Быстрее ИИ

Банк России инициировал множество изменений и дополнений в нормативные акты, касающиеся обеспечения непрерывности банковского бизнеса и обеспечения его ИБ. В чем суть изменений и каковы их причины?



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



В апреле 2024 года получило свое практическое подтверждение то, о чем так долго спорили специалисты: GPT-4 научился создавать рабочие эксплойты для критических уязвимостей ПО. ИИ смог абсолютно самостоятельно создать готовый код для удаленного выполнения программ без аутентификации, что является уязвимостью с максимальной оценкой по шкале CVSS.

Эта история показывает, как ИИ меняет правила игры в кибербезопасности. Чем мощнее становятся инструменты, тем меньше времени остается между обнаружением уязвимости и ее эксплуатацией. Раньше на ее поиск ушли бы дни работы серьезных экспертов. Теперь достаточно знать основные принципы промпт-инжиниринга. А вот автоматизация процесса поиска резко снижает барьер входа для злоумышленников.

О чем говорят официальные итоги 2024 года

Если у кибермошенников наблюдается некая эйфория, то профессиональные борцы с ними бьют тревогу.

В частности, **Рустэм Хайретдинов,** заместитель генерального директора компании «Гарда Технологии», комментируя у себя в социальных сетях некоторые итоги ИБ-рынка за 2024 год с учетом опубликованной отчетности ФНС по крупным игрокам, отметил: «Управлять ИБ-компанией, ориентируясь на отчеты за прошлый год, все равно, что вести машину, глядя в зеркало заднего вида. Из прошлогодних показателей не сильно понятно, куда бежать и что делать».

Одной из причин беспокойства является другой, но пока официально не зарегистрированный факт: «В игру “мы соберем из опенсорса свою сборку и сертифицируем ее” научились играть многие. Крупные заказчики могут сделать это сами для себя (уменьшив таким образом рынок ИБ), а обкатав на собственной крупной инфраструктуре — выпустить на рынок, увеличив конкуренцию».

Это уже приводит к тому, что рынок ИБ дробится. Теперь нужно поддерживать все больше и больше новорожденные СУБД и ОС, одной-двумя лидерскими уже не обойтись. Значит, вырастут расходы без роста доходов. Кроме того, в целом по рынку наблюдается падение доходов в секторе IT, а это означает появление интереса к соседнему ИБ-сегменту. Значит, доходы ИБ-компаний продолжат ускоренное снижение в то время как рост количества и качества угроз требуют значительных инвестиций в R&D.

Еще одна проблема, которая всерьез озаботила профессиональных участников ИБ-рынка, заключается в кризисе того, что раньше считалось краеугольным камнем безопасности: учебные центры. По мнению **Алексея Лукацкого,** известного эксперта в этой сфере, «центрам очень сложно конкурировать с бесплатным GPT (не говоря уже о платном), у которого сегодня можно

узнать почти все по интересующей теме. Ведь там, по сути, преподаватели в лице ИИ, не имеющие практического опыта, учат тому, что они прочитали и систематизировали. Раньше сам факт систематизации стоил многого, и за нее можно было платить. Сейчас любой GPT это делает быстрее и качественнее».

Что думают и делают регуляторы

Май 2025 года оказался богат на ответы государственных и финансовых регуляторов на значительную часть поднимаемых ИБ-сообществом вопросов, что, к сожалению, не всегда можно сказать про иные сферы. Это говорит только об одном: наработки Банка России будут привлекать все большее внимание всего отечественного бизнеса, что уже сейчас видно по аншлагам на мероприятиях, где обсуждаются актуальные проблемы кибербезопасности в банках.

Что касается самых свежих новостей, то с инициативой по криминализации DDoS-атак выступил заместитель Минюста **Вадим Федоров** на XIII Петербургском международном юридическом форуме. Пока такие атаки квалифицируются по действующим статьям 272 и 273 УК РФ. Эти меры являются более чем своевременными: практически в одно время с данным заявлением серверы Федеральной налоговой службы (ФНС) подверглись мощным DDoS-атакам, что привело к кратковременной недоступности электронных сервисов ФНС. Кроме того, поступали сообщения о проблемах в работе приложений «Госключ» и ЕМИАС «Электронная медицинская карта».

Помимо этого Минюст предожил ввести новую меру принуждения, касающуюся операций с денежными средствами: временное прекращение на 10 дней расходных операций по счетам, если они используются в преступных целях. Что касается наведения порядка в области обращения цифровых валют, то Минюст подготовил законопроект, который приравнивает цифровую валюту к имуществу, подлежащему аресту и последующей конфискации. Кроме того, предлагается закрепить специальные меры по обеспечению ее сохранности.

Непосредственно в сегменте обеспечения ИБ Банк России начал действовать на опережение, о чем сообщил консультант отдела нормативного регулирования и стандартизации управления методологии и стандартизации ИБ и киберустойчивости Департамента информационной безопасности Банка России **Георгий Ерохин.**

По результатам конференции «ИБ финансовых организаций: новое в нормативных требованиях и практике применения», проведенной 20 мая 2025 года компанией «ДиалогНаука» при поддержке АРБ, стал понятен смысл последних изменений в серии стандартов ГОСТ Р 57580 «Безопасность финансовых (банковских) операций» и множестве других нормативных актов.

Изменений довольно много, большинство из них сейчас находятся на стадии обсуждения с ИБ-сообществом в Техническом комитете (ТК) № 122, после чего будут утверждены официально.

Основную суть совместной работы банковских ассоциаций, ЦБ и финансистов выразил **Олег Скворцов,** председатель правления АРБ: «На повестке дня находятся вопросы стандартизации, нормативного регулирования, защиты ПДн, а также оценки соответствия требованиям по управлению рисками ИБ и операционной надежности». Говоря проще, Банк России твердо стоит на позициях приверженности концепции риск-ориентированного подхода к регулированию, который позволяет найти разумный компромисс между достаточностью обеспечения ИБ и затратами на этот процесс.

Понятно, что проблема, поднятая Рустэмом Хайретдиновым, не находится в компетенции финансового регулятора. Но Банк

Рустэм Хайретдинов:
«Управлять ИБ-компанией, ориентируясь на отчеты за прошлый год, все равно, что вести машину, глядя в зеркало заднего вида»



Алексей Лукацкий:
«Центрам очень сложно конкурировать с бесплатным GPT (не говоря уже о платном), у которого сегодня можно узнать почти все по интересующей теме»



Вадим Федоров:
«Предлагается криминализировать неправомерное воздействие на компьютерную информацию посредством DDoS-атак»



России в рамках своих полномочий будет облегчать жизнь и банкирам, и вендорам, непрерывно модифицируя и адаптируя к реалиям различные методические рекомендации (МР), в которых собраны лучшие практики в областях кибербезопасности, безопасной разработки ПО, реагирования на инциденты, управления непрерывностью бизнеса и т.д. Кроме этих документов вносятся правки в серию ГОСТ Р 57580 и некоторые Положения Банка России.

Помимо всего прочего возрастает роль независимого аудита ИБ, становящегося, по сути, «третьей доверенной стороной», статус которой повышается за счет повышения ее ответственности за результаты своей деятельности, обязанности банков предоставлять ей все необходимые документы, уточнении неоднозначной трактовки терминов и положений разных документов и т.д. Судя по всему, так или иначе будет ужесточен доступ к этой деятельности путем отдельного лицензирования вместо требования наличия простой лицензии ФСТЭК на техническую защиту конфиденциальной информации (ТЗКИ).

А вот значение обучения аудиторов, как и всех остальных ИБ-специалистов в финансовой сфере, под сомнение не ставится. Наоборот, регулятор не собирается сворачивать свои собственные программы, а сообщество аудиторов настаивает на более глубоком использовании опыта переподготовки кадров на основе рекомендаций PCI DSS и SWIFT.

Как в этой связи бороться со скоростями GPT? Очевидно, что стать быстрее ИИ можно только одним способом. Его суть заключается в том, что искусственный интеллект сегодня не способен создавать нечто новое и использует только известные факты. А вот сплоченное сообщество ИБ-специалистов благодаря коллективному разуму и возможностям уже в целом существующей IT-инфраструктуры может реально действовать на опережение! Б.О

ДОНОРСТВО КРОВИ. ФАКТЫ

Стандартный объем кроводачи 450 мл

Это минус твоего веса 477 гр

БРОСАЙ ДИЕТУ – СДАВАЙ КРОВЬ!

Утром перед сдачей крови необходим легкий завтрак. Не сдавайте кровь натощак!

Непосредственно перед кроводачей рекомендуется выпить 1-2 стакана горячего чая с сахаром



социальная реклама