Executive summary
Актуальные киберугрозы в странах Ближнего Востока

Исследование сосредоточено на ландшафте киберугроз для стран Ближнего Востока с учетом периодов эскалации геополитической напряженности вокруг Ирана в июне 2025 года и в Q1 2026 (со стартом военной операции США и Израиля 28 февраля 2026 г.). В исследовании представлены результаты анализа ландшафта киберугроз для наиболее атакуемых стран региона в контексте их отраслевой, экономической и геополитической ситуации, а также прогноз о будущих киберугрозах региона и рекомендации по защите от них.

Драйверы развития региона

Нефте- и газодобывающие страны Ближнего Востока (Катар, ОАЭ, Саудовская Аравия) стремятся диверсифицировать экономику с целью снижения зависимости от нефти. Для этого они массово переходят к высокотехнологичной промышленности, в частности, к биотехнологиям, квантовым вычислениям и атомной энергетике.

Вместе с этим, многие страны региона сосредоточены на развитии суверенного искусственного интеллекта, сопровождаемого разработкой моделей для арабского языка и локализацией дата-центров внутри стран. Стремление к цифровому суверенитету, особенно в условиях нестабильной геополитической ситуации, сформировало на Ближнем Востоке тенденцию к сокращению зависимости от трансграничных цифровых архитектур. Она распространилась не только на размещение данных, но и на локализацию критически важных аппаратных возможностей.

На сегодняшний день в этой сфере есть ряд сдерживающих факторов:

- нехватка квалифицированных специалистов;
- риски территориального расположения ЦОД, связанные с периодической эскалацией конфликтов;
- межгосударственные взаимоотношения, осложняющие для стран Ближнего Востока баланс между технологическими компаниями КНР и США.

Ведущие экономики региона

Драйверы развития региона во многом формируются за счет стран с сильной экономикой и определяются их направлением развития. Как правило, эти же страны лидируют по числу кибератак на них — в силу их более высокого уровня цифровизации инфраструктуры и заинтересованности злоумышленников в получении финансовой выгоды и краже конфиденциальных данных.

Среди арабских стран по прогнозу Международного валютного фонда на 2026 год лидерами являются **Катар, ОАЭ и Саудовская Аравия**.

- Экономика Катара преимущественно базируется на добыче нефти и газа;
- ОАЭ, стремясь диверсифицировать экономику, инвестируют в сервисные секторы экономики;
- Саудовская Аравия держит курс на цифровизацию промышленной инфраструктуры, инвестируя также в ненефтяные секторы экономики.

Общий ландшафт киберугроз Ближнего Востока

На рассматриваемый период (Q2 2025 — Q1 2026) пришлись сразу две острые фазы конфликта вокруг Ирана — в период **с 13 по 24 июня 2025 года** (однако часть кибератак была обнаружена уже в июле, это отразилось на данных за Q2 и Q3) и **в феврале — марте 2026 года** — что значительно повлияло на ландшафт киберугроз в регионе.

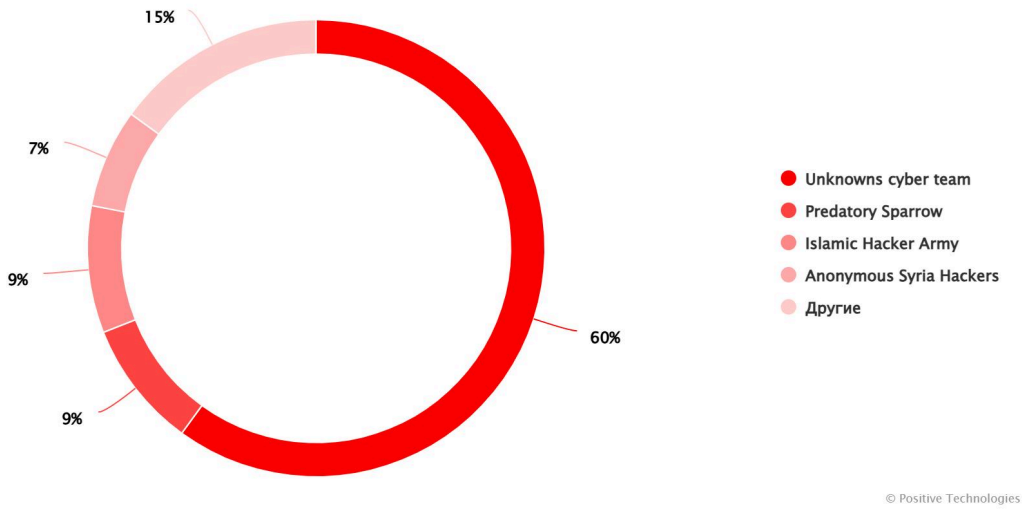
Инциденты, произошедшие в июне, затрагивали, в основном, Иран и Израиль, а инциденты Q1 2026, сопровождавшие военную операцию США и Израиля, стартовавшую 28 февраля, отразились и на других странах Ближнего Востока, затронутых конфликтом. Общим оставался характер кибератак: в основном они были направлены на остановку работы отраслеобразующих объектов инфраструктуры и на формирование общественного мнения за счет кибератак на СМИ, распространения дезинформации в соцсетях и демонстрации уязвимости крупнейших учреждений государств.

Июнь — июль 2025 года

В период с 13 по 20 июня, на который пришлась острая фаза конфликта, в киберпространстве ближневосточного региона было зафиксировано более 250 хактивистских атак, включая DDoS-атаки, утечки данных и взлом веб-сайтов. Преимущественно такие атаки затрагивали организации Ирана и Израиля, в то время как для других стран региона в большей степени наблюдались кибератаки финансово мотивированных группировок вымогателей.

В атаках на Иран по результатам анализа дарквеб-форумов и Telegram-каналов были замечены преимущественно хактивистские группировки **Unknowns cyber team** (60% объявлений на теневых ресурсах), **Predatory Sparrow и Islamic Hacker Army** (по 9%).

Рисунок 1. Группировки, атаковавшие Иран в июне 2025 года



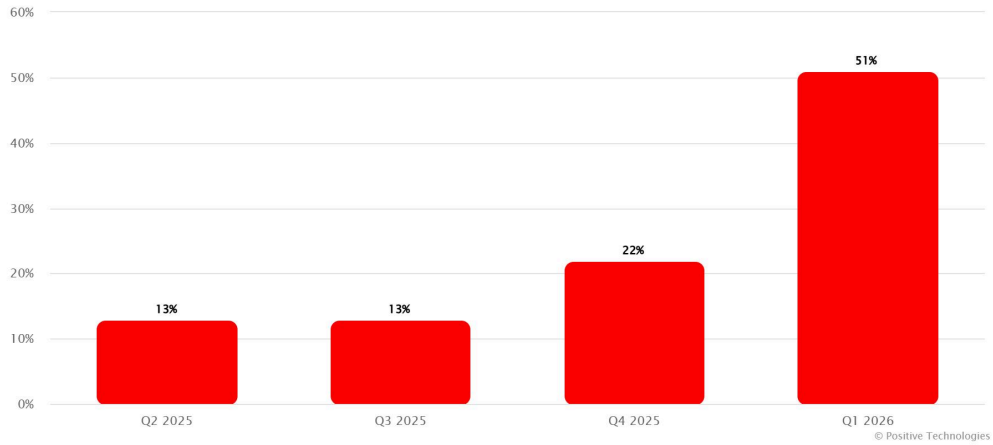
В Израиле наблюдалась активность хактивистов **Handala Hack Team**, а также проправительственных группировок **APT35 и APT42**. Handala Hack Team в своих атаках использует фишинг, кражу данных, вымогательство и деструктивные атаки с помощью вайперов. Их жертвами в Израиле за оба конфликтных периода стали промышленные и медицинские организации.

Группировки APT35 и APT42 позиционируются исследователями как действующие в интересах Ирана. APT35 проводит долгосрочные, ресурсоемкие операции по сбору стратегической разведывательной информации, их цель — военнослужащие, дипломаты и государственные служащие Ближнего Востока и США, организации сферы СМИ, энергетики и оборонной промышленности, телекоммуникаций и др. Группировка APT42 также нацелена на сбор разведывательной информации, полученной от организаций и частных лиц, преимущественно в ближневосточном регионе.

Февраль — март 2026 года

На первый квартал 2026 года пришелся 51% всех кибератак рассматриваемого периода, при этом **география атак существенно расширилась**, приблизив к Израилю, неизменно остающемуся в топ-3 атакуемых стран, Кувейт, Катар и Кипр. Относительно небольшой вклад конфликтного периода Q2 2025 объясняется, во-первых, краткосрочностью обострения, во-вторых, обнаружением инцидентов во втором и третьем кварталах (июнь и июль), что привело к распределению данных между ними.

Рисунок 2. Распределение числа атак по кварталам за весь рассматриваемый период

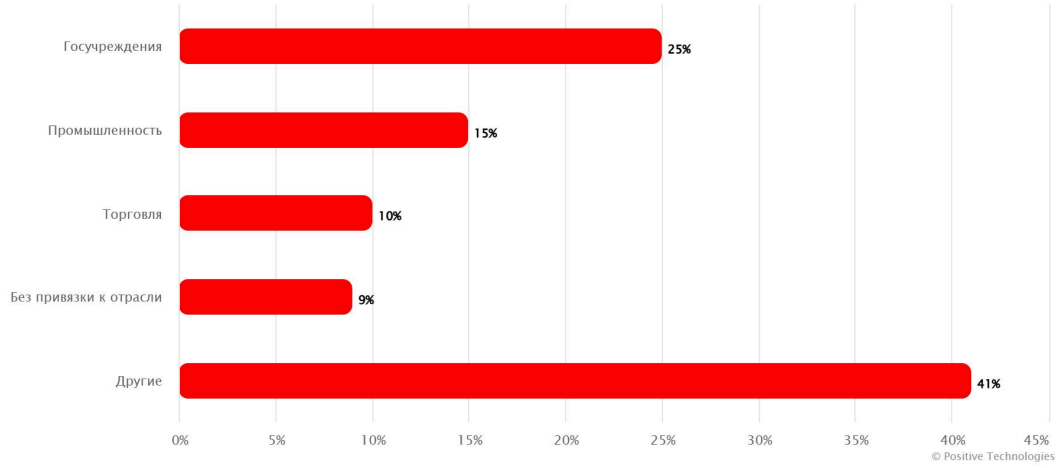


В «конфликтные» периоды на первый план вышли атаки на объекты КИИ — госучреждения и транспорт, а также на организации СМИ, чья значимость возрастает при обострении напряженности.

Среди пострадавших от кибератак организаций национального уровня в Q1 2026 года 45% составили государственные учреждения Катара, Кувейта, Израиля. В Иране наблюдались атаки, нацеленные на формирование определенного мнения у населения, и на вывод из строя веб-сайтов крупных информационных агентств. Вместе с этим в Q1 2026 киберинциденты происходили в отраслях, ранее минимально затрагиваемых атаками. Например, отмечается увеличение числа атак на образовательные и научные учреждения — со статистически малозначимого показателя до 5%.

Отраслевая картина кибератак на регион представляет собой смесь двух факторов: действия киберпреступников в отношении госучреждений (25% от всех кибератак), мотивированных обострением конфликта, и атаки на промышленность (15%) и торговлю (10%), характерные для региона в фазу смягчения конфликта.

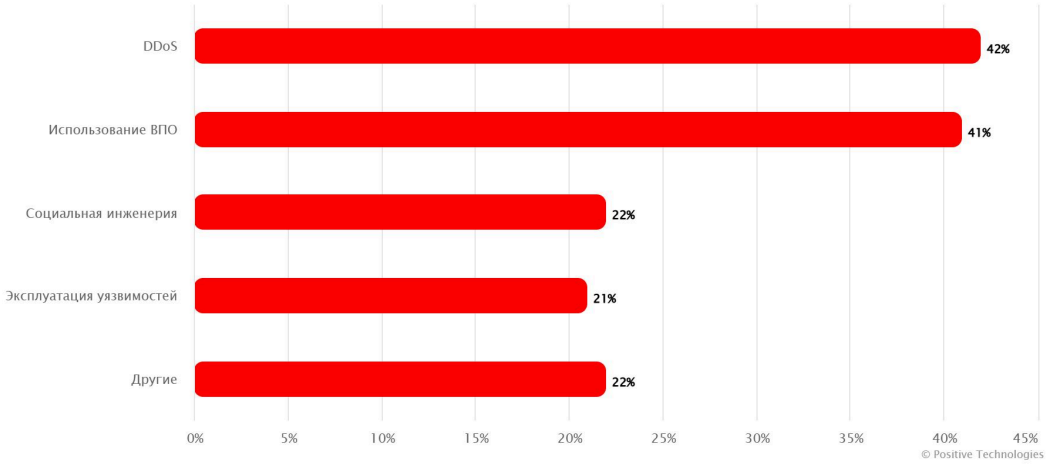
Рисунок 3. Распределение категорий жертв за весь рассматриваемый период



Методы кибератак

Влияние ирано-израильского конфликта на методы кибератак отразилось в вышедшей на первое место доле DDoS-атак (они использовались в 42% успешных атак). Такие воздействия характерны для хактивистов в силу их наглядности, возможности массовой реализации и влияния на общественные настроения.

Рисунок 4. Распределение методов кибератак за рассматриваемый период



Использование ВПО (41%) — глобальный тренд в силу его универсальности и высокой эффективности, использование вредоносных программ позволяет злоумышленникам реализовать все этапы кибератаки. Превалирующими типами ВПО за рассматриваемый период стали:

- шифровальщики (программы-вымогатели) с долей 29%;
- ВПО для удаленного управления (25%);
- шпионское ПО (18%).

Методы социальной инженерии (22%) часто сопровождают атаки с использованием ВПО на начальном этапе проникновения злоумышленников в инфраструктуру.

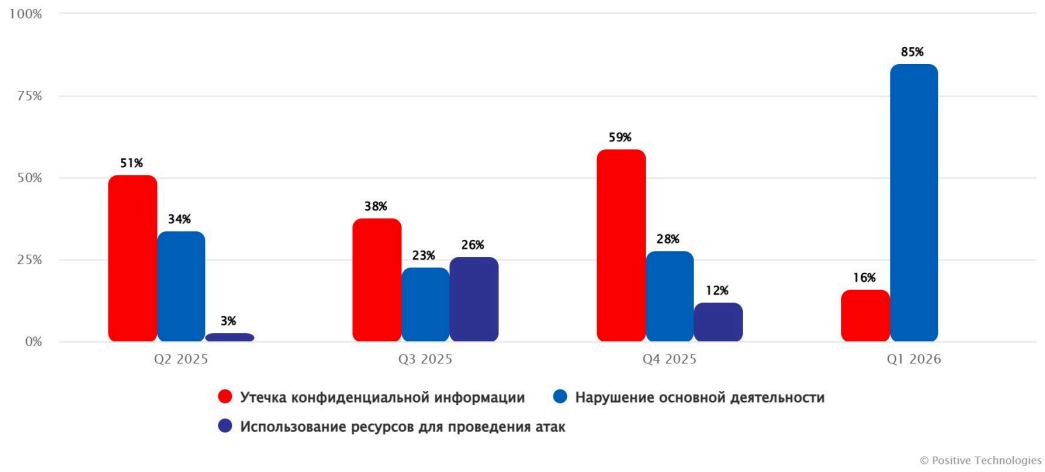
Эксплуатация уязвимостей (21%) остается успешной в регионе, поскольку, несмотря на цифровизацию, многие отрасли по-прежнему зависят от традиционных систем безопасности, что позволяет злоумышленникам эксплуатировать давно известные уязвимости устаревших компонентов инфраструктуры.

Внедрение IoT-устройств, которые на практике часто оказываются наименее защищенными объектами, также расширяет возможности киберпреступников по эксплуатации уязвимостей.

Последствия кибератак

Наиболее частым последствием кибератак на организации Ближнего Востока в рассматриваемый период стало нарушение основной деятельности (60%). Несомненно, **значительный вклад в эту категорию последствий внесли кибератаки, пришедшиеся на активные фазы конфликта**, особенно на первый квартал 2026 года: доля нарушений основной деятельности выросла на 57 п. п. по сравнению с Q4 2025 года.

Рисунок 5. Распределение последствий кибератак по кварталам



На втором месте — утечки конфиденциальной информации (44%), отчасти связанные с высокой активностью группировок шифровальщиков, отчасти — с недостаточно высоким уровнем кибергигиены пользователей.

На третьей позиции — «использование ресурсов для проведения атак» (10%). Во многом это связано с массовыми взломами и заражением устройств крупномасштабными ботнетами, чья инфраструктура охватывает множество C2-серверов, распределенных по разным странам.

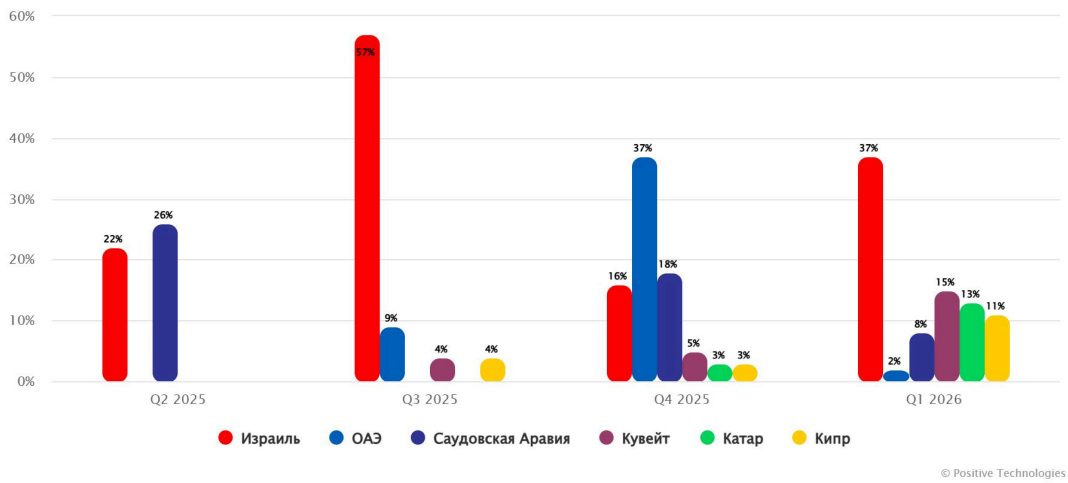
Ландшафт киберугроз наиболее атакуемых стран

За рассматриваемый период наиболее атакуемыми странами Ближнего Востока оказались:

- Израиль (33%);
- Саудовская Аравия (12%);
- ОАЭ (11%).

Доля успешных кибератак на Катар, Кувейт и Кипр приблизилась к лидерам только в первом квартале 2026 года в связи с обострением геополитической обстановки в регионе.

Рисунок 6. Распределение атакуемых стран по кварталам



Ландшафт киберугроз у всех стран различается. Топ-3 атакуемых отраслей за весь рассматриваемый период:

- для Израиля: 22% — промышленность; 16% — госучреждения, по 9% — отрасли IT и транспорта;
- для Саудовской Аравии: госучреждения — 35%, промышленность — 20%. торговля и сфера услуг — по 10%;
- для ОАЭ: 61% — торговля, 11% — промышленность, по 6% — финансовые организации, IT-компании и организации сферы услуг.

Для Израиля и Саудовской Аравии лидировала одна и та же тройка методов кибератак: DDoS, использование ВПО и эксплуатация уязвимостей, но с разным распределением. В связи с конфликтом для Израиля на первый план вышли DDoS-атаки (51%), доля атак с использованием ВПО составила 29%, с эксплуатацией уязвимостей — 27%. В Саудовской Аравии преобладали атаки, реализованные с использованием ВПО (55%), затем шла эксплуатация уязвимостей (40%), третье место заняли DDoS и социальная инженерия (по 30%).

Несколько нетипичная картина наблюдается в ОАЭ: за весь период в 56% атакующим удавалось скомпрометировать цепочки поставок или доверенные каналы связи. Выбор киберпреступников может быть связан с высокой цифровизацией бизнеса в ОАЭ, характеризующимся автоматизацией внутренних процессов, тесной интеграцией поставщиков, подрядчиков и партнеров с IT-системами компаний, а также наличием у некоторых поставщиков и доверенных партнеров привилегированного доступа к IT-системам. В топ-3 методов также вошли использование ВПО (44%) и методов социальной инженерии (28%).

В исследовании также был рассмотрен ландшафт киберугроз Ирана как одного из ключевых участников конфликта. В топ-3 атакуемых отраслей вошли стратегически значимые для страны финансовые организации (38%), СМИ (25%), организации отраслей промышленности и телекоммуникаций (по 13%). Такая картина характерна для обострения геополитического конфликта за счет сосредоточения атак на объектах КИИ и на организациях СМИ, направленных на формирование общественного мнения.

Прогнозы и рекомендации

В период затишья прогнозируется переключение внимания киберпреступников на ключевые отрасли (IT-компании для Израиля, промышленные организации и сфера услуг для Саудовской Аравии, организации торговли, сферы услуг и промышленности для ОАЭ) и объекты развивающихся направлений (энергетические объекты и инфраструктура суверенного ИИ). В кибератаках на частных лиц прогнозируется более частое использование генеративного ИИ.

В случае дальнейшей эскалации конфликта прогнозируется увеличение числа сложных и таргетированных кибератак на критически важные объекты инфраструктуры, попыток воздействия на спутниковые системы. В методах кибератак ожидается сохранение высокой доли DDoS-атак на организации различных отраслей.

Независимо от геополитической ситуации на Ближнем Востоке, рекомендации по кибербезопасности должны учитывать текущие мировые тренды киберугроз и специфику региона:

1. В условиях периодически обостряющейся геополитической напряженности особенное внимание должно быть сосредоточено на объектах, значимых для устойчивого функционирования КИИ, обеспечения жизнедеятельности населения и играющих важную роль в ВВП страны. Для них должны быть реализованы непрерывный мониторинг киберугроз и проактивная защита, например с использованием решений класса incident management, включая SIEM.

2. Для защиты инфраструктуры значимых организаций и промышленных объектов от глобального тренда в атаках с использованием ВПО необходимо сосредоточиться на защите сетевого периметра, а также на каналах доставки ВПО в инфраструктуру организаций, наиболее распространенным из которых является электронная почта.

3. Учитывая цифровую трансформацию региона, необходимо сосредоточиться на предотвращении киберугроз еще на стадии разработки ПО. Решения класса application inspector, используемые для статического анализа исходного кода, позволят выявить возможные уязвимости и дефекты до внедрения программного решения, а средства динамического анализа обеспечат устранение уязвимостей на этапе тестирования и доставки ПО.

4. Решения по обнаружению кибератак на ранней стадии, основанные на анализе сетевого трафика промышленных протоколов, могут существенно повысить уровень защиты многих критически важных объектов региона, характеризующегося высокой степенью цифровизации промышленной инфраструктуры.

5. Набирающее обороты использование генеративного ИИ для реализации кибератак требует сосредоточиться на создании решений для выявления дипфейков и на разработке обучающих программ для населения.

6. Цифровизация промышленной инфраструктуры увеличила поверхность атаки для злоумышленников, что потребовало перехода к архитектурам нулевого доверия и решениям, ориентированным на защиту КИИ. Ключевой технической задачей является интеграция современных решений безопасности с устаревшими системами и уже функционирующими промышленными средами. В этих условиях рекомендуется регулярное проведение кибериспытаний с участием квалифицированных специалистов для выявления типовых угроз.

Актуальные киберугрозы в странах Ближнего Востока

Узнать больше об исследованиях Positive Technologies