AI Native Bank: инновации под киберзащитой

В основе бизнес-процессов банков нового типа лежат хранилища данных и знаний, к которым должны иметь персонально настроенный доступ ИИ-агенты и сотрудники банка. Как в этих условиях дать всем свободу, сохранив безопасность?

Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ «Б.О»

«Определитесь, в какой момент времени вы начнете думать о кибербезопасности, и заранее заложите некие реперные точки ИБ-контроля при запуске стартапа или внедрении любой новой технологии в организации, включая ИИ. Если вы бежите вперед исключительно как бизнес, вы очень легко можете пропустить критические риск-события как поднадзорная регуляторам финансовая компания», — поделился практическим опытом **Всеслав Соленик**, директор по кибербезопасности компании «СберТех», в ходе сессии «Безопасность ИИ-агентов» в рамках Форума Data Fusion 2026, организованного банком ВТБ.

А что делать, если ИИ сам начинает проектировать IT-системы, сам пишет значительную часть программного кода, а главное — начинает сам перепроверять результаты работы другой модели ИИ при тестировании? По словам спикера, при сегодняшнем уровне развития технологий только те самые точки контроля вкупе с инфраструктурой логирования позволят обеспечить прозрачность ИИ-процессов.

Вопросы на засыпку

Но возникает вопрос: «А где именно нужно расставлять эти точки?» Частичный ответ может дать знание IT-архитектуры современного AI-native-банка, но и это знание сегодня на финансовом рынке является уникальным бизнес-преимуществом узкого круга участников. Часть ответа может находиться у бизнеса, который должен, опираясь на собственное критическое мышление, определиться, какие потенциальные риски он готов принять, поскольку международные практики и фреймворки грешат неточностями, а просчитанных кейсов того, что может пойти не так, например, при использовании ИИ-агентов, не так много.

Однако в качестве стартовой точки для ИБ-команды для начала внедрения ИИ в организации можно использовать критически осмысленные из-за наличия неточностей рекомендации OWASP Top 10 for Agentic Applications 2026. Это глобально рецензируемый фреймворк, который идентифицирует наиболее критические риски для автономных и агентных систем ИИ.

В блоге компании OWASP на портале «Хабр» так описывается актуальность документа: «Если LLM — это мозг, то агентные системы — это полноценный организм с руками и ногами. Это ИИ, которые не просто отвечают на вопросы, а могут самостоятельно ставить цели, планировать и выполнять многошаговые задачи, используя различные инструменты, например API и браузер».

При этом агентные системы — это следующий шаг в эволюции ИИ. Они обещают беспрецедентную производительность и автономию, но вместе с тем несут в себе риски, которые только начинают осознавать банкиры.

На основе ИИ-агентов, собственно, и строится архитектура AI Native Bank. Генеральный директор компании «ФлексСофт» **Аркадий Лобас** в интервью «Б.О» дал ей такое определение: «Суть концепции AI Native Bank заключается в переходе к автоматическим процессам на основе ИИ, тем самым позволяя в автоматическом режиме формировать новые ценности как для клиента, так и для банка, выстраивать персональный банкинг для каждого клиента».

На конференции «ИИ-БАНКИНГ_26: От инициатив к системе», организованной «Б.О», были предложены некоторые практические концепты реализации AI Native Bank. В их числе оказались динамически изменяемая IT-архитектура с использованием программно-определяемых хранилищ и сетей от «ФлексСофт», а также непрерывное улучшение процессов в реальном времени, в основе чего лежат AI driven BPMN-платформа и отраслевая банковская LLM-модель.

А о том, что находится «под капотом» в Сбере, в декабре 2025 года на конференции Sber AI Journey 2025 рассказал **Кирилл Меньшов,** старший вице-президент, руководитель блока «Технологии» СберБанка. По его словам, внедрение ИИ-агентов требует новых подходов к архитектуре платформ управления данными — перехода от развития Data Warehouse и Data Lake к Data Lakehouse, а также перестройки систем управления знаниями для представления данных в контексте для Gen AI.

Кто сказал «управление данными?»

Никто не будет спорить с тем, что ядро AI Native Bank — это платформы управления данными и знаниями, все остальное еще должно доказать свою жизнеспособность и востребованность. А как защищать данные?

В ходе Data Summit 2026, организованного ГК DIS Group, эксперты пришли к мнению, что помимо классических ИБ-механизмов, применимых к хранилищам информации, AI Native Bank должен решить две дополнительные задачи. Во-первых, обезопасить данные как актив организации, обеспечив контроль доступа, маскирование, регулирование и риск утечек чувствительной информации. Во-вторых, поскольку доступ к данным нужен всем (от сотрудников до ИИ-агентов, как своих собственных, так и принадлежащих регуляторам), в полный рост встает задача выстраивания механизмов AI Governance и Data-literacy, а также принципов федерализации и демократизации доступа к данным. А как вишенка на торте требуется решение задачи внедрения цифровым офисом банка концепции Data Mesh (этот вопрос банкиры и биржевики подняли на Форуме Data Fusion 2026, запись доступна).

По словам **Владимира Громова,** заместителя руководителя департамента технологического развития общебанковских систем ВТБ, демократизация не означает открытия данных для всех. Главная задача — выстроить прозрачную и быструю систему доступа, где каждый получает только те данные, которые необходимы ему для работы, с учетом требований безопасности.

Борис Рабинович, старший управляющий директор Сбера, добавил: «Демократизация должна сопровождаться четкими правилами: кто, к каким данным и на каких условиях получает доступ. Причем у ИИ-агентов появляется метрика time to data, а для всех потребителей, если они работают удаленно, должен включаться весь комплекс ИБ-мер, направленных на маскирование, шифрование, обезличивание и т.д. Надо помнить: для банка все это имеет свою стоимость, что заставляет думать о целесообразности тех или иных бизнес-решений. В Сбере демократизация данных сейчас прочно ассоциируется с сервисом “Супермаркет данных”».

Иван Глухов, исполнительный директор компании «СберТех», подробно рассмотрел, как расширение доступа к данным и искусственному интеллекту меняет ландшафт с точки зрения корпоративной безопасности, сделав акцент на четырех моментах:

1) ***рост числа утечек.*** Сотрудники все чаще используют большие языковые модели (LLM) для повышения эффективности, но при этом могут случайно или намеренно отправлять в ИИ чувствительные данные;
2) ***внутренние угрозы.*** Даже в защищенном контуре сотрудник не изолирован: коллеги могут попытаться получить доступ к чужим данным, а ИИ-агенты — стать инструментом для компрометации информации;
3) ***угрозы от ИИ-агентов.*** Автоматизированные агенты могут быть скомпрометированы, могут выполнять вредоносные действия, уничтожать или искажать данные;
4) ***галлюцинации и артефакты ИИ.*** Модели могут генерировать не только ошибочные, но и опасные артефакты (например, вредоносный код), которые требуют обязательной проверки.

Все эксперты согласились с тем, что, даже если ИИ работает исключительно внутри защищенного периметра, риски сохраняются. Сотрудники (как живые, так и цифровые), а также автоматизированные агенты остаются потенциальными источниками угроз, а сами модели могут быть использованы для создания новых векторов атак.

С чем еще соглашаются большинство ИБ-экспертов? С тем, что ИИ должен стать более управляемым, предсказуемым и прозрачным. Только в этом случае банки получают возможность развивать инновации, не опасаясь неконтролируемых утечек или атак, и могут строить долгосрочную бизнес-стратегию развития с учетом новых угроз. Б.О