

Как финтеху защититься от киберугроз и не перегрузить инфраструктуру



С увеличением популярности финтех-сервисов и увеличением объема цифровых финансовых операций растут и риски безопасности. Основная цель атак — коммерческая выгода, поэтому компании финансового сектора всегда под угрозой. Для них безопасность становится бизнес-приоритетом, так как утечки данных или инциденты могут нанести серьезный ущерб репутации. Регулирующие органы предъявляют к ним строгие требования по защите

Текст
ОЛЬГА МАЛАХОВСКАЯ,
 PR-МЕНЕДЖЕР КОМПАНИИ «АЙТИ БАСТИОН»

беспечение безопасности в финтехе требует значительных финансовых и организационных вложений, так как задачи усложняются, а изменения должны внедряться регулярно. Какие стратегии управления привилегированным доступом наиболее эффективны?

Финансовый сектор постоянно сталкивается с разными киберугрозами: фишингом и социальной инженерией, DDoS-атаками, атаками на API, мошенничеством и кражей данных. Все они требуют серьезного подхода к защите на каждом уровне инфраструктуры.

Баланс между защитой и бюджетом

Коммерческие ресурсы — один из ключевых факторов при выборе ИБ-решений. Компании часто ищут баланс между высоким уровнем защиты и оптимальными затратами, избегая перегрузки бюджета. Важно учитывать возможность использования комплексных решений, особенности лицензирования, поддержки и потенциал масштабирования для адаптации к новым угрозам.

Финтех-сервисы — сложные системы с высокими требованиями к надежности. Несмотря на автоматизацию, для многих процессов необходимо участие оператора, а ошибки могут приводить к простоям и снижению доходов.

Для управления такими системами подходят решения класса PAM, например СКДПУ НТ, которые позволяют управлять привилегированным доступом, мониторингом и снижением рисков безопасности, а также расширять функционал по мере необходимости. Это снижает затраты и упрощает администрирование, освобождая IT-специалистов для стратегических задач.



«PAM-платформа СКДПУ НТ создана как модульная система, способная внедряться в различных конфигурациях и выдерживать разнообразные нагрузки. Опыт разработки и внедрения таких решений подтверждается многолетней эксплуатацией у клиентов, часть которых используют систему более пяти лет. За это время изменяются не только задачи бизнеса, но и окружение системы: появляются новые требования к производительности, возникает необходимость интеграции с другими компонентами IT-инфраструктуры, а также появляются задачи по восстановлению после сбоев», — прокомментировал новинку технический директор компании «АйТи Бастион» **Дмитрий Михеев**.





Автоматизация и минимизация человеческого фактора

Ключевые компоненты IT-систем, особенно связанные с обработкой финансовых транзакций, подвержены наибольшему риску, так как именно они чаще всего становятся мишенью атак. Эти компоненты защищены, но требуют постоянного улучшения.

Для эксплуатации таких динамичных элементов, которые могут быть изолированы от остальной инфраструктуры, необходим постоянный мониторинг данных и обновлений. Для этого используются специализированные системы, такие как «Синоникс». Эти системы добавляют меры безопасности в существующие IT-структуры без серьезных изменений, минимизируют участие операторов, автоматизируют обнаружение угроз и разделяют зоны ответственности, что ускоряет реагирование на угрозы и снижает затраты на безопасность за счет автоматизации.

Гибкость и адаптивность

Финтех-компании быстро растут, и требования к информационной безопасности постоянно увеличиваются. ИБ-решения должны быть гибкими и масштабируемыми, чтобы адаптироваться к росту числа пользователей, объема данных и усложнению процессов.

Потенциал для расширения функционала — важный критерий, позволяющий компании реагировать на новые угрозы без значительных затрат. Масштабируемость достигается благодаря модульной архитектуре, гибкой интеграции и поддержке облачных технологий.

СКДПУ НТ имеет модульную архитектуру, позволяющую поэтапно вводить новые функции. Например, можно начать с мониторинга, а затем добавить контроль активности привилегированных пользователей.

Дмитрий Михеев добавил: «Важными аспектами успешного использования СКДПУ НТ являются постоянное сопровождение и обновление системы. Для крупных компаний, которые развивались вместе с продуктом, потребности изменялись: от базовой системы контроля доступа до комплексного решения с высокой производительностью, устойчивостью к катастрофам и распределением по нескольким дата-центрам. Это требует не только времени, но и глубокого опыта инженеров и разработчиков, что особенно важно для крупных клиентов».

Как правило, средства безопасности в сложных инфраструктурах развиваются вместе с ними через расширение ресурсов, усложнение архитектуры и интеграцию между разными решениями.

«В процессе эксплуатации систем часто возникает запрос на масштабирование. Многие проекты начинались с небольших конфигураций, а затем расширялись до многосерверных систем с требованием обеспечения катастрофоустойчивости. Запросы заказчиков на повышенную надежность и производительность идут следом за функциональностью. В таких ситуациях гибкость системы и готовность адаптироваться под новые задачи становится решающим фактором выбора», — дополнил *Дмитрий Михеев*.

Безопасность и нормативная база

Финансовый сектор строго регулируется на всех уровнях, и соблюдение нормативных требований критически важно для его участников. Ужесточение требований в области защиты данных заставляет компании интегрировать решения, которые не только соответствуют существующему законодательству, но и могут оперативно адаптироваться к изменяющимся нормативам.

Дмитрий Михеев рассказал: «Рост требований со стороны регуляторов — это неизбежный процесс для всех, кто работает в секторе информационной безопасности. Эти требования вызывают естественное сопротивление на рынке, так как их внедрение сопряжено с дополнительными затратами и организационными изменениями. Тем не менее компании (особенно те, которые работают с крупными государственными и коммерческими структурами) вынуждены следовать этим требованиям, чтобы соответствовать коммерческим и государственным стандартам».

В условиях изменяющегося регулирования компаниям важно учитывать несколько факторов при выборе ИБ-решений. Во-первых, соответствие международным стандартам для соблюдения требований и снижения риска штрафов. Во-вторых, автоматизация отчетности и аудита, как в системах СКДПУ НТ, упрощающая выполнение требований регуляторов. В-третьих, мониторинг активности пользователей для контроля доступа к конфиденциальным данным, что также обеспечивает СКДПУ НТ.

«Хотя интеграция новых нормативных требований часто вызывает задержки, компании понимают, что соответствие регуляторным нормам — это обязательное требование для ведения бизнеса. В таких условиях СКДПУ НТ предлагает инструменты, которые помогают предприятиям соответствовать нормативным требованиям без значительных сложностей и затрат», — заключил *Дмитрий Михеев*.

Фундамент работы в будущем

Рассмотренные выше решения не только защищают данные и обеспечивают соответствие нормативным требованиям, но и оптимизируют бизнес-процессы. Они позволяют финтех-компаниям автоматизировать обеспечение безопасности, сокращая ручной труд и снижая вероятность ошибок.

Интеграция с IT-инфраструктурой адаптирует продукты под потребности компании, создавая единое пространство для мониторинга и управления, что ускоряет обнаружение угроз и освобождает IT-специалистов для решения стратегических задач. Это повышает прозрачность, упрощает управление доступом и соблюдение требований регуляторов. Автоматизация и интеграция решений «АйТи Бастион» создают надежную основу для безопасного будущего бизнеса.

