Деньги целы: киберзащита финтеха

О том, как найти баланс между инновациями и защитой инфраструктуры банка или другой финансовой организации, какие преимущества открывают решения класса XDR, рассказано в этой статье

Текст
ЕВГЕНИЯ ЛАГУТИНА,
РУКОВОДИТЕЛЬ ГРУППЫ ПО СОПРОВОЖДЕНИЮ ПРОЕКТОВ ВНЕДРЕНИЯ СИСТЕМ МОНИТОРИНГА ИБ И SOC-СЕРВИСОВ, «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

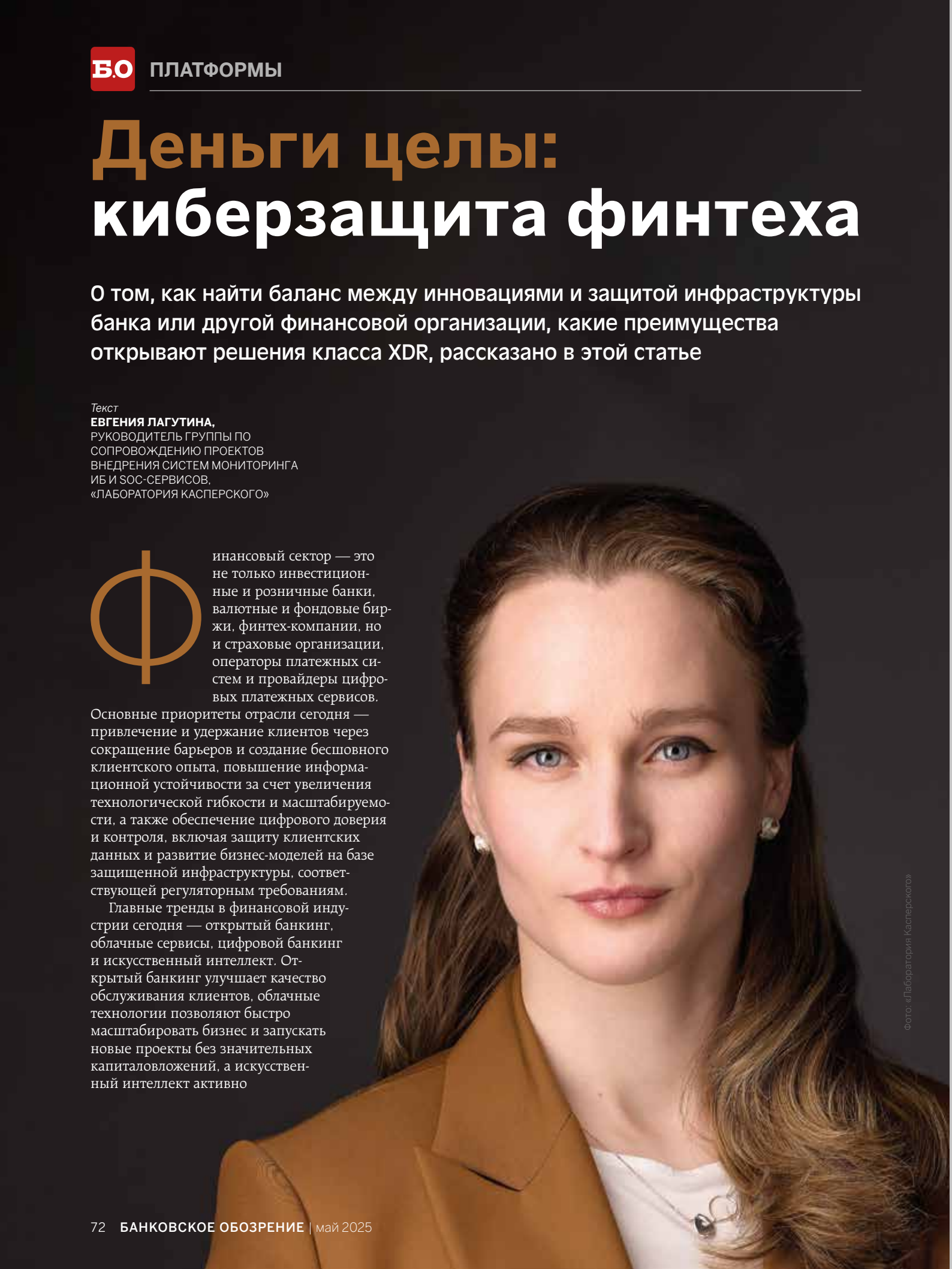


Фото: «Лаборатория Касперского»

Финансовый сектор — это не только инвестиционные и розничные банки, валютные и фондовые биржи, финтех-компании, но и страховые организации, операторы платежных систем и провайдеры цифровых платежных сервисов. Основные приоритеты отрасли сегодня — привлечение и удержание клиентов через сокращение барьеров и создание бесшовного клиентского опыта, повышение информационной устойчивости за счет увеличения технологической гибкости и масштабируемости, а также обеспечение цифрового доверия и контроля, включая защиту клиентских данных и развитие бизнес-моделей на базе защищенной инфраструктуры, соответствующей регуляторным требованиям.

Главные тренды в финансовой индустрии сегодня — открытый банкинг, облачные сервисы, цифровой банкинг и искусственный интеллект. Открытый банкинг улучшает качество обслуживания клиентов, облачные технологии позволяют быстро масштабировать бизнес и запускать новые проекты без значительных капиталовложений, а искусственный интеллект активно

внедряется для обработки данных и автоматизации рутинных операций. В условиях цифровой трансформации финансовая отрасль сталкивается с новыми вызовами и возможностями: финансовые маркетплейсы, цифровые валюты, гиперавтоматизация, встроенные финансы, цифровые двойники. Но новые возможности требуют управления сложной и распределенной инфраструктурой. Одновременно растут риски, связанные с безопасностью данных и инфраструктуры. Обязательным становится соблюдение строгих мер информационной безопасности, кроме того, необходимо соответствовать ужесточающимся требованиям регуляторов.

Для России характерны свои внутренние тренды: импортозамещение в IT-сфере, усиление регуляторных требований, активизация слияний и поглощений, рост внутренней разработки и увеличение объема трансграничных переводов. Финансовые организации, работающие с крупными объемами транзакций и «живыми» деньгами, становятся мишенью для продвинутых киберпреступников.

Какие именно угрозы актуальны для финансового сектора сегодня? В их числе — программы-шифровальщики, фишинговые атаки и инциденты, спровоцированные злонамеренными действиями сотрудников (так называемые инсайдерские атаки). Помимо массовых атак финансовые институты подвергаются спланированным нападениям. Среди распространенных угроз — атаки с использованием уязвимостей нулевого дня и атаки на цепочки поставок. В 2024 году эксперты «Лаборатории Касперского» обнаружили потенциально самую опасную атаку на цепочку поставок за все время существования Linux-систем, а также уязвимость нулевого дня в одном из самых популярных браузеров.

Еще одна ключевая угроза — банковские троянцы, которые крадут данные учетных записей электронных банковских систем, систем электронных платежей, пластиковых карт пользователей этих услуг. В 2024 году 1700 финансовых институтов и их пользователей стали целью троянца Grandoreiro, также эксперты «Лаборатории Касперского» обнаружили многоэтапный банковский троянец Coyote, нацеленный на клиентов более 60 финансовых учреждений.

Злоумышленники используют разнообразные методы: в 2024 году выросло число атак с применением искусственного интеллекта, а также атак на системы мгновенных платежей, увеличилось число бэкдоров в ПО с открытым исходным кодом, чаще эксплуатировались ошибки конфигурации и писалось вредоносное ПО на популярных кроссплатформенных языках.

В 2025 году, по данным экспертов, увеличивается активность стилеров, растет число атак на механизмы открытого банкинга и цепочки поставок в проектах с открытым исходным кодом, получила популярность модель «шифровальщик как услуга», растет число финансовых кибератак через смартфоны.

К чему приводят атаки на финансовый сектор? Помимо собственно кражи средств в числе последствий — утечки данных, сбои в бизнес-процессах и репутационные потери. При этом с 1 января 2025 года штраф за утечку персональных данных в России вырос до 500 млн рублей.

По данным аналитического отчета «Лаборатории Касперского», в 2024 году финансовый сектор вошел в число трех отраслей, которые чаще других сталкивались с киберугрозами. Решение Kaspersky Managed Detection and Response зафиксировало свыше 270 тыс. предупреждений по всему миру. По некоторым данным, средний ущерб от целевой атаки для финансовой организации может достигать 80 млн рублей.

Цифровая трансформация значительно расширяет поверхность атаки и порождает новые уязвимости, при этом финансовым организациям приходится защищать все более сложную инфраструктуру. Основные трудности — устаревшие системы, дефицит квалифицированных специалистов, бюджетные ограничения и жесткие регуляторные требования.

В 2025 году финансовым организациям необходимо совмещать инновации с усилением кибербезопасности, делая акцент на предиктивной аналитике и межотраслевых стандартах. В ответ на новые вызовы «Лаборатория Касперского» предлагает комплексный подход, обеспечивающий защиту всех элементов IT-инфраструктуры — от мобильных устройств до облачных сервисов. Такой подход позволяет обеспечить надежную защиту каждого звена IT-инфраструктуры, уберечь организацию от ущерба, связанного с целевыми атаками, сохранить ее репутацию и доверие клиентов.

«Лаборатория Касперского» создает продукты, которые не только отвечают сегодняшним вызовам, но и готовы к вызовам завтрашнего дня. Они позволяют прогнозировать, предотвращать, обнаруживать и реагировать на потенциальные угрозы, предоставляя высочайший уровень обнаружения кибератак, подтвержденный независимыми тестами. Например, линейка решений Kaspersky Symphony дает организациям все необходимое для постепенной или одночастной реализации подхода к построению надежной и адаптивной системы кибербезопасности. Все элементы этой экосистемы дополняют и усиливают друг друга.

Наиболее продвинутый уровень этой линейки — Kaspersky Symphony XDR. Его главное преимущество заключается в нативной интеграции компонентов на всех этапах работы с инцидентом информационной безопасности — от сбора информации до устранения последствий. Это экономит время, упрощает и облегчает своевременный анализ потенциальной вредоносной активности, обеспечивая точность и скорость этого процесса. Таким образом, ИБ-команды могут быстрее определять приоритетность данных об угрозах по степени их серьезности. Использование XDR для мониторинга всей активности в IT-инфраструктуре позволяет организациям выявлять подозрительную активность, свидетельствующую о наличии потенциальной угрозы, и предпринимать упреждающие шаги по ее снижению.

Финансовый сектор России стоит на пороге новых возможностей и вызовов, где успех зависит от баланса между инновациями и надежной защитой цифровой инфраструктуры. Б.О

реклама