



Прозрачность корпоративных сетей в России

2020

ptsecurity.com

**Мы провели
анонимный опрос среди
специалистов по ИБ, чтобы:**

**В опросе
принял участие
231 специалист**

01

Узнать, как они оценивают уровень прозрачности корпоративной сети

02

Понять их ожидания от инструментов анализа трафика

03

Сравнить полученные результаты с данными похожего исследования за рубежом компании **SANS**

SANS

[sans.org/reading-room/
whitepapers/detection/
paper/39490](https://sans.org/reading-room/whitepapers/detection/paper/39490)



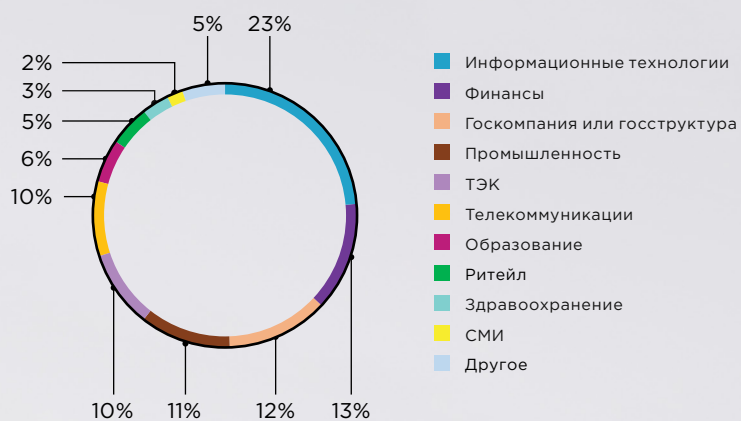
**ОПРОС ПРОВОДИЛСЯ
С 27 АВГУСТА ПО 14 СЕНТЯБРЯ.**

Мы разместили его на официальном сайте Positive Technologies, интернет-порталах, посвященных ИБ, социальных сетях, в тематических чатах и каналах в Телеграме.

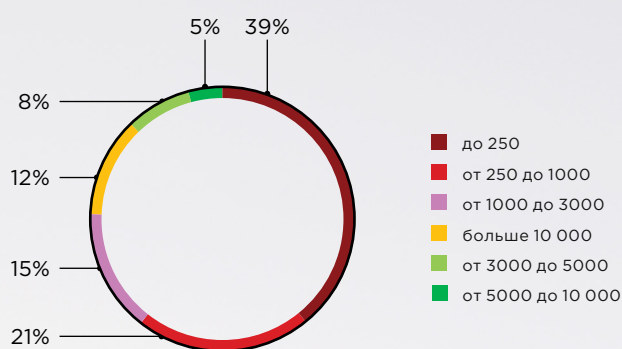


Кто участвовал в опросе

Какой сектор экономики представляет ваша компания?



Сколько сотрудников работает в вашей компании?



Большинство результатов опроса не зависит от размера компании респондентов или меняется незначительно.



Что мы выяснили (кратко)



NTA-системы анализируют трафик и на периметре, и в инфраструктуре. Они автоматически выявляют атаки по большому количеству признаков: от применения хакерского инструментария до отправки данных на сервер злоумышленников.



NTA-системы хранят информацию о сетевых взаимодействиях, а некоторые из них — еще и запись сырого трафика. Такие данные становятся полезными источниками знаний при отслеживании перемещения злоумышленника и расследовании инцидентов в целом.

01

Российские специалисты по ИБ примерно **одинаково оценивают прозрачность корпоративного внешнего и внутреннего трафика**. По данным исследования SANS, за рубежом не так: они хуже видят то, что происходит внутри сети, чем то, что на периметре.

02

За последний год реже всего респонденты замечали во внутреннем трафике **горизонтальное перемещение злоумышленников** (8%) и **активность хакерского инструментария** (17%). Вероятно, потому что у большинства специалистов нет подходящих инструментов для их выявления.

03

Выбирая между шифрованием и **прозрачностью внутренней сети**, 64% специалистов скорее склоняются в пользу второго.

04

По мнению участников опроса, **наиболее важные задачи**, которые должны решать инструменты анализа трафика, — выявление атак внутри сети (88%) и на периметре (86%), обнаружение сетевых аномалий (71%) и контроль соблюдения регламентов ИБ (71%). Это типовые задачи систем класса network traffic analysis, NTA.

05

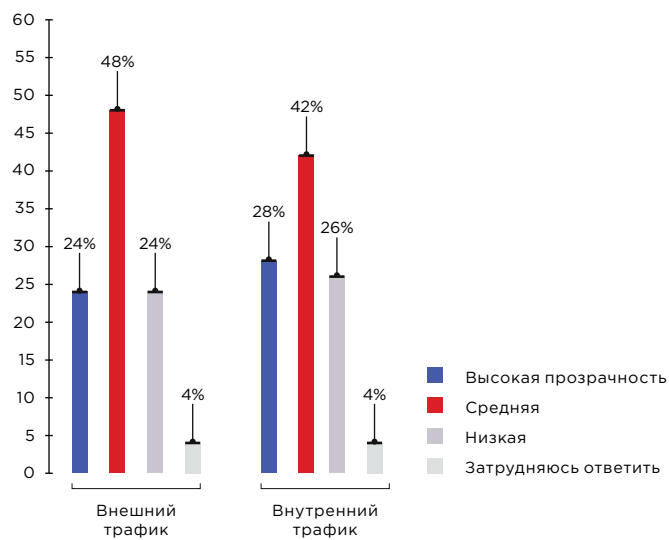
Менее приоритетные задачи — расшифровывать зашифрованный трафик и проводить ретроспективный анализ. За это проголосовали 29% и 27% специалистов соответственно.



Видимость трафика: в России и за рубежом

По результатам опроса мы пришли к выводу, что, вероятно, в большинстве российских компаний не хватает инструментов для анализа трафика, покрыты не все сегменты сети или прозрачности мешает шифрование данных. 72% опрошенных оценивают видимость внешнего трафика как низкую или среднюю, уровень прозрачности внутреннего трафика так же оценили 68% респондентов.

Как вы оцениваете уровень прозрачности трафика?



Как за рубежом?

Сравним результаты с мировыми данными. По результатам опроса американской компании SANS, зарубежные ИБ-специалисты в разы лучше видят трафик на периметре, чем тот, что генерится внутри сети.

Уровень прозрачности трафика в зарубежных сетях



В опросе SANS приняли участие 213 специалистов по ИБ из крупных компаний (минимум 1000 сотрудников) по всему миру. Главные офисы и филиалы компаний расположены в Северной и Южной Америке, Европе, Африке, Австралии и Азии.

Почему 52% зарубежных специалистов считают, что у них высокая прозрачность внешнего трафика на периметре, тогда как в России этим могут похвастаться только 24%? По мнению большинства участников [NTA-комьюнити в Телеграм](#), причина столь большой разницы в том, что многие российские компании еще не внедрили IDS, NGFW, UTM, NTA и другие популярные инструменты анализа трафика. Вероятно это связано с тем, что в России меньшие бюджеты на ИБ, чем за рубежом.

Влияние отрасли на прозрачность трафика

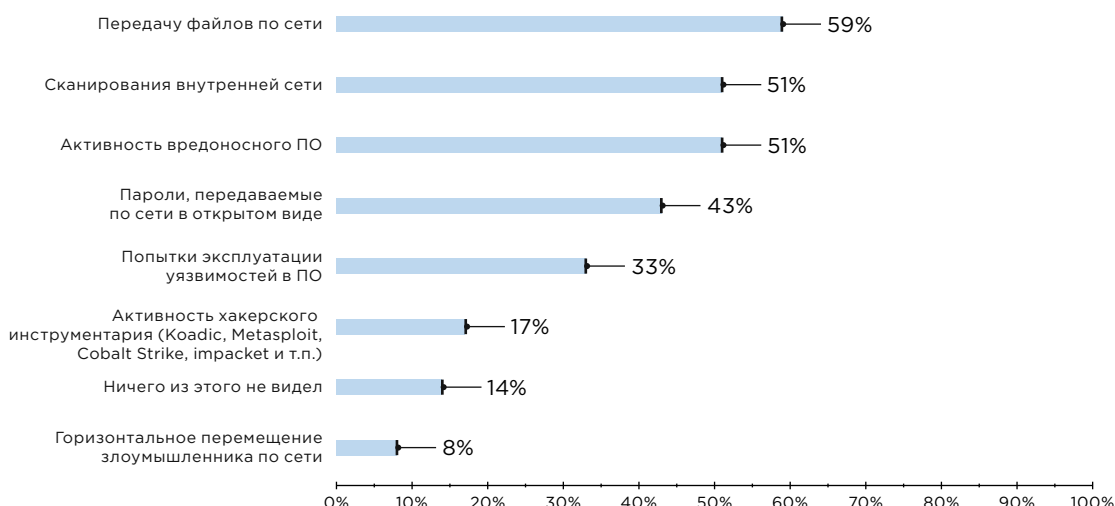
Больше других в России видимостью внешнего трафика довольны представители IT и финансовых компаний: высокую прозрачность отметили соответственно 42% и 38% специалистов из таких компаний. Антирейтинг возглавляет промышленный сектор: 36% его представителей считают внешний трафик непрозрачным.

Почти такая же ситуация с прозрачностью внутренней сети. Почти половина представителей IT-компаний (47%) заявили о высоком уровне видимости, а чуть больше половины специалистов промышленных компаний (52%) оценили ее низко.

Непрозрачность внутренней сети

За последний год 51% специалистов по ИБ замечал внутри периметра сканирования внутренней сети и вредоносную активность. Хуже обстоят дела, если злоумышленник перемещался по сети или использовал [специальный инструментальный для развития атаки](#). Только 8% и 17% специалистов обнаруживали такую активность за последний год.

Что из перечисленного вы наблюдали во внутреннем трафике за последний год?



Специалист экспертного центра безопасности PT ESC показал на вебинаре, **как обнаружить горизонтальное перемещение** в сети по трафику с помощью NTA-системы PT NAD и как помешать развитию атаки.

СМОТРЕТЬ

Сканирования сети и активность вредоносного ПО отлавливаются многими средствами безопасности (например, антивирусами или EDR). Вероятно, что опрошенные специалисты выявляли их, не используя системы анализа трафика network traffic analysis, NTA, которые в том числе предназначены для выявления горизонтального перемещения злоумышленников и активности хакерского инструментария.

Что должны уметь инструменты анализа трафика

Самые высокие оценки по важности получили задачи, связанные с обнаружением угроз. 88% опрошенных специалистов отметили высшими баллами (4 или 5) выявление атак внутри сети, 86% — выявление атак на периметре, 71% — обнаружение сетевых аномалий и такая же доля у контроля соблюдения регламентов ИБ.

Контролировать соблюдение регламентов ИБ (передача паролей в открытом виде, использование сотрудниками RAT, торрентов, Tor и т. п.)



Проводить ретроспективный анализ



Расшифровывать зашифрованный трафик



Проводить threat hunting



Видеть вредоносную активность в зашифрованном трафике



Выполнять требования законодательства по защите информации



Проводить расследования



Выявлять сетевые аномалии



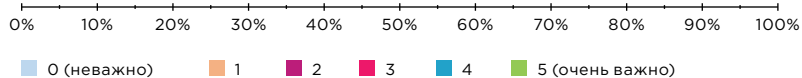
Автоматически блокировать атаки



Выявлять атаки внутри сети



Выявлять атаки на периметре



Антирейтинг приоритетных задач возглавляет расшифровка зашифрованного трафика. 29% специалистов оценили ее в 0, 1 или 2 балла. Но это не значит, что специалистам по ИБ неважно, что происходит внутри зашифрованного трафика: 70% специалистов по ИБ крупных компаний хотят видеть в нем вредоносную активность (оценили задачу в 4 и 5 баллов). Это возможно и без расшифровки, [анализируя сетевые пакеты](#).

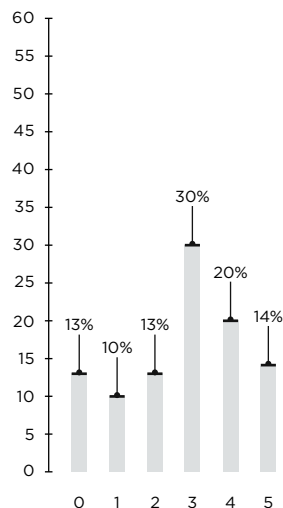
Также к непериприоритетным задачам 27% специалистов отнесли проведение [ретроспективного анализа](#). Мы спросили, что об этом думают участники [NTA-комьюнити в Телеграм](#). Среди причин они назвали не умение некоторых специалистов пользоваться ретроспективным анализом и высокую стоимость серверов для хранения трафика.

Шифрование vs прозрачность сети

64% российских специалистов по ИБ склоняются в сторону прозрачности сети: они оценили свое волнение по поводу шифрования внутреннего трафика в 3, 4 или 5 баллов.

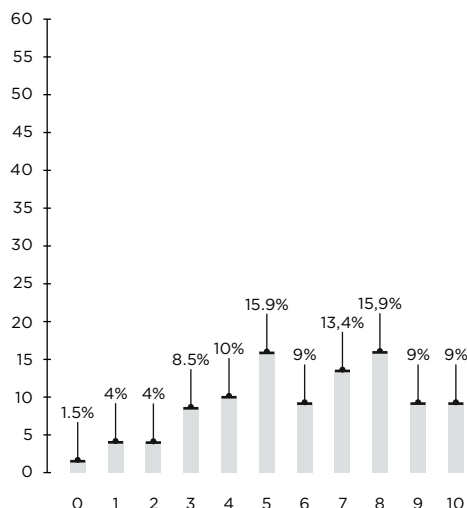
Насколько вас волнует то, что зашифрованный трафик внутри инфраструктуры препятствует прозрачности сети?

Ноль — «мне все равно на прозрачность сети, я за полное шифрование трафика внутри сети»,
Пять — «я предпочту не шифровать трафик, чтобы видеть сеть».



Это почти совпадает с мнением зарубежных коллег: 56,3% опрошенных SANS скорее обеспокоены тем, что шифрование препятствует прозрачности сети (оценили обеспокоенность в 6-10 баллов).

Оценка уровня волнения из-за шифрования трафика



Шифрование внутри корпоративной сети — тема неоднозначная. В некоторых случаях шифрование — необходимо, например, все пароли и электронные письма должны передаваться в зашифрованном виде. Но зашифровать весь трафик для многих инфраструктур, в особенности крупных, сложно из-за старого серверного оборудования и специфичного софта. Стоит учитывать, что даже если это получится, то действия злоумышленников тоже окажутся под прикрытием и обнаружить их будет сложнее.

Выводы

- NTA-системы ждет большое будущее, поскольку компании осознают важность и необходимость мониторинга безопасности внутренней сети. Об это говорит то, какие задачи для инструментов анализа трафика специалисты по ИБ оценили как наиболее приоритетные.
- Скорее всего, еще не во всех компаниях используются системы анализа трафика NTA для мониторинга внутренней сети. Мы можем об этом судить по тому, что за прошедший год специалистам удалось выявить внутри периметра.
- Большинство специалистов не поддерживают идею полного шифрования корпоративной сети, а значит у NTA-систем будет больше возможностей для обнаружения подозрительной активности. Тем, кто все-таки постарается зашифровать все по максимуму, NTA будут полезны в части выявления аномалий и вредоносного ПО.

Спасибо нашим партнерам за поддержку опроса: группе компаний Angara, компаниям «Анлим ИТ», «ДиалогНаука», «Инфосистемы Джет», «Софтлайн Кыргызстан», «Телеком Интеграция», «УЦСБ», «ХОСТ», Axxtel, OCS, TS Solution.

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «[Новости](#)» на сайте ptsecurity.com.