SOLAR

ОТЧЕТ

# АТАКИ НА РОССИЙСКИЕ КОМПАНИИ В III КВАРТАЛЕ 2023 ГОДА

W: RT-SOLAR.RU

W: RT.RU

МОСКВА 2023

# СОДЕРЖАНИЕ


О компании 3

Введение 4

Сводная статистика по инцидентам 5

Выводы по III кварталу 11

Контакты 12

# О КОМПАНИИ

Группа компаний «Солар» — ведущий поставщик ИБ-решений в России, архитектор комплексной кибербезопасности. Ключевые направления деятельности — аутсорсинг ИБ, разработка собственных продуктов, обучение ИБ-специалистов, аналитика и исследование киберинцидентов.

С 2015 года предоставляет ИБ-решения организациям от малого бизнеса до крупнейших предприятий ключевых отраслей.

Продукты и сервисы «Солара» объединены в домены экспертизы, которые закрывают все потребности заказчиков и включают собственные разработки, решения партнеров, услуги по созданию стратегии и архитектуры ИБ, консалтинг, обучение персонала.

Компания предлагает сервисы первого и крупнейшего в России коммерческого SOC — Solar JSOC, экосистему управляемых сервисов ИБ — Solar MSS. Линейка собственных продуктов включает DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, межсетевой экран нового поколения Solar NGFW, IdM-систему Solar inRights, PAM-систему Solar SafeInspect, анализатор кода Solar appScreener и другие.

ГК «Солар» развивает платформу для практической отработки навыков защиты от киберугроз «Солар Кибермир». Работа центра исследования киберугроз Solar 4RAYS нацелена на изучение тактик киберпреступников и обогащение решений данными при разработке.

СПИСОК СЕРВИСОВ SOLAR JSOC:

- Мониторинг и анализ инцидентов ИБ
- Мониторинг АСУ ТП
- Сервисы ГосСОПКА
- Защита конечных точек (EDR)
- Анализ сетевого трафика (NTA)
- Комплексный контроль защищенности
- Мониторинг внешних цифровых угроз (Aura)
- Управление процессами реагирования на киберинциденты (IRP)
- Экстренное реагирование на инциденты
- Построение SOC и консалтинг

## АРХИТЕКТОР КОМПЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ

**1800+**
экспертов по кибербезопасности

**850+**
организаций под защитой

**600+**
реализованных проектов в год

**180+** МЛРД
анализируемых событий ИБ в сутки

# ВВЕДЕНИЕ

В III квартале 2023 года количество кибератак продолжало расти, при этом наблюдалось существенное увеличение числа подтвержденных инцидентов ИБ. Основной целью злоумышленников все чаще становилось не нарушение работоспособности ресурсов или размещение манифестов провокативного характера, а проникновение в инфраструктуру, приводящее к деструктивным для нее последствиям с максимально длительным временем восстановления.

Вредоносное ПО в качестве инструмента кибератак усиливает позиции злоумышленников. Вектор проникновения продолжает смещаться с попыток эксплуатации уязвимостей на периметре и в веб-инфраструктуре в сторону атак на сотрудников компании — фишинговые письма все чаще используются как средство проникновения в инфраструктуру. При этом все большее число кибератак фиксируется только специальными сенсорами — EDR, NTA, Anti-APT, что говорит об усложнении техник и тактик хакеров.

В настоящем отчете приведены данные об инцидентах, выявленных командой Solar JSOC[1] в III квартале 2023 года, и их сравнение со статистикой предыдущих периодов. В исследовании отражена приоритизация инцидентов по степени критичности, а также процентное соотношение различных типов кибератак, которые наблюдались в отчетный период.

Хакеры тщательно готовятся к нанесению ударов и постоянно совершенствуют применяемые техники.

В фокус внимания экспертов попало более 300 компаний и организаций из разных отраслей экономики: госсектор, финансы, нефтегазовая отрасль, энергетика, телекоммуникации, крупный ретейл. Все компании представляют сегмент Large Enterprise и Enterprise с количеством сотрудников от 1000 человек, оказывают услуги в разных регионах страны и, как правило, являются крупнейшими в отрасли по своему региону или по стране в целом.

Совокупно в рамках оказания сервиса Solar JSOC обеспечивает контроль и выявление инцидентов для:

- более 3500 внешних сервисов, опубликованных в интернете,
- более 175 тыс. серверов общего, инфраструктурного и прикладного назначения.

[1] В отчет вошли агрегированные данные об атаках на компании, подключенные к сервису мониторинга киберинцидентов Solar JSOC. Аналитика не учитывает информацию о клиентах управляемых сервисов кибербезопасности Solar MSS (включая магистральный Anti-DDoS и WAF), результаты услуг по расследованию киберинцидентов и данные с сенсоров и ханипотов на сети «Ростелекома».

# СВОДНАЯ СТАТИСТИКА ПО ИНЦИДЕНТАМ

396 тысяч событий ИБ — подозрений на инцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний — было выявлено за отчетный период

на 22%

больше, чем во II квартале 2023 года

на 85%

больше, чем в III квартале 2022 года

10,2 тысячи подтвержденных инцидентов

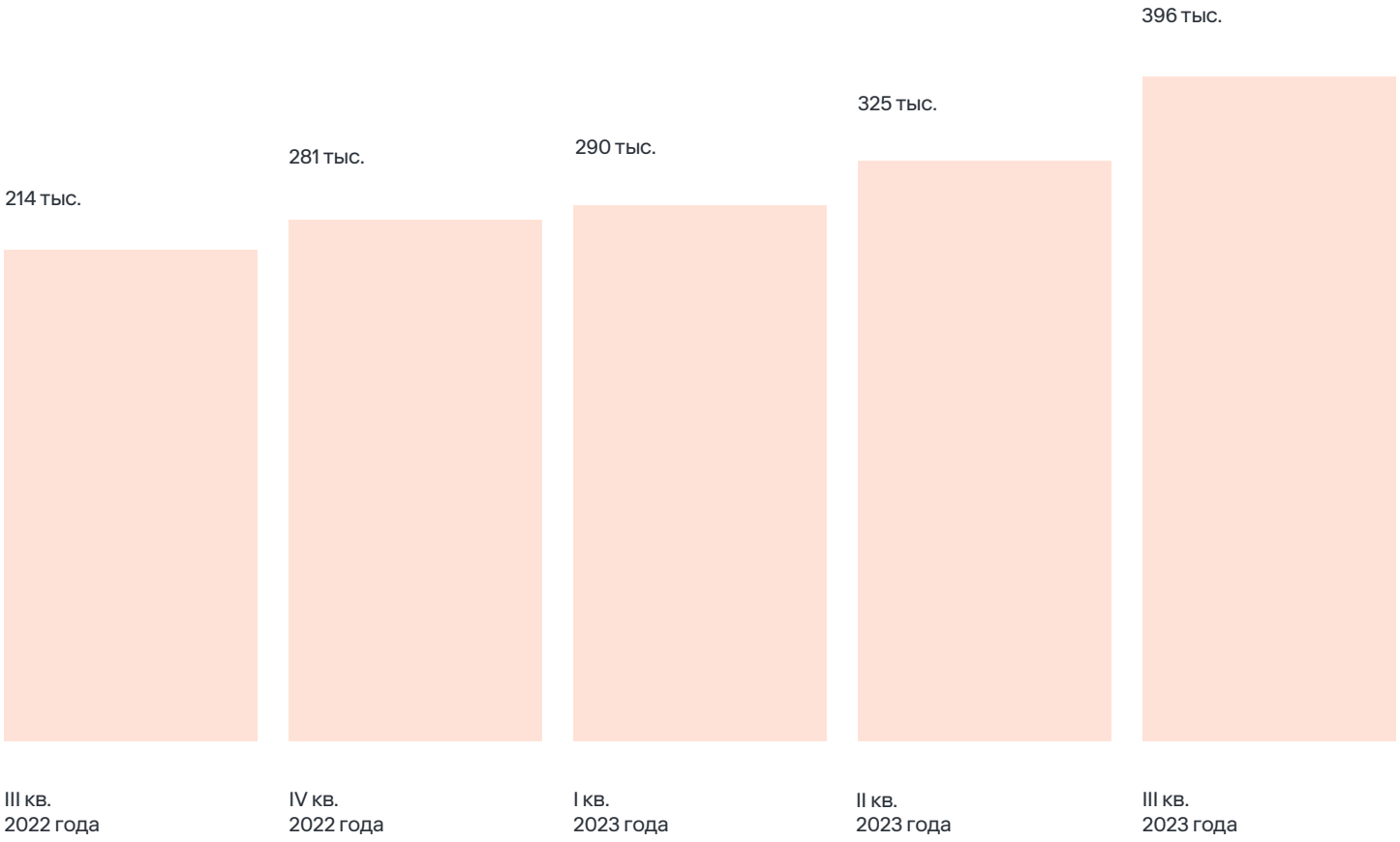
на 16%

больше, чем во II квартале 2023 года

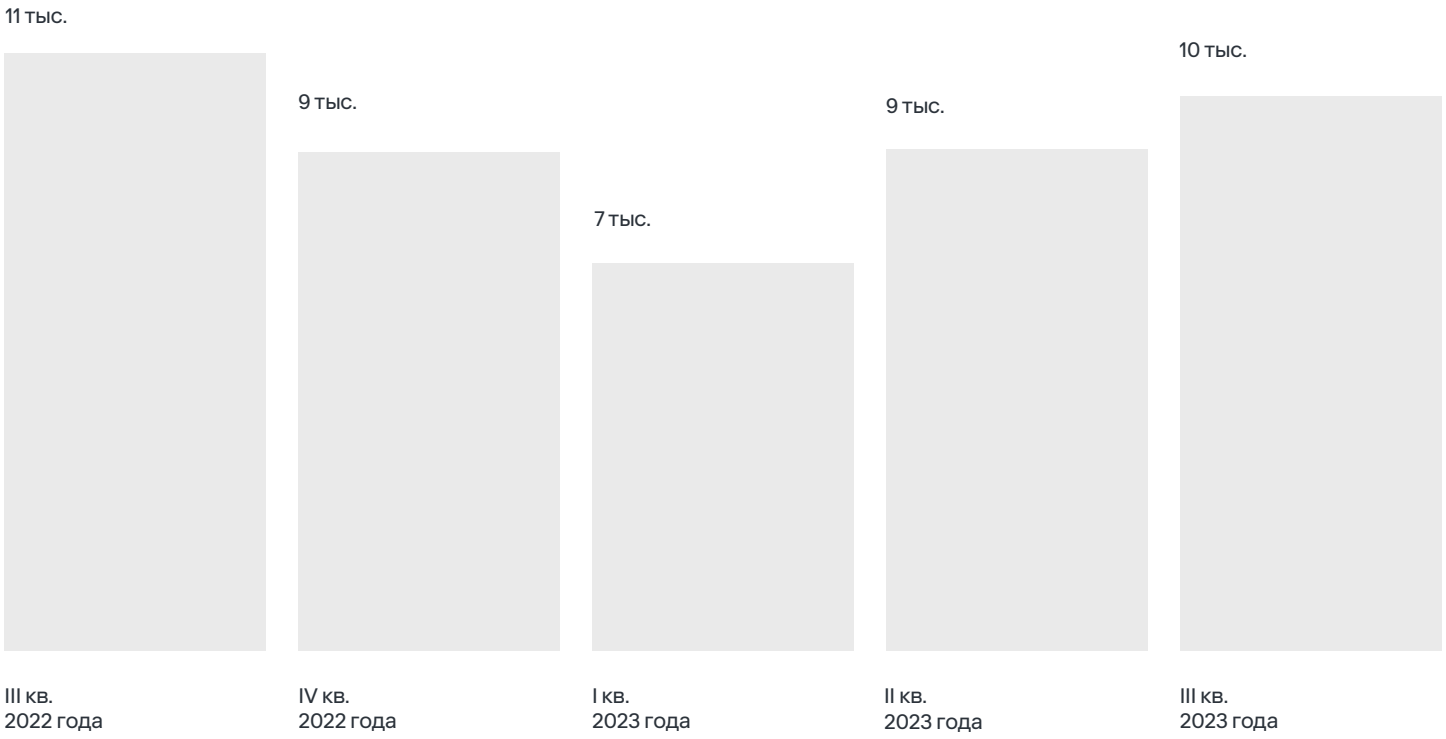
на 9%

меньше, чем в III квартале 2022 года

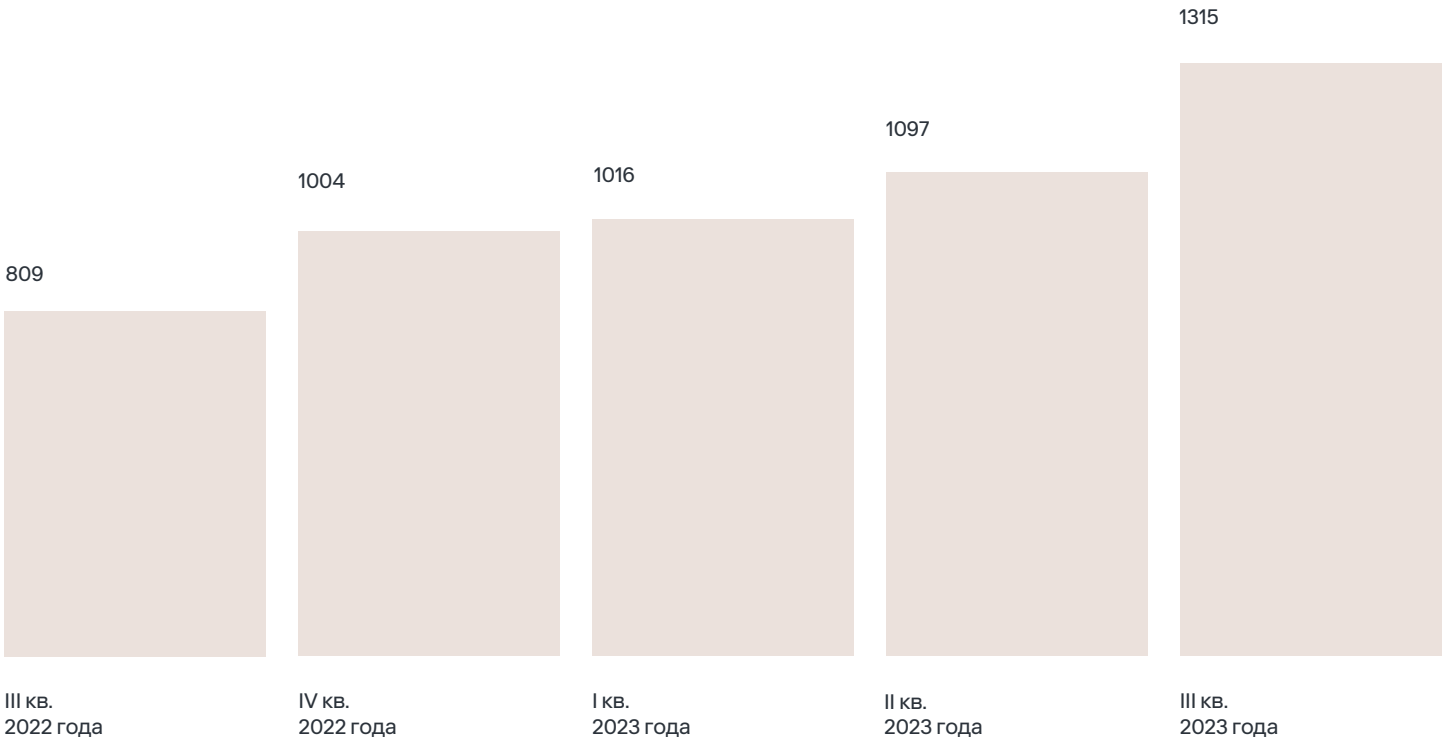
## РАСПРЕДЕЛЕНИЕ СОБЫТИЙ ИБ ПО КВАРТАЛАМ



## ПОДТВЕРЖДЕННЫЕ ИБ-ИНЦИДЕНТЫ




## СРЕДНЕЕ КОЛИЧЕСТВО ПОДОЗРЕНИЙ НА ИНЦИДЕНТЫ НА ОДНОГО ЗАКАЗЧИКА

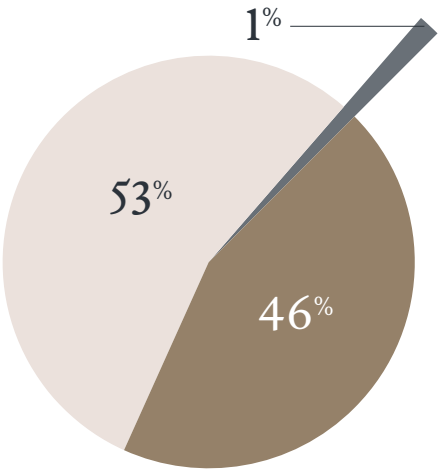


Наметившаяся с начала года тенденция на рост числа событий ИБ сохранилась и в третьем квартале: если во втором квартале по сравнению с первым рост составил 12%, то в третьем по сравнению со вторым коэффициент прироста увеличился практически в 2 раза. Также мы наблюдаем существенное увеличение числа подтвержденных инцидентов ИБ, о чем свидетельствует 20-процентный рост среднего значения по заказчикам всех подозрений на инциденты по сравнению со II кварталом 2023 года. Это говорит о том, что число событий ИБ в отношении каждой компании значительно возросло.

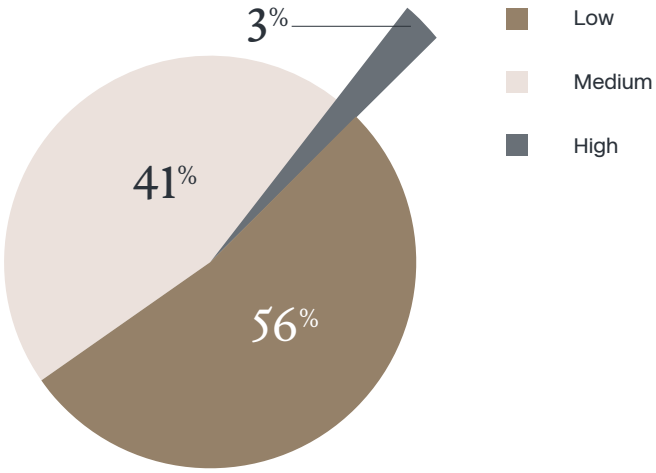
Подтверждаются ранее выдвинутые нами тезисы об усложнении атак и повышении квалификации злоумышленников с целью деструктивного воздействия на российские компании.

## РАСПРЕДЕЛЕНИЕ ИНЦИДЕНТОВ ПО УРОВНЮ КРИТИЧНОСТИ

### II квартал 2023




### III квартал 2023



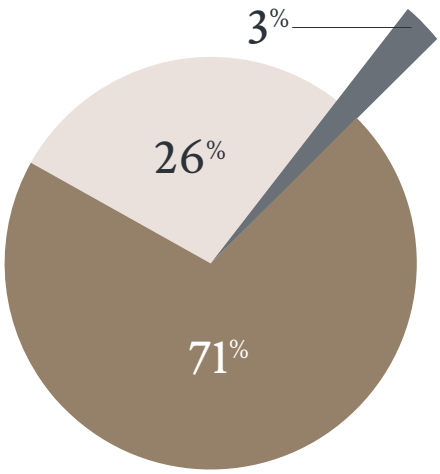

В целом резкого изменения соотношения инцидентов по уровню критичности за прошедший период мы не наблюдаем — показатели колеблются в характерном для II квартала диапазоне. Однако стоит обратить внимание, что число самих критических инцидентов возросло, хотя во II квартале 2023 года злоумышленники сделали акцент на более простые массовые атаки.

Также в прошлом году было «летнее затишье», когда в третьем квартале 2022 года снизилось число всех событий ИБ — в этом году такого спада не наблюдается.

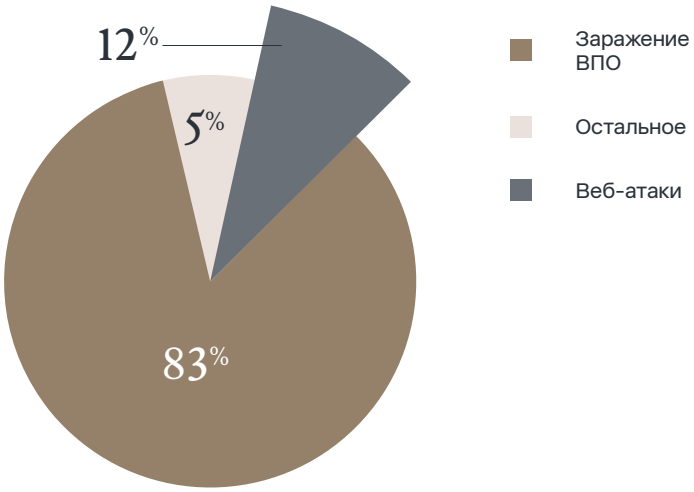
Увеличение в отчетном периоде числа событий ИБ и подтвержденных инцидентов, включая критические, указывает на то, что хакеры снова более тщательно готовятся к нанесению ударов и совершенствуют применяемые техники.

## РАСПРЕДЕЛЕНИЕ ВЫСОКОКРИТИЧНЫХ ИНЦИДЕНТОВ ПО КАТЕГОРИЯМ

II квартал 2023




III квартал 2023




Как и в предыдущие периоды, применение ВПО остается наиболее часто используемым хакерами инструментом, что приводит к наступлению критических инцидентов. Доля подобных атак продолжает расти, стремясь к 100%. Их основной вектор — фишинговые письма с фокусом на персонал компаний, которые составляют 2/3 от других способов доставки вредоносного софта. При этом фишинговые рассылки становятся все более опасными, поэтому критичность таких инцидентов возрастает, а универсального метода противодействия не существует. Потоковые антивирусы не решают проблему, а пользователи повышают свою киберграмотность слишком медленными темпами. Хостовые антивирусы могут фиксировать активность слишком поздно, а проникновение на российский рынок решений класса Sandbox, которые могли бы исправить ситуацию, на данный момент невелико.

Примечательно, что число веб-атак, резко сократившееся во II квартале (на 21%), в отчетном периоде снова продемонстрировало положительную динамику.

Это означает, что онлайн-ресурсы по-прежнему остаются довольно уязвимым местом в инфраструктуре и поэтому требуют пристального внимания. При этом рост веб-атак обусловлен в том числе событийными атаками. Например, хакеры фокусируются на системах по продаже проездных билетов в период отпусков в августе, порталах политических мероприятий (ПМЭФ, «Россия-Африка») в момент их проведения и ретейле в преддверии 1 сентября.

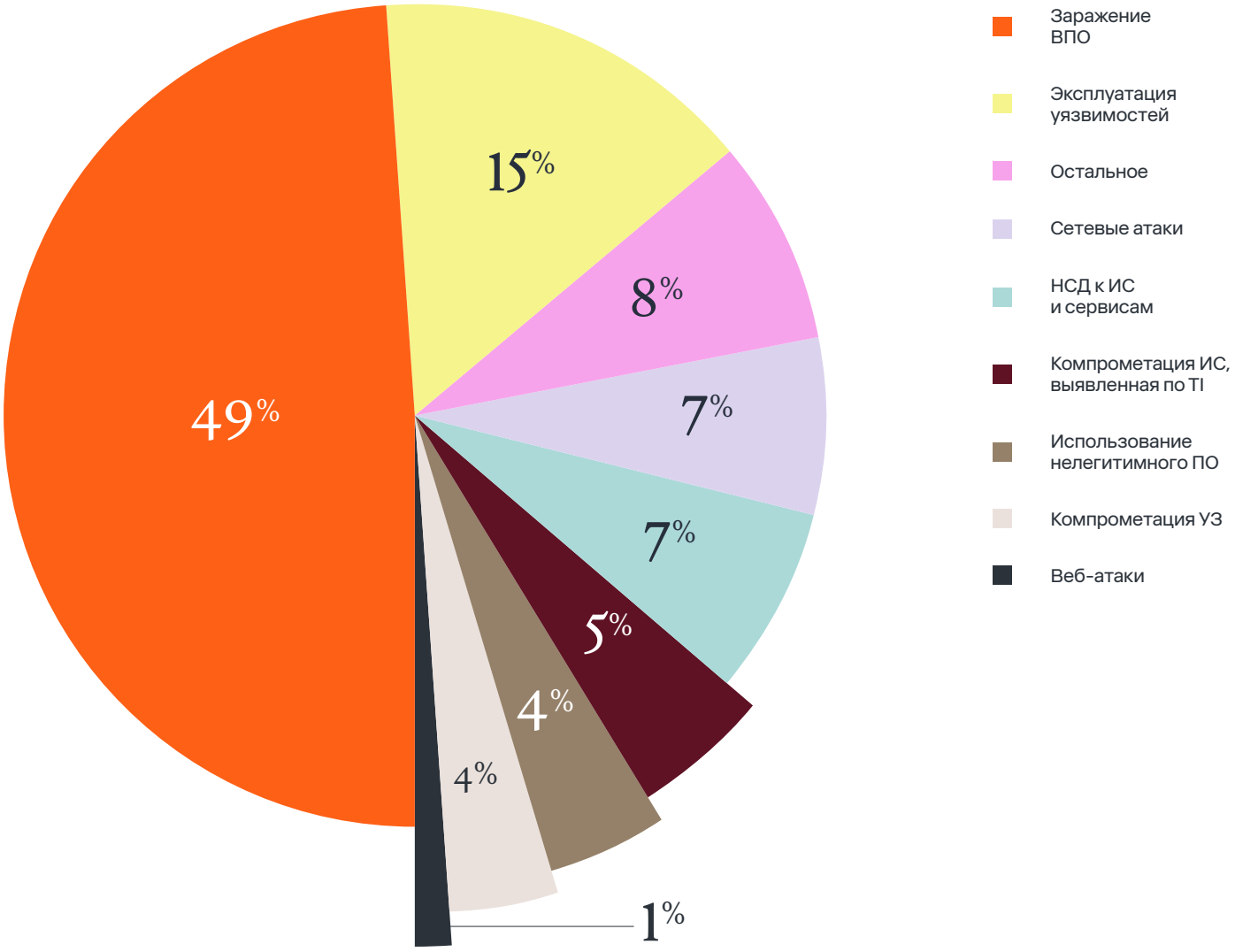
**1,5**

последних года нагрузка на отечественные ресурсы выросла, а сайты и приложения периодически требуют доработок и обновлений, из-за отсутствия которых могут образовываться различные «дыры» в безопасности.

Владельцам бизнеса, ведущим свою деятельность в интернете, следует обратить на это внимание, так как IV квартал традиционно сопровождается ростом веб-атак.

## РАСПРЕДЕЛЕНИЕ ВСЕГО ОБЪЕМА ИНЦИДЕНТОВ ПО КАТЕГОРИЯМ

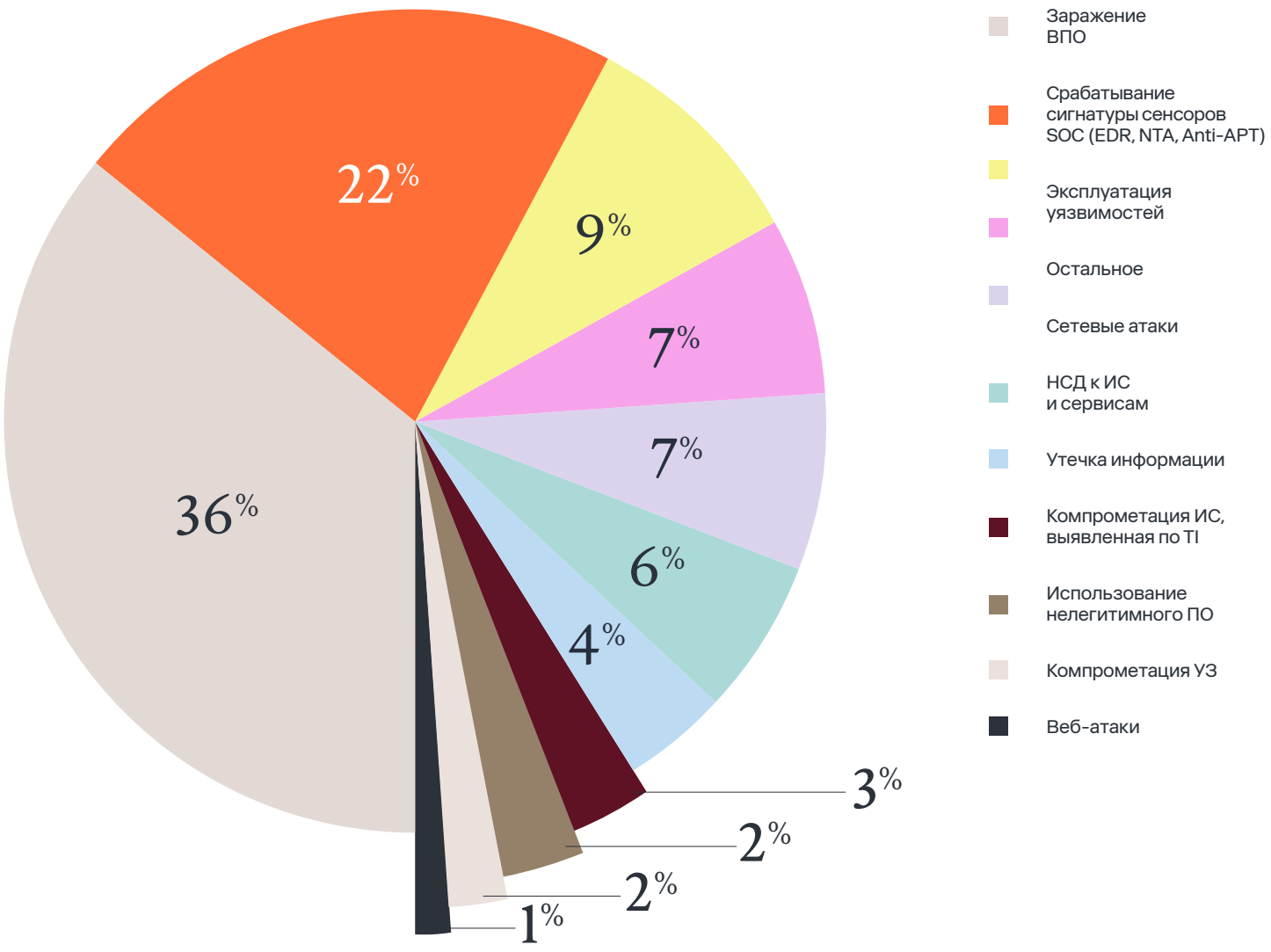
II квартал 2023




В сравнении со II кварталом 2023 года доля инцидентов, связанных с эксплуатацией уязвимостей, увеличилась в два раза. При этом количество инцидентов, вызванных срабатыванием сигнатур на сенсорах SOC (EDR, NTA, Anti-APT), выросло настолько существенно, что с этого периода мы выделяем их в отдельную категорию, которую будем анализировать в последующих отчетах. Рост объясняется как увеличением доли клиентов, использующих сервисы EDR и NTA в качестве дополнения к базовому SOC, так и в целом повышением интереса к данным направлениям из-за усложнения кибератак и роста активности продвинутых злоумышленников.

## РАСПРЕДЕЛЕНИЕ ВСЕГО ОБЪЕМА ИНЦИДЕНТОВ ПО КАТЕГОРИЯМ

III квартал 2023




Детектирование подобными средствами следует отделять от тех, что фиксируются антивирусом, IPS, WAF и другими средствами защиты, так как это напрямую указывает на повышение активности злоумышленников с целью проникновения и закрепления в инфраструктуре компаний, в том числе с использованием инструментария, не определяемого антивирусным ПО, — PowerShell-скриптов, легитимных утилит, ВПО, выполняемых в памяти.

Несмотря на повышение внимания к фишинговым атакам, злоумышленники с новой силой стали проводить и сетевые атаки.

Сетевые атаки не влекут за собой критических последствий благодаря повышению защищенности периметров и понимания порядка противодействия таким инцидентам на периметре организаций.

# ВЫВОДЫ ПО III КВАРТАЛУ

01

Общее число инцидентов продолжает расти. Значительную часть киберландшафта по-прежнему формируют инциденты низкой и средней степени критичности, однако за отчетный период число критических инцидентов несколько возросло. III квартал текущего года стал примечателен тем, что не было спада ИБ-событий, характерного для летнего периода. Мы прогнозируем, что в ближайшее время тренд на рост числа событий ИБ и подтвержденных инцидентов сохранится.

02

Кибератаки с использованием вредоносного ПО продолжают наращивать обороты, в III квартале их доля составила 83% от всех критических инцидентов. Основным каналом доставки ВПО являются фишинговые письма, применяемые в 2/3 подобных атак. Этот вектор продолжит набирать популярность, так как он направлен на самое уязвимое звено в защищенности компаний — персонал. На фоне того, что злоумышленники все чаще применяют ВПО, не детектируемое базовыми средствами, потребность в усилении защиты конечных узлов становится все более острой и актуальной — именно поэтому мы продолжаем наблюдать рост спроса на сервисы SOC с расширениями в части хостового и сетевого детекта (EDR и NTA).

03

Повышение интереса компаний к сетевым и хостовым сенсорам неслучайно: злоумышленники все чаще используют различные техники и тактики для скрытного проникновения и продвижения по инфраструктуре компании в попытке нанести ей максимальный урон. Хостовые сенсоры также позволяют минимизировать время детектирования сложных фишинговых атак с шифровальщиком во вложении писем, а следовательно, и урон от них.

04

Онлайн-ресурсы неизменно остаются одной из основных целей кибератак на компании, но конечные цели злоумышленников меняются. Согласно нашей статистике расследований, все чаще ключевым мотивом злоумышленников становится не дефейс, а проникновение в инфраструктуру или попытка хищения данных клиентов компаний.

SOLAR

W: RT-SOLAR.RU
W: RT.RU

T +7 (499) 755-07-70
E solar@rt-solar.ru

Центральный офис, 125009, Москва
Никитский переулок, 7с1