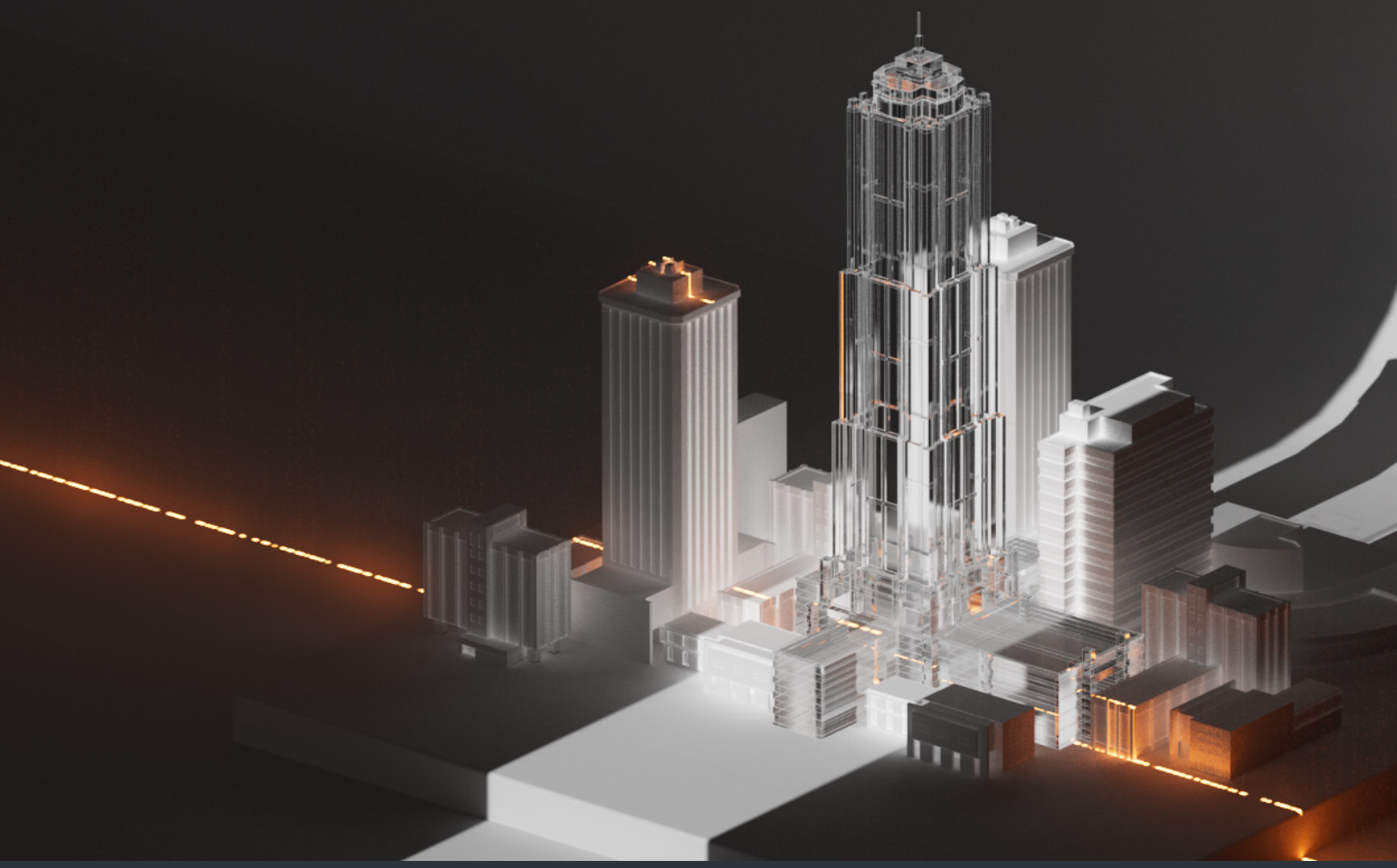
SOLAR

ОТЧЕТ



КИБЕРАТАКИ НА РОССИЙСКИЕ КОМПАНИИ В 2023 ГОДУ

W: RT-SOLAR.RU

МОСКВА 2024

СОДЕРЖАНИЕ

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

2000+
экспертов
по кибербезопасности

850+
организаций
под защитой

600+
реализованных
проектов в год

180+ МЛРД
анализируемых
событий ИБ в сутки

АРХИТЕКТОР КОМПЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ

ВВЕДЕНИЕ

В 2023 году фоновый шум ИБ-событий постоянно рос. При этом атаки хакеров стали более целенаправленными и сложными, а инструментарий – более продвинутым. Вредоносное ПО осталось наиболее популярным инструментом злоумышленников, но при этом они стали чаще использовать легитимные утилиты типа not-a-virus и нелегитимное ПО для закрепления и продвижения в инфраструктуре, а также вернулись к эксплуатации уязвимостей на периметре компаний. К концу года также выросло число кибератак, фиксируемых только специализированными сенсорами – EDR, NTA, AntiAPT, что дополнительно говорит об усложнении атак.

В настоящем отчете приведены данные об инцидентах, выявленных командой центра противодействия кибератакам Solar JSOC в IV квартале 2023 года, и их сравнение со статистикой предыдущих периодов. Также представлены общие выводы по итогам 2023 года. В исследовании отражена приоритизация инцидентов по степени критичности и процентное соотношение различных типов кибератак, которые наблюдались в отчетный период.

В фокус внимания экспертов попало около 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:

3600+

внешних сервисов, опубликованных в интернете

178+ 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.

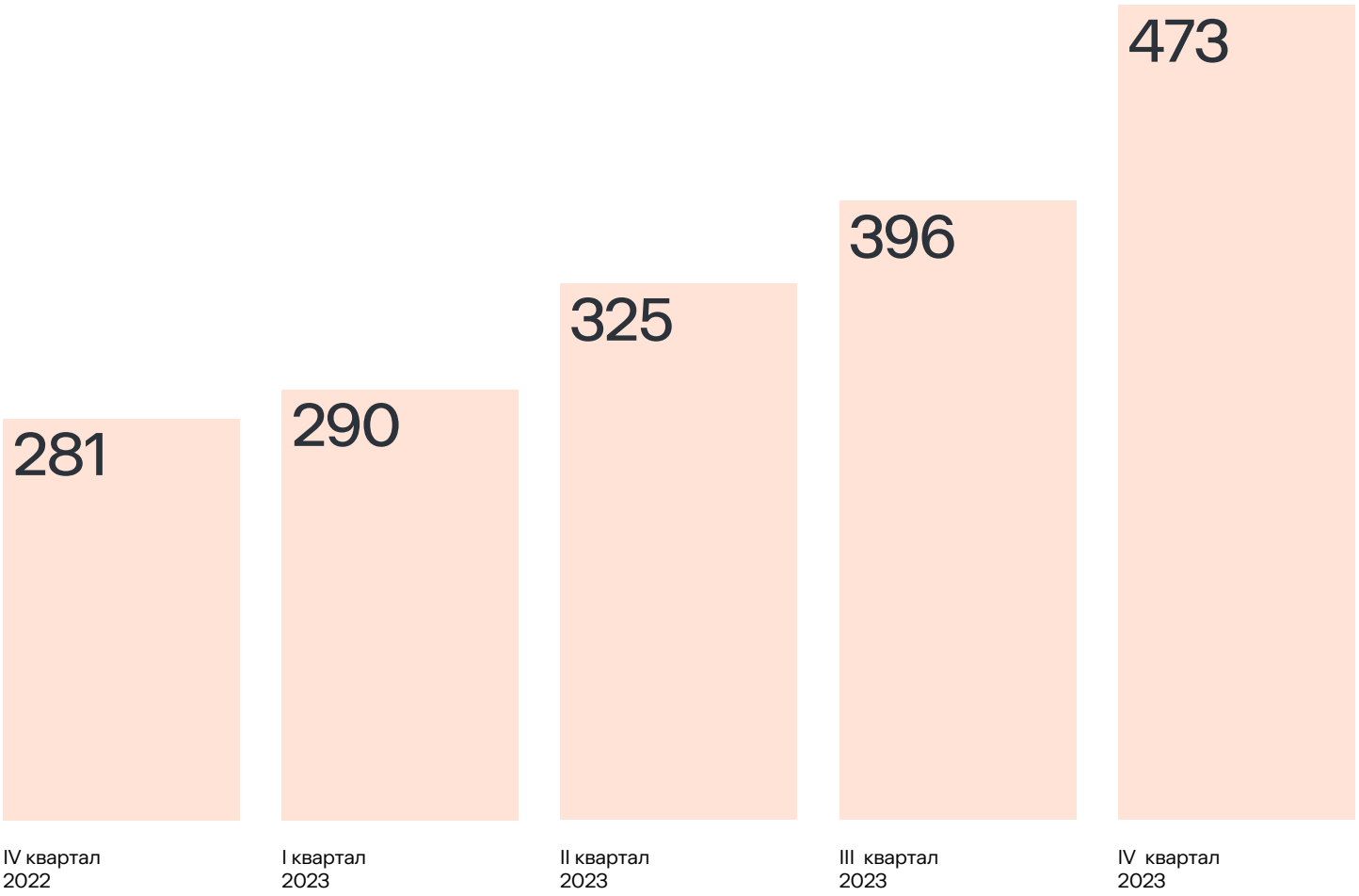
СВОДНАЯ СТАТИСТИКА ПО ИНЦИДЕНТАМ ЗА IV КВАРТАЛ

В октябре-декабре 2023 года было выявлено 473 тыс. событий ИБ – подозрений на инцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний. Это на 20% больше, чем в предыдущем квартале, и на 68% больше показателя IV квартала 2022 года. Рост событий ИБ в разрезе одной компании в IV квартале, по сравнению с предыдущим составляет 18%, а год к году – 55%. При этом количество подтвержденных заказчиками инцидентов в IV квартале в сравнении с III кварталом 2023 года показало падение почти в два раза – до 5,7 тысячи инцидентов. Таким образом, в IV квартале на одну компанию приходилось 19 инцидентов, тогда как в III квартале 2023 года данный показатель составлял 34 инцидента.

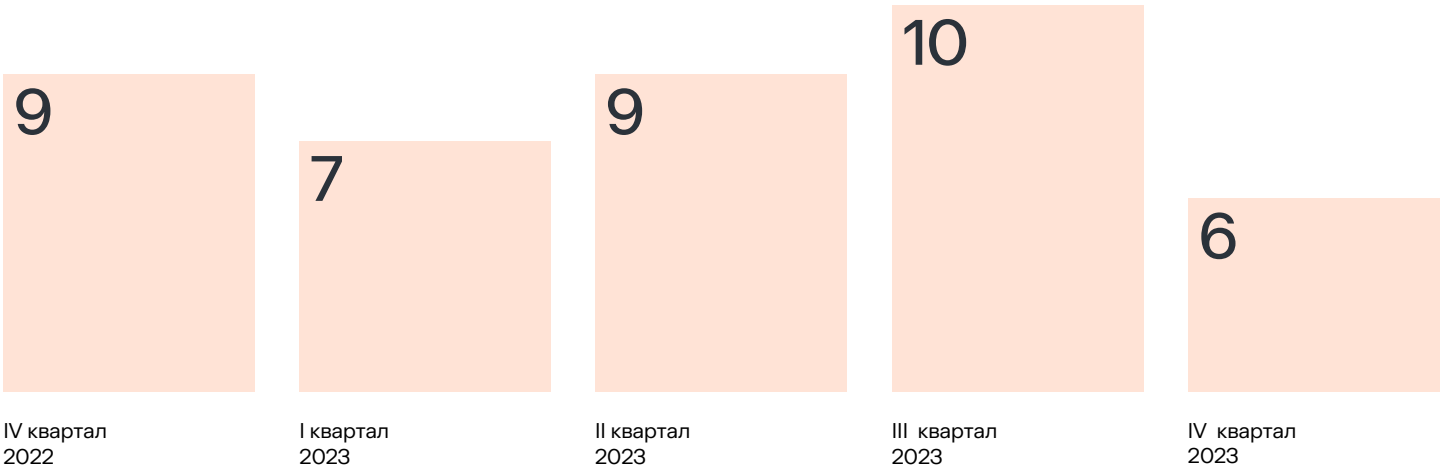
473 ТЫС.

События ИБ – подозрений на инцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний – было выявлено в октябре-декабре 2023 года.

Распределение событий ИБ по кварталам, тыс. штук



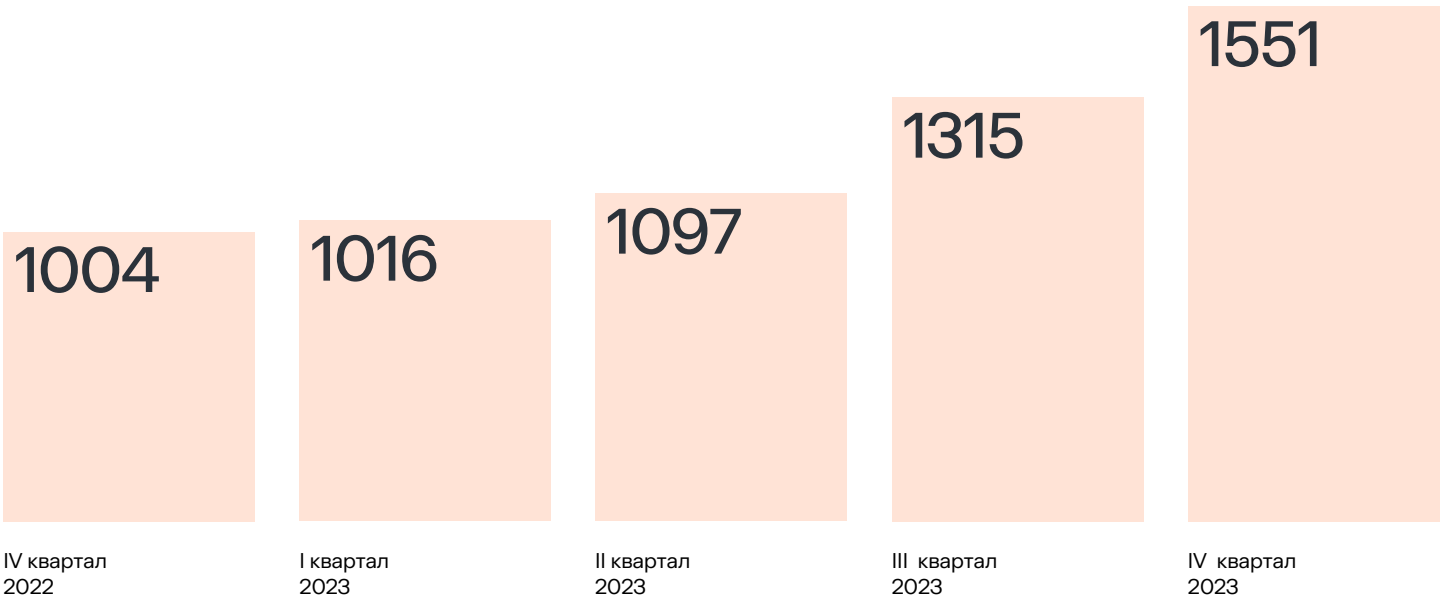
Подтвержденные
ИБ-инциденты, тыс. штук



В целом картина говорит о росте «фонового шума» подозрений на инциденты – их количество постоянно увеличивается в связи с продолжающейся цифровизацией бизнеса и повышением количества информационных систем в компаниях практически всех отраслей. При этом доля подтвержденных инцидентов в среднем не превышает 2% – показатели остаются стабильными, но опасность таких инцидентов также растет в первую очередь за счет роста квалификации злоумышленников.

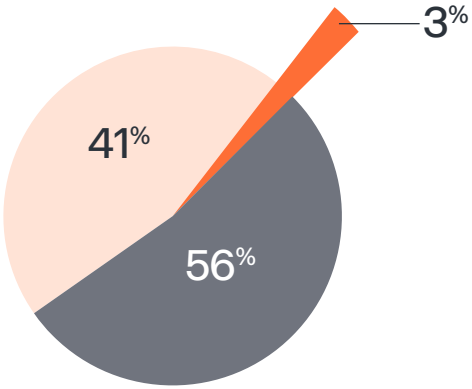
В связи с общим ростом событий ИБ мы рекомендуем командам SOC и ИБ-специалистам заказчиков грамотно приоритизировать те инциденты, которые являются действительно важными для оперативного реагирования и снижения негативных последствий от возможных кибератак. Достичь этого можно путем построения правильных скоринг-систем и выстраивания инцидентов в kill-chain.

Среднее количество подозрений
на инциденты на одного заказчика

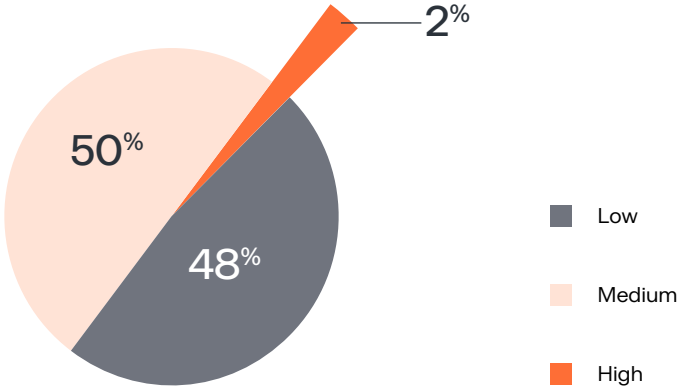


Распределение инцидентов по уровню критичности

III квартал 2023



IV квартал 2023



Распределение инцидентов по уровню критичности остается неизменным на протяжении длительного периода времени, и переориентации в киберландшафте не наблюдается. Доля критических инцидентов остается в допустимых пределах от 1 до 3%.

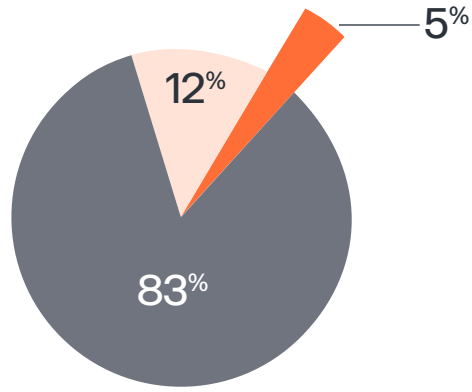
Обратим внимание на то, что, несмотря на общий рост количества ИБ-событий, число высококритичных инцидентов сохраняется на стабильном уровне.

Это означает, что удары хакеров становятся более точечными и адресными, а инструментарий – все более продвинутым. Злоумышленники все чаще действуют скрытно на всех этапах атаки – от начального этапа разведки и проникновения до перемещения и закрепления в инфраструктурах компаний. Квалификация встречаемых нами хакеров все чаще соответствует третьему и четвертому уровню нарушителей.

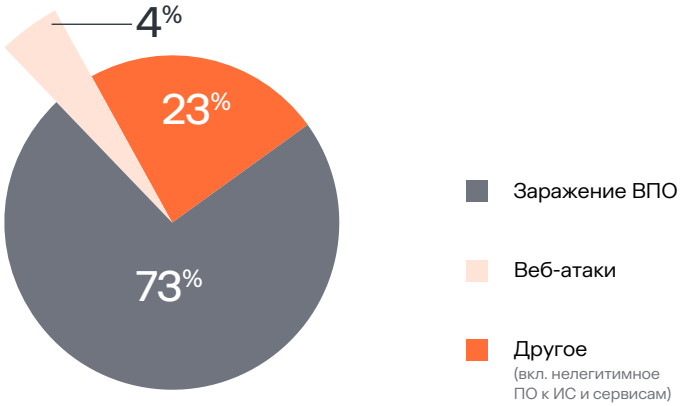
Читать об уровнях злоумышленников

Распределение высококритичных инцидентов по категориям

III квартал 2023



IV квартал 2023

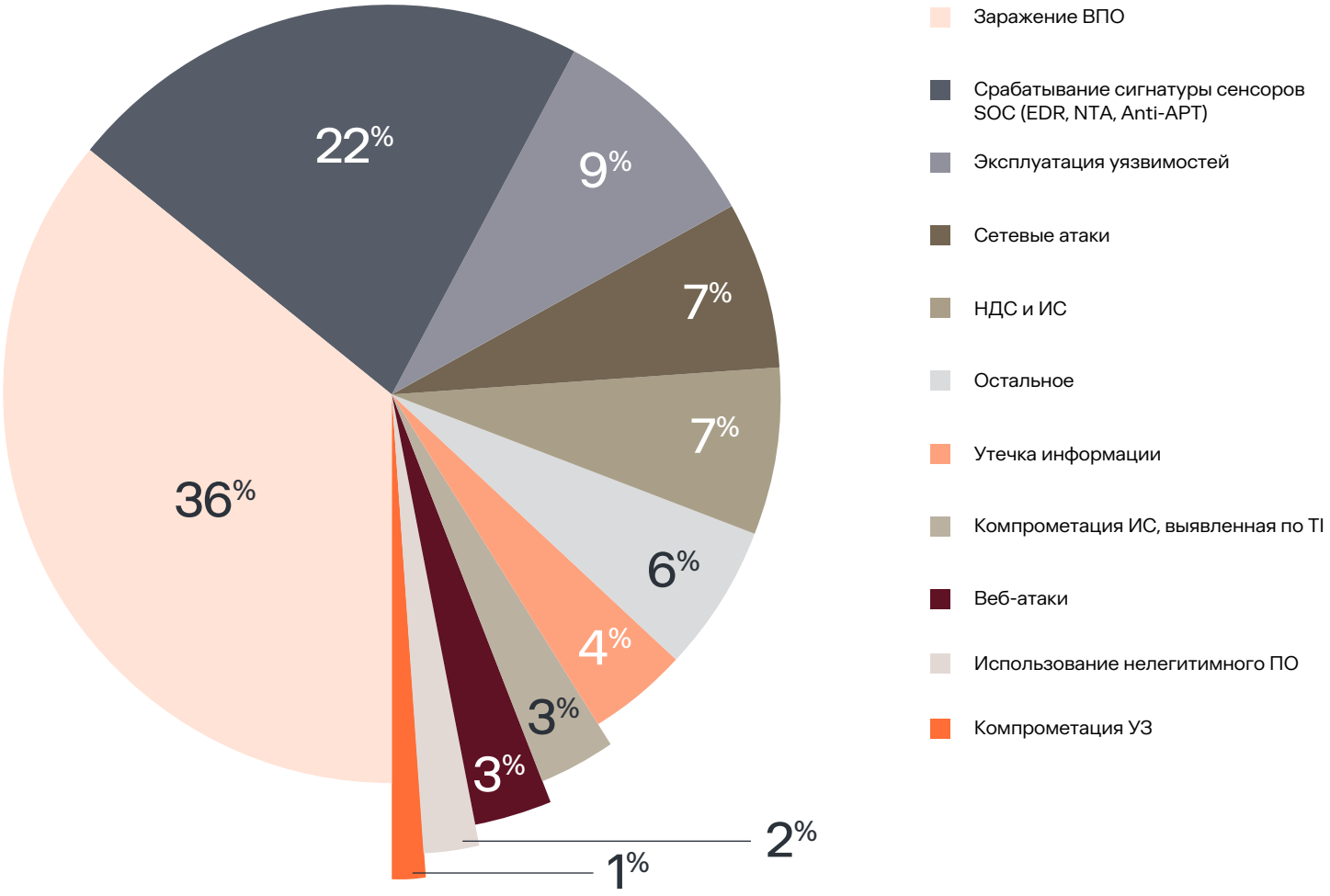


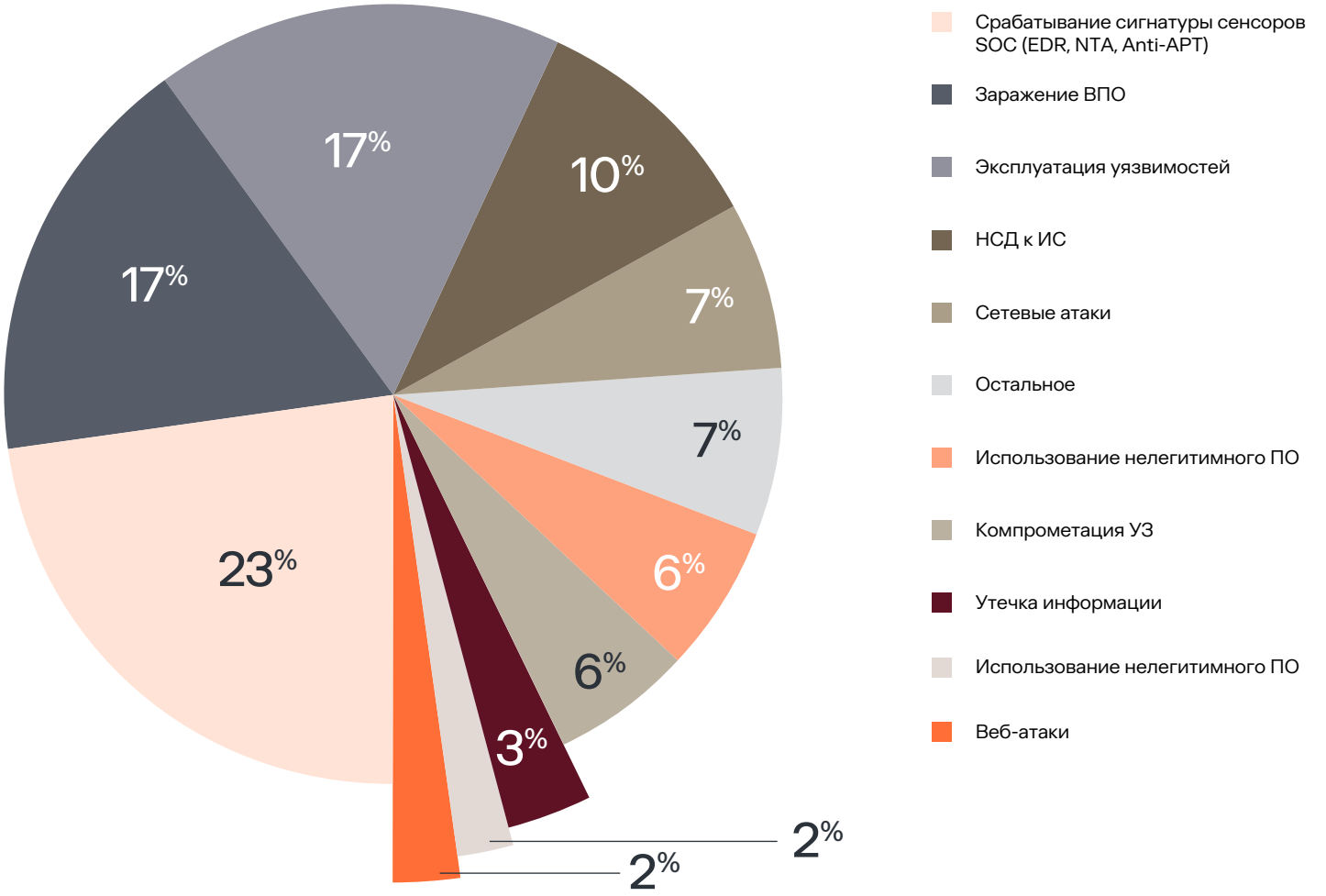
ВПО остается самой частой причиной критических инцидентов, однако в IV квартале доля таких случаев снизилась на 10 п. п. Доля веб-атак также снизилась в три раза. Это связано с ростом доли использования нелегитимного ПО на 11,5 п. п., до 12,5%.

Также участились случаи получения несанкционированного доступа к инфраструктуре и сервисам заказчиков – доля таких инцидентов выросла до 6,3% (оба инструмента входят в категорию «Остальное»).

Распределение всего объема инцидентов по категориям

III квартал 2023





Среди всего объема подтвержденных инцидентов также фиксируется снижение доли заражения ВПО, что, на наш взгляд, связано с ростом использования нелегитимного софта (средства удаленного администрирования, хакерские утилиты, исследовательский софт пентестеров и т. д.) и повышением количества срабатываний специализированных сенсоров – EDR, NTA и AntiAPT.

При этом, как правило, установка нелегитимного софта исходит от внутреннего нарушителя – когда сотрудник компании устанавливает на рабочий компьютер софт, применение которого не регламентировано политиками безопасности компании. Но и от внешнего нарушителя (хакера) данная угроза также может исходить – например, в периоды закрепления на хосте после первичного доступа в инфраструктуру и распространения по инфраструктуре компании.

Этот тренд лишний раз доказывает, что базовая антивирусная защита мешает хакерам и значительно усложняет их продвижение по инфраструктуре, и тогда они вынуждены искать другие методы закрепления и продвижения, что усложняет и увеличивает время развития кибератаки.

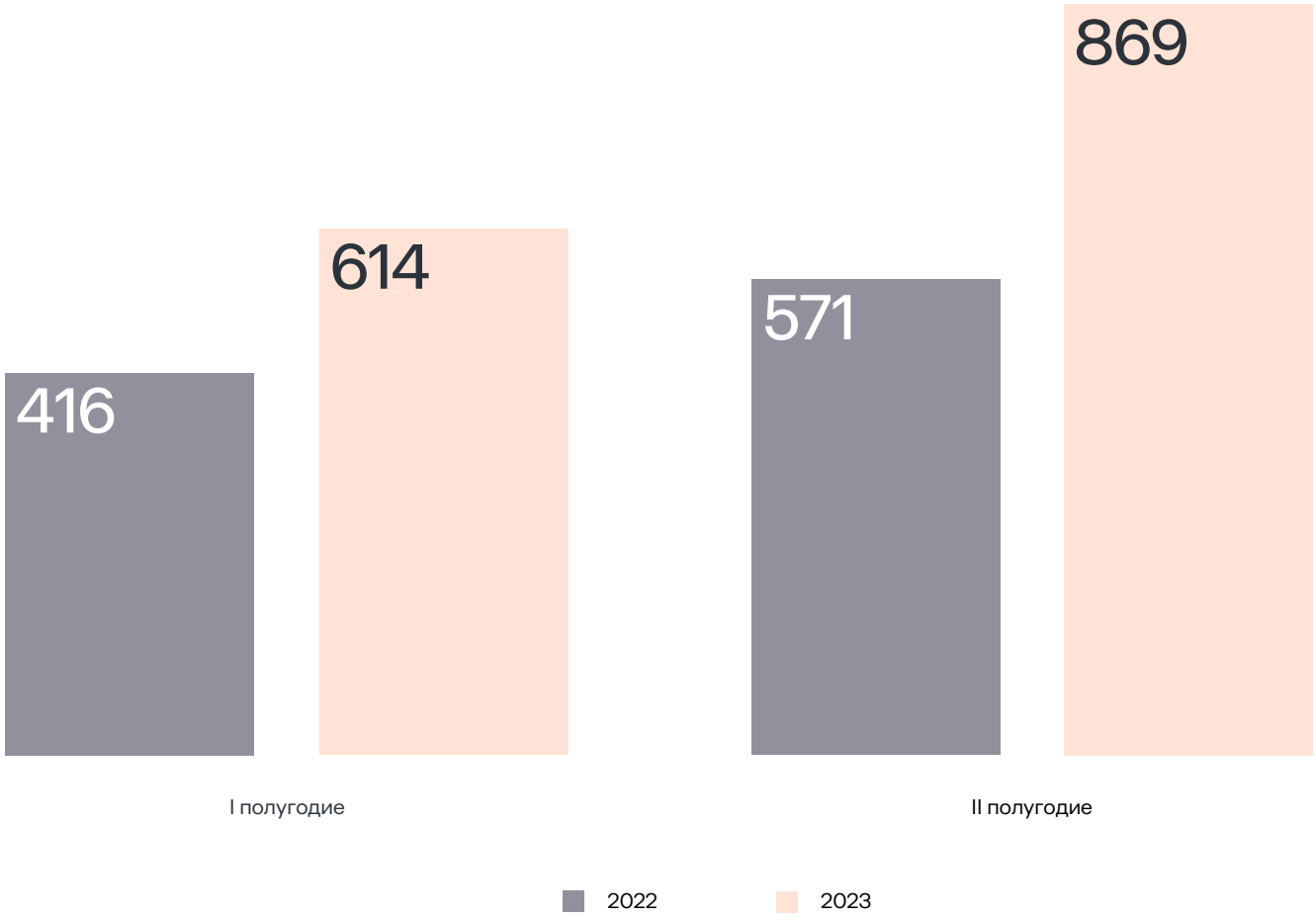
Рост объема подобных инцидентов означает, что злоумышленники стали чаще использовать хакерские (но не вредоносные, так называемые not-a-virus) утилиты и применять бесфайловые методы (когда вредоносное ПО загружается напрямую в оперативную память устройства, а файл не сохраняется на жестком диске) для закрепления и продвижения в атакуемой инфраструктуре. В дополнение мы фиксируем очередной всплеск попыток прощупывания периметра жертвы – об этом говорит в том числе рост случаев попыток эксплуатации уязвимостей. Мы видим, что киберугрозы меняются циклично: простые атаки сменяют сложные, и наоборот.

СВОДНАЯ СТАТИСТИКА ЗА I И II ПОЛУГОДИЕ

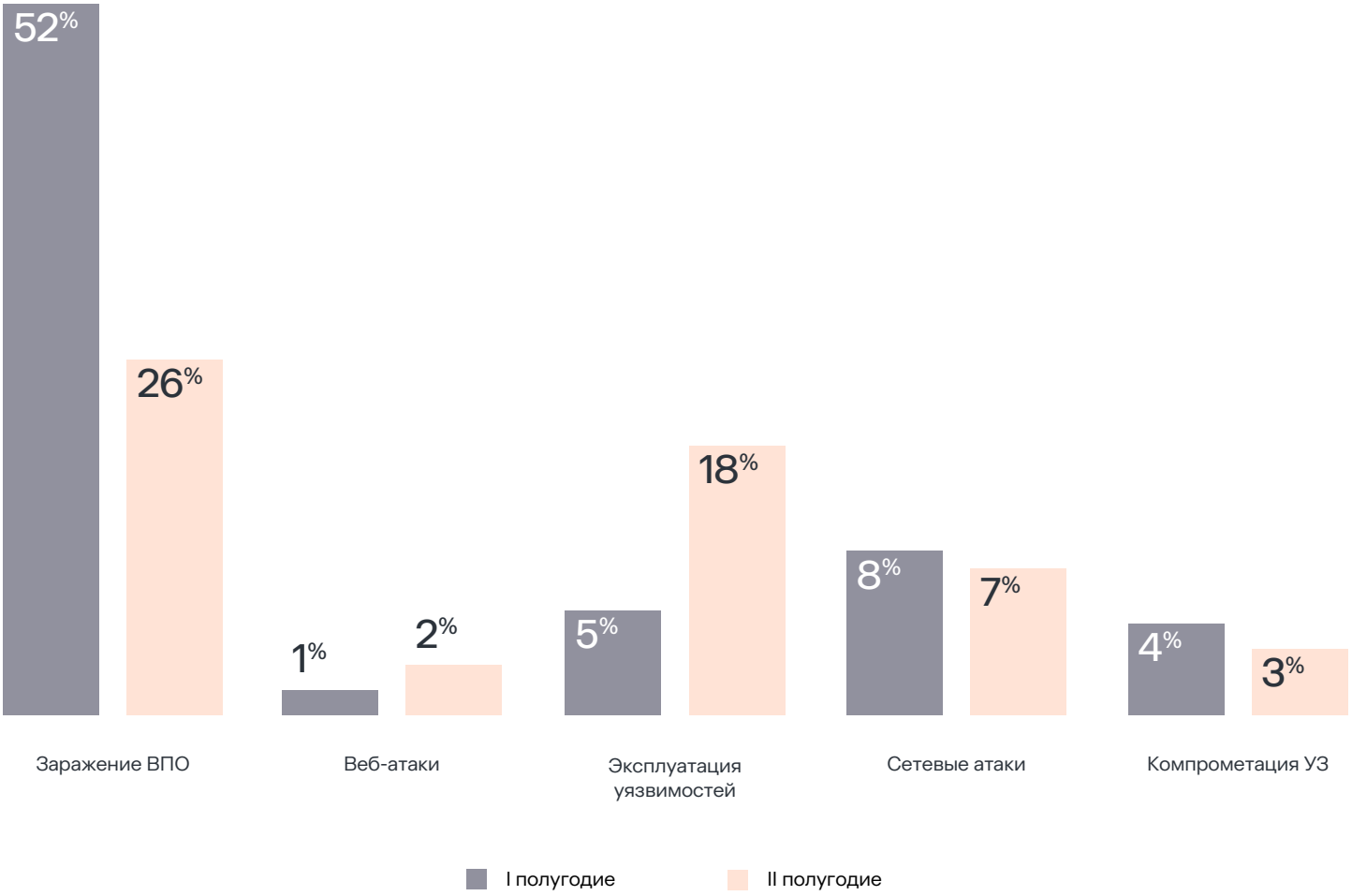
В I полугодии 2023 года число ИБ-событий составило 614 тысяч, во II их количество выросло на 42%, до 869 тысяч.

Наиболее популярным критическим инцидентом во втором полугодии 2023 года стало заражение ВПО – доля составила 75,5% от всех критических инцидентов, увеличившись на 20 п. п. Доля веб-атак, наоборот, снизилась с 13,35 до 8%. Сетевые атаки, которые еще в первом полугодии существенно утратили свою критичность, практически пропали с радаров. Однако в прошедший период им на смену пришло использование нелегитимного ПО – доля подобных инцидентов во второй половине 2023 года составила 18%.

Распределение событий ИБ по полугодиям, тыс. штук



Распределение инцидентов
с разным уровнем критичности



Отметим, что в раздел "Эксплуатация уязвимостей" попали сработки всех сенсоров – WAF, AntiAPT, EDR, NTA, IPS, IDS и других, которые начиная со второго полугодия выделены в отдельную категорию.

Если давать ретроспективную оценку, можно сделать вывод, что роль специализированных сенсоров SOC – EDR, NTA, AntiAPT – сегодня значительно выросла.

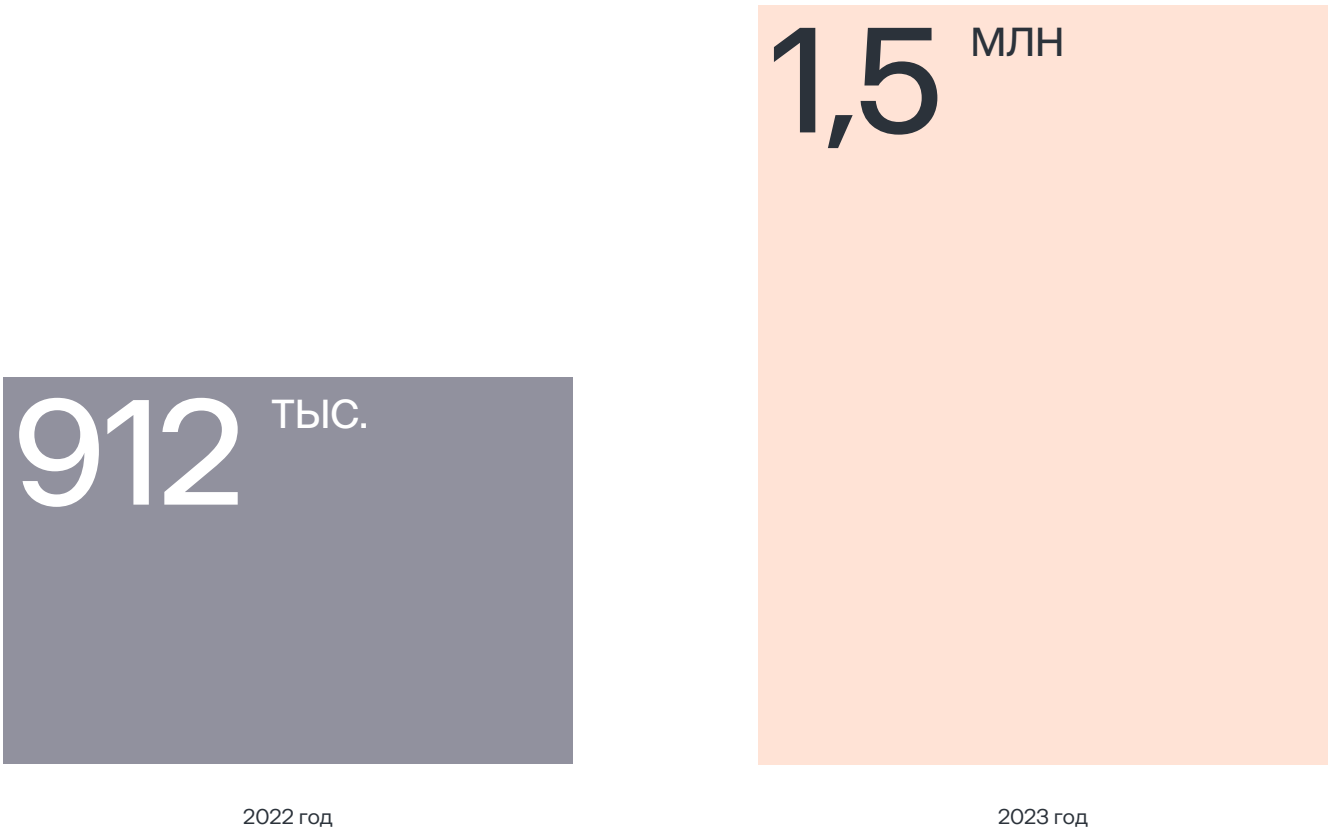
СВОДНАЯ СТАТИСТИКА ЗА 2022–2023 ГГ.

За 2023 год число подозрений на инцидент увеличилось на 64%, до 1,5 млн событий ИБ. Доля подтвержденных инцидентов от общего количества событий ИБ в 2022 году составляла 3,5%, а в 2023 снизилась до 2%. В целом в 2023 году российские компании начали адаптироваться к реальности, а массовые атаки – сменяться точечными и продуманными ударами злоумышленников.

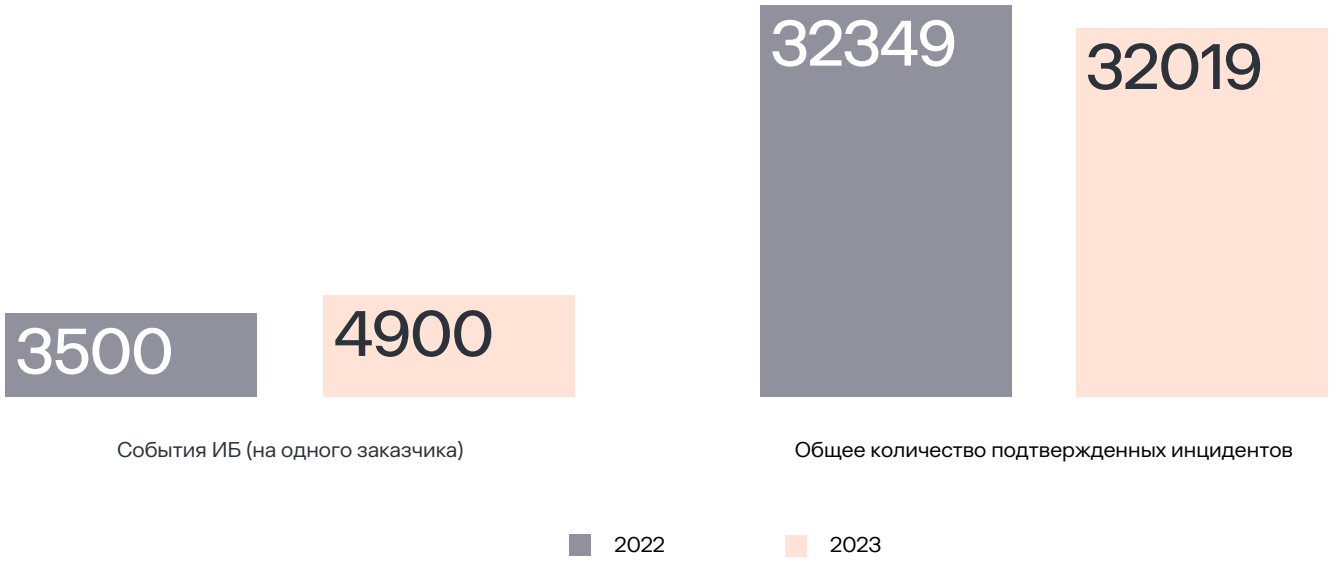
64%

Составил рост числа подозрений на инцидент за 2023 год.

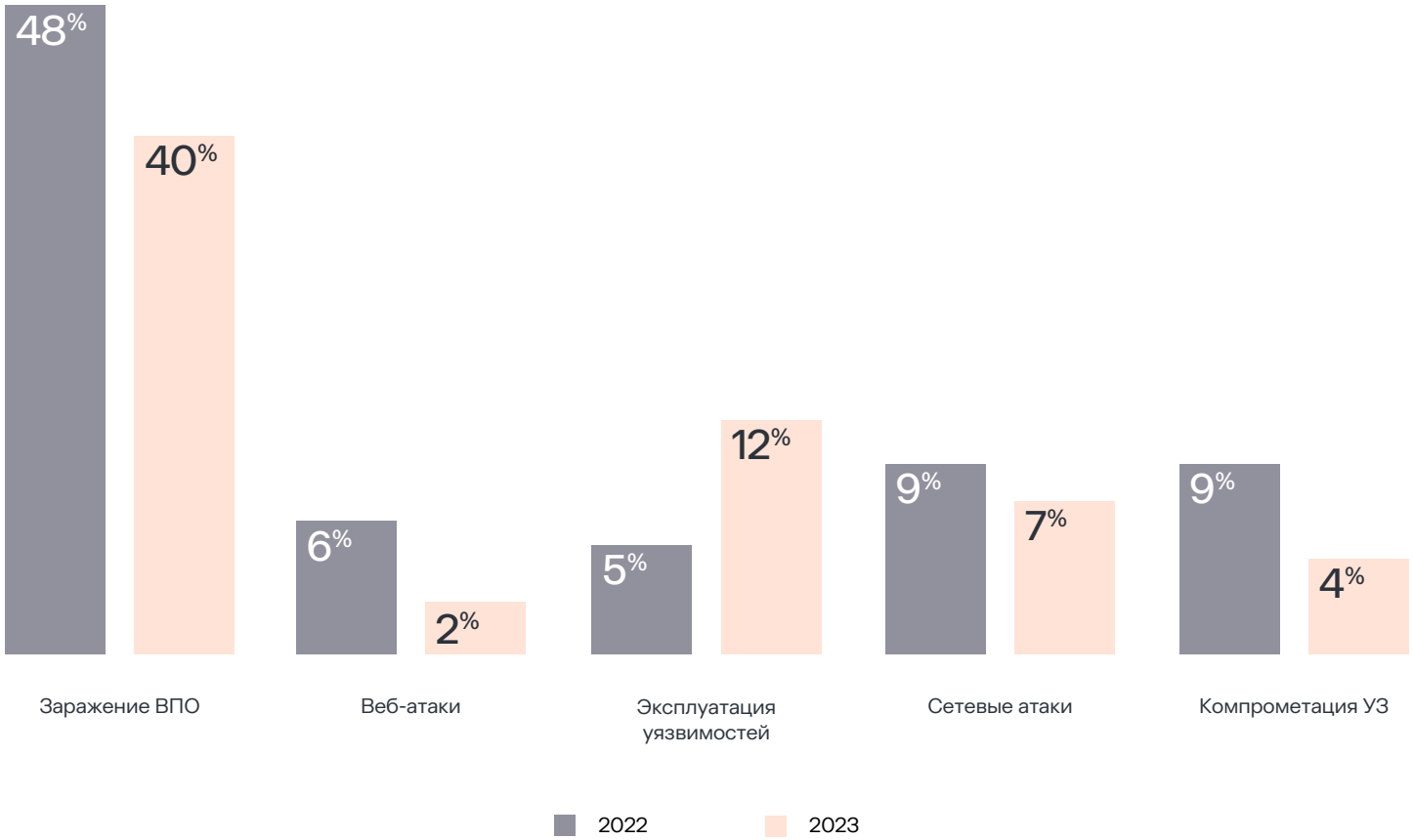
Распределение событий ИБ



Распределение событий ИБ
(в разрезе на одного заказчика)

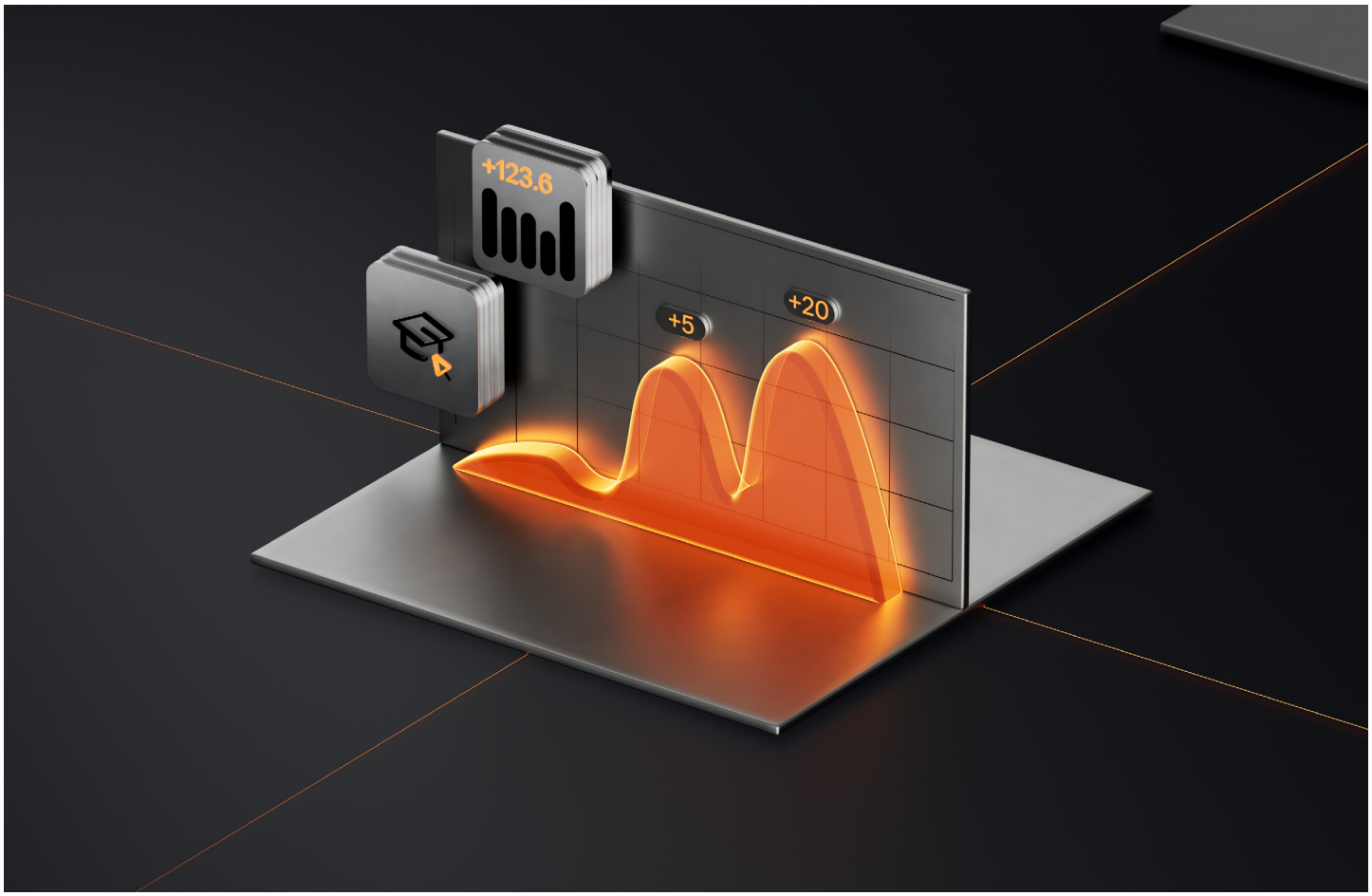


Распределение инцидентов
с разным уровнем критичности



Вместе с этим доля всех типов инцидентов, за исключением эксплуатации уязвимостей, несколько снизилась, что было прогнозируемо по следующим причинам:

1. Отсутствие выстроенных процессов патч-менеджмента и регулярной инвентаризации публичных сервисов и ресурсов. Злоумышленники активно пользуются этим с февраля 2022 года. Какие-то компании делают выводы, но большинство пока держат это в планах, закрывая данный вектор лишь частично.
2. Повышение роли сенсоров SOC из-за усложнения кибератак и попыток злоумышленников вести скрытое распространение в инфраструктурах жертв.
3. Смена фокуса внимания хакеров на отечественное ПО, количество уязвимостей в котором не меньше по сравнению с западными аналогами.



ВЫВОДЫ

Злоумышленники по-прежнему генерируют большое количество шума, но на общем фоне ИБ-событий число подтвержденных инцидентов снижается, что говорит о повышении киберграмотности сотрудников российских компаний. Тем не менее, специалистам SOC и ИБ-специалистам необходимо заняться внедрением системы приоритизации инцидентов и их выстраивания в kill-chain.

Заражение ВПО – по-прежнему самый популярный инструмент, но хакеры стали чаще использовать либо легитимные утилиты (not-a-virus), либо вредоносное ПО, не детектируемое антивирусом, а также вернулись к эксплуатации уязвимостей на периметре компаний.

Использование нелегитимного ПО – прогрессирующий вектор атаки, который может исходить как от сотрудника компании, так и от внешнего нарушителя – например, когда хакер после получения первичного доступа в инфраструктуру и распространения по ней пытается закрепиться на хосте. Это объясняет важность установки базового антивируса, который сможет распознать такой софт и усложнить жизнь хакерам.

Рост числа инцидентов, вызванных эксплуатацией уязвимостей, говорит о том, что во многих компаниях до сих пор не развит на должном уровне патч-менеджмент, а на рынок зачастую попадает сырое ПО, требующее доработок. Так, например, хакеры по-прежнему эксплуатируют log4j, proxylogon, MS1710 (WannaCry) и все чаще ориентируются на уязвимости отечественного ПО. Помимо этого, в категорию попадают сенсоры SOC, которые стали более востребованными на фоне усложнения кибератак.

ПРИЛОЖЕНИЕ 1.
ТОП-10 ИНЦИДЕНТОВ ЗА 3 ГОДА (2021–2023)

2021

Срабатывание критичной сигнатуры СЗИ	10,69%
Отсутствие в профиле аутентификации	6,02%
Удаление виртуальной машины	4,80%
Обнаружение индикатора компрометации Threat Intelligence	4,00%
Создание новой виртуальной машины	3,18%
Обнаружение вируса на хосте	3,08%
Добавление пользователя в критичные группы	3,06%
Попытка подбора пароля на критичных системах	2,77%
Внутреннее сетевое сканирование	2,52%
Отсутствие в профиле аутентификации критичной УЗ	2,28%

2022

Административный доступ за пределы сети	8,65%
Отсутствие в профиле аутентификации	6,62%
Срабатывание критичной сигнатуры СЗИ	4,85%
Обнаружение вируса на хосте	4,75%
Обнаружение индикатора компрометации Threat Intelligence	3,57%
Попытка подбора пароля	2,84%
Попытка подбора пароля на критичных системах	2,33%
Удаление пользователя из критичной группы	2,31%
Добавление пользователя в критичные группы	2,21%
Запуск RAT на хосте	2,15%

2023

Отсутствие в профиле аутентификации	6,83%
Срабатывание критичной сигнатуры СЗИ	4,18%
Обнаружение вируса на хосте	3,93%
Попытка подбора пароля на критичных системах	3,62%
Внутреннее сетевое сканирование	3,38%
Попытка подбора пароля	3,23%
Обнаружение индикатора компрометации Threat Intelligence	2,80%
Обнаружение сетевой атаки средствами АВПО	2,62%
Модификация критичных веток реестра	2,54%
Установка ПО на критичном хосте	2,49%

ТОП-10 ПОДТВЕРЖДЕННЫХ ИНЦИДЕНТОВ ЗА 3 ГОДА (2021–2023)

2021

Попытка эксплуатации критичной веб-уязвимости	12,32%
Попытка подбора учетных записей к словарному паролю	9,26%
Обнаружение вируса на хосте	8,30%
Потенциальное сканирование на уязвимости	8,03%
Обнаружение хакерских утилит средствами АВПО	5,34%
Срабатывание критичной сигнатуры СЗИ	4,73%
Блокирование 3 запросов ДБО	4,55%
Срабатывание критичной сигнатуры IDS	4,18%
Повторное заражение хоста	3,92%
Обнаружение вируса на критичном хосте	3,36%

2022

Обнаружение вируса на хосте	16,61%
Повторное заражение хоста	8,62%
Обнаружение хакерских утилит средствами АВПО	8,02%
Обнаружение вируса на критичном хосте	7,70%
Потенциальное сканирование на уязвимости	6,44%
Успешный административный доступ из интернета	4,74%
Вирусная эпидемия	3,73%
Попытка подбора учетных записей к словарному паролю	3,25%
Срабатывание критичной сигнатуры СЗИ	2,93%
Вирус обнаружен и не удален	2,84%

2023

Срабатывание критичной сигнатуры СЗИ	20,28%
Обнаружение вируса на хосте	11,26%
Повторное заражение хоста	6,07%
Обнаружение вируса на критичном хосте	5,78%
Успешный административный доступ из интернета	5,76%
Обнаружение индикатора компрометации Threat Intelligence	5,15%
Обнаружение хакерских утилит средствами АВПО	5,10%
Вирусная эпидемия	3,20%
Вирус обнаружен и не удален	3,07%
Длительное сканирование системы	3,04%

ПРИЛОЖЕНИЕ 2.
НАИБОЛЕЕ ПОПУЛЯРНЫЕ ИНЦИДЕНТЫ ПО ОТРАСЛЯМ ЗА 2023 ГОД

Банки

Отсутствие в профиле аутентификации	11,06%
Внутреннее сетевое сканирование	5,41%
Срабатывание критичной сигнатуры СЗИ	5,00%
Экспорт данных виртуальной машины	3,79%
Использование УЗ отсутствующего сотрудника	3,42%
Отключение антивирусного ПО на хосте	3,13%
Отсутствие источника в профиле геолокации VPN	3,03%
Отключение антивирусного ПО на критичном хосте	2,88%
Административный доступ за пределы сети	2,20%
Обнаружение индикатора компрометации Threat Intelligence	2,17%

Промышленность

Срабатывание критичной сигнатуры СЗИ	4,59%
Административный доступ за пределы сети	4,57%
Попытка подбора пароля	4,05%
Исходящая сетевая активность к потенциально опасным хостам	3,68%
Попытка подбора пароля на критичных системах	3,61%
Смена пароля для критичного пользователя	3,24%
Отсутствие в профиле аутентификации	3,05%
Временное повышение привилегий пользователя	2,83%
Добавление пользователя в критичные группы	2,69%
Обнаружение индикатора компрометации Threat Intelligence	2,61%

Энергетика

Обнаружение вируса на хосте	9,88%
Отсутствие в профиле аутентификации критичной УЗ	4,29%
Обнаружение нового хоста в критичной сети	4,10%
Установка ПО на критичном хосте	4,08%
Отсутствие в профиле аутентификации	4,07%
Попытка подбора пароля	3,97%
Попытка подбора пароля на критичных системах	3,88%
Обнаружение индикатора компрометации Threat Intelligence	3,31%
Обнаружение сетевой атаки средствами АВПО	3,19%
Потенциальное сканирование на уязвимости	3,11%

Ритейл

Срабатывание критичной сигнатуры СЗИ	13,19%
Многочисленные блокировки учетной записи	7,82%
Административный доступ за пределы сети	5,63%
Обнаружение утечки информации	5,35%
Обнаружение индикатора компрометации Threat Intelligence	3,99%
Попытка подбора пароля	3,38%
Несанкционированные действия над учетной записью в обход IDM	3,00%
Отсутствие в профиле аутентификации	2,78%
Модификация критичных веток реестра	2,66%
Удаление пользователя из критичной группы	2,06%

Транспорт

Потенциальное сканирование на уязвимости	10,65%
Обнаружен вирус на критичном хосте	8,44%
Включение отключенной учетной записи	5,62%
Попытка подбора пароля	4,14%
Временное повышение привилегий пользователя	4,14%
Обнаружение нового сервиса во внешнем периметре	3,74%
Установка новой системной службы	3,49%
Срабатывание критичной сигнатуры СЗИ	3,25%
Успешный административный доступ из сети Интернет	3,24%
Добавление пользователя в критичные группы	3,07%

Госсектор

Срабатывание критичной сигнатуры СЗИ	12,82%
Отсутствие в профиле аутентификации	8,40%
Обнаружение индикатора компрометации Threat Intelligence	4,62%
Срабатывание сигнатуры AntiAPT	4,09%
Попытка подбора пароля на критичных системах	3,60%
Модификация критичных веток реестра	3,59%
Обнаружен вирус на хосте	3,54%
Попытка подбора пароля	3,33%
Обнаружение сетевой атаки средствами АВПО	3,22%
Удаление виртуальной машины	3,20%

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