

Теоретические основы информационной безопасности

Обзорная статья

DOI 10.66424/2071-8217-2026-3-1

УДК 004.056

СИСТЕМАТИЗАЦИЯ ОТКРЫТЫХ МЕХАНИЗМОВ ЗАЩИТЫ АГЕНТНЫХ СИСТЕМ НА ОСНОВЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ И АНАЛИЗ ПОКРЫТИЯ ЛАНДШАФТА УГРОЗ

А. С. Истомина^{1*}, А. А. Яковлев²

¹Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Россия

²АО «Позитив Текнолоджиз», Москва, Россия

✉ *isto.anastasiya@gmail.com

ДЛЯ ЦИТИРОВАНИЯ

Истомина А. С., Яковлев А. А.
Систематизация открытых
механизмов защиты агентных
систем на основе больших языковых
моделей и анализ покрытия
ландшафта угроз // Проблемы
информационной безопасности.
Компьютерные системы.
2026. № 3. С. 9–24.
DOI: 10.66424/2071-8217-2026-3-1

ПОСТУПИЛА 04.06.2026

ПРИНЯТА 18.08.2026

ОПУБЛИКОВАНА 13.10.2026

© Истомина А. С., Яковлев А. А.

Издатель: Санкт-Петербургский
политехнический университет
Петра Великого

АННОТАЦИЯ

Средства защиты агентных систем на основе больших языковых моделей развиваются разрозненно. Они существуют как отдельные проекты с открытым исходным кодом, коммерческие продукты и научные публикации, а общего представления о полноте перекрытия ими актуальных классов угроз нет. Цель работы – систематизировать механизмы защиты агентных систем и оценить полноту перекрытия ими ландшафта угроз. Результатом систематизации стала двухосевая классификация, в которой каждый механизм характеризуется архитектурным уровнем применения и характером воздействия. По единой схеме описаны 46 механизмов, отобранных из каталога 118 репозиторий. Построена количественная карта перекрытия угроз и механизмов относительно перечней OWASP Top 10 for Agentic Applications 2026 и OWASP Top 10 for Large Language Model Applications 2025. Введен показатель эшелонирования защиты. Совокупность механизмов перекрывает все 10 классов агентных угроз, но глубина перекрытия распределена неравномерно. Выявлены типовые заблуждения при выборе средств защиты и предложен минимальный набор защит для проектирования агентных систем.

КЛЮЧЕВЫЕ СЛОВА

Агентные системы, большие языковые модели, механизмы защиты, ландшафт угроз, OWASP, инъекция запроса, карта перекрытия угроз

Review article

DOI 10.66424/2071-8217-2026-3-1

SYSTEMATIZATION OF OPEN PROTECTION MECHANISMS FOR AGENT SYSTEMS BASED ON LARGE LANGUAGE MODELS AND ANALYSIS OF THREAT LANDSCAPE COVERAGE

A. S. Istomina^{1*}, A. A. Iakovlev²

¹Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia

²JSC “Positive Technologies”, Moscow, Russia

✉ *isto.anastasiya@gmail.com

FOR CITATION

Istomina A. S.,
Iakovlev A. A. Systematization
of open protection mechanisms
for agent systems based on large
language models and analysis of
threat landscape coverage. *Problems of
information security. Computer systems.*
2026. No. 3, pp. 9–24.
DOI: 10.66424/2071-8217-2026-3-1
(In Russian)

RECEIVED 04.06.2026

ACCEPTED 18.08.2026

PUBLICATION 13.10.2026

ABSTRACT

Protection tools for agent systems based on large language models develop in a fragmented way. They exist as separate open-source projects, commercial products, and research publications, and there is no unified view of how completely they cover current threat classes. This work systematizes the protection mechanisms of agent systems and assesses how completely they cover the threat landscape. A two-axis classification is proposed, in which each mechanism is characterized by its architectural level of application and its nature of impact. Following a unified scheme, 46 mechanisms selected from a catalog of 118 repositories are described. A quantitative coverage map of threats and mechanisms is built against the OWASP Top 10 for Agentic Applications 2026 and the OWASP Top 10 for Large Language Model Applications 2025. A defense-in-depth indicator is introduced. The set of mechanisms covers all 10 classes of agentic threats, but coverage depth is distributed unevenly. “Tool misuse” is covered most fully, while “memory poisoning”, “insecure inter agent communication”, and “compromised agents” remain structural gaps without a mature preventive tool. Typical misconceptions in selecting protection tools are identified, and a minimal set of protections for designing agent systems is proposed.

KEYWORDS

Agent systems, large language models, protection mechanisms, threat landscape, OWASP, prompt injection, threat coverage map

1. ВВЕДЕНИЕ

Агентная система – это программа, которая принимает задачу, планирует шаги, вызывает внешние инструменты и проверяет результат. Большая языковая модель служит в такой системе компонентом принятия решений, а сама система получает доступ к инструментам, коду, сети, долговременной памяти и поисковым индексам. В расширенных конфигурациях работа распределяется между несколькими агентами. При росте самостоятельности агентов расширяется поверхность атаки. Успешное воздействие приводит к нежелательному действию во внешней системе, а вредоносные данные, попавшие в память или поисковый индекс, влияют на решение агента в последующих сессиях. Поэтому защита агентных систем требует иных мер, чем защита изолированной языковой модели.

Средства защиты агентных систем развиваются разрозненно и существуют в виде отдельных программных проектов с открытым исходным кодом, коммерческих продуктов и научных публи-

каций. Каждое средство создается под конкретную угрозу или архитектуру, а общего представления о том, в какой мере их совокупность перекрывает актуальные классы угроз, не сформировано. В итоге не установлено, какие угрозы перекрыты избыточно несколькими сильными средствами, а какие содержат структурные пробелы и не устраняются ни одним из зрелых средств.

Цель работы – систематизировать механизмы защиты агентных систем на основе больших языковых моделей и оценить, в какой мере их совокупность перекрывает актуальный ландшафт угроз. Для этого необходимо решить следующие задачи:

- выработать основания классификации механизмов защиты;
- описать по единой схеме репрезентативный набор из открытых проектов, продуктов и публикаций;
- построить карту перекрытия «угроза – механизм» с количественным показателем глубины защиты;
- выявить структурные пробелы в перекрытии угроз и типовые ошибки при выборе средств;

- предложить минимальный эшелонированный набор средств защиты.

Исследование ставит целью получить ответы на следующие вопросы исследования:

1. На каких основаниях целесообразно систематизировать механизмы защиты агентных систем?

2. В какой мере совокупность известных механизмов перекрывает классы угроз OWASP Top 10 for Agentic Application 2026 [1] и OWASP Top 10 for Large Language Model Applications (2025) [2]?

3. Где расположены пробелы в перекрытии угроз, и какие средства защиты систематически переоцениваются либо недооцениваются?

Научная новизна работы состоит в следующем: предложена двухосевая классификация механизмов защиты, в которой каждое средство характеризуется архитектурным уровнем применения и характером воздействия. Построена количественная карта перекрытия «угроза – механизм» с показателем эшелонирования защиты, т.е. числом независимых сильных средств, перекрывающих каждую угрозу. Выявлены и обоснованы структурные пробелы в перекрытии угроз, а также типовые заблуждения при выборе средств защиты, когда одни систематически переоцениваются, а другие недооцениваются.

Практическая значимость работы состоит в том, что карта перекрытия и показатель эшелонирования позволяют обоснованно выбирать средства защиты при проектировании агентных систем, а предложенный минимальный набор задает отправную точку для построения эшелонированной защиты с учетом соотношения результативности и стоимости внедрения.

Работа рассматривает механизмы защиты, действующие во время исполнения агента. К ним относятся контроль входа и выхода модели, вызова инструментов, состояния и инфраструктуры исполнения. Средства уровня самой модели, относящиеся к этапам обучения, дообучения и выравнивания, вынесены за рамки работы, потому что они изменяют поведение модели до развертывания и не образуют барьера на этапе исполнения.

Ландшафт угроз ограничен перечнями OWASP Top 10 for Agentic Application 2026 [1] и OWASP Top 10 for Large Language Model Applications (2025) [2]. Они выбраны как стандарты, которые поддерживаются профильным сообществом, регулярно пересматриваются и совместно покрывают оба уровня системы, модель и агента. Элементы перечней разнородны по своей природе, поэтому в работе они трактуются единообразно как классы угроз, т.е. совокупность сценариев, в которых соответствующий риск реализуется нежелательным событием для агентной системы.

2. АГЕНТНЫЕ СИСТЕМЫ НА ОСНОВЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ И МОДЕЛЬ УГРОЗ

Под агентной системой на основе большой языковой модели понимается программный комплекс, в котором языковая модель не только порождает текст, но и управляет циклом действий: воспринимает вход, строит план, выбирает и вызывает внешние инструменты, наблюдает результат и повторяет цикл до достижения цели. От изолированной языковой модели такую систему отличают три свойства:

- система обладает набором инструментов (функций, обращений к API, исполнителей кода), через которые воздействует на внешние системы;

- система опирается на сохраняемое состояние [11] (рабочую память диалога, долговременную память, поисковый индекс), которое влияет на последующее решение;

- система способна действовать самостоятельно, т.е. принимать решения о вызове инструментов без пошагового участия человека. В расширенных конфигурациях несколько агентов и оркестратор распределяет задачи между агентами-исполнителями, обмениваясь с ними сообщениями по протоколу межагентного взаимодействия.

Успешной атакой при наличии инструментов считается действие во внешней системе. Это может быть отправка данных,

изменение записей или исполнение кода. Использование состояния означает, что вредоносные данные, однажды попавшие в память или поисковый индекс, влияют на решения агента в будущих сессиях без новой инъекции. Из-за самостоятельности действий между поступлением вредоносного входа и необратимым действием может не быть точки, в которой человек успел бы вмешаться. В многоагентных конфигурациях добавляется поверхность межагентного обмена, где подмененное или внедренное сообщение распространяется по цепочке агентов. Поэтому защита агентной системы должна охватывать, помимо фильтрации входа и выхода модели, вызов инструментов, состояние агента, инфраструктуру исполнения и межагентное взаимодействие.

Для систематизации угроз принят перечень OWASP Top 10 for Agentic Application 2026 (ASI) [1] с 10 классами угроз, специфичных для агентов:

1. ASI01 Захват цели агента [12] – подмена цели, плана или приоритетов прямой или косвенной инъекцией инструкций. Агент действует выданными инструментами, но преследует чужую задачу.

2. ASI02 Злоупотребление инструментами – использование легитимных инструментов не по назначению: одиночный опасный вызов, токсичная цепочка вызовов, подделка запроса к внутреннему сервису. Интерфейс не взламывается – модель сама выбирает вредное действие в пределах прав.

3. ASI03 Злоупотребление идентичностью и привилегиями – эксплуатация делегированных агенту учетных данных и ролей для действий с большими правами, чем требует задача.

4. ASI04 Уязвимости цепочки поставок [13] – скомпрометированный или подмененный сторонний артефакт (навык, сервер протокола инструментов, плагин, пакет, конвейер сборки) меняет поведение агента после установки или обновления.

5. ASI05 Неожиданное исполнение кода – прохождение и запуск кода вне границ изолированной среды, ведущие к компрометации хоста.

6. ASI06 Отравление памяти и контекста [3] – вредоносные данные в долговременной памяти, поисковом индексе или длинном диалоге влияют на решения агента без новой явной инъекции.

7. ASI07 Небезопасная связь между агентами – отсутствие аутентификации, подписи и ограничения доверия в межагентном обмене, позволяющее подменять и внедрять сообщения.

8. ASI08 Каскадные сбои – распространение ошибки или атаки из одного звена многошагового процесса по цепочке нижележащих систем.

9. ASI09 Эксплуатация доверия человека к агенту [10] – агент убедительно обосновывает опасное действие или подделывает официальный контекст, и оператор одобряет то, чего сам бы не сделал.

10. ASI10 Скомпрометированные агенты – устойчивое отклонение агента от целей вследствие компрометации, дрейфа политики или сговора агентов, когда контроль на входе уже неэффективен.

Перечень ASI дополнен перечнем OWASP Top 10 for Large Language Model Applications (2025) (далее LLM) [2], где собраны угрозы уровня самой языковой модели, сохраняющиеся и в агентном применении:

1. LLM01 Инъекция запроса [12] – изменение поведения модели недоверенным вводом (прямым в диалоге или косвенным через документ, письмо, веб-страницу).

2. LLM02 Раскрытие конфиденциальной информации – выдача моделью персональных данных, секретов, фрагментов контекста или обучающей выборки.

3. LLM03 Уязвимости цепочки поставок модели – компрометация зависимостей модели (веса, наборы данных, пакеты).

4. LLM04 Отравление данных и модели – внедрение вредоносных примеров на этапах обучения, закрепляющее нежелательное поведение.

5. LLM05 Неправильная обработка вывода – передача ответа модели в нижележащие системы без проверки, при которой текст интерпретируется как код или разметка.

6. LLM06 Избыточная автономия – чрезмерные полномочия без пошагового

контроля; у агентов раскрывается в классах ASI02, ASI03, ASI05, ASI10.

7. LLM07 Утечка системного запроса – раскрытие скрытых инструкций, политик и внутренних имен инструментов, упрощающее последующие атаки.

8. LLM08 Слабости векторов и эмбедингов – атаки на векторное хранилище и поиск: отравление эмбедингов, составительные фрагменты, манипуляция поиском по близости.

9. LLM09 Дезинформация – правдоподобные ложные утверждения с высокой уверенностью, включая галлюцинации как проблему качества модели.

10. LLM10 Неограниченное потребление ресурсов [15] – неконтролируемый расход запросов, токенов и вызовов, ведущий к отказу в обслуживании и финансовым потерям.

Два перечня описывают одну систему на разных уровнях и используются в работе совместно. LLM фиксирует угрозы уровня модели, ASI их продолжение на уровне агента. Часть классов связана напрямую. Инъекция запроса (LLM01) служит основным механизмом захвата цели агента (ASI01). Избыточная автономия (LLM06) у агентов раскрывается в классах ASI02, ASI03, ASI05 и ASI10. Цепочка поставок присутствует в обоих перечнях с разными объектами. LLM03 охватывает зависимости модели, ASI04 – компоненты агента (от навыков до конвейеров сборки). Отравление памяти и контекста (ASI06) опирается на слабости уровня модели из LLM04 и LLM08, закрепление вредоносных данных в индексе и атаки на векторное хранилище. Классы ASI07-ASI09 порождены многоагентностью и участием человека-оператора. Прямых аналогов на уровне модели не имеют.

3. СИСТЕМАТИЗАЦИЯ МЕХАНИЗМОВ ЗАЩИТЫ

Механизмы защиты систематизированы по двум независимым признакам, совместно образующим сводный перечень (табл. 1). Каждая строка описывает один

механизм и указывает его архитектурный уровень, характер воздействия и перечень перекрываемых классов угроз OWASP.

Первый признак – архитектурный уровень, на котором механизм включается в работу агента:

- «текст/входные данные» – обработка запроса пользователя, ответа модели и содержимого от внешних источников до того, как оно повлияет на решения агента;
- «действие/инструменты» – контроль вызова инструментов (состав аргументов, допустимость операции, последовательность вызовов, объем полномочий);
- «сеть и инфраструктура» – ограничение исходящих обращений и изоляция среды исполнения;
- «цепочка поставок и код» – проверка описаний инструментов, зависимостей и исходного кода до подключения;
- «подлинность и аудит» – идентификация агента, фиксация действий и разбор инцидентов;
- «измерение» – оценка качества средств защиты.

Второй признак – характер воздействия, отражающий роль механизма в жизненном цикле инцидента:

- предупреждающий не допускает нежелательное действие до его совершения (проверка аргументов, политики на вызовы, изоляция среды);
- выявляющий обнаруживает признак атаки, но сам действие не блокирует (классификаторы вредоносных инструкций, выявление секретов, анализ потоков данных);
- реагирующий прерывает или ограничивает уже начавшийся инцидент (аварийное отключение, отзыв артефактов);
- поддерживающий не образует самостоятельного барьера, но повышает результативность других средств (нормализация Unicode, инвентаризация компонентов);
- аудит обеспечивает разбор действий после события (неизменяемый журнал, телеметрия);
- измерительный оценивает результативность самих средств защиты и не действует во время исполнения (регрессионные испытания, эталонные наборы).

Таблица 1 | Сводный перечень механизмов защиты агентных систем**Table 1** | Summary list of protection mechanisms for agent systems

№	Механизм	Уровень	Воздействие	Перекрывает
1	Классификация инъекций и обхода ограничений с помощью машинного обучения	Текст	Выявл.	ASI01, ASI06, LLM01, LLM05
2	Аудит цепочки рассуждений моделью-судьей (CoT-аудит) [5]	Текст	Выявл.	ASI01, LLM01, ASI02
3	Правила и шаблоны для выявления инъекций	Текст	Выявл.	ASI01, LLM01
4	Нормализация Unicode	Текст	Поддерж.	LLM01
5	Выявление и маскирование персональных данных	Текст	Выявл.	LLM02
6	Инспекция контента на утечки данных (DLP) [6]	Текст	Выявл.	LLM02, LLM05, ASI03
7	Выявление секретов в тексте	Текст	Выявл.	LLM02
8	Фильтры токсичности и модерация контента	Текст	Выявл.	LLM05
9	Проверка фактической точности и выявление вымышленных утверждений	Текст	Выявл.	ASI09, LLM05, LLM09
10	Валидация структуры ответа по JSON-схеме	Текст	Предупр.	LLM05
11	Ограничение расхода токенов, средств и частоты вызовов	Действие	Предупр.	ASI02, ASI08, LLM10
12	Политики доступа к инструментам	Действие	Предупр.	ASI02, ASI03, LLM06
13	Проверка аргументов по JSON-схеме и строгим типам	Действие	Предупр.	ASI02, LLM06, LLM07
14	Запрет по умолчанию и белые списки	Действие	Предупр.	ASI02, ASI03, LLM06
15	Правила последовательности вызовов и потоков данных	Действие	Предупр.	ASI01, ASI06, ASI07, ASI08, LLM01, LLM06
16	Разметка полномочий и контроль потоков данных (capability/IFC/taint)	Действие	Предупр.	LLM01, LLM02, LLM06, ASI01, ASI02
17	Формальная проверка политик и только сужающихся привилегий [7]	Действие	Предупр.	ASI02, ASI03, ASI08, ASI10, LLM06
18	Разграничение доступа на основе отношений (ReBAC, SpiceDB)	Действие	Предупр.	ASI03, ASI02
19	Правила против инъекций в аргументах инструментов	Действие	Предупр.	ASI02, ASI09
20	Отбрасывание призрачных аргументов и строгая типизация	Действие	Предупр.	LLM05, ASI02
21	Одобрение опасных действий человеком	Действие	Предупр.	ASI02, ASI03, ASI08, ASI09, LLM06
22	Аварийное отключение агента (kill switch/circuit breaker)	Действие	Реагир.	ASI08, ASI10
42	Диалоговые ограничители (rails, Colang)	Действие	Предупр.	ASI09, ASI01
43	Две модели с разделением доверия и карантин [8]	Действие	Предупр.	ASI01, ASI02, ASI03, ASI06, ASI07, ASI08, ASI09, LLM01, LLM02, LLM06
23	Единый прокси исходящих запросов и защита от SSRF	Сеть/инфр.	Предупр.	ASI02, ASI08, LLM02, LLM10

Конец таблицы 1**End of table 1**

№	Механизм	Уровень	Воздействие	Перекрывает
24	Шлюз инструментов MCP/LLM с ролевым доступом (RBAC)	Сеть/инфр.	Предупр.	ASI03, ASI07
33	Изоляция агента в микровиртуальных машинах и контейнерах	Сеть/инфр.	Предупр.	ASI02, ASI03, ASI05, ASI08, LLM10
34	Песочница на уровне операционной системы (OpenShell)	Сеть/инфр.	Предупр.	ASI05, ASI02, ASI08
35	Уровни исполнения и изоляция рабочего каталога	Сеть/инфр.	Предупр.	ASI02, ASI03, ASI05, LLM06
25	Контроль целостности описаний инструментов по контрольной сумме	Цепочка поставок	Предупр.	ASI04, LLM03, LLM04
26	Проверка на отравление и подмену инструментов (tool poisoning/shadowing)	Цепочка поставок	Выявл.	ASI04, LLM03, LLM01
27	Статическая проверка навыков и плагинов	Цепочка поставок	Выявл.	ASI01, ASI04, ASI06, LLM02, LLM03, LLM04, LLM06
28	Анализ опасных потоков данных (toxic flow/dataflow)	Цепочка поставок	Выявл.	ASI01, ASI02, LLM02
29	Проверка зависимостей, конвейера сборки (CI) и сценариев установки	Цепочка поставок	Предупр.	ASI04, LLM03, LLM04
30	Статический анализ кода	Цепочка поставок	Выявл.	ASI05, LLM05, ASI04
31	Допуск артефактов при установке и отзыв по черному списку	Цепочка поставок	Реагир.	ASI04, ASI10, LLM03, LLM04
32	Инвентаризация ИИ-компонентов (AIBOM)	Цепочка поставок	Поддерж.	ASI04
36	Криптографическая идентичность агента и доверие между агентами (A2A)	Подлинность/аудит	Предупр.	ASI07, ASI03, ASI10
37	Выявление поведенческих отклонений по базовому профилю [4]	Подлинность/аудит	Выявл.	ASI02, ASI08, ASI10, LLM06
38	Атрибуция действий к навыкам агента	Подлинность/аудит	Выявл.	ASI04, ASI10
39	Неизменяемый журнал с цепочкой хешей и подписями	Подлинность/аудит	Аудит	ASI10
40	Сбор телеметрии и передача событий в SIEM (OpenTelemetry) [14]	Подлинность/аудит	Аудит	ASI08, ASI10
41	Сопоставление защит с требованиями стандартов и регуляторов	Подлинность/аудит	Поддерж.	—
46	Защита памяти агента	Подлинность/аудит	Предупр.	ASI06, LLM04
44	Пробы красной команды и регрессионное тестирование защит	Измерение	Измер.	—
45	AgentDojo [9] как эталонный набор испытаний защит	Измерение	Измер.	ASI01, ASI02, ASI03, ASI04, ASI05, ASI06, ASI07, ASI08, ASI09, ASI10, LLM01, LLM02, LLM03, LLM04, LLM05, LLM06, LLM07, LLM08, LLM09, LLM10

Всего систематизировано 46 механизмов, неравномерно распределенных по уровням: «текст/входные данные» – 10, «действие/инструменты» – 14, «сеть и инфраструктура» – 5, «цепочка поставок и код» – 8, «подлинность и аудит» – 7, «измерение» – 2.

На рис. 1 представлена тепловая карта распределения 46 механизмов по характеру воздействия: 23 предупреждающих и 14 выявляющих против всего 2 реагирующих (№ 22, 31), 2 аудита (№ 39, 40), 2 измерительных и 3 поддерживающих. Предупреждение сосредоточено на уровнях действия и сети, а выявляющие на уровнях текста и цепочки поставок. Способность прервать уже начавшийся инцидент и обеспечить его разбор представлена кратко слабее.

4. АНАЛИЗ ПЕРЕКРЫТИЯ УГРОЗ

Систематизация опирается на три категории источников: открытые программные проекты; нормативные перечни угроз OWASP ASI (2026) [1] и OWASP LLM Top 10 (2025) [2]; научные публикации, обосновывающие отдельные механизмы и содержащие их экспериментальную проверку.

Классы OWASP ASI и OWASP LLM относятся к разным уровням системы, агенту и модели. На осях карты это разделение сохраняется. Единая трактовка их элементов как классов угроз принята только для описания механизмов по общей схеме и не означает, что уровни равнозначны. Связанные пары классов «модель – агент», например, LLM01/ASI01, описывают одну

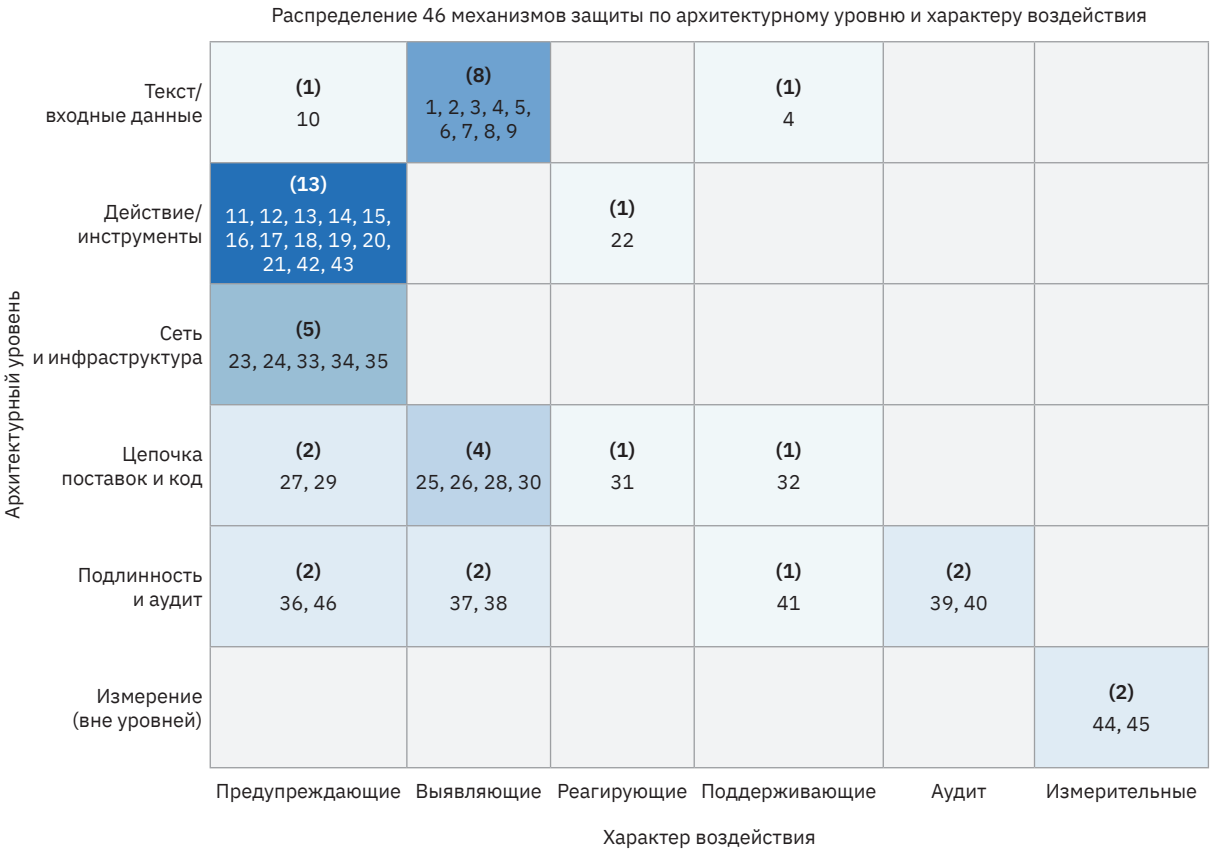


Рис. 1 | Тепловая карта распределения 46 механизмов защиты по архитектурному уровню и характеру воздействия

Fig. 1 | Heat map showing the distribution of 46 protection mechanisms by architectural level and nature of the impact

угрозу на двух уровнях, хотя средство может действовать против них разными механизмами. Поэтому средство, перекрывающее оба класса такой пары, не считается двумя независимыми барьерами. Показатель $\Delta(C)$ вычисляется по каждому классу в отдельности и силу средств между классами не суммирует, что исключает двойной учет одного средства.

Отбор открытых проектов проводился в два этапа. Сначала сформирован обзорный каталог из 118 репозиторий, отражающий состояние рынка средств защиты агентных систем за последний календарный год. Затем из каталога отобраны репрезентативные реализации. На каждый механизм от одной до трех реализаций, наиболее полно раскрывающих принцип его работы. Такой порядок исключает многократный разбор функционально совпадающих средств и одновременно обеспечивает, что каждый механизм подкреплен конкретной реализацией. В итоге отбора сформировалось 46 механизмов, действующих во время исполнения агента либо на этапе поставки его компонентов.

Глубину перекрытия каждого класса угроз характеризует показатель эшелонирования – число различных средств защиты, получивших высшую оценку. Обозначим через M – множество механизмов, а $\sigma(m, C) \in \{0, 1, 2, 3\}$ – силу средства m против класса угрозы C . Значение $\sigma(m, C)$ задает роль средства в предотвращении угрозы по порядковой шкале из четырех уровней: $\sigma = 0$ – средство к классу C не относится и защиты не образует; $\sigma = 1$ – средство выявляет угрозу, но не останавливает ее; $\sigma = 2$ – средство останавливает угрозу, но реализация незрелая; $\sigma = 3$ – средство

останавливает угрозу и является зрелым барьером. Четыре уровня – наименьшее число, разделяющее качественно различные роли средства. Две градации (перекрывает/не перекрывает) не отделивают вспомогательное влияние от самостоятельного барьера. Трех уровней недостаточно, так как уровни $\sigma = 1$ и $\sigma = 2$ задают разные типы пробелов и объединению не подлежат. На их основе построена классификация пробелов в табл. 2. Пять и более уровней ввести нельзя, так как оценки ставятся по описаниям и документации средств, а они не позволяют различать более тонкие степени силы.

Оценка $\sigma(m, C)$ определяется тремя признаками средства против класса C : P – средство предупреждает угрозу, а не только выявляет ее; G – реализация зрелая; R – устойчивость к типовому обходу подтверждена документацией или публикацией.

Тогда показатель эшелонирования класса C :

$$\Delta(C) = \#\{m \in M : \sigma(m, C) = 3\}.$$

Средние и низкие оценки, а также поддерживающие, измерительные и аудиторские механизмы, в показатель не входят. Показатель $\Delta(C)$ подсчитывает средства с высшей оценкой, но не доказывает их независимость, поэтому его следует понимать как верхнюю оценку глубины эшелонирования. Фактическое число независимых барьеров может быть меньше. Значение $\Delta(C)$ вычисляется при аналитическом допущении, что средства с $\sigma = 3$ образуют барьеры, не преодолеваемые единым приемом обхода. Проверка этого допущения требует эмпирического воспроизведения атаки на общей испытательной среде

Таблица 2 | Критерии присвоения силы средства

Table 2 | Criteria for assigning the force of a means

σ	P	G	R
0	Нет	–	–
1	Да	Нет	–
2	Да	Да	Нет
3	Да	Да	Да

и вынесена в дальнейшую работу. Таким образом, карта перекрытия является аналитической и служит основой для последующей эмпирической проверки, а не заменяет ее. Распределение показателя по классам ASI/LLM (рис. 2) служит основой дальнейшего анализа. Полученная тепловая карта показывает, на каких уровнях сосредоточена защита каждой угрозы, и служит переходом от поэлементного описания к анализу глубины перекрытия.

Для количественной оценки глубины перекрытия по каждому классу угроз подсчитано число независимых средств, перекрывающих его с высокой силой (рис. 3).

Угрозы с высоким показателем эшелонирования защиты перекрыты несколькими независимыми средствами разных уровней, что обеспечивает устойчивость к обходу отдельного барьера.

Злоупотребление инструментами (ASI02) перекрыто наиболее полно. Против него действуют ограничение расхода ресурсов (№ 11), политики на вызовы (№ 12), проверка аргументов по схеме (№ 13), контроль инфор-

мационных потоков (№ 15, 16), формальное сужение привилегий (№ 17), правила против инъекций в аргументах (№ 19), подтверждение опасных действий человеком (№ 21), архитектура с разделением доверия (№ 43), сетевой прокси (№ 23), изоляция среды (№ 33, 34) и анализ опасных потоков (№ 28).

Средства принадлежат уровням действия, сети и цепочки поставок и не преодолеваются единым приемом обхода.

Каскадные сбои (ASI08) перекрыты восемью средствами, включая ограничение ресурсов (№ 11), контроль потоков (№ 15), формальное сужение привилегий (№ 17), сетевой прокси (№ 23) и изоляцию среды (№ 33, 34). Сочетание ограничения ресурсов и изоляции ограничивает распространение сбоя.

Злоупотребление привилегиями (ASI03) перекрыто пятью средствами уровня действия и инфраструктуры (№ 12, 17, 21, 43, 33), а захват цели агента (ASI01) – четырьмя средствами контроля потоков и разделения доверия (№ 15, 16, 43, 28). Общий признак хорошо перекрытых угроз состоит



Рис. 2 | Число сильных средств защиты по архитектурным уровням для сценариев атак (повторяющиеся коды обозначают разные сценарии атак внутри одного класса угроз)

Fig. 2 | The number of strong security measures by architectural levels for attack scenarios (duplicate codes indicate different attack scenarios within the same threat class)

в том, что их проявления сводятся к недопустимому вызову инструмента или недопустимому потоку данных, т. е. к событиям, наблюдаемым на уровне действия. Именно к этим событиям отрасль выработала наибольшее число зрелых предупреждающих средств.

5. ПРОБЕЛЫ В ЗАЩИТЕ И ЗАБЛУЖДЕНИЯ

Структурным пробелом называется класс угроз, для которого ни одно средство не обеспечивает надежного перекрытия (табл. 3). Сильные средства отсутствуют

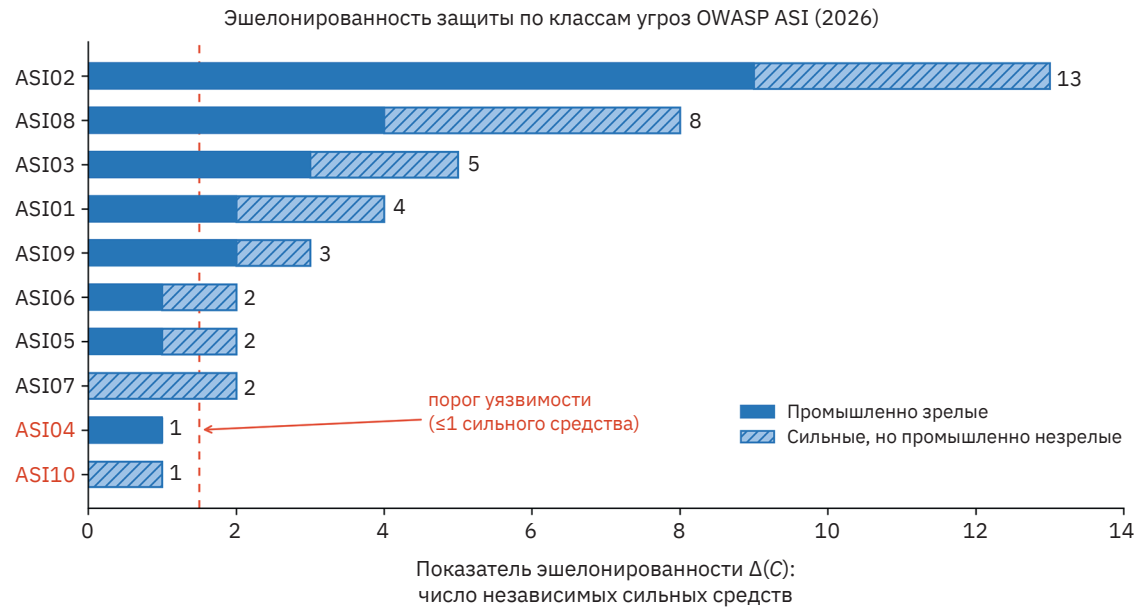


Рис. 3 | Число независимых сильных средств на угрозу

Fig. 3 | The number of independent strong means to counter the threat

Таблица 3 | Структурные пробелы в защите

Table 3 | Structural gaps in protection

Угроза	Доступные частичные меры	Чего недостает
ASI06 Отравление памяти и контекста	Защита памяти агента (№ 46, без промышленной готовности); правила потоков данных (№ 15) и разделение доверия (№ 43) – частично	Зрелого специализированного средства защиты долговременной памяти
ASI07 Небезопасная связь между агентами	Разделение доверия (№ 43) и криптографическая идентификация (№ 36) – в стадии становления; шлюз с RBAC (№ 24) – только сетевая граница	Результативного и промышленно готового средства контроля содержания межагентного обмена
ASI10 Скомпрометированные агенты	Формальное сужение привилегий (№ 17, готовность частична); обнаружение отклонений (№ 37), отзыв артефактов (№ 31), аудит (№ 39, 40)	Зрелого предупреждающего средства выявления и сдерживания скомпрометированного агента
ASI04 Уязвимости цепочки поставок	Выявление отравления описаний (№ 26); контроль целостности (№ 25), проверка зависимостей (№ 29), статический анализ (№ 30) – средняя сила	Предупреждающего средства высокой силы, а не только обнаружения на этапе поставки
Обход текстовых фильтров	Классификаторы (№ 1) и сигнатурные правила (№ 3); нормализация Unicode (№ 4) – частично	Устойчивого текстового барьера против кодирования и семантического обхода

либо лишь выявляют угрозу, но не предупреждают. Эти же классы слабо перекрыты по показателю эшелонирования (рис. 3).

Переоценка средства состоит в возложении на него функции защиты, которую оно в одиночку не выполняет. Выявлено три типовых случая:

1. Применение единственного обучаемого классификатора вредоносных инструкций (№ 1) как основной защиты от захвата цели агента. Классификатор обладает низкой устойчивостью к обходу и результативен лишь как один из вспомогательных компонентов. Без правил контроля потоков (№ 15), проверки аргументов по схеме (№ 13) и сетевого прокси (№ 23) он не обрывает защиты.

2. Трактовка отчета о соответствии требованиям стандартов (№ 41) как доказательство защищенности. Такой отчет лишь фиксирует, что нужные средства формально есть.

3. Опора исключительно на статическое сканирование навыков и плагинов (№ 27) без последующего принудительного блокирования.

Выявлено четыре недооцененных средства защиты из-за кажущейся простоты:

- ограничение расхода токенов, средств и частоты вызовов (№ 11) – простое по реализации средство с высокой результативностью и устойчивостью, сдерживающее каскадное разрастание действий и неконтролируемое потребление ресурсов;
- связка проверки аргументов по схеме (№ 13) и правил против инъекций в аргументах (№ 19) обеспечивает дешевый детерминированный контроль вызова инструмента, не требующий обучаемых моделей;
- архитектурная связка сетевого прокси исходящих запросов (№ 23) и изоляции среды в виртуальных машинах (№ 33) ограничивает одновременно сетевые обращения и последствия компрометации, образуя слой защиты;
- формальная проверка политик и только сужающихся привилегий (№ 17) обеспечивает гарантию, что права агента могут лишь уменьшаться, но не расти, поэтому эскалация привилегий исключена.

Отдельного разграничения требуют средства, которые не действуют во время исполнения агента и потому барьером не являются, но нередко учитываются как защита.

К ним относятся регрессионное тестирование методами красной команды (№ 44) и эталонные наборы испытаний защит, в частности AgentDojo (№ 45). Они измеряют результативность самих средств защиты. Позволяют оценить, насколько надежно защиты перекрывают угрозы. По этой причине измерительные средства вынесены в отдельную группу и в показатель эшелонирования не входят.

6. РЕКОМЕНДУЕМЫЙ НАБОР СРЕДСТВ ЗАЩИТЫ

Анализ перекрытия показал, что устойчивость защиты зависит от числа независимых барьеров на пути угрозы. Если атака обходит один барьер, ее должен перехватить следующий. Самодостаточных уровней в цепочке нет. Текстовый уровень распознает признаки атаки, но целенаправленный обход его преодолевает. Уровень действия принимает решение о блокировке, опираясь на текстовый. Инфраструктурный уровень ограничивает последствия, однако содержание вызовов для него неразличимо.

Минимальный эшелонированный набор образован средствами с высокой результативностью при широком перекрытии угроз и умеренной стоимостью внедрения. Его состав изображен на рис. 4.

Уровень текста включает обучаемый классификатор вредоносных инструкций (№ 1) и сигнатурные правила (№ 3). В уровень действия входят ограничение расхода ресурсов (№ 11), проверка аргументов по схеме (№ 13) с правилами против инъекций в аргументах (№ 19), правила последовательности вызовов и потоков данных (№ 15) и подтверждение опасных действий человеком (№ 21). В уровень сети и инфраструктуры включены: единый прокси исходящих запросов с защитой от SSRF (№ 23) и изоляция агента в виртуальных машинах и контейнерах (№ 33). Обоснованность набора подтверждается картой перекрытия.

Средства набора целесообразно внедрять в порядке убывания отношения отдачи защиты к затратам. Первыми внедряются средства уровня действия и инфраструктуры, обладающие высокой результативностью и устойчивостью при умеренной сто-

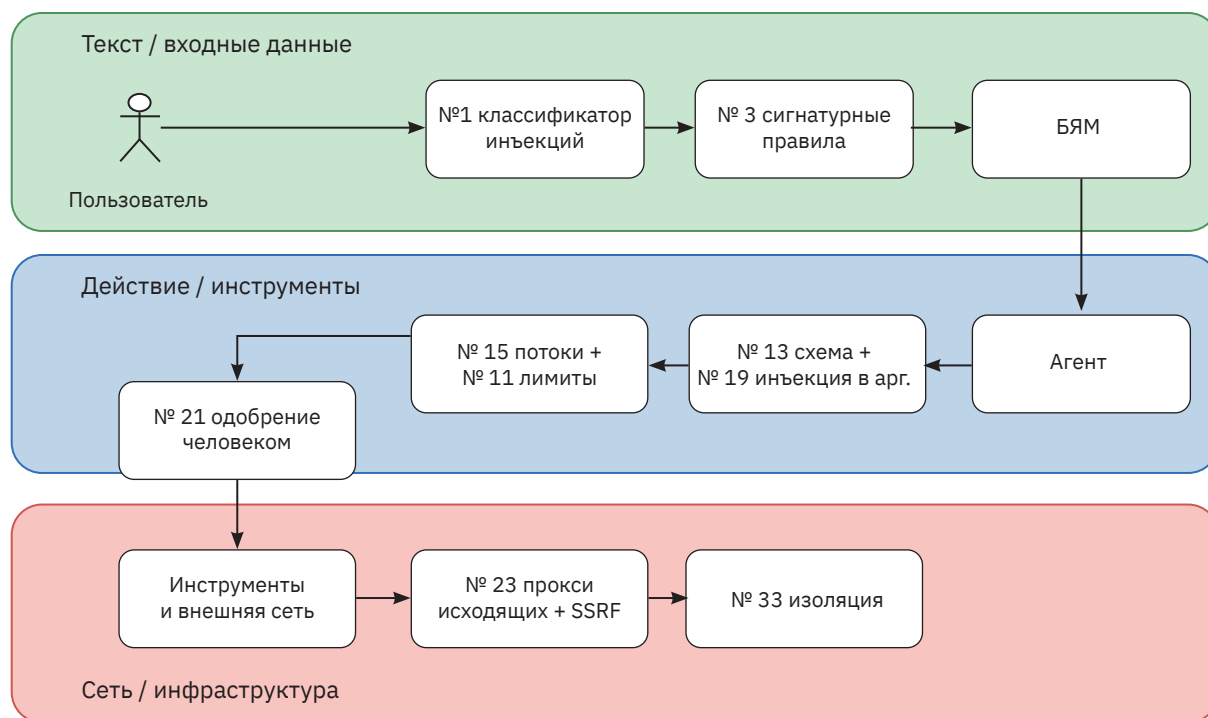


Рис. 4 | Минимальный набор защитных средств

Fig. 4 | Minimum set of protective equipment

имости: ограничение ресурсов (№ 11), проверка аргументов по схеме (№ 13), сетевой прокси (№ 23) и изоляция среды (№ 33). Эти средства детерминированы, не требуют обучаемых моделей и дают наибольший прирост защищенности на единицу затрат.

Вторыми внедряются средства контроля потоков и участия человека – правила последовательности вызовов (№ 15) и подтверждение опасных действий (№ 21), требующие настройки под конкретный набор инструментов и сценарии применения. Последними внедряются средства текстового уровня (№ 1, 3): они замыкают набор как первый рубеж обнаружения, но при отсутствии барьеров действия и инфраструктуры защиты не образуют, поэтому их внедрение в отрыве от нижележащих уровней нецелесообразно.

7. РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЯ

Полученные результаты ограничены принятым подходом к систематизации,

и это следует учитывать при их применении. Опишем ограничения:

1. Аналитические оценки: результативность и устойчивость средств, сила перекрытия угроз и показатель эшелонирования определены по описаниям средств, документации реализаций и публикациям, а не в едином эксперименте. Оценки отражают согласованное суждение об известных свойствах средств, но не заменяют измерение на общей испытательной среде.

2. Отсутствие эмпирического набора испытаний, применимого ко всем 46 механизмам одновременно: существующие наборы, включая AgentDojo, охватывают отдельные классы угроз и типы средств, что не позволяет сопоставить все средства по единой шкале.

3. Различная зрелость реализаций: в совокупность вошли как промышленно готовые средства, так и исследовательские прототипы.

4. Привязка ландшафта угроз к перечням OWASP ASI (2026) [1] и LLM (2025) [2]: при их пересмотре отдельные оценки перекрытия потребуют уточнения.

5. Сила средства зависит от его конфигурации: результативность механизма меняется с режимом развертывания и настройками, а оценка $\sigma(m, C)$ присвоена по типовому описанию и фиксирует одно значение. Неопределенность устранима только измерением в заданной конфигурации на общей испытательной среде.

Из выявленных пробелов и ограничений вытекают три направления дальнейшей работы:

1. Защита долговременной памяти и контекста агента. Отравление памяти (ASI06) остается без зрелого специализированного средства контроля целостности долговременной памяти и поискового индекса.

2. Безопасность взаимодействия нескольких агентов. Небезопасная связь между агентами (ASI07) и скомпрометированные агенты (ASI10) перекрыты средствами в стадии становления. Нужна аутентификация и ограничение доверия в межагентном обмене.

3. Единый порядок эмпирической проверки перекрытия угроз. Устранение первого и второго ограничений работы предполагает построение общей испытательной среды, позволяющей измерять силу разнородных средств по единой шкале и тем самым перевести карту перекрытия из аналитической в эмпирическую.

8. ЗАКЛЮЧЕНИЕ

Систематизированы механизмы защиты агентных систем на основе больших языковых моделей, и оценена полнота перекрытия ими актуального ландшафта угроз. Полученные результаты дают ответы на три поставленных вопроса исследования.

На вопрос об основаниях систематизации (B1) работа отвечает двухосевой классификации, в которой каждое средство характеризуется архитектурным уровнем применения и характером воздействия. Две оси независимы и вместе описывают, где и как средство действует. Классифика-

ция по типу продукта отвергнута как не отражающая защитных свойств.

На вопрос о полноте перекрытия (B2) работа отвечает картой перекрытия «угроза – механизм» и показателем эшелонирования. Совокупность из 46 механизмов перекрывает все 10 классов угроз ASI, однако глубина перекрытия распределена неравномерно: злоупотребление инструментами (ASI02) перекрыто 13 независимыми сильными средствами, каскадные сбои (ASI08) 8, тогда как уязвимости цепочки поставок (ASI04) и скомпрометированные агенты (ASI10) лишь 1. По характеру воздействия совокупность смещена к предупреждению и выявлению и заметно слабее в реагировании и проверяемости действий.

На вопрос о пробелах и заблуждениях (B3) работа отвечает перечнем структурных пробелов и типовых ошибок выбора средств. Структурными пробелами являются защита долговременной памяти и контекста (ASI06), безопасность взаимодействия нескольких агентов (ASI07) и сдерживание скомпрометированных агентов (ASI10). Зрелого предупреждающего средства для них не выработано. Типовые заблуждения состоят в переоценке отдельных средств, в отрыве от нижележащих уровней, и недооценке простых детерминированных средств с высоким фактическим вкладом в защиту.

Основной вывод исследования состоит в том, что зрелость средств защиты агентных систем смещена. Отрасль выработала многочисленные средства для угроз, сводимых к вызову инструмента или потоку данных на несущем уровне действия, но оставила недостаточно перекрытыми угрозы, затрагивающие состояние агента, межагентное взаимодействие и подлинность компонентов. Двухосевая классификация, карта перекрытия с показателем эшелонирования и минимальный набор средств защиты образуют основу для обоснованного выбора защиты при проектировании агентных систем и указывают приоритетные направления восполнения выявленных пробелов.

КОНФЛИКТ ИНТЕРЕСОВ / CONFLICT OF INTERESTS

Авторы заявляют об отсутствии конфликта интересов / The authors declare no conflict of interests.

СПИСОК ИСТОЧНИКОВ

1. OWASP Top 10 for Agentic Applications for 2026. URL: <https://genai.owasp.org/resource/owasp-top-10-for-agentic-applications-for-2026/> (дата обращения: 20.07.2026).
2. OWASP Top 10 for Large Language Model Applications for 2025. URL: <https://owasp.org/www-project-top-10-for-large-language-model-applications/> (дата обращения: 20.07.2026).
3. **Chen Z., Xiang Z., Xiao C. et al.** AgentPoison: Red-teaming LLM Agents via Poisoning Memory or Knowledge Bases // *Advances in Neural Information Processing Systems (NeurIPS)*. 2024. arXiv:2407.12784. URL: <https://arxiv.org/abs/2407.12784> (дата обращения: 20.07.2026).
4. **Liu J., Ruan B., Yang X. et al.** TraceAegis: Securing LLM-Based Agents via Hierarchical and Behavioral Anomaly Detection. URL: <https://arxiv.org/abs/2510.11203> (дата обращения: 20.07.2026).
5. **Chennabasappa S., Nikolaidis C., Song D. et al.** LlamaFirewall: An Open-Source Guardrail System for Building Secure AI Agents. URL: <https://arxiv.org/abs/2505.03574> (дата обращения: 20.07.2026).
6. **Manakul P., Liusie A., Gales M.** SelfCheck-GPT: Zero-Resource Black-Box Hallucination Detection for Generative Large Language Models // *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing (EMNLP)*. 2023. P. 9004–9017. DOI: 10.18653/v1/2023.emnlp-main.557.
7. **Shi T., He J., Wang Z. et al.** Progent: Securing AI Agents with Privilege Control. URL: <https://arxiv.org/abs/2504.11703> (дата обращения: 20.07.2026).
8. **Debenedetti E., Shumailov I., Fan T. et al.** Defeating Prompt Injections by Design (CaMeL). URL: <https://arxiv.org/abs/2503.18813> (дата обращения: 20.07.2026).
9. **Debenedetti E., Zhang J., Balunović M. et al.** AgentDojo: A Dynamic Environment to Evaluate Prompt Injection Attacks and Defenses for LLM Agents // *Advances in Neural Information Processing Systems, Datasets and Benchmarks Track (NeurIPS)*. URL: <https://arxiv.org/abs/2406.13352> (дата обращения: 20.07.2026).
10. **Богина В. М., Борисов Г. И., Братко В. В. и др.** Анализ применимости больших языковых моделей к моделированию реалистичных диалогов в целях симуляции атак социальной инженерии // *Проблемы информационной безопасности. Компьютерные системы*. 2025. № 4. С. 9–22. DOI: 10.48612/jisp/kfvm-3811-vmk4.
11. **Богина В. М., Величко К. А., Макеева А. А. и др.** Подход к созданию персонализированных LLM-агентов на основе личностных черт MBTI // *Проблемы информационной безопасности. Компьютерные системы*. 2024. № 3. С. 127–141. DOI: 10.48612/jisp/4pum-m1b1-96kh.
12. **Greshake K., Abdelnabi S., Mishra S. et al.** Not What You've Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection // *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security (AISEC '23)*. New York: Association for Computing Machinery, 2023. P. 117–134. DOI: 10.1145/3605764.3623985.
13. **Бугаев В. А., Жуковский Е. В., Лырчиков А. А.** Обнаружение потенциально вредоносной активности в конвейерах CI/CD на основе анализа поведения сборщика // *Проблемы информационной безопасности. Компьютерные системы*. 2025. № 1. С. 69–82. DOI: 10.48612/jisp/at5b-46tf-zet9.
14. **Тумаков М. Д., Иванова Л. А.** Использование больших языковых моделей в задачах анализа событий безопасности // *Проблемы информационной безопасности. Компьютерные системы*. 2026. № 1. С. 201–203. DOI: 10.66424/2071-8217-2026-1-15.
15. **Морозов Д. С., Истомина А. С., Лаврова Д. С.** Атаки губки на большие языковые модели: современная угроза отказа в обслуживании при авторегрессивном декодировании / под ред. Д. П. Зегжды, М. О. Калинина // *Неделя науки ИКНХ : материалы Всероссийской научно-практической конференции, 1–20 апреля 2026 г., Санкт-Петербург, Россия*. СПб. : ПОЛИТЕХ-ПРЕСС, 2026. С. 92–94. DOI: 10.18720/SPBPU/2/i26-137.

REFERENCES

1. OWASP Top 10 for Agentic Applications for 2026. URL: <https://genai.owasp.org/resource/owasp-top-10-for-agentic-applications-for-2026/> (accessed: 20.07.2026).

2. OWASP Top 10 for Large Language Model Applications for 2025. URL: <https://owasp.org/www-project-top-10-for-large-language-model-applications/> (accessed: 20.07.2026).
3. **Chen Z., Xiang Z., Xiao C. et al.** AgentPoison: Red-teaming LLM Agents via Poisoning Memory or Knowledge Bases. *Advances in Neural Information Processing Systems (NeurIPS)*. 2024. arXiv:2407.12784. URL: <https://arxiv.org/abs/2407.12784> (accessed: 20.07.2026).
4. **Liu J., Ruan B., Yang X. et al.** TraceAegis: Securing LLM-Based Agents via Hierarchical and Behavioral Anomaly Detection. URL: <https://arxiv.org/abs/2510.11203> (accessed: 20.07.2026).
5. **Chennabasappa S., Nikolaidis C., Song D. et al.** LlamaFirewall: An Open-Source Guardrail System for Building Secure AI Agents. URL: <https://arxiv.org/abs/2505.03574> (accessed: 20.07.2026).
6. **Manakul P., Liusie A., Gales M.** SelfCheckGPT: Zero-Resource Black-Box Hallucination Detection for Generative Large Language Models. *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing (EMNLP)*. 2023, pp. 9004–9017. DOI: 10.18653/v1/2023.emnlp-main.557.
7. **Shi T., He J., Wang Z. et al.** Progent: Securing AI Agents with Privilege Control. URL: <https://arxiv.org/abs/2504.11703> (accessed: 20.07.2026).
8. **Debenedetti E., Shumailov I., Fan T. et al.** Defeating Prompt Injections by Design (CaMeL). URL: <https://arxiv.org/abs/2503.18813> (accessed: 20.07.2026).
9. **Debenedetti E., Zhang J., Balunović M. et al.** AgentDojo: A Dynamic Environment to Evaluate Prompt Injection Attacks and Defenses for LLM Agents. *Advances in Neural Information Processing Systems, Datasets and Benchmarks Track (NeurIPS)*. URL: <https://arxiv.org/abs/2406.13352> (accessed: 20.07.2026).
10. **Bogina V. M., Borisov G. I., Bratko V. V. et al.** Analysis of the applicability of large language models to the simulation of realistic dialogues for the purpose of simulating social engineering attacks. *Problems of information security. Computer systems*. 2025. No. 4, pp. 9–22. DOI: 10.48612/jisp/kfvm-3811-vmk4. (In Russian)
11. **Bogina V. M., Velichko K. A., Makeeva A. A. et al.** Approach to creating personalised LLM agents based on MBTI personality traits. *Problems of information security. Computer systems*. 2024. No. 3, pp. 127–141. DOI: 10.48612/jisp/4pum-m1b1-96kh. (In Russian)
12. **Greshake K., Abdelnabi S., Mishra S. et al.** Not What You've Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection. *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security (AISEC '23)*. New York: Association for Computing Machinery, 2023, pp. 117–134. DOI: 10.1145/3605764.3623985.
13. **Bugaev V. A., Zhukovskii E. V., Lyrchikov A. A.** Detection of potentially malicious activity in CI/CD pipelines based on analysis of runner behavior. *Problems of information security. Computer systems*. 2025. No. 1, pp. 69–82. DOI: 10.48612/jisp/at5b-46tf-zet9. (In Russian)
14. **Tumakov M. D., Ivanova L. A.** Use of large language models for security event analysis. *Problems of information security. Computer systems*. 2026. No. 1, pp. 201–213. DOI: 10.66424/2071-8217-2026-1-15. (In Russian)
15. **Morozov D. S., Istomina A. S., Lavrova D. S.** Attacks on large language models: a modern threat of denial of service in autoregressive decoding. *Nedelya nauki IKNK: materialy Vserossijskoj nauchno-prakticheskoy konferencii*, 1–20 aprelya 2026 g., St. Petersburg, Russia. St. Petersburg: POLYTECH-PRESS, 2026, pp. 92–94. DOI: 10.18720/SPBPU/2/i26-137. (In Russian)

СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

ИСТОМИНА Анастасия Сергеевна – аспирант, ассистент, Санкт-Петербургский политехнический университет Петра Великого, Россия, 195251, Санкт-Петербург, ул. Политехническая, д.29
E-mail: isto.anastasiya@gmail.com
ORCID: 0009-0007-8669-8081

ЯКОВЛЕВ Андрей Андреевич – специалист, АО «Позитив Текнолоджиз», Россия, 107061, Москва, Преображенская пл., д.8
E-mail: Andrew42ru@icloud.com
ORCID: 0009-0008-9678-2428

ISTOMINA Anastasiya S. – Postgraduate Student, Assistant, Peter the Great St. Petersburg Polytechnic University, Russia, 195251, St. Petersburg, Polytechnicheskaya str., 29

IAKOVLEV Andrei A. – Specialist, JSC “Positive Technologies”, Russia, 107061, Moscow, Preobrazhenskaya sq., 8