



POSITIVE
TECHNOLOGY

Positive Tech Press Club

**Мониторинг событий ИБ:
рынок SIEM и технологические тренды**

ptsecurity.com

SIEM в России: рынок сегодня, динамика, прогнозы

РТ



Максим Филиппов,
директор по развитию бизнеса
компании в России

Российский рынок SIEM

РТ

2014 – 2015	2016 – 2017	2018 – 2020
40–50%	30–40%	20–25%

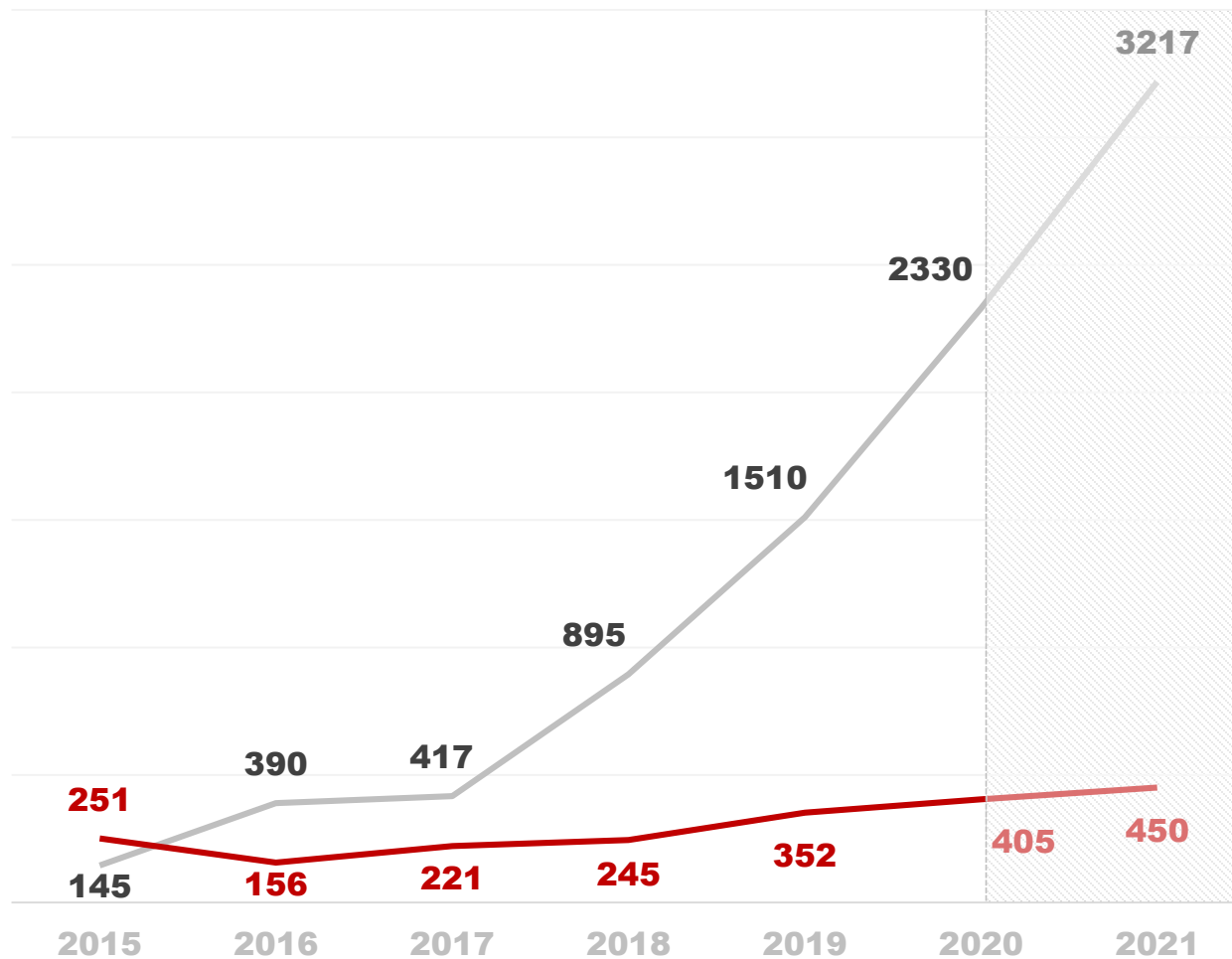
**5 миллиардов
рублей**



**Российский рынок
растет в 2 раза
быстрее, чем
мировой**

Бизнес с MaxPatrol SIEM

РТ



■ Продажи, млн руб.

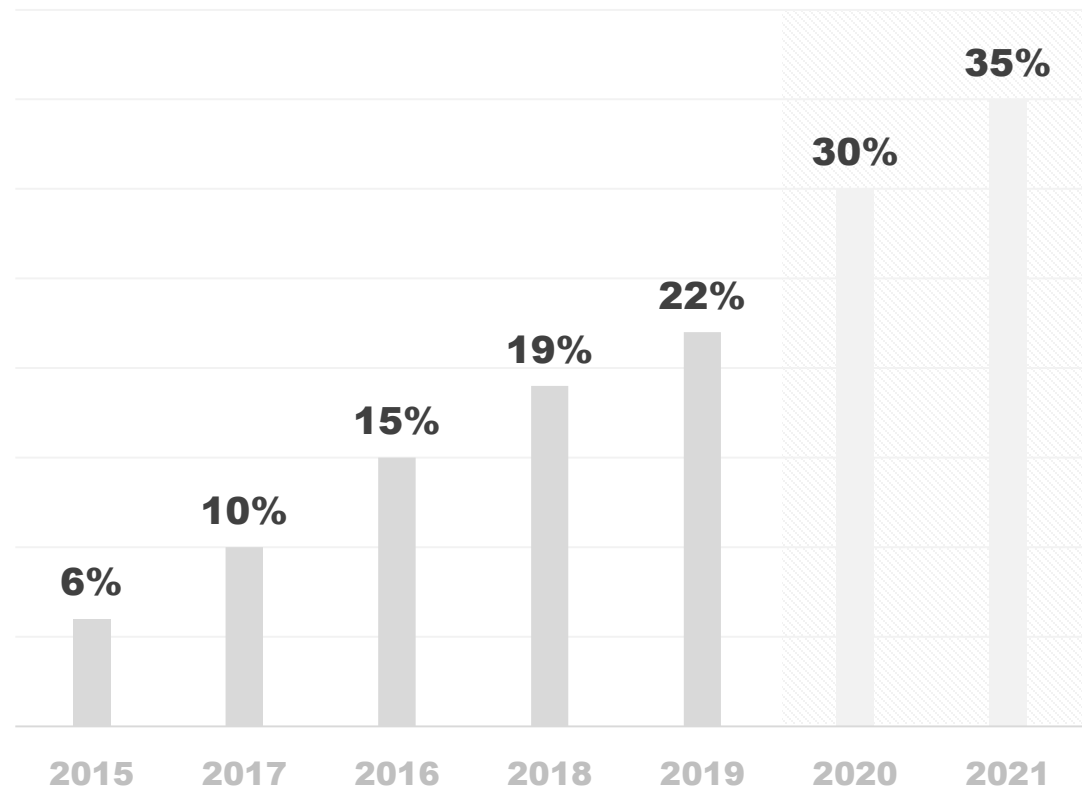
■ Инвестиции, млн руб.

Бизнес с MaxPatrol SIEM

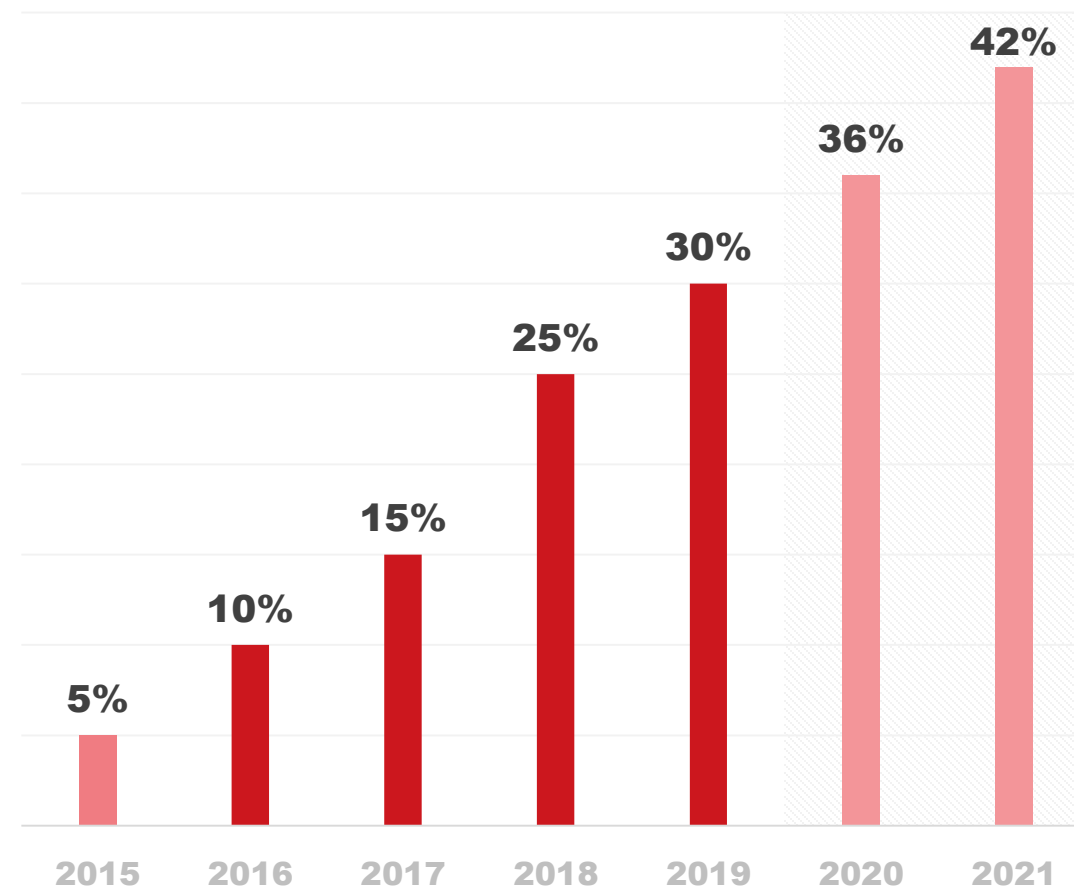
РТ



Доля SIEM в выручке компании



Объем рынка



Бизнес с MaxPatrol SIEM



Партнеры

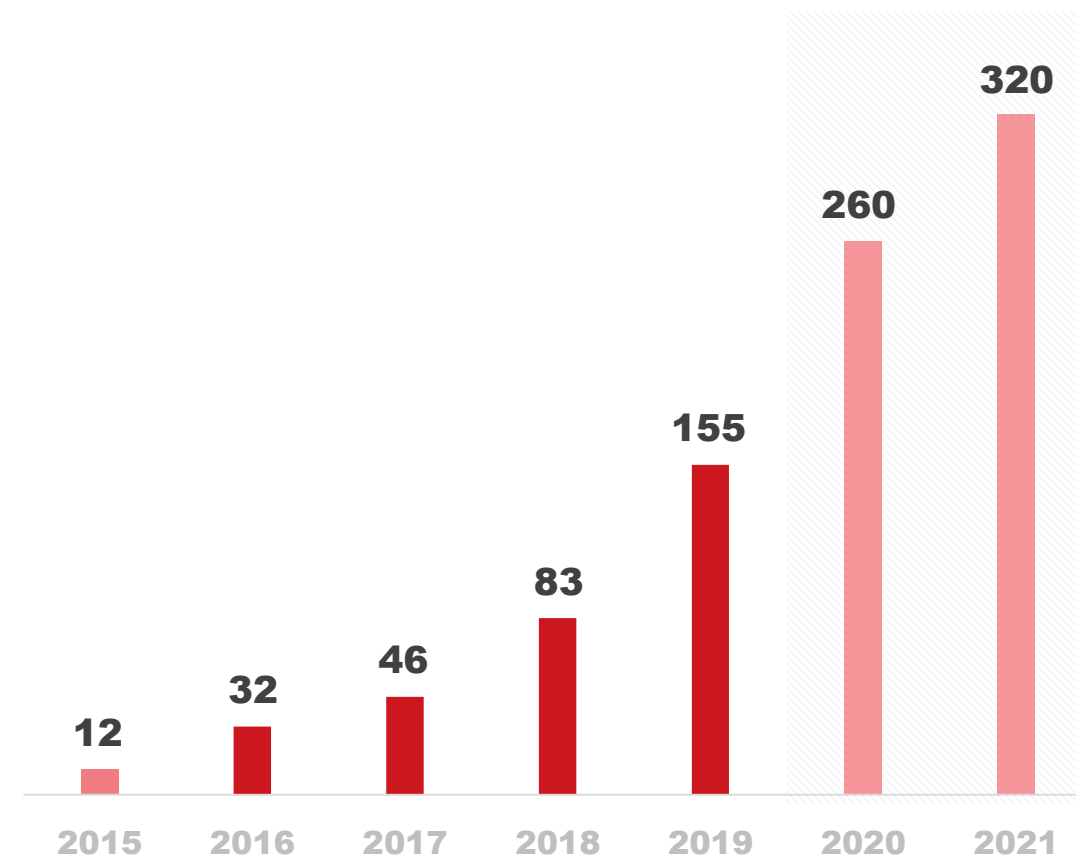
470

специалистов

Прошли спецификацию
с 2016 года: 70 пресейловых
и 400 технических



Заказчики



Профиль пользователей SIEM



SOC* без SIEM невозможен



**Государственные
организации**



Банки



Энергетика



Телеком



Промышленность



Ритейл

*security operation center – центр реагирования на киберугрозы

Платформа MaxPatrol



Positive Technologies Expertise



Топ технологий, формирующих будущее SIEM

РТ



Алексей Андреев,
управляющий директор департамента
исследований и разработки

Экспертиза в SIEM

PT



50–60%

Покрытие технологии

По результатам экспертной оценки специалистов Positive Technologies.



Качество реализации

Оценивается по шкале от 1 до 5, где 1 – плохо реализовано, 2 – качество реализации ниже среднего, 3 – среднее качество реализации, 4 – качество реализации выше среднего, 5 – хорошо реализовано. По результатам экспертной оценки специалистов Positive Technologies.

**Больше, чем маппинг
правил корреляции
по матрице MITRE ATT&CK**

Автоматизация реагирования на инциденты

РТ



60–70%

Покрытие технологии

По результатам экспертной оценки специалистов Positive Technologies.



Качество реализации

Оценивается по шкале от 1 до 5, где 1 – плохо реализовано, 2 – качество реализации ниже среднего, 3 – среднее качество реализации, 4 – качество реализации выше среднего, 5 – хорошо реализовано. По результатам экспертной оценки специалистов Positive Technologies.

Самые трудоемкие задачи*:

- донастройка правил корреляции – 58%,
- разбор инцидентов – 52%,
- настройка источников данных и отслеживание их работоспособности (30%).

* По мнению участников нашего опроса

Автоматизация внедрения SIEM-систем

Конвергенция анализа трафика, логов и происходящего на конечных узлах

РТ



60–70%

Покрытие технологии

По результатам экспертной оценки специалистов Positive Technologies.



Качество реализации

Оценивается по шкале от 1 до 5, где 1 – плохо реализовано, 2 – качество реализации ниже среднего, 3 – среднее качество реализации, 4 – качество реализации выше среднего, 5 – хорошо реализовано. По результатам экспертной оценки специалистов Positive Technologies.

**Единая исчерпывающая
картина происходящего
в инфраструктуре
на экране оператора SIEM**

Анализ поведения пользователей и сущностей

РТ



70–80%

Покрытие технологии

По результатам экспертной оценки специалистов Positive Technologies.



Качество реализации

Оценивается по шкале от 1 до 5, где 1 – плохо реализовано, 2 – качество реализации ниже среднего, 3 – среднее качество реализации, 4 – качество реализации выше среднего, 5 – хорошо реализовано. По результатам экспертной оценки специалистов Positive Technologies.

2 главных челленджа:

- снизить количество ложных срабатываний,
- разработать понятные для операторов алгоритмы интерпретации результатов.

Построение поведенческих моделей

Облака – источник данных и формат предоставления SIEM as a service

PT



60–70%

Покрытие технологии

По результатам экспертной оценки специалистов Positive Technologies.



Качество реализации

Оценивается по шкале от 1 до 5, где 1 – плохо реализовано, 2 – качество реализации ниже среднего, 3 – среднее качество реализации, 4 – качество реализации выше среднего, 5 – хорошо реализовано. По результатам экспертной оценки специалистов Positive Technologies.

**Добавление популярных
облачных сервисов
в список поддерживаемых
SIEM источников**

SIEM as a service

Куда ведут эти тренды

РТ

Процент покрытия

Экспертиза в SIEM	50–60
Автоматизация реагирования на инциденты	60–70
Анализ трафика, логов и происходящего на конечных узлах	60–70
Анализ поведения пользователей и сущностей	70–80
Облака	60–70



Повышение качества мониторинга и реагирования на инциденты



Сокращение объема ручной работы операторов

Куда ведут эти тренды

РТ

Качество реализации



Повышение качества мониторинга и реагирования на инциденты



Сокращение объема ручной работы операторов

MaxPatrol SIEM 6: новая версия и ее ключевые отличия

PT



Наталия Казанькова,
менеджер по продуктовому маркетингу

Трудозатраты на работу в SIEM-системе

PT

25%

от **двух**
до **четырех**
часов ежедневно

**СПЕЦИАЛИСТЫ
ПО ИБ ПРОВОДЯТ
В SIEM-СИСТЕМЕ**

22%

от **четырех**
часов ежедневно

Источник: Трудозатраты на работу в SIEM-системе, Positive Technologies, 2019

Поэтапно снижаем трудозатраты на работу в SIEM

РТ

4.0

Поставка пакетов экспертизы

Апрель 2018

5.0

Конструкторы отчетов
и правил корреляции

Июль, 2019

5.1

Агрегация похожих событий
в один инцидент

Март, 2020

6.0

Июнь, 2020



01. Чек-лист настройки системы



01. Чек-лист настройки системы



ЧЕМ ПОЛЕЗНО

Поможет быстро настроить систему и получить работающий SIEM без изучения документации

☰

PT

Площадка · MaxPatrol SIEM

Активы

События

Инциденты

Сбор данных

Система

Чек-лист настройки системы

Список проверок

Администрирование0 из 2

Сервис обновлений установлен и настроен

Компоненты системы обновлены

Инфраструктура3 из 4

Выделены значимые активы

Настроен поиск активов

Проводится периодический аудит активов

Данные о значимых активах актуальны

Добавлена информация об Active Directory

Экспертиза0 из 4

Проводится расширенный аудит активов (Windows)

Включены необходимые правила корреляции

Проводится расширенный аудит активов (Linux)

Настроен мониторинг значимых источников событий

✓ Выделены значимые активы

Запустить проверкуИсключить

Для эффективного управления активами и инцидентами (например, для приоритизации инцидентов) необходимо понимать, насколько **каждый актив значим**. Сведения о значимости активов позволят фильтровать и группировать активы и инциденты, в том числе с помощью PDQL-запросов. Значимость актива нужно задать вручную.

Чтобы выделить значимые активы:

- Добавьте активы в систему.

Для удобства работы с активами вы можете объединить их в группы.
- Присвойте самым важным для вашей IT-инфраструктуры активам и группам активов **высокий уровень значимости**.

PDQL-запрос для поиска значимых активов

```
filter(Host.@Importance != 'ND' AND Host.@Importance != 'L' AND Host.@Importance != 'M') | select(@Host, Host.@Importance)
```

См. также

[Группы активов](#)

[Чек-лист настройки системы](#)



02. Упрощение работы с false positive

Снизит количество ложных срабатываний
и сократит время на разбор инцидентов



03. Виджет по табличным спискам

Табличный список
можно быстро
превращать в виджет
и использовать
в отчетах

ЧЕМ ПОЛЕЗНО

Мониторинг
обновлений в табличных
списках и оперативное
реагирование

Запущенные процессы в организации		16:57		
_last_changed	process			
05.06.2020 14:09:12	ntoskrnl.exe			
05.06.2020 14:09:12	taskmgr.exe			
05.06.2020 14:09:12	procexp64.exe			
05.06.2020 14:09:12	wmiprvse.exe			
05.06.2020 14:09:12	svchost.exe			
05.06.2020 14:09:12	tasklist.exe			
05.06.2020 14:09:12	procexp.exe			
Всего 7 строк, выбрано 0 строк				

04. Уведомления

О НОВЫХ ПАКЕТАХ ЭКСПЕРТИЗЫ

РТ

Пользователи не забудут
о невыполненных шагах
в чек-листе и будут узнавать
об обновлениях базы знаний
прямо из интерфейса

ЧЕМ ПОЛЕЗНО

Поможет не пропустить
новые правила корреляции

The screenshot displays the 'Knowledge Base' (База знаний) interface. At the top, there's a header with the 'РТ' logo, 'Knowledge Base', and 'SIEM Content'. Below the header, a section titled 'Пакеты экспертизы' (Expertise Packages) is visible. On the left, a notification panel shows '4 уведомления' (4 notifications) for June 5th. The notifications list updates to expert packages for 'Безопасность удаленной работы', 'Linux. Подозрительные изменения системных объектов', 'Microsoft SQL Server до версии 1.1', and 'Linux. Подозрительная сетевая активность до версии 1.1'. Each notification includes a timestamp of 14:13 and a link to 'Описание пакета' (Package description). On the right, a list of expert packages is shown under the heading 'Папки' (Folders). The list includes 'Базовый пакет', 'Active Directory', and various ATT&CK categories like 'Подозрительная активность пользователя', 'Выполнение', 'Предотвращение обнаружения', 'Закрепление', 'Перемещение внутри периметра', and 'Получение учетных данных'. A tooltip indicates that the 'Linux. Подозрительная сетевая активность' package has been updated to version 1.1.

Knowledge Base SIEM Content

Пакеты экспертизы

Папки

Все объекты

- Базовый пакет
- Active Directory
- Active Directory. Подозрительная активность пользова...
- ATT&CK: «Выполнение» и «Предотвращение обнаруже...
- ATT&CK: «Закрепление»
- ATT&CK: «Перемещение внутри периметра»
- ATT&CK: «Получение учетных данных»
- Пакет экспертизы обновлен до версии 1.1
- Linux. Подозрительная сетевая активность
- Linux. Подозрительные изменения системных объектов
- Microsoft SQL Server
- Oracle Database
- SAP NetWeaver AS
- SAP NetWeaver AS. Подозрительная активность польза...
- Атаки методом перебора
- Атаки с помощью специализированного ПО
- Безопасность удаленной работы
- Вирусы-шифровальщики в Windows
- Кампания SongXY



05. Поддержка Windows Server 2016 и 2019 для установки MaxPatrol SIEM

Ключевые новинки 6.0

РТ



Чек-лист
настройки системы



Упрощение разбора
ложных срабатываний



Виджет по табличным
спискам



Обновление работы
центра уведомлений



Поддержка Windows
Server 2016 и 2019