Отчет SOC

по мониторингу информационной безопасности

за III квартал 2026 года

Содержание

03 ВВЕДЕНИЕ

03 ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

04 РЕЗУЛЬТАТ РАБОТЫ ЗА 3 КВАРТАЛ 2026 ГОДА

08 РЕЗЮМЕ

08 РЕКОМЕНДАЦИИ

10 О КОМПАНИИ

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

Введение

В данном отчёте приведена статистика по компьютерным инцидентам, выявленным командой Центра мониторинга компьютерных атак АО «ПМ» за 3 квартал 2026 года, а также рекомендации по повышению защищённости инфраструктуры.

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ:

ПО – программное обеспечение

ВПО – вредоносное программное обеспечение

КИ – компьютерный инцидент

КА – компьютерная атака

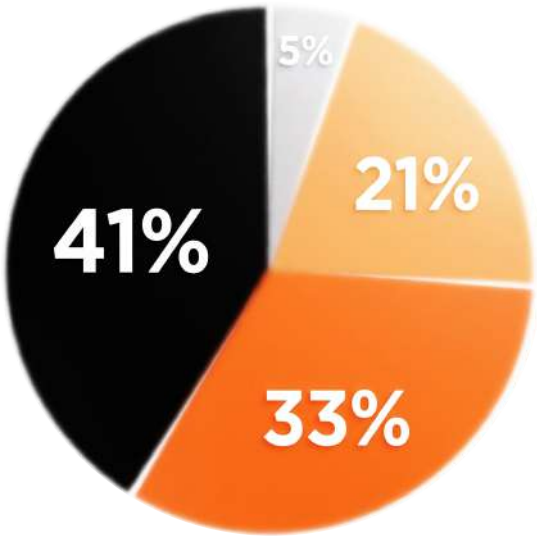
ИБ – информационная безопасность

РЕЗУЛЬТАТ РАБОТЫ ЗА 3 КВАРТАЛ 2026 ГОДА

Фиксируется снижение числа КИ: низкого уровня критичности — на 5 %, высокого уровня критичности — на 4 %, а также событий критического уровня — на 1 %. Вместе с тем фиксируется рост на 10 % числа инцидентов среднего уровня критичности.

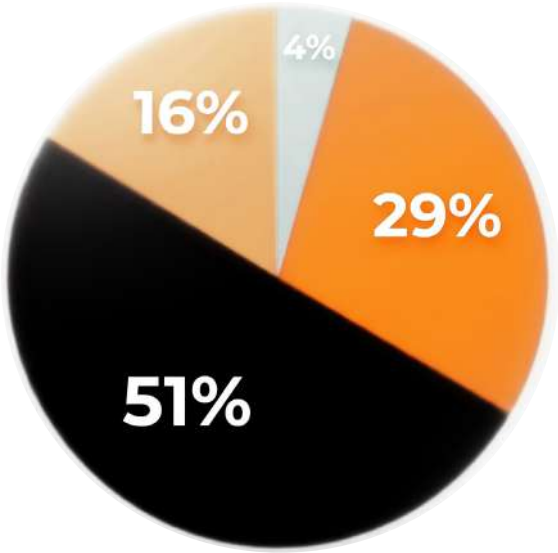
Классификация КИ по уровням критичности
во 2 квартале 2026 года

- Критический уровень
- Высокий уровень
- Средний уровень
- Низкий уровень



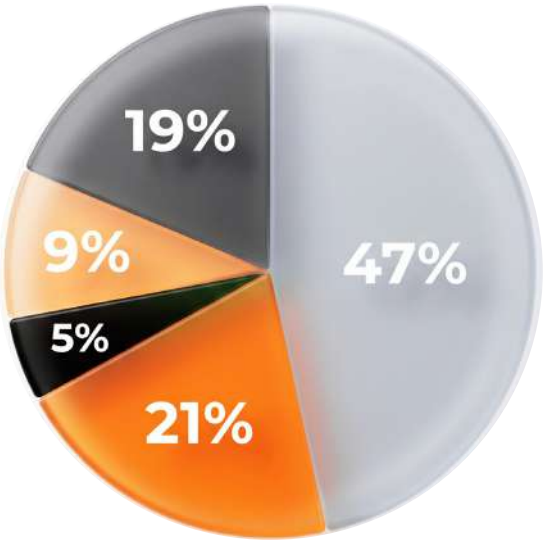
Классификация КИ по уровням критичности
в 3 квартале 2026 года

- Критический уровень
- Высокий уровень
- Средний уровень
- Низкий уровень



КЛАССИФИКАЦИЯ ПО ТИПАМ КИ:

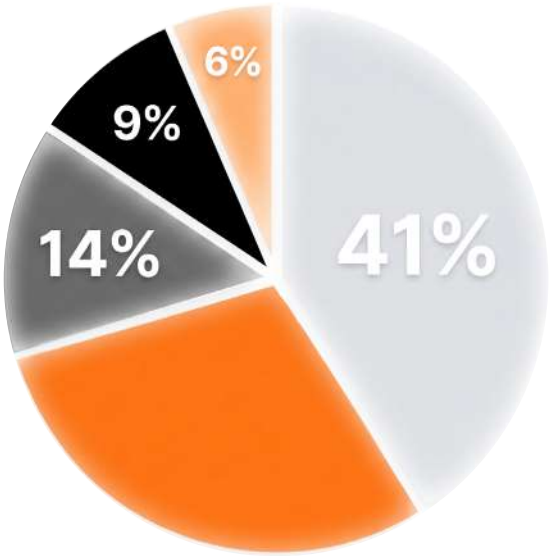
При анализе распределения КИ по времени суток во втором квартале 2026 года количество КИ, совершённых в дневное время, фиксировалось в 87 % случаев, а в третьем квартале 2026 года отмечается снижение этого показателя до 84 %.



Классификация по типам КИ

во 2 квартале 2026 года

- Заражение ВПО
- Попытки эксплуатации уязвимости
- Сетевое сканирование
- Нарушение политик ИБ
- Иные



Классификация по типам КИ

в 3 квартале 2026 года

- Заражение ВПО
- Попытки эксплуатации уязвимости
- Сетевое сканирование
- Нарушение политик ИБ
- Иные

В третьем квартале 2026 года отмечается снижение числа КИ, связанных с заражением ВПО (–6 %), нарушением политик ИБ (–3 %), а также иных КИ (–5 %). Вместе с тем отмечается значительный рост числа попыток эксплуатации уязвимостей (+8 %), а также сетевого сканирования (+4 %).

В течение 2026 года специалисты SOC ПМ фиксируют стабильный рост числа попыток эксплуатации уязвимостей ПО. Перечисленные ниже уязвимости объединяет угроза компрометации веб-приложений и обеспечивающей их работу ИТ-инфраструктуры: от обхода контроля доступа и хищения конфиденциальных данных до выполнения произвольного кода на сервере.

НАИБОЛЕЕ ЧАСТО ЭКСПЛУАТИРУЕМЫЕ УЯЗВИМОСТИ В 3 КВАРТАЛЕ:

CVE-2025-55182 — (React2Shell) React Server Components (8 %)

CVE-2025-29927 — Next.js (10 %)

CVE-2025-30208 — сервер разработки Vite (5 %)

CVE-2026-4020 — плагин Gravity SMTP для WordPress (3 %)

CVE-2026-63030 — (wp2shell) ядро WordPress (5 %)

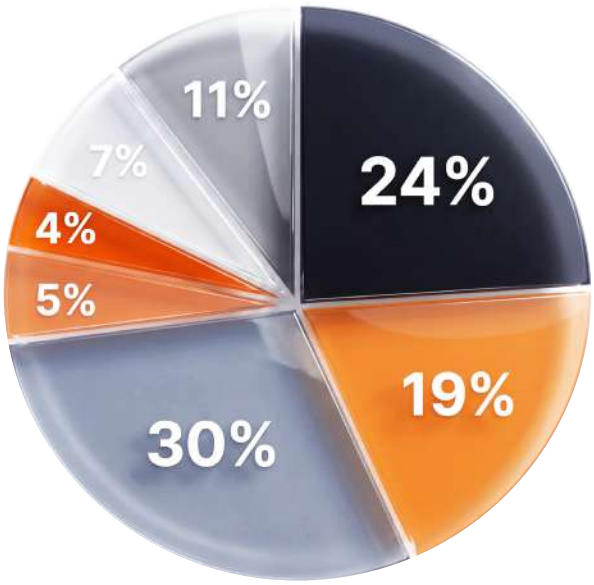
PHP-ИНЪЕКЦИИ (3 %)

SQL-ИНЪЕКЦИИ (3 %)

Показательно, что ¼ всех уязвимостей относится к 2025 году. Эти данные подтверждают важность своевременного обновления ПО (процесса патч-менеджмента), периодического аудита ИТ-инфраструктуры, а также проактивного поиска угроз и формирования правил их обнаружения.

Благодаря своевременному обновлению ПО заказчиков заметно снизилось число фиксируемых во втором квартале попыток эксплуатации уязвимостей **CMS Bitrix и CVE-2026-48907** (уязвимость в расширении Joomla Content Editor (JCE)).

Среди КИ с использованием ВПО в третьем квартале 2026 года превалируют случаи обнаружения майнеров криптовалюты (24 %), программ-вымогателей (19 %), троянских программ (30 %), червей (4 %), дропперов (7 %) и стиллеров (5 %).

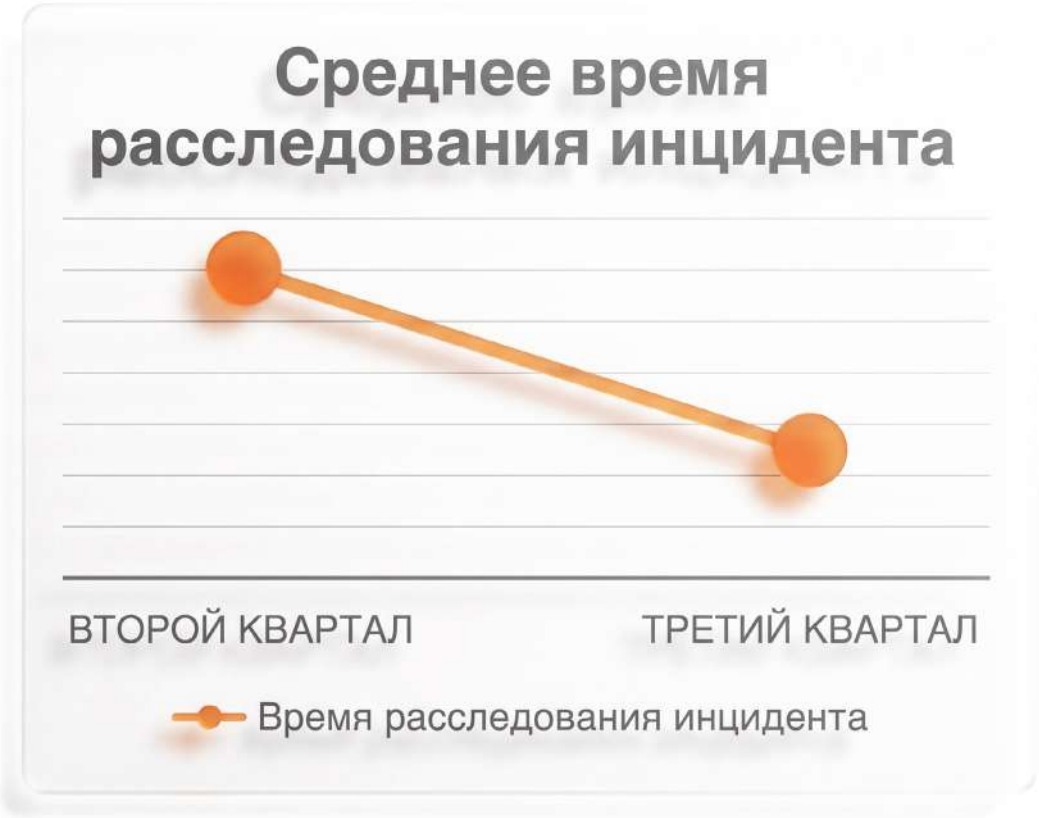


Классификация КИ по типам ВПО

во 2 квартале 2026 года

- Майнеры криптовалюты (24%)
- Троянские программы (30%)
- Черви (4%)
- Иные (11%)
- программы-вымогатели (19%)
- Стиллеры (5%)
- Дропперы (7%)

Среднее время расследования инцидентов в третьем квартале 2026 года снизилось по сравнению с предыдущим кварталом на 58 % благодаря эффективному взаимодействию заказчиков с SOC ПМ и своевременному выполнению рекомендаций по повышению безопасности инфраструктуры.



РЕЗЮМЕ:

- Наибольшее число КИ происходит в дневное время суток по часовому поясу заказчика.
- Наблюдается снижение числа КИ низкого и высокого уровней критичности, а также критических событий при росте числа инцидентов среднего уровня критичности.
- Отмечается снижение среднего времени расследования КИ на 58 %.
- Отмечается сохранение тенденции к росту числа эксплуатаций уязвимостей с незначительным снижением числа внедрений ВПО.
- При попытках эксплуатации уязвимостей злоумышленники продолжают искать и эксплуатировать всё более новые уязвимости.

РЕКОМЕНДАЦИИ:

На основе анализа текущих угроз (подробная информация об актуальных видах компьютерных угроз доступна на сайте ПМ), статистики инцидентов и оценки наиболее актуальных сценариев атак команда SOC ПМ предлагает реализовать следующие меры для повышения защищённости ИТ-инфраструктуры:

- Расширять количество средств обнаружения аномального поведения пользователей и систем, которое не поддаётся выявлению классическими сигнатурными методами.
- На регулярной основе повышать осведомлённость сотрудников в области информационной безопасности, включая безопасную работу с электронной почтой и вложениями.
- В целях защиты от кибератак, эксплуатирующих программные уязвимости, своевременно обновлять всё используемое ПО, а также периодически проверять настройки конфигурации и усиливать безопасность веб-приложений.
- Для предотвращения компьютерных атак рекомендуется использовать базу решающих правил для сетевых и хостовых средств AM Rules. В части сигнатурного анализа данная база обеспечивает надёжное и точное обнаружение вредоносной активности на всех этапах компьютерной атаки — от проникновения до попыток эксплуатации уязвимостей (в том числе CVE-2025-55182, CVE-2025-29927, CVE-2025-30208 и других), также действий хакерских группировок.

РЕКОМЕНДАЦИИ ПО ЗАКРЫТИЮ ПОПУЛЯРНЫХ ЭКСПЛУАТИРУЕМЫХ УЯЗВИМОСТЕЙ:

Для закрытия уязвимости CVE-2025-55182 рекомендуется выполнить обновление компонентов:

1) react-server-dom-webpack до версии не ниже 19.2.4.
2) react-server-dom-parcel до версии не ниже 19.2.4.
3) react-server-dom-turbopack до версии не ниже 19.2.4.

Для закрытия уязвимости CVE-2025-29927
требуется обновление компонента Next.js до версий:

13.x до 13.5.9;
14.x до 14.2.25;
15.x до 15.2.3.

Для закрытия уязвимости CVE-2025-30208
требуется обновить компонент Vite до версий не ниже:

4.x до 4.5.10;
5.x до 5.4.15;
6.0.x до 6.0.12;
6.1.x до 6.1.2;
6.2.x до 6.2.3.

Для закрытия уязвимости CVE-2026-4020 требуется обновление компонента Gravity SMTP для WordPress до версии не ниже 2.1.5.

Для закрытия уязвимости CVE-2026-63030
требуется обновить ядро WordPress до версий:

6.9.x до 6.9.5;
7.0.x до 7.0.2.

Для закрытия возможных PHP и SQL-инъекций рекомендуется проводить регулярное обновление модулей до последней версии.

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

О КОМПАНИИ

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

«Перспективный мониторинг» — один из лидеров российского рынка коммерческих SOC и Центров ГосСОПКА, исследований защищённости и расследования инцидентов, а также разработчик собственных продуктов в области информационной безопасности: киберполигон Ampire, веб-сервис поставки экспертных данных об угрозах AM Threat Intelligence Portal, база решающих правил AM Rules, система защиты веб-ресурсов от компьютерных атак AML Web Protection.

В штате компании более 150 технических специалистов: аналитиков, реверс-инженеров, экспертов-исследователей, специалистов по тестированиям на проникновение, компьютерных криминалистов.

amonitoring.ru

