История успеха

# PT Network Attack Discovery еженедельно выявляет около 3000 попыток проникновения в инфраструктуру Генбанка

*«В качестве инструмента специалиста по информационной безопасности PT Network Attack Discovery разрушает монополию IT-службы на всевидящее око, — рассказывает **Игорь Серёгин, начальник отдела защиты информации АО «Генбанк»**. — Каждую неделю система обрабатывает порядка 150 миллионов сессий примерно с 400 тысячами узлов, обнаруживая не менее 3000 попыток проникновения в инфраструктуру банка, включая массовые атаки. Почти треть обнаруженных атак — высокой степени опасности».*

**ПРОФИЛЬ КОМПАНИИ**

**Название:** АО «Генбанк»

**Отрасль:** финансы

**Клиенты:** коммерческие предприятия, торговые компании, российские финансовые институты, а также частные лица

**IT- инфраструктура:** более 2000 узлов

**Задача:** выявление целевых атак на ранних этапах, расследование инцидентов, контроль появления новых устройств в сети

**Решение:** PT NAD — система поведенческого анализа сетевого трафика (network traffic analysis, NTA) для контроля вредоносной активности на периметре и внутри сети

**КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА**

- Показывает злоумышленников во всей сети
- Выявляет хакерский инструментарий и модифицированное вредоносное ПО
- Помогает выполнить требования к защите информации, в том числе к безопасности объектов КИИ и финансовых операций
- Интегрируется с решениями классов SIEM и sandbox
- Требует меньше одного часа на внедрение в промышленную эксплуатацию

## О клиенте

По данным независимых информационно-аналитических агентств, акционерное общество «Генбанк» входит в топ-150 российских банков. АО «Генбанк» включено в реестр кредитных организаций, признанных Банком России значимыми на рынке платежных услуг, а также в реестр банков, входящих в систему обязательного страхования вкладов физических лиц, обладает всеми видами лицензий, необходимых для осуществления банковских операций, и является членом Ассоциации банков России.

## Задача

Positive Technologies отмечает рост количества целенаправленных атак на банки, однако этот рост нельзя назвать стремительным: доля атак на финансовые организации от общего числа атак на компании к 2021 году уменьшилась вдвое. Причина в том, что для вывода денег из банка злоумышленник должен иметь высокую квалификацию. Банки уделяют большое внимание кибербезопасности, следуют отраслевым стандартам ИБ, поэтому по сравнению с остальными организациями их защищенность за последние годы выросла.

Генбанк не является исключением и ответственно подходит к обеспечению собственной информационной безопасности. Чтобы иметь полную картину о состоянии инфраструктуры ИТ и ИБ и вовремя замечать попытки атаковать компанию как внутри, так и снаружи, было решено внедрить для анализа сетевого периметра и контроля внутреннего трафика систему класса NTA. Как рассказал Игорь Серёгин, отделу ИБ важно видеть сетевой трафик и контролировать появление новых узлов или теневых активов. У службы ИБ был перечень требований к продукту: возможность быстро настроить и начать эксплуатировать систему; простой и понятный интерфейс продукта; возможность расследования инцидентов без специальной квалификации; низкое количество ложных срабатываний и отзывчивая техподдержка.

## Решение

В апреле 2022 года Генбанк выбрал для защиты сетевого периметра и контроля внутреннего трафика систему поведенческого анализа трафика Positive Technologies — PT Network Attack Discovery (PT NAD). Продукт соответствует всем требованиям, которые служба ИБ Генбанка выдвигала к системам класса NTA. Кроме того, важным критерием при выборе решения стали функциональные возможности, а именно поведенческий и статистический анализ трафика и включение в продукт знаний о противодействии атакам, собранных экспертным центром безопасности Positive Technologies (PT Expert Security Center).

PT NAD позволяет оперативно выявлять и расследовать сложные целевые атаки на предприятия и предоставляет инструменты для проактивного поиска злоумышленников в сети (threat hunting), делая сетевую инфраструктуру прозрачной для аналитика security operations center. В Генбанке PT NAD покрывает критически важные узлы и проверяет трафик, который проходит через периметровые шлюзы.

**PT NAD ВЫЯВЛЯЕТ**

- Угрозы в зашифрованном трафике
- Применение хакерского инструментария, включая самописный
- Горизонтальное перемещение злоумышленника
- Сетевые аномалии
- Зараженные сетевые узлы
- Атаки на контроллер домена
- Признаки атак, не обнаруженных ранее
- Эксплуатацию уязвимостей в сети
- Признаки сокрытия активности от средств защиты
- Автоматически сгенерированные домены
- Нарушения регламента ИБ

Специалисты отдела ИБ банка дополнительно прошли обучение, чтобы ознакомиться со всеми возможностями PT NAD. По словам Игоря Серёгина, команде хватило просмотра трех вебинаров, чтобы уверенно работать с продуктом и уже через неделю после развертывания системы видеть первые атаки. Команда Генбанка также выделила отзывчивость службы поддержки, помощь Telegram-сообщества PTNADChat и отметила пользу вебинаров экспертов Positive Technologies и электронных курсов на сайте edu.ptsecurity.com.

## Результат

**С помощью PT NAD специалисты банка за несколько месяцев выявили:**

- Использование словарных паролей. Так, например, оказалось, что удаленные сотрудники использовали для подключения простейшие пароли. Служба ИБ совместно с IT-отделом скорректировала парольные политики: было увеличено количество знаков — с восьми, рекомендуемых Центральным банком Российской Федерации, до двенадцати, а IT-специалисты были переведены на двухфакторную аутентификацию. В планах — переход на беспарольную защиту. Также сотрудникам банка рассказали об опасности использования простых паролей; информация о парольной политике была добавлена во вводный инструктаж.
- Подключения к ресурсам банка из-за границы. Теперь все сторонние подключения проводятся с территории России.
- Обращения ряда узлов к командным серверам APT-группировок. В качестве противодействия злоумышленникам специалисты банка обновили сигнатуры межсетевых экранов и защиту конечных точек.
- Новые неучтенные узлы внутри сети — около 30. На них были установлены средства защиты конечных точек.
- Передачу учетных данных (логинов, паролей и адресов электронной почты) в открытом виде между компонентами инфраструктуры. Сотрудники службы ИБ банка передали информацию о работе софта подрядчику, который исправил проблему в соответствии с требованиями Центрального банка Российской Федерации. Сейчас коммуникация переведена на защищенные протоколы.

---

*«Всего в „Ленте активностей" за время работы PT NAD было зафиксировано 5700 потенциальных угроз, включая 90 высокого уровня опасности. При этом результаты мониторинга сети Генбанка не выявили успешных проникновений в сеть организации. Это доказывает ответственный подход Генбанка в обеспечении информационной безопасности», — рассказывает* ***Дмитрий Ларин, начальник управления информационной безопасности АО «Генбанк».***

**ptsecurity.com**
pt@ptsecurity.com