Кибербезопасность на кону

Развитие ГосСОПКА позволяет устранить регуляторные барьеры, ограничивающие участие высокотехнологичных компаний и банков в предупреждении и ликвидации последствий компьютерных атак

Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

14 апреля 2026 года на первом форуме по проблематике государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы (ГосСОПКА) **Вадим Уваров,** директор департамента информационной безопасности Банка России, в ходе своего выступления на основе опыта, накопленного ФинЦЕРТ (Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере), дал коллегам несколько рекомендаций на 2026 год. Сделано это было, очевидно, в целях обозначения направлений реальных усилий для получения синергии от усилий структур ФСБ и Банка России.

Во-первых, он затронул крайне болезненную тему современной криптографии, используемой злоумышленниками для политически мотивированных атак с зашифровыванием всей IT-инфраструктуры организаций в целях полного паралича бизнес-процессов. Во-вторых, это кража данных у «безобидных» компаний с дальнейшим использованием механизма «атака через посредника на реальную жертву». Этот механизм, по всей видимости, стал тормозом для прохождения в Госдуме проекта закона «Об аутсорсинге в финансовой сфере». Совместными усилиями наверняка можно будет сдвинуть законопроект с мертвой точки. И, наконец, это абсолютно новый класс атак с использованием ИИ. В этой связи спикер упомянул об инциденте, связанном с компанией Anthropic.

Скорость против «искусственных мозгов»

Вадим Уваров не указал на конкретный кейс, но можно утверждать, что имелся виду вызов 7 апреля 2026 года министром финансов США **Скоттом Бессентом** и председателем ФРС **Джеромом Пауэллом** руководителей крупнейших американских банков на срочное совещание в связи с опасениями, что новейшая ИИ-модель Mythos от компании Anthropic положит начало «эре повышенных киберрисков».

Издание Bloomberg отметило, что организованная в сжатые сроки встреча — признак того, что регуляторы рассматривают новый тип кибератак как одну из крупнейших угроз для финансовой отрасли. Согласно данным самой Anthropic, Mythos уже обнаружила тысячи серьезных уязвимостей, в том числе «во всех основных операционных системах и веб-браузерах», которые оставались незамеченными более десяти лет. При этом, как отметили в Financial Times, ранее в Сеть уже утекали связанные с моделью ИИ документы и исходный код ассистента от компании Anthropic — модели Mythos. Даже Пентагон официально уведомил Anthropic, что компания и ее продукция несет риски для цепочек поставок в США.

Но это все «у них». У нас с ИИ своих проблем хватает. По данным Банка России, это использование моделей для создания все более изощренных схем мошенничества, включая фишинг и дипфейки. Кроме того, отмечается рост числа атак на финансовые организации и их клиентов с помощью автоматизированных инструментов. Здесь же генерация и распространение ложной информации и фейков, что может дестабилизировать рынки и подорвать доверие к финансовым институтам.

Представитель Банка России в итоге задал залу риторический вопрос: «Как блокировать уязвимости финансовой системы из-за чрезмерной автоматизации и зависимости от ИИ?»

Опыт ФинЦЕРТ позволил ответить на этот вопрос так: «Здесь важны максимально возможные скорость реакции и количество источников информации об аналогичных инцидентах со всей страны».

ФинЦЕРТ и 7 приказов ФСБ

«С началом СВО ландшафт угроз очень сильно изменился — выросли масштабы, увеличилась интенсивность этих угроз. Также выросла изощренность компьютерных атак, которые мы наблюдаем», — заявил заместитель директора Национального координационного центра по компьютерным инцидентам (НКЦКИ) **Петр Белов,** выступая на форуме.

В интервью телеканалу «Вести» он добавил: «Банковская система сейчас относительно устойчива к компьютерным атакам, о чем говорит отсутствие крупных инцидентов в этой сфере. Наверное, это обусловлено тем, что Банк России является регулятором, в том числе по вопросам ИБ, и много внимания уделяет всем этим процессам. Кроме того, в рамках Банка России функционирует ФинЦЕРТ — центр ГосСОПКА в кредитно-финансовой области. Мы с ними плотно работаем».

Почему же представители НКЦКИ так любезны с финансистами? Никто не скрывал, что ГосСОПКА, подведомственная НКЦКИ, как ИБ-система была создана для масштабирования успешного опыта работы ФинЦЕРТ, который эффективно справлялся с киберугрозами в финансовом секторе. Это позволяет внедрять луч-

Вадим Уваров (Банк России)

Фото: ГосСОПКА

шие практики и технологии, разработанные в рамках ФинЦЕРТ, в масштабах всей страны, что значительно повышает уровень защиты от компьютерных атак и инцидентов.

В рамках изменений, внесенных в Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», безопасность значимых объектов КИИ теперь включает в себя не только защиту от инцидентов, но и контроль цепочек поставок, технологическую независимость и управление обновлениями. Это расширяет обязанности организаций и требует более тесного взаимодействия с НКЦКИ для обеспечения комплексной безопасности.

Согласно обновленной редакции закона, организации обязаны не только сообщать о компьютерных инцидентах, но и передавать информацию о компьютерных атаках, включая данные, выявленные на ранних стадиях. Это изменение в законодательстве требует от финансовых организаций более активного взаимодействия с НКЦКИ и центрами ГосСОПКА.

Для реализации новых требований ФСБ обновила семь своих приказов, что способствовало улучшению взаимодействия между НКЦКИ и финансовыми организациями. В частности, в августе 2025 года был продлен переходный период, позволяющий организациям привлекать сторонние компании для взаимодействия с ГосСОПКА до 2027 года. Это создает дополнительные возможности для организаций в области кибербезопасности с применением технологий на базе ИИ.

А вот здесь у Банка России и его поднадзорных оказалась огромная фора, что отразилось на количестве секций и дискуссий с участием финансистов в ходе форума.

Работает киберразведка

Чем конкретно банкиры готовы помочь коллегам? В ходе представительной пленарной сессии «Роль ГосСОПКА в противодействии преступлениям, совершаемым с использованием информационно-коммуникационных технологий» **Сергей Лебедь,** вице-президент по кибербезопасности СберБанка, заявил о необходимости совместными усилиями усовершенствовать нормативно-правовую базу для проактивного выявления и блокировки вредоносных ресурсов. Конечная цель — сделать фишинг экономически нецелесообразным для мошенников.

«Сбер готов предложить свои наработки в этой области. Наша внутренняя платформа киберразведки содержит модуль для работы с фишингом. Этот модуль мы успешно перенесли на нашу внешнюю платформу управления киберугрозами — X Threat Intelligence. Подключенные к ней организации уже узнали о десятках тысяч фишинговых ресурсов, которые имитировали их бренд», — поделился информацией Сергей Лебедь.

Сбер уже разработал техническую основу для общероссийского сервиса оперативного реагирования на фишинговые атаки. Однако банк не обладает необходимыми регуляторными полномочиями для делегирования доменов и блокировки доступа к вредоносным ресурсам. Кроме того, необходимо объединить возможности высокотехнологичных компаний с административным ресурсом госструктур, что может стать прорывом в борьбе с фишингом.

По информации Сбера, «Платформа киберразведки» банка позволяет собирать актуальную информацию о новых киберугрозах и технологиях на разных языках. Сообщения поступают каждый час. С помощью ИИ сервис ежедневно обрабатывает информацию из более чем 1,5 тыс. источников. Данные киберразведки позволяют выявить и блокировать серверы злоумышленников до начала атак.

Конечно же, банкирам есть что предложить и сверх того. Но очевидно, они ждут первых результатов деятельности ГосСОПКА, после чего диалог, без сомнения, продолжится. Б.О