо акцентировать внимание на том, что различные виды атак, как правило, должны обрабатываться по-разному.

На сегодняшний день в системах обнаружения сетевых вторжений широко используются традиционные методы машинного обучения, такие как байесовские сети, машины опорных векторов, деревья решений, логистическая регрессия и т. д. Все они достигли хороших результатов.

Однако эти методы не подходят для массивных и высокоразмерных данных, а также не могут преодолеть высокую чувствительность к шуму, что приводит к ухудшению эффективности классификации [3].

В связи с ограниченностью традиционных методов в последнее время фокус исследований сместился в сторону нейронных сетей и методов глубокого обучения. На сегодняшний день рассматриваются несколько видов нейронных сетей, например, многослойный персептрон, сети прямого распространения, рекуррентные сети. Однако особого внимания заслуживают конволюционно-спайковые сети, которые предлагают очень хорошую производительность, превосходя большинство классических подходов.

Здесь необходимо сделать пояснение касаемо терминологии нейронных сетей в данной работе.

1. Сверточная нейронная сеть (Convolutional neural network,): тип нейронной сети, специально разработанный для обработки данных с сетчатой структурой. Термины сверточная и конволюционная в работе имеют идентичное значение.

2. Спайковая нейронная сеть: это тип нейронной сети, который имитирует работу биологических нейронов, используя концепцию спайков для передачи информации, в отличие от традиционных нейронных сетей, которые работают с непрерывными значениями.

3. Спайк (импульс): нейроны в предложенной архитектуре передают информацию в виде спайков (дискретных событий), которые происходят в определенные моменты времени.

Необходимость более детального исследования возможностей и перспектив применения конволюционных нейронных сетей для обеспечения обнаружения вторжений и атак на информационные ресурсы и предопределила выбор темы данной статьи.

Различные модели и алгоритмы обнаружения сетевых атак с использованием методов глубокого обучения рассматривают в своих трудах Супрун А.Ф., Соболев Н.В., Власов А.И., Yi Lu, Menghan Liu, Jie Zhou.

Над развитием и усовершенствованием иерархической системы обнаружения вторжений, основанной на пространственных и временных признаках, трудятся Федорова В.С., Стригунов В.В., Сергадеева А.И., Лаврова Д.С., P. Ravi Kiran Varma.

Однако, несмотря на широкий интерес ученых и имеющиеся наработки, ряд вопросов в данной предметной плоскости остается открытым. Так, нерешенной является проблема избыточности признаков. Отдельного внимания заслуживает сложность, связанная с несбалансированной выборкой положительных и отрицательных классов в наборе данных, которые используются для оценки эффективности модели обнаружения.

Итак, с учетом вышеизложенного, цель статьи заключается в рассмотрении подходов к построению модели обнаружения сетевых атак на основе конволюционно-спайковой нейронной сети (К-СНС).

**Обоснование применения К-СНС**

Обнаружение вторжений в систему сетевой безопасности - довольно обширная область исследований. Ученые использовали целый ряд различных подходов для решения проблем низкой точности обнаружения и сложности идентификации нескольких классов образцов вторжений и угроз [4].

На сегодняшний день особого внимания заслуживают К-СНС, которые эффективны при извлечении пространственных и временных признаков трафика данных (таких, например, как позиционные отношения внутренней организационной структуры в сетевом коммуникационном трафике, временная последовательность пакетов данных и длительность сетевого потока) [5].

Традиционно модель обнаружения сетевых вторжений на базе (К-СНС) состоит из трех основных этапов.

Во-первых, этап предварительной обработки, на котором исходные данные преобразуются в числовые признаки и нормализуются.

Во-вторых, этап обучения, на котором предварительно обработанным данным присваиваются различные веса признаков модулем конволюционного блочного внимания на основе остатков, затем пространственные признаки извлекаются, и информация агрегируется путем комбинирования Averagepooling и Maxpooling.

В-третьих, этап тестирования, на котором тестовый набор передается в обученную модель для классификации.

Выбор К-СНС для построения модели обнаружения вторжений обусловлен следующими факторами:

1. К-СНС могут быть более эффективными в использовании вычислительных ресурсов по сравнению с традиционными полносвязными нейронными сетями. Спайковая природа обработки информации позволяет активировать только те нейроны, которые "срабатывают", что может снизить нагрузку на систему и улучшить производительность;

2. Сетевые вторжения часто имеют временные характеристики, такие как последовательность пакетов данных или временные интервалы между событиями. Спайковые нейронные сети, благодаря своему принципу работы с дискретными событиями, могут эффективно обрабатывать такие временные последовательности, что позволяет лучше выявлять аномалии и паттерны.

3. Конволюционные слои в К-СНС могут извлекать пространственные признаки из входных данных, таких как трафик сети. Это позволяет модели выявлять локальные паттерны и структуры в данных, что особенно важно для анализа сетевого трафика.

4. Сетевой трафик может содержать много шумов и нерелевантных данных. Спайковые нейронные сети могут быть более устойчивыми к шуму благодаря своей способности фокусироваться на значимых спайках и игнорировать менее важные данные

5. К-СНС могут использовать методы обучения, основанные на событиях, что позволяет им адаптироваться к изменяющимся условиям сети и новым типам атак. Это особенно важно для задач, связанных с кибербезопасностью, где новые угрозы появляются постоянно.

6. Сочетание конволюционных и спайковых архитектур может обеспечить лучшее представление данных, поскольку каждая из них имеет свои сильные стороны. Конволюционные слои могут извлекать важные признаки, а спайковые слои могут обрабатывать временные аспекты данных

7. Отсутствие проблемы забывания в процессе обучения, когда нейронная сеть теряет ранее усвоенную информацию при обучении на новых данных;

8. Возможность нейронной сети абстрактно представлять низкоуровневые признаки трафика вторжений в качестве высокоуровневых признаков благодаря спайкам.

**Модель конволюционно-спайковой нейронной сети**

На рис. 1 показан пример архитектуры предлагаемой конволюционной спайковой нейронной сети. В зависимости от желаемой задачи обнаружения сетевых атак, могут быть оптимизированы архитектурные свойства сети (например, количество слоев и размеры рецептивных полей), а также параметры обучения.

В представленной на рис. 1 нейронной сети самой базовой функциональной единицей является спайковый нейрон. Каждый слой сети состоит из одного или нескольких нейронов. Информация обрабатывается этими нейронами в течение определенного промежутка времени.

Рис. 2 (а) показывает ошибку квантования и ошибку спайки, вызванную дискретностью и недостаточным количеством временных шагов. Рис. 2 (б) отражает отсутствие ошибки спайка инактивированных нейронов, что обусловлено динамическими переходными процессами нейронов. В последнем слое расположены IF-нейроны, которые накапливают мембранный потенциал, используя его в качестве выхода сети.

Предположим, что $t$ — это текущее временное окно. Тогда у каждого нейрона будет $t$ шансов рассчитать потенциал перезарядки на основе входных данных и попытаться сгенерировать спайк.

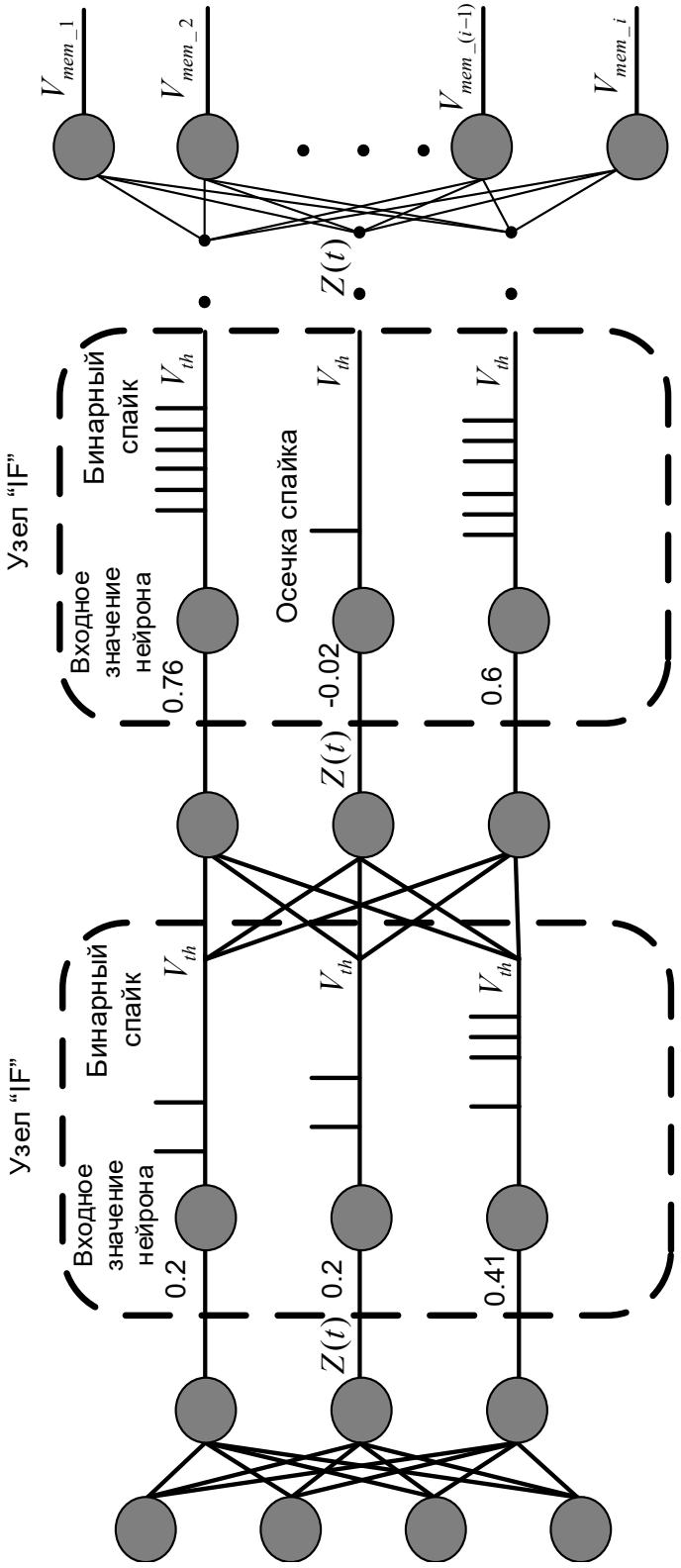



Рис. 1. Архитектура многослойной спайковой нейронной сети для обнаружения сетевых атак

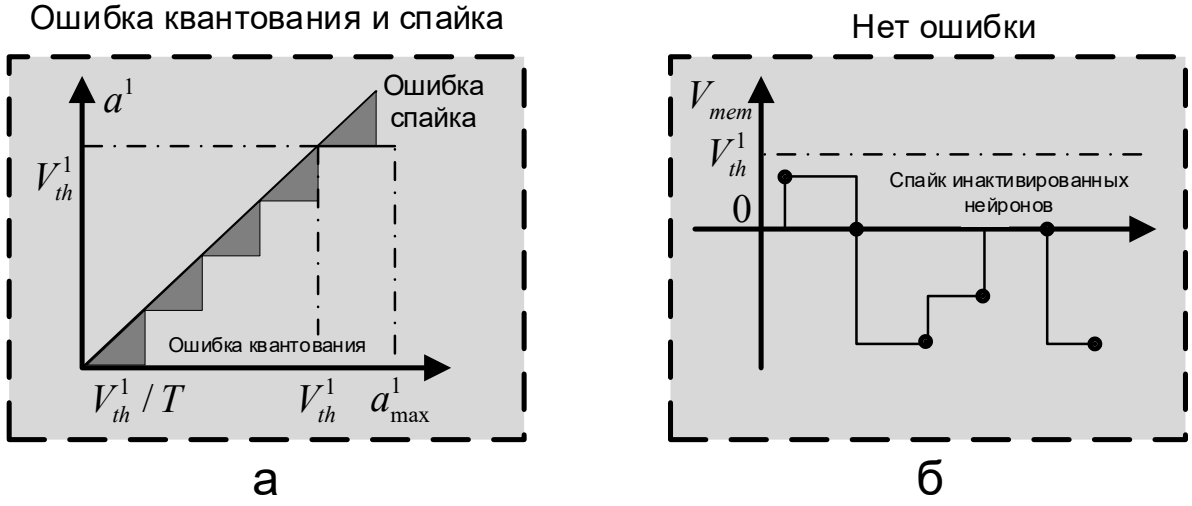



Рис. 2. Ошибка квантования и спайка (а) и отсутствие ошибки (б)

Все нейроны начинают с нулевым мембранным потенциалом. Мембранный потенциал *i*-го нейрона обновляется на каждом временном шаге следующим образом (1):

$$V_i(t) = V_i(t-1) + I_i(t-1), \quad (1)$$

где $V_i(t)$ и $V_i(t-1)$ обозначают мембранные потенциалы *i*-го нейрона на временном шаге *t* и *t* - 1 соответственно,

$I_i(t-1)$ представляет собой приращение мембранного потенциала на временном шаге *t* - 1, который рассчитывается на основе весов входов и связей (2):

$$I_i(t-1) = \Sigma_j W_{ji} J_j(t-1), \quad (2)$$

где $W_{ji}$ обозначает веса, подключенные к *i*-му нейрону;

$J_j(t-1)$ обозначает значение, переданное *i*-му нейрону с *j*-го входа предыдущего слоя на временном шаге *t* - 1.

Спайк генерируется, когда *Vi* превышает свой порог, *Vthr*, и *Vi* сбрасывается:

$$V_i(t) = (V_i(t) - V_{thr}) \times \alpha. \quad (3)$$

Здесь $\alpha \in (0, 1)$ обозначает коэффициент затухания. То есть, при срабатывании спайка потенциал *Vi* сбрасывается до значения, равного произведению части превышенного порога спайка и α. Чтобы различить разницу в мембранных потенциалах нейронов во время возбуждения сигнала спайка, сброс обычно неравномерно устанавливается на 0. В этом случае потенциал, накопленный во время предыдущего спайка, может сыграть роль в срабатывании спайка при следующем:

$$S_i(t) = 1 \text{ если } V_i(t) > V_{thr}, \quad (4)$$

где $S_i(t)$ указывает на срабатывание спайка *i*-го нейрона на временном шаге *t*. Значение 1 означает, что он сработал, а по умолчанию - 0.

Информация о спайках, генерируемая этими нейронами во временном окне *t*, будет в дальнейшем закодирована и подана в качестве входной информации на следующий слой нейронной сети. Другими словами, последовательность 0 и 1, полученная от каждого нейрона в хронологическом порядке, кодируется с помощью выбранного правила и передается на следующий слой нейронной сети.

Отдельного внимания в рамках использования спайковой нейронной сети для обнаружения сетевых атак заслуживает карта активации спаек (КАС).

КАС — это новая парадигма для построения нейронной сети. КАС использует только активность спаек при прямом распространении.

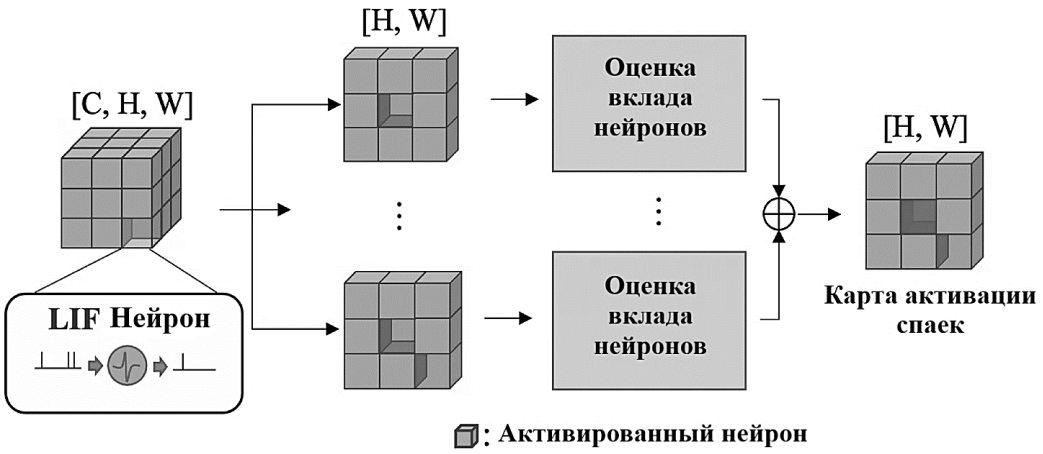



Рис. 3. Иллюстрация карты активации спаек

Таким образом, это позволяет выделять области, на которые ориентируется сеть для любого конкретного анализа поступающих данных. КАС демонстрирует значимую визуализацию даже без каких-либо меток истинности (рис. 3). На рисунке показан промежуточный тензор признаков с каналом *C*, высотой *H* и шириной *W*. Для каждого канала вычисляется оценка вклада нейронов. После этого суммируются все оценки вклада нейронов вдоль оси канала, чтобы получить в итоге КАС.

Математически эта задача может быть сформулирована как нахождение функции отображения:

$$M_t \leftarrow f(S_0, 1, \dots, S_{t-1}), \qquad (5)$$

где $M_t$ – SAM,

$S_t$ – спайковая активность на временном шаге *t*.

Для повышения производительности модели и качества обнаружения сетевых атак представляется целесообразным использовать биологическое наблюдение о том, что спайки с коротким межспайковым интервалом (КМИ) вносят большой вклад в процесс принятия решения нейронами. Это связано с тем, что короткие спайки с КМИ с большей вероятностью стимулируют постсинаптические нейроны, передавая больше информации.

С целью применения этого к задаче распознавания сетевых атак сначала необходимо определить оценку вклада временных спаек. (OBBC). Для каждого нейрона OBBC оценивает вклад предыдущего спайка в момент времени $t'$ по отношению к текущему времени *t*. Естественно, что вклад предыдущего спайка по отношению к текущему состоянию нейрона будет уменьшаться с течением времени. Поэтому значение OBBC можно сформулировать как:

$$T(t, t') = exp\,(-\gamma|-t'|), \qquad (6)$$

где $\gamma$ - гиперпараметр, управляющий крутизной экспоненциальной функции ядра.

Чтобы учесть несколько предыдущих спайков, определим набор $P_{ij}^k$, состоящий из предыдущих спайков нейрона в позиции (*i, j*) в *k*-м канале. Для каждого временного шага вычисляется показатель вклада нейрона (ПКН) $N_{ij,t}^k$ на временном шаге *t*, суммируя все значения OBBC предыдущих спаек в $P_{ij}^k$:

$$N_{ij,t}^k = \sum_{t' \in P_{ij}^k} T(t, t'). \qquad (7)$$

Таким образом, нейрон имеет высокий ПКН, если он часто участвует в спайке в течение короткого промежутка времени, и наоборот. И в завершении рассчитывается тепловая карта КАС $M_{ij,t}$ на временном шаге *t*, в месте (*i, j*) путем умножения спайковой активности $S_{ij,t}$ на значение ПКН $N_{ij,t}$ и суммирования по всем *k* каналам:

$$M_{ij,t} = \sum_k N_{ij,t}^k S_{ij,t}^k. \qquad (8)$$

Предлагается следующий алгоритм возможного использования К-СНС для решения задачи обнаружения сетевых атак.

1. Извлечение признаков:

а) сверточные слои: Первые слои К-СНС являются сверточными, которые автоматически извлекают признаки из входных данных. Они могут выявлять паттерны, такие как:

– частота появления определенных типов трафика;

– аномальные пики в объемах данных;

– неправильные последовательности пакетов,

б) спайковые нейроны: С помощью спайковых нейронов учитываются временные аспекты, такие как интервалы между пакетами и их последовательность. Это важно для распознавания атак, которые могут происходить в определенные временные окна.

2. Обучение модели:

а) обучение на метках: Модель обучается на размеченных данных, где атаки уже известны. Это может включать в себя различные типы атак, такие как DDoS, атаки,

б) обучение без учителя: В некоторых случаях модель может обучаться без меток, выявляя аномалии в данных, которые не соответствуют нормальному поведению сети.

3. Обнаружение аномалий:

а) анализ выходных данных: После обучения нейросеть может анализировать входящий трафик в реальном времени. Она будет генерировать спайки в ответ на обнаруженные паттерны,

б) пороговые значения: Сеть может использовать пороговые значения для определения аномалий. Если уровень активности превышает заданный порог, это может указывать на потенциальную атаку.

**Заключение**

В работе предложены принципы и подходы для построения модели обнаружения сетевых атак, основу которой составляет конволюционно-спайковая нейронная сеть. Описано получение карты активации спаек.

Преимуществом данной сети является то, что она позволяет преодолеть проблему неполного извлечения признаков, может быть решен вопрос дисбаланса набора данных и избыточности признаков, так же К-СНС способна обрабатывать временные и пространственные данные, и быть устойчивой к шуму и обучаться на основе событий.

**Список литературы**

1. Тимочкина, Т.В. Применение нейронных сетей для обнаружения сетевых атак / Т.В. Тимочкина // Известия высших учебных заведений. 2021. № 5. С. 357-363.

2. Gebrekiros Gebreyesus Gebremariam Localization and Detection of Multiple Attacks in Wireless Sensor Networks Using Artificial Neural Network / Gebreyesus Gebremariam Gebrekiros // Wireless Communications and Mobile Computing. 2023. Volume 2023. Issue 1. P. 23-29.

3. Изотова О.А. Применение нечувствительных к весам нейронных сетей для распознавания сетевых атак / О.А. Изотова, Д.С. Лаврова, Е.Ю. Павленко // Методы и технические средства обеспечения безопасности информации. 2023. № 32. С. 86-87.

4. Karthik V. Residual based temporal attention convolutional neural network for detection of distributed denial of service attacks in software defined network integrated vehicular adhoc network / V. Karthik // International Journal of Network Management. 2023. Issue 3. P. 45-49.

5. Болдырихин, Н.В. Аналитический обзор нейронных сетей для обнаружения сетевых атак / Н.В. Болдырихин // Научный аспект. 2024. № 3. С. 5-10.

Воронежский государственный технический университет
Voronezh State Technical University

Концерн «Созвездие», г. Воронеж
Concern «Sozvezdie», Voronezh

Поступила в редакцию 30.03.2025

**Информация об авторах**

**Чурсин Андрей Германович** – аспирант, Воронежский государственный технический университет, e-mail: mnac@comch.ru

**Ермаков Сергей Александрович** – канд. техн. наук, доцент, Воронежский государственный технический университет, начальник отдела, «Концерн «Созвездие», г. Воронеж, e-mail: mnac@comch.ru

# APPROACHES TO BUILDING A NETWORK ATTACK DETECTION MODEL BASED ON CONVOLUTIONAL SPIKE NEURAL NETWORK

**A.G. Chursin, S.A. Ermakov**

The article is devoted to highlighting the current problem, which is related to the ever-increasing threats and risks to the security of information networks and the data that are transmitted through them. This problem can be solved through the development and improvement of methods for detecting attacks on networks using advanced analytical methods and artificial intelligence tools. In this regard, the purpose of the paper is to examine the features of a network attack detection model based on a convolutional neural network. In the process of research, the stages of attack detection are formalized. It is also proposed to use a convolutional spike neural network, which has a number of advantages over conventional recurrent neural networks. The paper pays special attention to the convolutional spike activation mapping and the evaluation of the contribution of temporal spikes.

Keywords: network attack, detection, neural network, spike, data, training.

Submitted 30.03.2025

**Information about the authors**

**Andrey G. Chursin –** Graduate Student, Voronezh State Technical University, email: mnac@comch.ru

**Sergey A. Ermakov** – Cand. Sc. (Technical), Associate Professor, Voronezh State Technical University, Head of Department, Concern “Sozvezdie”, Voronezh, email: mnac@comch.ru

**DOI 10.36622/1682-7813.2025.28.3.010**
**УДК 621.372.004**

# АВТОМАТИЗАЦИЯ ОЦЕНКИ И РЕГУЛИРОВАНИЯ РИСКОВ РЕАЛИЗАЦИИ КИБЕРАТАК: ПРОГРАММНО-ТЕХНИЧЕСКИЙ КОМПЛЕКС

**Г.А. Остапенко, А.А. Остапенко, М.В. Кондратьев, А.С. Кривошеин, С.Е. Сотников**

Программно-технический комплекс для автоматизированной генерации сценариев реализации противодействия в отношении кибератак – это инструмент для их моделирования и анализа с адаптивной генерацией мер противодействия для них. Программно-технический комплекс может работать как автономно, так и взаимодействуя с внешними программно-техническими комплексами через базу данных или файлы, которые она использует или генерирует. Учитывая тенденции в усиленном развитии киберугроз, данная программно-технический комплекс позволяет повысить киберустойчивость автоматизированных систем различной архитектуры и назначения.

Ключевые слова: программно-технический комплекс, кибербезопасность, кибератака, моделирование угроз, оценка рисков, автоматизация.

**Структура данных**

Фундаментальной основой любого программного обеспечения является правильно спроектированная структура хранения, обработки и передачи данных. В программе для автоматизированной генерации мер и сценариев противодействия кибератакам правильный выбор структуры данных играет одну из ключевых ролей, чтобы обеспечить высокую производительность, масштабируемость и интегрированность программного обеспечения.

В разработанном программном обеспечении основным форматом для обмена данными является JSON (JavaScript Object Notation), который является легковесным человекочитаемым форматом серилазиции данных. Решение о применении данного формата было обосновано рядом следующих преимуществ:

- кроссплатформенность. Формат поддерживается подавляющим большинством языков программирования;

- универсальность. Данный формат, дает возможность описания сложных структур данных, такие как: вложенные объекты, массивы и примитивы;

- читаемость и простота парсинга. Эти преимущества упрощают отладку и разработку.

Файлы JSON применяется во всех модулях программы для автоматизированной генерации мер и средств противодействия кибератакам, а именно:

- централизованный сбор, обработка и хранение информации в компонентах кибератак. Информация об уязвимостях, слабостях, техниках, тактиках и шаблонах атак загружается модулем из внешних источников в виде JSON-файлов, после чего происходит парсинг этих данных и сохранение в графовую базу данных Neo4j;

- генерация сценариев кибератак. Сценарий кибератаки формируется как последовательность техник, соответствующих определенным тактикам злоумышленника. JSON-файл используется для хранения информации о тактической модели кибератак, представляющей ориентированный граф в виде структурированного документа;

- генерация мер противодействия кибератакам. Генерация происходит на основе типовых мер противодействия, которые были объединены в общий JSON документ из авторитетных стандартов и источников в области информационной

безопасности. Также каждая уязвимость относится к конкретной категории уязвимостей со своими мерами противодействия, поэтому данные о категориях уязвимостей и мерах противодействия им хранятся в виде базы знаний в JSON-файле.

Во внутренней работе программного обеспечения, для хранения и обработки информации, применяется база данных Neo4j, которая использует графовый формат данных, что позволяет эффективно проводить анализ взаимосвязей между компонентами кибератак и выявлять пути их реализации [1]. В Neo4j данные представлены следующим образом:

1) узлы представляют хранимые в графовой базе данных сущности, а именно: уязвимости, слабости, техники и шаблоны кибератак.

2) ребра хранят информацию о связях между узлами базы данных, в контексте разработанного программного обеспечения взаимосвязаны следующие пары компонентов кибератак:

- шаблоны атак с техниками атак описывают как конкретные техники атаки могут быть использованы для реализации шаблона атаки, что позволяет строить возможные пути реализации атаки;

- техники атак с техниками атак описывают логическую последовательность применения техник при реализации атаки, что позволяет формировать реалистичные сценарии кибератак;

- техники атак со слабостями показывают, какие слабости системы могут быть использованы в процессе применения той или иной техники атаки, что позволяет выявлять недостатки архитектуры, которые могут привести к появлению уязвимостей;

- слабости с уязвимостями демонстрируют как конкретные уязвимости возникают из-за неустраненных слабостей в архитектуре, что позволяет перейти от более абстрактных уровней представления кибератаки к конкретным ее случаям.

3) Свойства – дополнительная информация об узлах, реализованная в парах ключ-значение, где ключами являются конкретные узлы или ребра графовой базы данных, а значениями свойства этих узлов или ребер, например:

- название, описание и вероятность эксплуатации для всех узлов графа;

- CVSS, EPSS оценки и наличие в CISA KEV для уязвимостей;

- соответствующие тактики для техник.

Взаимодействие с графовой базой данных Neo4j происходит через специализированный декларативный язык запросов Cypher, который был специально создан для эффективной работы с графовой структурой данных [2]. Данный язык запросов изначально оперирует именно понятиями узлов, ребер и их свойств, в отличие от классических SQL-подобных языков, которые ориентированы на работу с таблицами.

Основные функциональные возможности Cypher с примерами запросов, которые используются в программном обеспечении (рис. 1-5):

- создание графовых структур (добавление новых узлов, ребер и их свойств):

```
CREATE (:Technique {
    name: "Поиск на общедоступных сайтах",
    id: "T1593",
    description: "Злоумышленники могут искать информацию о своих жертвах на
        общедоступных сайтах и (или) доменах, чтобы использовать ее для атак.
        Информация о жертвах может быть доступна на различных онлайн-ресурсах,
        таких как социальные сети, новостные сайты или сайты с деловой информацией,
        например о найме и предлагаемых и выполненных контрактах."
})
```

Рис. 1. Cypher-запрос для создания узла техники T1593

- обновление графовых структур (редактирование свойств узлов и ребер):

```
MATCH (t:Technique {external_id: "T1593"})
SET t.tactics = "reconnaissance"
```

Рис. 2. Cypher-запрос для обновления свойства узла техники T1593, с соответствующими ему тактиками

- удаление графовых структур (удаление узлов, ребер или их свойств):

```
MATCH (technique)-[relation:SCENARIO]→(technique)
DELETE relation
```

Рис. 3. Cypher-запрос для удаления ребер, которые образуют петли у узлов техник

- запросы данных (поиск конкретных узлов или подграфов по заданным критериями):

```
MATCH (technique:Technique {tactics: "reconnaissance"})
RETURN technique.name, technique.description
```

Рис. 4. Cypher-запрос для получения данных о названиях и описаниях всех техник, соответствующих тактике “Разведка”

- анализ графовых структур (обнаружение путей между конкретными узлами; подсчет статистики узлов, ребер или их свойств по заданным шаблонам; группировка и ранжирование узлов или ребер по различным свойствам):

```
MATCH (cve:CVE {in_cisa_kev: "true"})
WHERE exists(cve.cvss)
RETURN cve.id, cve.cvss
ORDER BY cvss DESC
LIMIT 10
```

Рис. 5. Cypher-запрос для ранжирования уязвимостей из каталога CISA KEV по CVSS-оценке и получения данных о первых 10 из них

Таким образом, данное решение о комбинировании JSON в качестве формата обмена данными и графовой структуры данных Neo4j для хранения и обработки данных, реализованное в программном обеспечении для автоматизированной генерации мер и сценариев противодействия кибератакам, обеспечивает высокую производительность, гибкость и выразительность программы в контексте управления данными.

**Технологическое обеспечение**

Данная программно-технический комплекс разработана в рамках клиент-серверной архитектуры, что обеспечивает эффективное взаимодействие пользователя с программным обеспечением, так как такая архитектура направлена на обеспечение взаимосвязанности пользовательского интерфейса с основной логикой обработки данных серверной части [3]. Такая архитектура обеспечивает программу для автоматизированной генерации мер и сценариев противодействия кибератакам высокими показателями гибкости и масштабируемости, что важно для моделирования сложных атак и их последующего анализа.

Программное обеспечение полностью разработано с помощью языка программирования Python, который является одним из самых популярных и мощных языков в мире, применяемых для анализа больших данных, искусственного интеллекта, автоматизации и веб-разработки [4]. Python был выбран языком программирования для данной программы за счет следующего ряда преимуществ:

- простота синтаксиса - повышает скорость разработки и будущих улучшений за счет более понятного исходного кода;

- большое количество библиотек - дает возможность разрабатывать объемные программы за более короткие сроки, за счет готовых библиотек, включая средства работы с графиками (Plotly), базами данных (py2neo), анализом данных (NumPy) и машинным обучением (PyTorch, Scikit-learn и transformers);

- кроссплатформенность - гарантирует возможность запуска программы на любой операционной системе без каких-либо изменений в исходном коде, что важно в условиях напряженности с основными владельцами операционных систем;

**Серверная часть**

Серверная часть программного обеспечения для автоматизированной генерации мер и сценариев противодействия кибератакам реализована по принципам паттерна программирования “Модульный монолит”, который сочетает в себе как преимущества классической реализации программ (простоту развертывания, отладки и обновлений), так и модульной реализации (работа с отдельными частями программного обеспечения без необходимости внесения изменений в другие части) [5]. Но все же данное решение не было отнесено к полностью модульной реализации за счет того, что модули программы взаимосвязаны между собой через базу данных Neo4j или JSON-файл, в которых хранится промежуточная информация.

Вся функциональность программного обеспечения разделена на следующие самостоятельные программные модули, которые разработаны в соответствии с алгоритмическим обеспечением, сформированных в результате предыдущих глав настоящей работы:

- централизованный сбор, обработка и хранение информации о компонентах кибератак;

- генерация и анализ сценариев кибератак;

- генерация мер противодействия кибератакам.

В данном подходе к реализации серверной части у каждого модуля имеются свои строго разделенные задачи, но все же данные модули взаимосвязаны за счет общей базы данных, информация из которой важна для правильной и эффективной работы всего программного комплекса в целом.

**Клиентская часть**

Клиентская часть программного комплекса для автоматизированной генерации мер и средств противодействия кибератакам реализована с помощью фреймворка Dash, который является высокоуровневым набором инструментов веб-разработки на языке программирования Python [6].

С помощью Dash был реализован пользовательский интерфейс, который позволяет не только просматривать обработанную информацию о кибератаках, но и взаимодействовать с наблюдаемыми данными, перемещаясь между страницами, описывающими те или иные характеристики кибератак, тем самым углубляясь в детали и получая подробное представление о рассматриваемой атаке. Можно перечислить следующие страницы клиентской части программного комплекса.

1. Анализ шаблона атаки. Данная страница является начальной в пользовательском интерфейсе, на ней пользователь может рассмотреть название и описание интересующего его шаблона атаки. Также реализована возможность рассмотреть трехмерные графы компонентов кибератак, измерениями которого являются значения риска нарушения целостности, доступности и конфиденциальности информации в системе. Узлы в данных графах являются интерактивными и при клике на них позволяют перейти на соответствующую им страницу, для последующего более подробного ознакомления. Кроме того, при выборе определенного шаблона атаки у пользователя появляется возможность сгенерировать сценарии данной атаки нажатием на соответствующую кнопку “Сценарии”. Пример страницы анализа шаблонов атаки изображен на рис.6.


Рис. 6. Пример страницы анализа шаблона атаки CAPEC-10

2. Генерация сценариев атаки - данная страница генерирует и отображает таблицу всех возможных сценариев атаки, шаблон которой был выбран на начальной странице. В таблице для каждого сценария указаны такие данные, как:

- уникальный идентификатор сценария, генерируемый программным обеспечением;
- значения рисков нарушения конфиденциальности, целостности и доступности информации в системе;
- кнопка перехода на страницу анализа этого сценария атаки.

Также присутствует возможность отображения атак, реализуемых только с помощью одной техники, нажатием на соответствующую кнопку. Пример данной страницы можно увидеть на рис. 7.

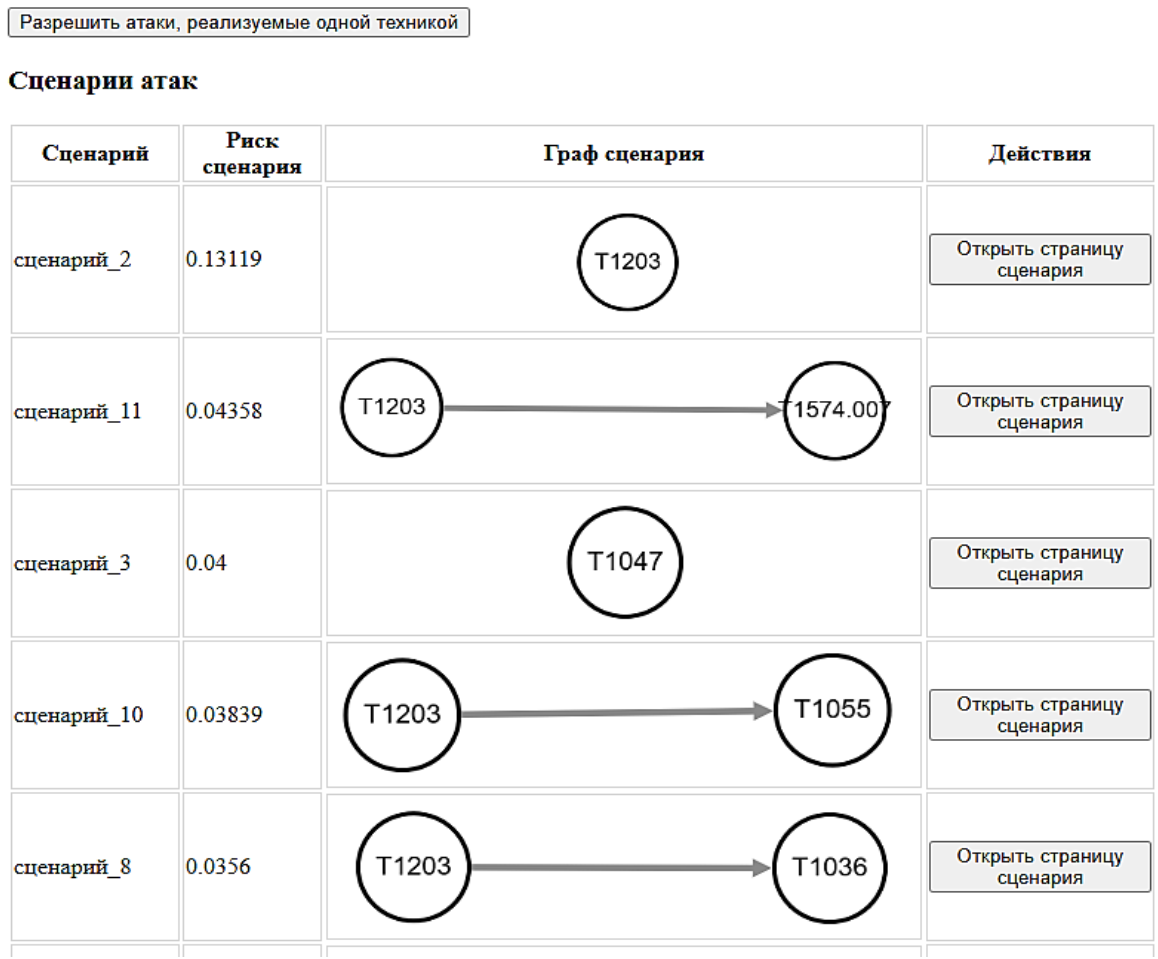



Рис. 7. Пример страницы генерации сценариев для атаки CAPEC-10

3. Анализ сценария атаки - данная страница содержит основную информацию о конкретном сценарии кибератаки. В отображаемую информацию входят:

- граф сценария, который показывает порядок техник, используемых злоумышленником в ходе атаки. Узлы являются интерактивными и позволяют перейти на страницу техники, по который был совершен клик в пользовательском интерфейсе;
- график рисков, показывающий распределение вероятностей нанесения нормированного ущерба определенной величины успешной реализацией атаки, где у каждого пика графика находится подпись с идентификатором соответствующей техники атаки. Данная подпись является

интерактивной и позволяет осуществить переход на страницу соответствующей техники.

Пример страницы анализа сценария атаки изображен на рис. 8.

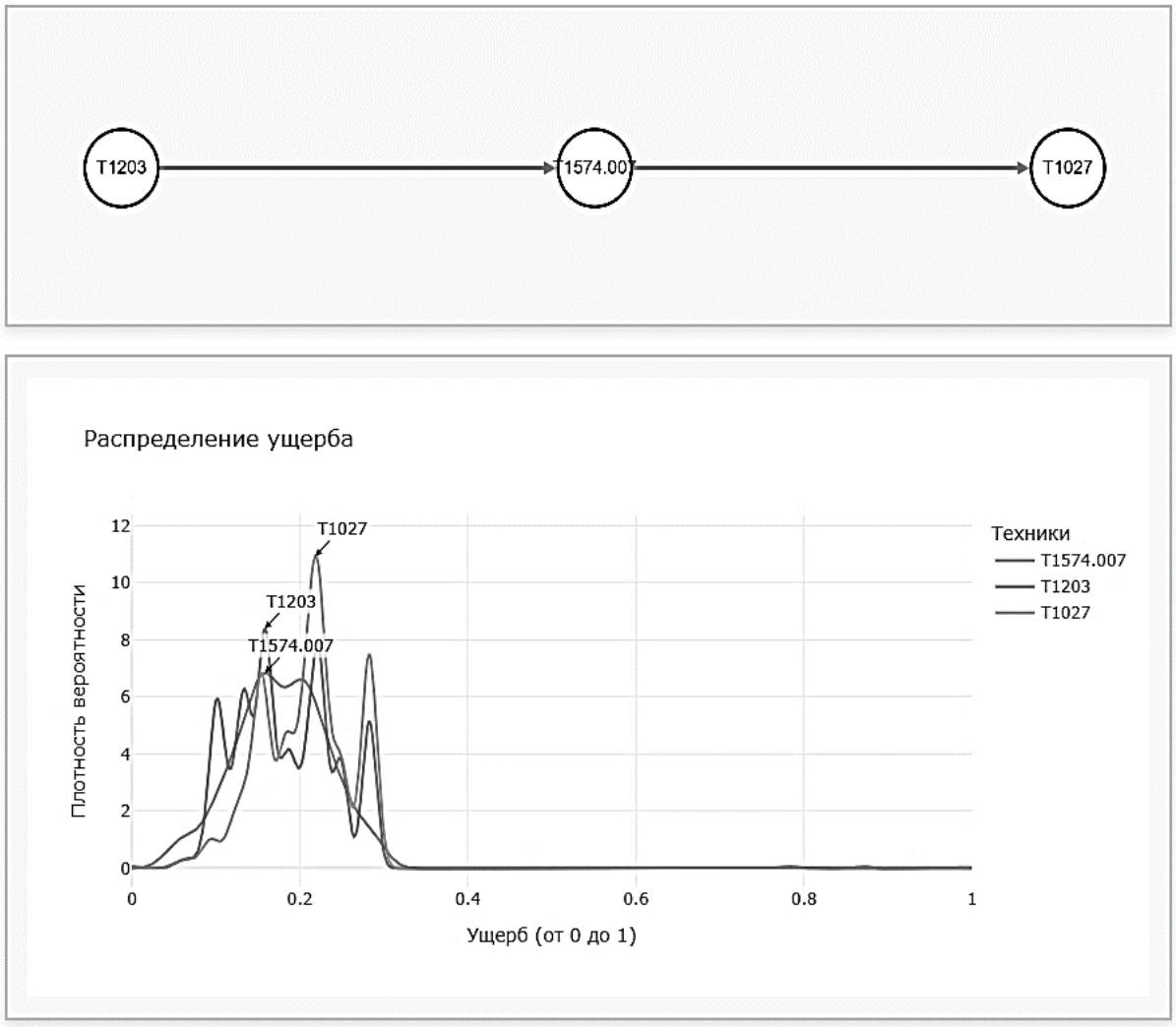



Рис. 8. Пример страницы анализа сценария 41 атаки CAPEC-10

4. Техника атаки - на этой странице отображена информация о технике, которая включает в себя:

- название;
- описание;
- таблица уязвимостей, которые могут быть проэксплуатированы данной техникой в ходе атаки со значениями риска нарушения конфиденциальности целостности и доступности информации в системе с возможностью гибкой сортировки по типу риска, который важен для пользователя. Также в данной таблице есть кнопки, которые позволяют пользователю перейти на страницу соответствующей уязвимости.

Пример данной страницы изображен на рис. 9.

**T1203: Эксплуатация уязвимостей в клиентском ПО**

**Злоумышленники могут эксплуатировать уязвимости в клиентских приложениях для выполнения кода. В программном обеспечении могут существовать уязвимости из-за применения небезопасных методов программирования, которые могут привести к непредвиденному поведению программы. Злоумышленники могут целенаправленно эксплуатировать определенные уязвимости с целью выполнения произвольного кода. Зачастую самыми ценными эксплойтами в арсенале злоумышленников являются те, которые можно использовать для выполнения кода на удаленной системе, поскольку с их помощью можно получить доступ к этой системе. Файлы, относящиеся к распространенным рабочим приложениям, привычны для пользователей и поэтому являются выгодной целью для исследования и разработки эксплойтов.**

Важность конфиденциальности в общем риске

100

Важность целостности в общим риске

100

Важность доступности в общем риске

100

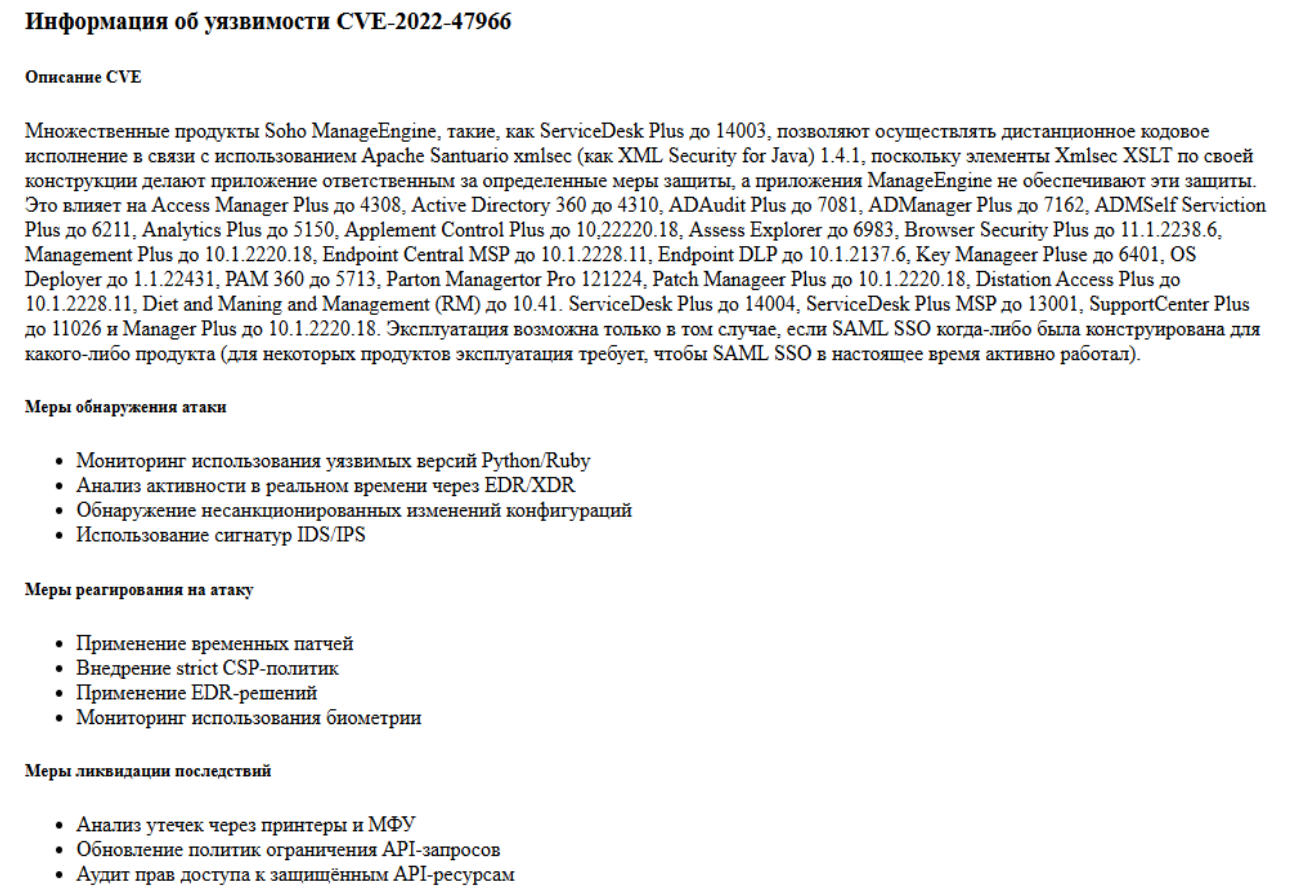
| CVE | Риск для конфиденциальности | Риск для целостности | Риск для доступности | Общий риск | Меры противодействия |
|---|---|---|---|---|---|
| CVE-2023-32560 | 0.087 | 0.087 | 0.087 | 0.26101 | Подробнее |
| CVE-2019-1663 | 0.08669 | 0.08669 | 0.08669 | 0.26006 | Подробнее |
| CVE-2019-1663 | 0.08669 | 0.08669 | 0.08669 | 0.26006 | Подробнее |
| CVE-2015-3105 | 0.0862 | 0.0862 | 0.0862 | 0.2586 | Подробнее |
| CVE-2015-3090 | 0.08582 | 0.08582 | 0.08582 | 0.25745 | Подробнее |
| CVE-2014-7187 | 0.08572 | 0.08572 | 0.08572 | 0.25717 | Подробнее |
| CVE-2010-3962 | 0.08572 | 0.08572 | 0.08572 | 0.25717 | Подробнее |
| CVE-2018-6892 | 0.08567 | 0.08567 | 0.08567 | 0.257 | Подробнее |
| CVE-2011-0923 | 0.08552 | 0.08552 | 0.08552 | 0.25657 | Подробнее |
| CVE-2017-0149 | 0.08549 | 0.08549 | 0.08549 | 0.25648 | Подробнее |
| CVE-2011-2140 | 0.08547 | 0.08547 | 0.08547 | 0.25641 | Подробнее |
| CVE-2008-0244 | 0.08546 | 0.08546 | 0.08546 | 0.25638 | Подробнее |
| CVE-2013-0634 | 0.08545 | 0.08545 | 0.08545 | 0.25634 | Подробнее |

Рис. 9. Пример страницы техники T1203

5. Уязвимость атаки - на данной странице пользовательского интерфейса отображена информация о выбранной уязвимости, которая включает в себя:

- уникальный идентификатор;
- описание;
- меры обнаружения, реагирования и ликвидации последствий от атаки через эксплуатацию этой уязвимости.

Пример страницы уязвимости атаки изображен на рис. 10.



**Информация об уязвимости CVE-2022-47966**

**Описание CVE**

Множественные продукты Soho ManageEngine, такие, как ServiceDesk Plus до 14003, позволяют осуществлять дистанционное кодовое исполнение в связи с использованием Apache Santuario xmlsec (как XML Security for Java) 1.4.1, поскольку элементы Xmlsec XSLT по своей конструкции делают приложение ответственным за определенные меры защиты, а приложения ManageEngine не обеспечивают эти защиты. Это влияет на Access Manager Plus до 4308, Active Directory 360 до 4310, ADAudit Plus до 7081, ADManager Plus до 7162, ADMSelf Serviction Plus до 6211, Analytics Plus до 5150, Applement Control Plus до 10,22220.18, Assess Explorer до 6983, Browser Security Plus до 11.1.2238.6, Management Plus до 10.1.2220.18, Endpoint Central MSP до 10.1.2228.11, Endpoint DLP до 10.1.2137.6, Key Manageer Pluse до 6401, OS Deployer до 1.1.22431, PAM 360 до 5713, Parton Managertor Pro 121224, Patch Manageer Plus до 10.1.2220.18, Distation Access Plus до 10.1.2228.11, Diet and Maning and Management (RM) до 10.41. ServiceDesk Plus до 14004, ServiceDesk Plus MSP до 13001, SupportCenter Plus до 11026 и Manager Plus до 10.1.2220.18. Эксплуатация возможна только в том случае, если SAML SSO когда-либо была конструирована для какого-либо продукта (для некоторых продуктов эксплуатация требует, чтобы SAML SSO в настоящее время активно работал).

**Меры обнаружения атаки**

- Мониторинг использования уязвимых версий Python/Ruby
- Анализ активности в реальном времени через EDR/XDR
- Обнаружение несанкционированных изменений конфигураций
- Использование сигнатур IDS/IPS

**Меры реагирования на атаку**

- Применение временных патчей
- Внедрение strict CSP-политик
- Применение EDR-решений
- Мониторинг использования биометрии

**Меры ликвидации последствий**

- Анализ утечек через принтеры и МФУ
- Обновление политик ограничения API-запросов
- Аудит прав доступа к защищённым API-ресурсам

Рис. 10. Пример страницы уязвимости CVE-2022-47966

**Функциональные библиотеки**

При разработке программного комплекса для автоматизированной генерации мер и сценариев противодействия кибератакам использовались следующие библиотеки Python, информация о которых представлена в табл. 1.

Таблица 1

Функциональные библиотеки программного обеспечения

| Название библиотеки | Описание библиотеки | Роль библиотеки в программном обеспечении |
|---|---|---|
| py2neo | Используется для работы с графовой базой данных Neo4j через API для взаимодействия с языком запросов Cypher. | Создание, обновление и удаление узлов, ребер и свойств для них в графовой базе Neo4j. |
| threading | Позволяет выполнять одновременно несколько задач в одном процессе программы. | Обеспечивает многопоточное выполнение задач на серверной части программы, например генерацию большого числа сценариев одновременно или обработка нескольких Cypher-запросов к базе данных. |

Продолжение табл. 1

| Название библиотеки | Описание библиотеки | Роль библиотеки в программном обеспечении |
|---|---|---|
| re | Предназначен для работы с регулярными выражениями, что применяется для поиска текста по заданным шаблонам. | Используется при обработке входных данных, во время загрузки информации о компонентах кибератак из внешних источников. |
| scipy | Предоставляет инструменты для научных вычислений, таких как: линейная алгебра, оптимизация, интегрирование и так далее. | Применяется при расчете и построении распределений вероятностей возникновения ущерба определенной величины для сценариев кибератак. |
| numpy | Обеспечивает работу с многомерными массивами и матрицами, а также множество распространенных математических функций. | Работа с данными о компонентах кибератак. Расчет рисков, вероятностей и подготовка данных для машинного обучения. |
| scikit-learn | Предоставляет алгоритмы машинного обучения для классификации, кластеризации, регрессии и других задач. | Обработка уязвимостей, слабостей, техник и шаблонов атак перед генерацией смысловых векторов BERT. |
| transformers | Предоставляет доступ к предобученным нейросетевым моделям, таким как BERT, GPT и другим. | Генерация смысловых векторов BERT для текстовых описаний компонентов кибератак для создания ребер между соответствующими узлами. |
| torch | Фреймворк глубокого машинного обучения, позволяющий строить и обучать нейросетевые модели. | Построение модели генерации ребер в графе между узлами компонентов кибератак. |
| nltk | Используется для обработки естественного языка, в том числе выполнения следующих действий: токенизация, лемматизация и другие. | Предобработка текстовых описаний компонентов кибератак перед генерацией смысловых векторов BERT или векторов ключевых слов TF-IDF. |
| hdbscan | Модуль, реализующий алгоритм кластеризации на основе плотности данных. | Кластеризация смысловых векторов уязвимостей для создания их категорий по семантическому смыслу. |

Окончание табл. 1

| Название библиотеки | Описание библиотеки | Роль библиотеки в программном обеспечении |
|---|---|---|
| dash | Фреймворк для создания интерактивных веб-приложений. | Реализация всей клиентской части программы. |
| json | Встроенный модуль, позволяющий обрабатывать данные в формате JSON. | Передача данных между частями программного обеспечения. |
| plotly | Предназначена для построения интерактивных графиков и диаграмм. | Визуализация графов атак, графиков распределений рисков, а также графов трехмерных представлений узлов различных компонентов кибератаки. |

**Заключение**

Использование данного набора библиотек образует ряд преимуществ для разрабатываемого программного комплекса, а именно:

- производительность - перечисленные библиотеки хорошо оптимизированы, что повышает скорость работы программы в целом;

- читаемость исходного кода - используются только популярные библиотеки, которые хорошо документированы;

- функциональная интеграция - большинство перечисленных библиотек поддерживают взаимодействие друг с другом, что еще больше объединяет программу в единое целое.

Данный (табл. 1) ряд библиотек обеспечивает структурированное и комплексное программное обеспечение, эффективно выполняющее все возложенные на него задачи.

**Список литературы**

1. Neo4j documentation - Neo4j Documentation. URL: https://neo4j.com/docs/ (дата обращения: 15.07.25).

2. Introduction - Cypher Manual | Neo4j Graph Data Platform. URL: https://neo4j.com/docs/cypher-manual/current/introduction/ (дата обращения: 15.07.25).

3. Клиент-серверная архитектура. URL: https://servergate.ru/articles/klient-servernaya-arkhitektura/?ysclid=mcpcbzpkok871268226 (дата обращения: 15.07.25).

4. Python documentation. URL: https://docs.python.org/3/ (дата обращения: 15.07.25).

5. Модульный монолит. Начало / Хабр. URL: https://habr.com/ru/companies/dododev/articles/650721/ (дата обращения: 15.07.25).

6. Dash Documentation & User Guide | Plotly. URL: https://dash.plotly.com/ (дата обращения: 15.07.25).

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 18.07.2025

**Информация об авторах**

**Остапенко Григорий Александрович** – д-р техн. наук, профессор, Финансовый университет при Правительстве Российской Федерации, e-mail: ost@fa.ru

**Остапенко Александр Алексеевич** – аспирант, Воронежский государственный технический университет, e-mail: alexostap123@gmail.com

**Кондратьев Максим Витальевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Кривошеин Александр Сергеевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Сотников Сергей Евгеньевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

# AUTOMATION OF ASSESSMENT AND REGULATION OF RISKS OF IMPLEMENTATION OF CYBER-ATTACKS: SOFTWARE AND HARDWARE COMPLEX

**G.A. Ostapenko, A.A. Ostapenko, M.V. Kondratyev, A.S. Krivoshein, S.E. Sotnikov**

The program for automated generation of scenarios for counteraction against cyber attacks is a tool for their modeling and analysis with adaptive generation of counteraction measures for them. The program can work both autonomously and interacting with external programs through a database or files that it uses or generates. Given the trends in the increased development of cyber threats, this program allows you to increase the cyber resilience of automated systems of various architectures and purposes.

**Keywords:** software and hardware complex, cybersecurity, cyberattack, threat modeling, risk assessment, automation.

Submitted 18.07.2025

**Information about the authors**

**Gregory A. Ostapenko** – Dr. Sc. (Technical), Professor, Financial University under the Government of the Russian Federation, e-mail: ost@fa.ru

**Alexander A. Ostapenko** – graduate student, Voronezh State Technical University, e-mail: alexostap123@gmail.com

**Maksim V. Kondratyev** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Alexander S. Krivoshein** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Sergey E. Sotnikov** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**DOI 10.36622/1682-7813.2025.28.3.011**
**УДК 004.588**

# УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ: МЕТОДИКА И РЕЗУЛЬТАТЫ

**В.А. Минаев, А.С. Эрдниев**

В статье рассматривается состояние информационной безопасности в образовательных учреждениях Российской Федерации, имеющих свою специфику в сфере защиты информационных ресурсов учебного процесса и научно-исследовательской деятельности. Показывается, что массовое, не всегда четкое контролирование компьютерной техники и информационных систем в образовательном учреждении приводит к особому проявлению информационных рисков, требующих специальной методики их оценивания и управления. Результаты проведения экспертных процедур свидетельствуют о том, что в рейтинге наиболее опасных рисков находятся – сбои и отказы технических средств, ошибки специалистов по информационным технологиям, сбои и отказы программных средств, сбои и отказы сетевого оборудования, вредоносное программное обеспечение, несанкционированный доступ к информации. Степень опасности рисков оценена, исходя из значения произведения вероятности реализации угрозы на значение возможного ущерба. Всего рассмотрено одиннадцать видов информационных угроз, оцененных экспертами, в качестве которых выступили около ста респондентов (преподаватели, технические работники, студенты старших курсов). Для управления информационными рисками применена методика «затраты-эффект», разработанная и адаптированная в Институте проблем управления РАН им. В. А. Трапезникова Российской академии наук. Методика позволила упорядочить проекты минимизации информационных рисков в образовательном учреждении по их эффективности. В заключении статьи приводится перечень мер по реализации каждого из восьми предложенных проектов.

**Ключевые слова:** образовательное учреждение, информационный риск, оптимизация, экспертная оценка, проект «затраты-эффект», эффективность.

## Введение

Современная учебная и научно-исследовательская деятельность организаций образовательного типа неразрывно связана с процессами получения, хранения, обработки и передачи информации. Информационные системы вузов обеспечивают доступ профессорско-преподавательскому составу, сотрудникам и обучающимся к библиотекам, приложениям и сервисам, связанным с едиными базами данных.

Весь этот комплекс активно развивается, вовлекая в процесс своего функционирования все более современные информационные технологии.

Однако, как отмечается в работах [1-3], многие образовательные системы изначально разрабатывались без должного внимания к информационной защите, что делает их уязвимыми к кибератакам, утечкам данных и другим угрозам.

По информации МВД РФ в 2024 году 40% всех преступлений совершены с использованием IT-технологий. Причем их количество нарастает – таких деяний зарегистрировано на 13% больше, чем в предыдущем году.

В связи с этим анализ и управление информационными рисками становятся ключевыми задачами обеспечения нормальной работы образовательных организаций.

Исследования в области управления информационными рисками активно проводятся как в России, так и за рубежом. При этом ученые в своих работах все чаще фокусируются на технологических аспектах кибербезопасности [4-6], подчеркивая критическую важность адаптивных моделей, способных динамически реагировать на изменяющиеся угрозы.

## Этап 1. Ранжирование информационных рисков

В рамках исследования информационных рисков в образовательном учреждении авторами проведен экспертный опрос руководящего состава,

преподавателей, технического персонала и обучающихся. В анкетировании приняли участие около ста респондентов, что обеспечило достаточную репрезентативность полученных результатов.

Информационный риск рассчитывался как произведение вероятности реализации угрозы на значение возможного ущерба. В табл. 1 представлены результаты проведения экспертной оценки информационных рисков и их ранжирование.

Проведенное исследование позволило получить детальную картину распределения информационных рисков, характерных для современного образовательного учреждения.

Анализ позволил систематизировать основные риски, способные нанести ущерб информационной инфраструктуре учебного заведения. На основе эмпирических данных, полученных в результате проведения анкетирования среди преподавателей, сотрудников и студентов старших курсов, а также экспертных оценок специалистов в области информационной безопасности, осуществлён комплексный анализ существующих рисков.

Наибольший риск, согласно исследованию, представляют ***«Сбои и отказы технических средств»*** (318 баллов). Данный риск обусловлен высокой степенью зависимости научно-образовательного процесса от функционирующей техники – серверов, рабочих компьютеров, сетевого оборудования и прочих компонентов IT-инфраструктуры.

Выход из строя даже одного элемента может привести к полному или частичному прекращению доступа к ключевым информационным ресурсам, что особенно критично в условиях интенсивного использования цифровых технологий в преподавании и научной деятельности.

Таким образом, стабильная работа технической базы является фундаментом бесперебойного функционирования вуза.

Таблица 1

Результаты оценки информационных рисков

| № | Вид информационной угрозы | Информационный риск, баллы | Ранг |
|---|---|---|---|
| **1.** | Сбои и отказы технических средств | 318 | 1 |
| **2.** | Ошибки IT-специалистов | 258 | 2 |
| **3.** | Сбои и отказы программных средств | 222 | 3 |
| **4.** | Сбои и отказы сетевого оборудования | 195 | 4 |
| **5.** | Вредоносное ПО | 185 | 5 |
| **6.** | Несанкционированный доступ | 128 | 6 |
| **7.** | Шпионские программы | 85 | 7 |
| **8.** | Нарушение авторских прав | 62 | 8 |
| **9.** | Аварии | 45 | 9 |
| **10.** | Пожары | 24 | 10 |
| **11.** | Другие стихийные бедствия | 17 | 11 |

На втором месте в рейтинге наиболее опасных рисков находятся ***«Ошибки IT-специалистов»*** (258 баллов). Человеческий фактор продолжает оставаться одним из самых уязвимых звеньев в системе защиты информации. Непреднамеренные действия персонала, некорректная настройка программ, несанкционированное изменение конфигураций систем, пренебрежение установленными правилами безопасности могут стать причиной серьёзных инцидентов, вплоть до утечки конфиденциальных данных или повреждения их целостности. Это подчеркивает необходимость усиления подготовки пользователей и внедрения механизмов контроля за выполнением стандартов безопасности.

Третье место занимают ***«Сбои программных средств»*** (222 балла). Проблемы, связанные с использованием устаревшего, несертифицированного или плохо совместимого программного

обеспечения, увеличивают вероятность возникновения уязвимостей, которые используются злоумышленниками для совершения кибератак.

Особое внимание следует уделить вопросам своевременного применения критических обновлений, поскольку задержки в этом процессе, вызванные бюрократическими процедурами или отсутствием централизованного управления, создают дополнительные риски.

К числу угроз, характеризующихся средним уровнем риска, относятся: ***«Сбои сетевого оборудования»*** (195 баллов). В современном образовательном пространстве, где дистанционное обучение стало неотъемлемой частью учебного процесса, надёжность сетевой инфраструктуры имеет особое значение. Потери соединения или снижение скорости передачи данных могут привести к нарушению коммуникации между обучающимися и преподавателями.

***«Вредоносное программное обеспечение»*** (185 баллов). Фишинговые атаки, использование заражённых USB-накопителей, загрузка непроверенных приложений остаются основными угрозами распространения вредоносного кода. Эти угрозы требуют постоянного улучшения антивирусных решений и повышения осведомлённости пользователей о новых опасностях.

***«Несанкционированный доступ к информации»*** (128 баллов). Опасность заключается в возможной утечке персональных данных преподавателей, сотрудников и студентов, а также другой конфиденциальной информации, связанной с научно-образовательной деятельностью и внутренним управлением вуза.

Риски, имеющие более низкий уровень опасности, также не должны игнорироваться, среди них:

***«Шпионские программы»*** (85 баллов) могут быть использованы для сбора информации о деятельности вуза, что влечёт за собой репутационный и правовой ущерб.

***«Нарушение авторских прав»*** (62 балла) представляет собой важный аспект, так как использование нелицензированных программ или контента может негативно отразиться на имидже учреждения и повлечь административную ответственность.

***«Аварии, пожары и другие стихийные бедствия»*** (оценка – от 17 до 45 баллов) имеют весьма низкую вероятность возникновения, однако последствия таких событий могут быть катастрофическими.

Необходимо поэтому разработать и регулярно корректировать планы аварийного восстановления, а также внедрить процедуры резервного копирования информации и дублирования критически важных систем.

Итак, анализ результатов, полученных экспертным путем, показал, что наиболее актуальной и значимой проблемой в сфере безопасности информационной деятельности образовательного учреждения являются технические неисправности оборудования.

Этот вид рисков занял лидирующую позицию по количеству упоминаний среди респондентов – 75%. Таким образом, ***технические сбои и отказы в аппаратной части*** представляют собой главную угрозу для надежной работы информационных систем учреждения.

На втором месте по распространенности и значимости находится ***человеческий фактор***, а именно – ошибки сотрудников при взаимодействии с информационными системами. Они занимает важное место в общей структуре рисков, поскольку неправильные действия IT-персонала приводят к существенным уязвимостям в защите данных и нарушению функционирования систем.

Третью позицию в рейтинге рисков заняли ***сбои и отказы программного обеспечения***, которые, хотя и менее часты, но все же существенно влияют на устойчивость информационных систем. Этот вид риска говорит о необходимости постоянного контроля и своевременного обновления программных продуктов для минимизации возможных уязвимостей.

В целом исследование выявило, что технические неисправности оборудования, человеческий фактор и программные сбои составляют основу угроз информационной безопасности в вузе. Тем не менее, важно учитывать и другие угрозы, указанные в табл. 1.

**Этап 2. Расчет приоритетов проектов информационной защиты**

Для достижения основной цели, ориентированной на минимизацию информационных рисков в учебном заведении, учтем данные из табл. 1. Для этого выделим четыре подцели: предотвращение технических сбоев и отказов, снижение ошибок персонала, защита от внешних угроз и утечек данных,
минимизация последствий стихийных бедствий. А затем определим проекты, ведущие к их достижению – по два на каждую подцель (рис.1).


Рис. 1. Дерево подцелей и проектов по снижению информационных рисков

Определим эффективность каждого проекта, рассчитав отдачу с единицы вложенных в него затрат, и проведем их упорядочивание в порядке убывания.

Пусть каждый $i$-ый проект характеризуется затратами $s_i$ на его реализацию и ожидаемым эффектом $w_i$. Обозначим через $m = \{1, 2, ..., M\}$ – множество проектов; $u_i$ – объем затрат. Эффективность проекта определим как частное от деления эффекта на затраты $h_i = w_i/u_i$. Положим, что затраты на проекты (в условных единицах) и эффекты от проектов имеют значения, показанные в табл. 2.

Таблица 2

Значения затрат на проекты, их эффекты и эффективность

| № проекта | Затраты на реализацию, $u_i$ | Эффект, $w_i$ | Эффективность, $h_i$ |
|---|---|---|---|
| **1** | 50 000 | 7 | 0,00014 |
| **2** | 30 000 | 5 | 0,00017 |
| **3** | 20 000 | 5 | 0,00025 |
| **4** | 55 000 | 3 | 0,000055 |
| **5** | 200 000 | 10 | 0,00005 |
| **6** | 150 000 | 7 | 0,000047 |
| **7** | 80 000 | 8 | 0,0001 |
| **8** | 55 000 | 5 | 0,000091 |

**Этап 3. Визуализация порядка выполнения проектов**

Для удобства представления графика «затраты – эффект» перестроим табл. 2 в виде табл. 3, отранжировав проекты по мере снижения показателя эффективности: на первом месте находится самый результативный проект, далее – остальные в порядке убывания показателей.

В табл. 3 представлены два

дополнительных столбца с данными о кумулятивных затратах и совокупном эффекте.

На основе информации из указанных столбцов строится график «затраты-эффект» (рис. 2), который отражает приоритет выполнения проектов, а также эффект, который может быть получен от их реализации, и какие средства, при ограничениях на них, необходимо вложить в осуществление проектов.

Таблица 3

Ранжирование проектов по эффективности

| № проекта | Затраты на реализацию, $u_i$ | Эффект, $w_i$ | Эффективность, $h_i$ | Затраты нарастающим итогом | Эффект нарастающим итогом |
|---|---|---|---|---|---|
| **3** | 20 000 | 5 | 0,00025 | 20 000 | 5 |
| **2** | 30 000 | 5 | 0,00017 | 50 000 | 10 |
| **1** | 50 000 | 7 | 0,00014 | 100 000 | 17 |
| **7** | 80 000 | 8 | 0,0001 | 180 000 | 25 |
| **5** | 55 000 | 5 | 0,000091 | 380 000 | 35 |
| **8** | 55 000 | 3 | 0,000055 | 435 000 | 40 |
| **4** | 200 000 | 10 | 0,00005 | 585 000 | 47 |
| **6** | 150 000 | 7 | 0,000047 | 640 000 | 50 |

Оценку эффективности проектов удобно представить графически, разместив по горизонтальной оси показатели затрат, а по вертикальной – величины ожидаемых эффектов.

В результате образуется набор лучей, исходящих из начала координат. При этом эффективность каждого проекта соответствует тангенсу угла наклона соответствующей прямой.

Алгоритм распределения ресурсов согласно методике «затраты-эффект» [7, 8] предполагает порядок реализации проектов в следующем виде.

Первоочередной реализации подлежит наиболее результативный, за ним – следующий по эффективности, и так далее. В рассматриваемом случае наибольшую эффективность имеет третий проект, за ним следуют второй, первый, седьмой, восьмой, четвертый, пятый и завершает список шестой проект.

На рис. 2 по горизонтальной оси графика отображаются совокупные затраты, а по вертикальной – суммарный эффект проектов.

Анализ графика позволяет определить необходимый объем средств для реализации рассматриваемых проектов по минимизации информационных рисков. С помощью данных табл. 3 и рис. 2 можно определить первостепенность, количество и порядок реализации проектов при наличии ограничений на их общий бюджет.

**Обсуждение и выводы**

На основании результатов исследования сформулируем комплекс мер, направленных на минимизацию угроз информационной безопасности образовательных учреждений. Предлагаемые решения учитывают специфику их деятельности и направлены на создание устойчивой системы защиты информации, используемой в учебном процессе и научно-исследовательской работе.

*Для снижения вероятности сбоев и отказов в работе технических средств* целесообразно внедрить систему их предупредительного обслуживания. Плановые мероприятия и мониторинг состояния аппаратных компонентов позволят выявлять потенциальные проблемы на ранних стадиях. Особое внимание следует уделить созданию резервных возможностей для критически важных систем, включая серверное оборудование и средства связи. Разработка четких алгоритмов действий при возникновении аварийных ситуаций и проведение тренировочных мероприятий для технического персонала значительно

повысят готовность к оперативному реагированию.

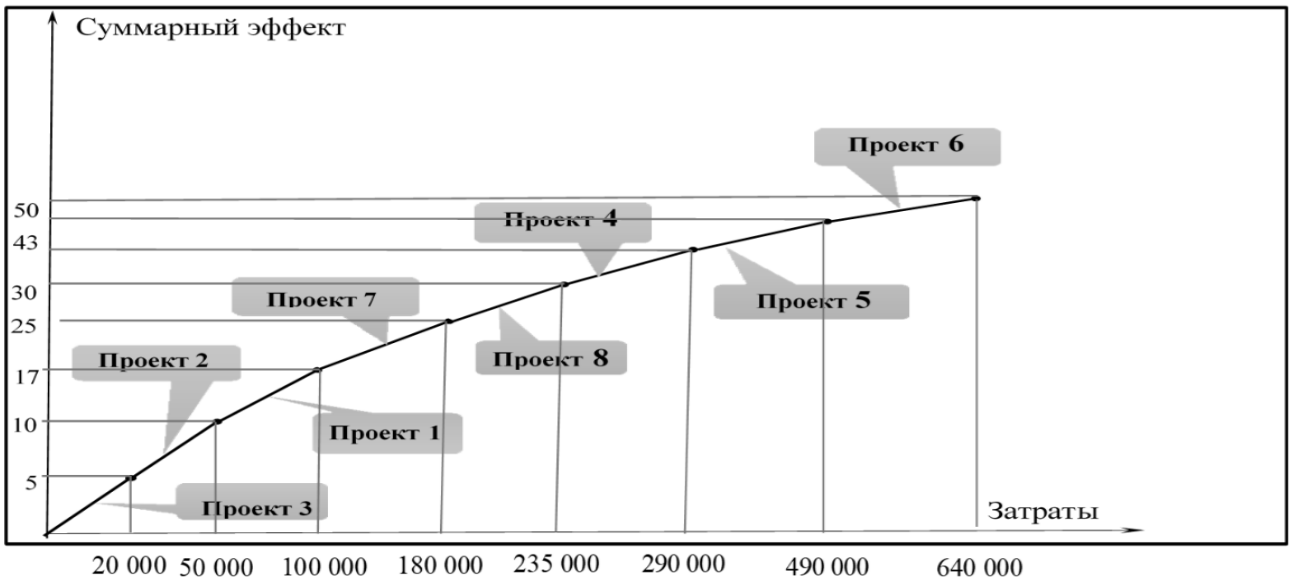



Рис. 2. График «затраты-эффект» при реализации проектов минимизации информационных рисков в образовательном учреждении

*Проблема ошибок персонала при работе с информационными системами* требует комплексного подхода для своего решения. Необходимо организовать постоянное обучение сотрудников основам кибербезопасности с акцентом на практическое применение полученных знаний. Внедрение системы контроля доступа с аутентификацией на нескольких уровнях и строгим разграничением полномочий позволит минимизировать последствия ошибок. Разработка четких инструкций и чек-листов для выполнения критически важных операций снизит вероятность человеческого фактора.

*Для защиты программного обеспечения от сбоев* рекомендуется внедрить систему управления обновлениями. Регулярный аудит программного обеспечения и своевременная установка патчей безопасности помогут устранить известные уязвимости. Следует предусмотреть механизмы проверки критически важных приложений перед их обновлением. Особое внимание необходимо уделить разработке и регулярному тестированию планов аварийного восстановления для обеспечения непрерывности учебного процесса.

*Борьба с вредоносным программным обеспечением* должна включать многоуровневую систему защиты. Помимо антивирусных решений, стоит внедрить системы анализа поведения приложений и обнаружения аномальной активности. Ограничение использования съемных носителей информации и внешних сервисов должно сопровождаться разъяснительной работой с педагогами, техническим персоналом и студентами.

*Противодействие несанкционированному доступу* требует реализации принципа минимальных необходимых привилегий. Внедрение систем мониторинга и анализа событий безопасности позволит оперативно выявлять подозрительную активность. Особое внимание следует уделить контролю доступа к помещениям с критически важным оборудованием.

*Для обеспечения устойчивости сетевой* инфраструктуры необходимо создать резервные каналы связи и дублирующие маршруты передачи данных. Регулярный аудит сетевого оборудования и своевременное обновление прошивок помогут предотвратить многие проблемы.

Разработка детальных схем аварийного переключения между основными и

резервными каналами должна сопровождаться целевыми тренировками технического персонала.

*Вопросы соблюдения авторских прав* требуют создания системы учета лицензионного программного обеспечения и учебных материалов. Внедрение специализированных решений для управления правами поможет контролировать применение защищенного контента. Регулярное обучение сотрудников и студентов основам соблюдения интеллектуальной собственности должно стать неотъемлемой частью образовательного процесса.

*Защита от стихийных бедствий и пожаров* предполагает тщательный выбор мест размещения критически важного оборудования. Использование дата-центров с системами резервного питания и климат-контроля значительно повысит устойчивость инфраструктуры. Регулярная проверка процедур резервного копирования и восстановления данных должна сопровождаться обновлением рабочих инструкций.

Реализация предложенных мер позволит создать эффективную систему безопасности, соответствующую организации работы образовательного учреждения в сфере информации. При этом важным аспектом является постоянная адаптация применяемых мер к нарастающим и изменяющимся информационным угрозам, а также к технологическим и правовым возможностям противодействия им. Системный подход к управлению информационными рисками должен стать неотъемлемой частью культуры безопасности учебного заведения.

**Заключение**

Основной смысл и главный вывод статьи заключается в том, что обеспечение информационной безопасности в образовательном учреждении – это не просто набор правил и инструкций. В первую очередь, это комплекс мер и технологий, включающий организационно-правовые, программно-аппаратные и физико-технические процедуры защиты информации учебного процесса, исследовательской и управленческой деятельности.

Важно при этом осознавать, что информационные угрозы постоянно эволюционируют, информационные риски принимают самые разнообразные формы и содержание.

Поэтому обучение и повышение квалификации преподавательского состава, IT-специалистов, технического персонала и студентов новым технологиям и системам противодействия в сфере кибербезопасности должны быть непрерывными. Таким образом, современные технологии и подходы к обучению, а также стремительный характер изменения киберугроз требуют постоянного внимания и адаптации стратегий и тактики защиты информации в образовательном учреждении.

Если исходить из мировоззренческих категорий, то информационная безопасность образовательных структур сегодня – одна из основополагающих, влияющих на качество современного образования и перспективы жизни в стране.

Как итог, внедрение передовых практик киберзащиты и методик обучения информационной безопасности всего социума образовательной организации позволит создать в ней устойчивую к угрозам систему, способную противостоять нарастающим вызовам времени.

**Список литературы**

1. Барабанов А.В., Марков А.С., Цирлов В.Л. Актуальные вопросы выявления уязвимостей и недекларированных возможностей в программном обеспечении // Системы высокой доступности. 2018. № 3. С 12-17.

2. Буйневич М.В, Покусов В.В., Израилов К.Е. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации // Информатизация и связь. 2021. № 4. С. 66-73.

3. Буйневич М.В., Израилов К.Е. Аналитическое моделирование работы программного кода с уязвимостями // Вопросы кибербезопасности. 2020. № 3(37). С. 2-12.

4. Булдакова Т.И., Миков Д.А. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечёткой модели // Наука и

образование: научное издание МГТУ им. Н.Э. Баумана. 2013. № 11. С. 295-310.

5. Малюк А.А., Минаев В.А., Сычев М.П. Образование как инструмент информационной войны // Информация и безопасность. 2019. Т. 22, № 4. С. 485-494.

6. Yu-Chih Wei, Wei-Chen Wu, Ya-Chi Chu. Performance Evaluation of the Recommendation Mechanism of Information Security Risk Identification // Neurocomputing. 2018.

7. Коробец Б.Н., Минаев В.А., Щепкин А.В. Комплексное оценивание научно-технического уровня программ вооружений, военной и специальной техники // Радиотехника. 2017. № 4. С. 149-156.

8. Коробец Б.Н., Минаев В.А., Сычев М.П., Щепкин А.В. Игровой имитационный анализ механизма оценивания научно-технических проектов с участием активных экспертов // Системы высокой доступности. 2017.-Т. 13, № 3. С. 47-54.

Московский университет МВД РФ им. В.Я. Кикотя
Moscow University of the Internal Affairs Ministry of Russia

Поступила в редакцию 7.09.25

**Информация об авторах**

**Минаев Владимир Александрович,** д-р техн. наук, профессор, профессор кафедры специальных информационных технологий, Московский университет МВД РФ им. В.Я. Кикотя, Москва, e-mail: m1va@yandex.ru

**Эрдниев Александр Сергеевич**, кандидат пед. наук, доцент, начальник Учебно-научного комплекса информационных технологий, Московский университет МВД РФ им. В.Я. Кикотя, Москва, e-mail: konfuci@inbox.ru

## INFORMATION RISK MANAGEMENT OF EDUCATIONAL INSTITUTIONS: METHODOLOGY AND RESULTS

**V.A. Minaev, A.S. Erdniev**

The article examines the state of information security in educational institutions of the Russian Federation, which have their own specifics in the field of protecting information resources of the educational process and research activities. It is shown that the massive, not always clear control of computer equipment and information systems in an educational institution leads to a special manifestation of information risks that require special methods for their assessment and management. The results of expert procedures indicate that the rating of the most dangerous risks includes failures of technical means, errors by information technology specialists, failures of software, failures of network equipment, malicious software, unauthorized access to information. The degree of danger of risks is estimated based on the value of the product of the probability of the threat being realized by the value of possible damage. In total, eleven types of information threats were considered, evaluated by experts, who were represented by about 100 respondents (teachers, technical staff, senior students). To manage information risks, the cost-effect methodology was used, developed and adapted at the V. A. Trapeznikov Institute of Management Problems of the Russian Academy of Sciences. The methodology allowed us to streamline information risk minimization projects in an educational institution based on their effectiveness. The article concludes with a list of measures to implement each of the eight proposed projects.

Keywords: educational institution, information risk, optimization, expert assessment, cost-effect project, efficiency.

Submitted 7.09.25

**Information about the authors**

**Vladimir A. Minaev** – Doctor Sc. (Technical), Professor, Professor of the Special Information Technologies Department, V.Ya. Kikot Moscow University of the Internal Affairs Ministry, Moscow, e-mail: m1va@yandex.ru

**Alexander S. Erdniev**, Candidate Sc.(Pedagogical), Associate Professor, Head of the Educational and Scientific Complex of Information Technologies, V.Ya. Kikot Moscow University of the Internal Affairs Ministry, Moscow, e-mail: konfuci@inbox.ru

## ПРАВИЛА

### оформления и представления рукописей для публикации в журнале «Информация и безопасность»

В целях улучшения качества оформления настоящего издания редколлегия просит авторов направляемых материалов руководствоваться следующими правилами оформления:

1. Рукопись общим объемом не менее 8 и не более 20 **полных** страниц (четное число страниц) для научной статьи (тезисов пленарного доклада), 4 **полных** страницы для статьи (тезисов доклада) представляют в отпечатанном виде на одной стороне листа формата А4 шрифтом Times New Roman Cyr 12 пунктов через 1 интервал и отправляют на почту журнала alexanderostapenkoias@gmail.com (в формате docx).
2. Страницы рукописи должны иметь следующие размеры полей: верхнее - 2 см, нижнее -2, левое- 2 см, правое-2 см.

   На первой странице текста располагают DOI (номер заполняется в редакции), следующей строкой УДК (в левом углу листа от поля, размер шрифта 12), название статьи (заглавными буквами, размер шрифта 12), инициалы и фамилию автора (авторов) (размер шрифта 12), аннотацию (100-150 слов) и ключевые слова (от трех до пяти слов или словосочетаний). Для аннотации и ключевых слов размер шрифта 10, отступы слева и справа – 1,25 см, абзацный отступ – 0,8 см. На первой странице в левом столбце внизу сноской знак охраны авторского права (©), авторы (инициалы после фамилий); год; фамилии иностранных авторов пишутся на русском языке. Далее следуют текст рукописи (размер шрифта 12) и список литературы (размер шрифта 12). Текст рукописи и список литературы представляют на листе в две колонки шириной по 8,25 см каждая (межколоночное расстояние 0,5 см).
3. Абзацный отступ, равный 0,8 см, должен начинаться после ввода (автоматически**). Не допускается формирование абзацного отступа при помощи пробелов и табуляции!**
4. **Обе колонки текста должны быть заполнены равномерно и полностью!**
5. **Номера страниц не проставляются!**
6. Сведения об авторах приводятся после списка литературы на русском и английском языках. Сначала полное название учреждений, в которых выполнялось исследование, с указанием, в каком из учреждений работает каждый из авторов, указываются традиционные названия академических и учебных институтов без характеристик формы учреждения, далее страна для иностранных авторов (размер шрифта 12) на русском и английском языках. Далее информация об авторах 10 шрифтом на русском языке: фамилия, имя, отчество (если есть) полностью, через тире ученая степень, должность, название учреждения (места работы), e-mail. Название статьи на английском языке (размер шрифта 12), инициалы и фамилии авторов на англиском языке (размер шрифта 12), аннотация и ключевые слова на английском языке (размер шрифта 10), информация об авторах на английском языке (форматирование такое же, как на русском)
7. Используемые в работе термины, единицы измерения и условные обозначения должны быть общепринятыми. Все употребляемые авторами обозначения (за исключением общеизвестных констант) и аббревиатуры должны быть определены при их первом упоминании в тексте.
8. Таблицы располагают по тексту. Каждый элемент таблицы должен представлять собой отдельную ячейку. **Не допускается размещать колонку или строку с данными в одной ячейке!** Если в рукописи одна таблица, то слово “Таблица” в названии не пишут. Если в статье несколько таблиц, то перед названием таблицы справа пишут “Таблица 1 (2, 3 и т.д.)”. Ссылку на таблицу оформляют следующим образом: “табл. 1 (2, 3 и т.д.)”. Заголовок таблицы располагают следующей строкой после слова «Таблица», по центру.

9. Оформление рисунков осуществляется в формате png. Подрисуночные подписи не входят в состав рисунков, а располагаются отдельным текстом с размером шрифта 10 под рисунками. Буквы и цифры на рисунке должны быть разборчивы. Тоновые фотографии представляют в двух экземплярах на белой матовой фотобумаге, пояснительные надписи на одной из этих фотографий должны отсутствовать. Если в рукописи несколько рисунков, то перед названием пишут “Рис. 1 (2, 3 и т.д.)”. Ссылка на рисунок оформляется следующим образом “рис. 1 (2, 3 и т.д.)”. Если в статье один рисунок, то слово “Рис.” в подрисуночной подписи не пишут. **Рисунки должны четко воспроизводиться при черно-белой печати!**
10. Формулы нумеруют в круглых скобках (2), по правой границе текста, литературные ссылки - в прямых [2], подстрочные примечания - арабскими цифрами.

***Пример оформления текста:***

Если приходит следующий ($J_{lim}$+1)-й пакет с запросом на соединение, то этот пакет отбрасывается.

Если атака обнаруживается до этого момента времени с некоторой вероятностью $P_{det}$ и ее развитие блокируется, то вероятность реализации атаки может быть рассчитана по формуле:

$$P_u(t) = 1 - \frac{\lambda_{syn} \cdot \bar{\tau}_u \cdot e^{-\frac{(t-t_0)\cdot(1-P_{\det})}{\bar{\tau}_u}}}{\lambda_{syn} \cdot \bar{\tau}_u - (1-P_{\det})} + \frac{(1-P_{\det}) \cdot e^{-\lambda_{syn}\cdot(t-t_0)\cdot}}{1-\bar{\tau}_u \cdot \lambda_{syn} \cdot (1-P_{\det})}, \quad (3)$$

где $P_{det}$ – вероятность обнаружения атаки;

$t_0$ – время ожидания подтверждения сеанса связи.

Рассмотрим модель динамики реализации атаки – шторм ICMP – "эхо-ответов" (Smurf) [3]. Суть атаки заключается в посылке "эхо-запроса" по протоколу ICMP по широковещательному адресу с указанием в качестве адреса отправителя IP-адреса компьютера – цели атаки, ответить на которые может множество компьютеров.

**Библиографические ссылки** даются по следующим образцам (ГОСТ Р 7.05-2008 СИБИД):

- Для учебников, учебных пособий и т.п.:
  1. История России : учеб. пособие для студентов всех специальностей / В. Н. Быков [и др.] ; отв. ред. В. Н. Сухов ; М-во образования Рос. Федерации, С.-Петерб. гос. лесотехн. акад. 2-е изд., перераб. и доп. / при участии Т. А. Суховой. СПб. : СПбЛТА, 2001. 231 с.
- Для законодательных актов, стандартов, правил:
  1. О противодействии терроризму: Федер. закон Рос. Федерации от 6 марта 2006 г. N 35-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 26 февр. 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 1 марта 2006 г. // Рос. газ. 2006. 10 марта.
  2. Федеральный закон № 149-ФЗ от 37.07.2006 «Об информации, информационных технологиях и защите информации». URL: http://www.kremlin.ru/acts/bank/ 24157 (дата обращения 18.08.2021).
  3. ГОСТ 7.25-2001 СИБИД. Тезаурус информационно-поисковый одноязычный. Правила разработки, структура, состав и форма представления. М.: Стандартинформ, 2002. 16 с.
- Для книг – фамилия, инициалы автора; название книги; инициалы, фамилия автора; место издания; наименование издательства; год издания; номер тома; объем. Если авторов более одного и менее четырех - фамилия, инициалы первого автора; название книги; инициалы, фамилия всех авторов (включая первого); место издания; наименование издательства, год издания; номер тома; объем. Примеры:
  1. Шульце Г. Металлофизика / Г. Шульце. М.: Мир, 1971. 503 с.
  2. Ландау Л.Д. Квантовая механика / Л.Д. Ландау, Е.М. Лифшиц. М.: Физматгиз, 1963. 25 с.

- Для статей в сборнике (журнале) – фамилия, инициалы автора; название статьи; инициалы, фамилия автора; название сборника, серии; год издания; том издания; номер издания; объем. Если авторов двое или трое – фамилия, инициалы первого автора; название статьи; инициалы, фамилия каждого автора (включая первого); название сборника, серии; год издания; том издания; номер издания; объем. Если авторов более трех: фамилия первого автора, название статьи; инициалы, фамилии авторов, можно сократить список фамилий: [и др.]; название сборника; место издания, название издательства; год издания; номер тома; объем. Примеры:
  1. Кузнецов, В.Ю. Немонотонный потенциал в обогащенных слоях / В.Ю. Кузнецов // Изв. вузов. Сер. Химия (или Сер. физ.). 1989. Т. 43, № 5. С. 106-111.
  2. Леготин Е.Ю. Организация метаданных в хранилище данных // Научный поиск. Технические науки: Материалы 3-й науч. конф. аспирантов и докторантов / отв. за вып. С.Д.Ваулин; Юж.-Урал. гос. ун-т. Т.2. Челябинск: Издательский центр ЮУрГУ, 2011. - С.128-132.
- Для авторефератов и диссертаций – фамилия, инициалы автора; название работы; название вида работы; название ученой степени; место написания; год написания; объем. Примеры:
  1. Недорезов, С.С. Особенности зарождения и структура пленок некоторых металлов при конденсации из ионного потока // Автореф. дис. … д-ра физ.-мат. наук/ ФТИНТ. - Харьков, 1985. - 16 с.
- Для авторских свидетельств и патентов – вид документа; его номер; название страны; индекс МКИ; название работы; инициалы и фамилия(и) автора(ов); регистрационный номер заявки; дата подачи заявки; дата публикации; издание, в котором опубликован документ; объем. Примеры:
  1. Пат. 2187888 Российская Федерация, МПК H 04 B 1/38, H 04 J 13/00. Приемопередающее устройство [Текст] / Чугаева В. И. ; заявитель и патентообладатель Воронеж. науч.-исслед. ин-т связи. - N 2000131736/09 ; заявл. 18.12.00 ; опубл. 20.08.02, Бюл. N 23 (II ч.). - 3 с. : ил.
  2. Заявка 1095735 Российская Федерация, МПК B 64 G 1/00. Одноразовая ракета-носитель [Текст] / Тернер Э. В. (США) ; заявитель Спейс Системз/Лорал, инк. ; пат. поверенный Егорова Г. Б. - N 2000108705/28 ; заявл. 07.04.00 ; опубл. 10.03.01, Бюл. N 7 (I ч.) ; приоритет 09.04.99, N 09/289,037 (США). - 5 с. : ил.
- Для электронных ресурсов обязательно указывать дату обращения, причем дата должна быть как можно более поздней. Примеры:
  1. Члиянц Г. Создание телевидения // QRZ.RU: сервер радиолюбителей России. 2004. URL: http://www.qrz.ru/articles/article260.html (дата обращения: 21.09.2019).

### *Общие требования*

Для публикации материалов в журнале авторам необходимо представить в редакцию:

- *электронную версию статьи;*
- *рецензию внешнего ведущего специалиста в области излагаемого материала;*
- *экспертное заключение о возможности ее публикации в открытой печати, заверенное руководителем организации или его заместителем и печатью;*
- *сведения об авторах, включающие фамилию, имя, отчество, дату рождения, место работы и должность, ученую степень и звание, контактный телефон, почтовый (с индексом) и электронный адрес для переписки.*

Редакционная коллегия оставляет за собой право осуществлять дополнительное рецензирование и техническое редактирование представленных работ.

Научное издание

ИНФОРМАЦИЯ И БЕЗОПАСНОСТЬ

Том 28. Выпуск 3. 2025

Главный редактор А.Г. Остапенко
Компьютерная верстка Е.А. Москалевой, А.С. Кривошеина

Дата выхода в свет 31.10.2025
Формат 60х84/8. Бумага писчая.
Усл. печ. л. 16,6
Тираж 44 экз. Заказ № 248
Цена свободная

ФГБОУ ВО «Воронежский государственный технический университет»
394006, г. Воронеж, ул. 20-летия Октября, 84

Отпечатано: отдел оперативной полиграфии издательства ВГТУ
394006, г. Воронеж, ул. 20-летия Октября, 84