финейтив

Согласно исследованию, опубликованному Cybersecurity Ventures, мировые расходы на киберпреступность достигнут 10,5 трлн долларов в год уже в 2025 году — это чуть меньше, чем вся экономика Соединенных Штатов или Китая.

10,5 трлн долларов → 2025 г

В этой статье мы расскажем, что могут сделать руководители в банковской сфере, чтобы уже сегодня сделать цифровые продукты безопасными для своих клиентов.

Пять шагов к созданию безопасного банковского сектора

Банк России продолжает фиксировать высокий уровень кибермошенничества в отношении финансовых институтов. Вот что можно предпринять уже сегодня:

Сделать кибербезопасность приоритетной задачей

Многие компании до сих пор склонны рассматривать кибербезопасность как техническую функцию, которая зависит от инцидентов и соблюдения нормативных требований. Часто банк начинает усиливать меры безопасности только после того, как обнаружит уязвимость или столкнется с последствиями атак.

Такой реакционный подход увеличивает репутационные риски и затраты на устранение последствий. Исправление ошибки в системе безопасности на этапе кодирования обходится в пять раз дороже, чем при первоначальном планировании, а после релиза — в тридцать раз дороже.

Осознание возможных финансовых потерь, репутационного ущерба и критических сбоев в работе, которые могут возникнуть в результате кибератак, должно стать главной движущей силой подхода к обеспечению безопасности.

Формировать культуру киберграмотности на всех уровнях

На уровне компании:
осведомленность и постоянное обучение сотрудников основам кибербезопасности – ключевой фактор предотвращения атак. Обратите особое внимание на формат удаленного доступа для сотрудников на дистансе. Здесь потребуется дополнительная защита: многофакторная аутентификация и ограничение количества возможных соединений от одного IP-адреса.

На уровне экосистемы:
создавайте прозрачную среду для совместной работы, чтобы избежать неожиданностей и свести к минимуму последствия кибератак. Уделите внимание процессу обмена информацией об атаках. Демонстрируя прозрачность и открыто делясь информацией, банки задают тон для обеспечения кибербезопасности во всей цепочке экосистемы.

На уровне общей банковской среды:
на повестке дня довольно остро стоит вопрос о том, что финансовым институтам необходимо объединить усилия, чтобы не допустить перетекания кибермошенников из одного банка в другой. Здесь важно понимание того, что проблема кибербезопасности не может быть решена каждым банком отдельно. Нужно стремиться к достижению единой консолидированной структуры, которая будет максимально технологична, автоматизирована и в состоянии бороться с вызовами кибератак.

Обеспечить защиту цифрового ядра компании

Безопасность должна быть заложена в архитектуре самой системы компании, во всех критически важных элементах, которые входят в цифровое ядро банка. Используйте встроенные решения, например, межсетевые экраны нового поколения (NGFW), они обеспечивают многоуровневую защиту. Эти технологии способны обнаруживать и блокировать продвинутое вредоносное ПО и предотвратить потенциальные кибератаки. Внедряйте возможности генеративного анализа и машинного обучения для прогнозирования киберугроз.

Оптимизируйте подготовку к атаке, включая регулярное создание резервных копий критически важного ПО, отработку восстановления данных из резервных копий и поддержание актуального плана реагирования на инциденты. Не храните резервные копии в той же инфраструктуре – используйте внешние хранилища.

Выделяйте больше ресурсов на обеспечение кибербезопасности архитектуры системы по мере продвижения по пути новых технологий.

Обращать внимание на внешний сетевой периметр

Способы кибератак постоянно совершенствуются. Например, хакеры начинают искать слабые звенья системы безопасности через филиалы, поставщиков ПО, дочерние предприятия, подрядчиков или аутсорсеров. Наблюдая данную тенденцию, банк должен не только уделять больше внимания своей киберзащите, но также предъявлять требования по кибербезопасности к контрагентам и поставщикам.

В обеспечении безопасности может помочь следование концепции «нулевого доверия» (Zero Trust). Концепция становится все более востребованной, так как в работе банков все чаще используются облачные и гибридные среды. Данная концепция предлагает по умолчанию считать опасными любые устройства и пользователей. Прежде чем предоставить доступ к какому-либо элементу системы, пользователю необходимо пройти строгую многофакторную аутентификацию и авторизацию.

Продвигая принципы «нулевого доверия», банки запускают комплексную трансформацию цифровой архитектуры банковской сферы.

Уделять больше внимания соблюдению требований регулятора

В 2023 году Центральный банк России ввел для банков новую форму отчетности по операциям без согласия клиентов. На основе показателей этой отчетности можно проследить огромное количество неуспешных операций, заблокированных антифрод-системами кредитных организаций.

Сотрудничество между государственным регулятором и банками имеет решающее значение для устранения системных киберрисков. Регулятор продолжает расширять и углублять свои подходы к киберзащите перед лицом постоянно растущего количества угроз в банковском секторе.

Как мы видим, развитие передовых технологий диктует необходимость совершенствования систем безопасности. Геополитическая обстановка, технологические инновации, включая возможности искусственного интеллекта, кратно увеличивают количество уязвимостей в области цифровых технологий. Многие угрозы сегодня уже нельзя решить простой установкой средств информационной защиты. Важно выстроить систему реальной кибербезопасности, которая усложнит путь злоумышленника и обеспечит бесперебойную работу банковского сектора.

«Мы видим, что схемы мошенников становятся все сложнее, они активно используют методы социальной инженерии, заставляя граждан добровольно отдавать свои средства, задействуют новые приемы обмана. Для противодействия злоумышленникам мы будем совершенствовать наши методы регулирования», — отмечает директор Департамента информационной безопасности Банка России Вадим Уваров.