Фокина Оксана Геннадьевна

кандидат экономических наук, доцент кафедры экономики, финансов и бухгалтерского учета Орловского государственного университета имени И.С. Тургенева, г. Орел, fokoksana@mail.ru

Шиленок Анастасия Олеговна

магистрант направления подготовки 38.04.08 Финансы и кредит Орловского государственного университета имени И.С. Тургенева, г. Орел, shilenok2010@yandex.ru

ЛИДЕРСТВО СБЕРБАНКА КАК ЭКОСИСТЕМЫ В КИБЕРБЕЗОПАСНОСТИ

Аннотация. В статье рассмотрен процесс технологической трансформации Сбербанка в условиях цифровизации экономики, исследованы основные компоненты экосистемы Сбербанка, делается упор на технологию «больших данных», искусственный интеллект и блокчейн для эффективного управления экосистемой, изучена культура кибербезопасности экосистемы Сбербанка на базе технологии Threat Intelligence, выявлены качества и навыки, которыми должен обладать современный специалист по кибербезопасности, а также обоснованы причины, по которым служба кибербезопасности Сбербанка считается одной из лучших в стране.

Ключевые слова: кибербезопасность, кибератака, цифровизация, технологическая трансформация, экосистема, Сбербанк.

Fokina Oksana Gennadyevna

Candidate of Science (Economics), Associate Professor of the Department of Economics, Finance and Accounting, Orel State University, Orel, fokoksana@mail.ru

Shilenok Anastasia Olegovna

Master's student in the field of training 38.04.08 Finance and Credit, Orel State University, Orel, shilenok2010@yandex.ru

SBERBANK'S LEADERSHIP AS AN ECOSYSTEM IN CYBERSECURITY

Abstract. The article examines the process of Sberbank's technological transformation in the context of the digitalization of the economy, examines the main components of the Sberbank ecosystem, focuses on the technology of "big data", artificial intelligence and blockchain for effective ecosystem management, examines the culture of cybersecurity of the Sberbank ecosystem based on

Threat Intelligence technology, identifies the qualities and skills that a modern cybersecurity specialist should possess, and justifies the reasons why Sberbank's cybersecurity service is considered one of the best in the country.

Keywords: cybersecurity, cyberattack, digitalization, technological transformation, ecosystem, Sberbank.

Общемировым трендом в последнее десятилетие является переход от традиционной экономики к цифровой, включающий цифровую трансформацию финансовой сферы, системное и поступательное внедрение новых финансовых технологий. Для компаний, осуществляющих свою деятельность в финансовом секторе, на сегодняшний день ключевыми конкурентными характеристиками выступают инновационность, гибкость, адаптивность и скорость внедрения технологических изменений.

Перманентное развитие информационных технологий, в частности цифровизация банковского сектора, способны привести к вытеснению традиционных кредитных учреждений, предлагающих стандартный набор финансовых услуг, и бизнес-модель «цифрового банка» с использованием передовых технологий станет вполне реальной.

В настоящее время российский банковский сектор претерпевает большие технологические изменения, и уже существуют кредитные организации, «оцифровавшие» свои отношения с клиентами, что позволяет превращать их в открытые «экосистемы». Следуя глобальной тенденции, к созданию «экосистем» – систем взаимодействия, наделенных стандартами интеграции, стремятся Альфа-Банк, ВТБ, Тинькофф и другие банки.

Говоря о Сбербанке, как об одном из ведущих финансовых институтов, его ребрендинг начался еще в 2017 году, когда организация широко анонсировала в СМИ новую стратегию, согласно которой Сбербанк в скором времени перестанет быть исключительно финансовой организацией и превратится в технологическую компанию, предоставляя другие услуги для своих клиентов.

Технологическая трансформация Сбербанка осуществляется по следующим направлениям:

- обеспечение безопасности данных и систем;
- развитие платформы для экосистемы;
- обеспечение надежности и эффективности;
- развитие организации на основе данных и алгоритмов;
- расширение инфраструктуры инноваций [1].

К основным компонентам экосистемы Сбербанка относятся системы двух типов: общие сервисы и ключевые площадки (рисунок 1).

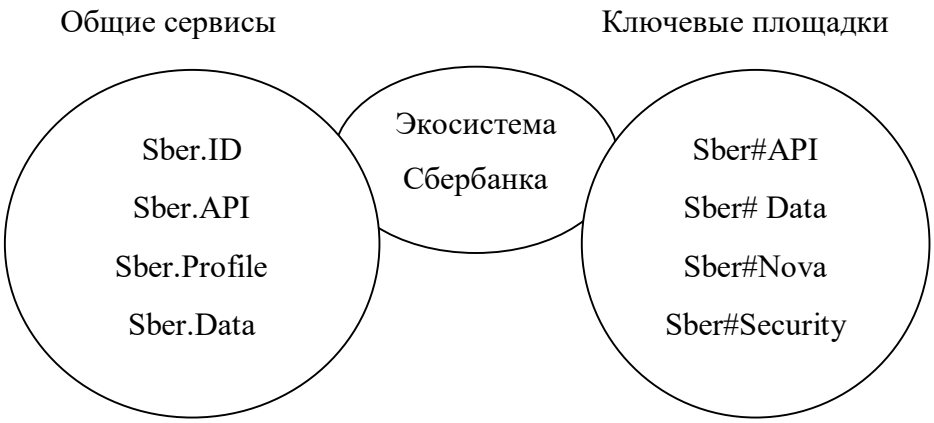

Рисунок 1. Основные компоненты экосистемы Сбербанка

Источник: составлено автором по данным [2]

Все крупные технологические гиганты обладают как первым блоком экосистемы, так и вторым. Перечень сервисов, представленных на рисунке 1, является неполным, однако мы рассмотрим ключевые из них.

Sber.ID позволяет любому цифровому резиденту идентифицировать себя на площадке экосистемы. Sber.Profile подразумевает, что аутентифицированные пользователи должны иметь свой профиль, одинаковый для всех резидентов площадки. Sber.ID и Sber.Profile хранят информацию о человеке, как о новом объекте экосистемы. Разумеется, имеется сервис и для обмена данными. Ценность экосистемы в том, что, используя информацию от разных резидентов, площадок экосистемы, можно формировать новые услуги для потребителя.

Ключевые площадки экосистемы «приземляют» сервисы и осуществляют функционирование экосистемы. Sber#API – это маркетплейс открытых программных интерфейсов, приложений с целью обмена информации и обеспечения взаимодействия с участниками экосистемы и другими экосистемами. Sber# Data – место сбора, хранения, анализа данных об участниках экосистемы. Sber#Nova – это своего рода «песочница» для создания, тестирования, запуска и тиражирования инновационных продуктов и решений. Sber#Security – услуги кибербезопасности для участников экосистемы.

В условиях будущего развития IT-технологий, цифровизации рынка банковских услуг кибербезопасность будет играть ключевую роль в становлении экономики. Стоит заметить, что при этом 20% успеха при обеспечении кибербезопасности зависит от технологий и нововведений, а целых 80% – от точности, правильности и слаженности протекающих процессов по обеспечению информационной экономической безопасности [3].

Для обеспечения кибербезопасности в экосистеме Сбербанка в условиях цифровой трансформации произошли следующие изменения (инновации) (рисунок 2).

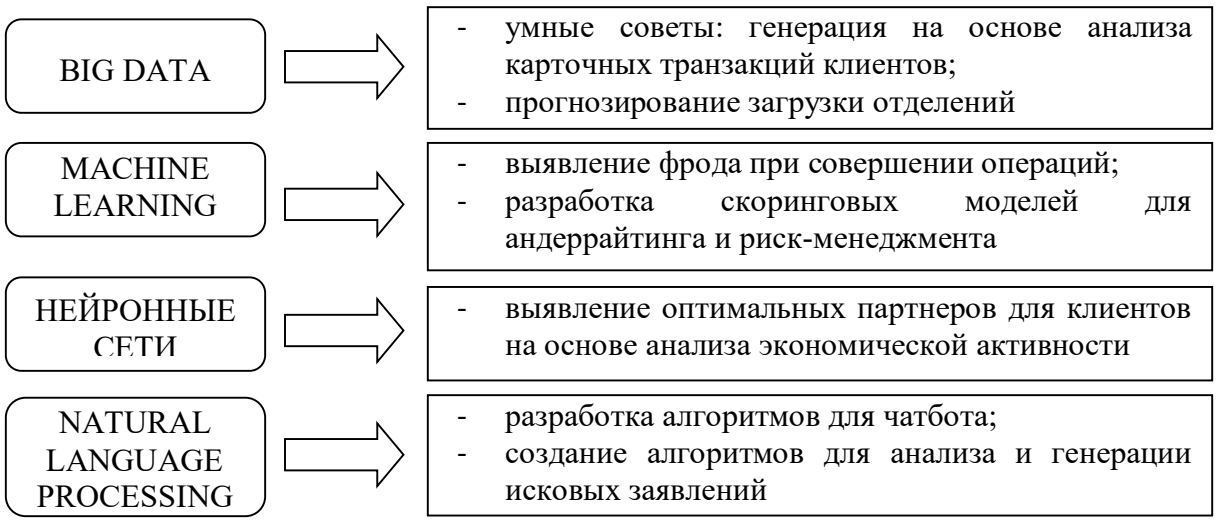

Рисунок 2. Инновации в экосистеме Сбербанка

Источник: составлено автором по данным [4]

Ставка делается на распространение технологии больших данных (Big Data), поскольку Сбербанк ежедневно осуществляет более 100 млн. транзакций во всех каналах. Применение роботов и цифровых помощников вместо реальных сотрудников уже сейчас позволяет сэкономить в год миллиарды рублей чистой прибыли. Еще в 2017 году Сбербанк разработал сообщество и Академию технологий и данных (так называемое Data Science). Кроме того, сформировались институты CDO (Chef data officer) и CDS (Chief data scientist), созданные для управления корпоративными моделями данных и разработки проектов на базе технологий искусственного интеллекта.

Опираясь на статистику, Сбербанк ежегодно зарабатывает на искусственном интеллекте 2-3 млрд. долларов за счет применения технологии в оценке рисков, скоринговых моделях и управлении продажами. В 2018 году около 99% решений по кредитам физическим лицам принимались с помощью искусственного интеллекта, т.е. автоматизировано. Скорость обслуживания выросла в 2 раза по результатам тестового проекта роботизации колл-центра для корпоративных клиентов [5].

Приведем непосредственные преимущества использования искусственного интеллекта для современного банка и для клиента на рисунке 3.

Кроме того, в 2018 году Сбербанк запустил собственную блокчейн-лабораторию. По окончании этого же года банк реализовал свыше 20 разных блокчейн-пилотов, к примеру, совместно с «Северсталью», «М.Видео», ФАС. Побочным продуктом технологии «блокчейн» выступает биткоин. Вступивший в силу с 1 января 2021 года Федеральный закон № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [6], который законодательно закрепляет

возможность цифровых валют, но не для оплаты товаров и услуг. Поскольку биткоин, как считается, имеет определенную долю анонимности, он достаточно распространен у кибермошенников, которые через вирусные программы заражают информационные системы пользователей и требуют выкуп (в качестве оплаты биткоинами) за расшифровку зашифрованных ими данных.

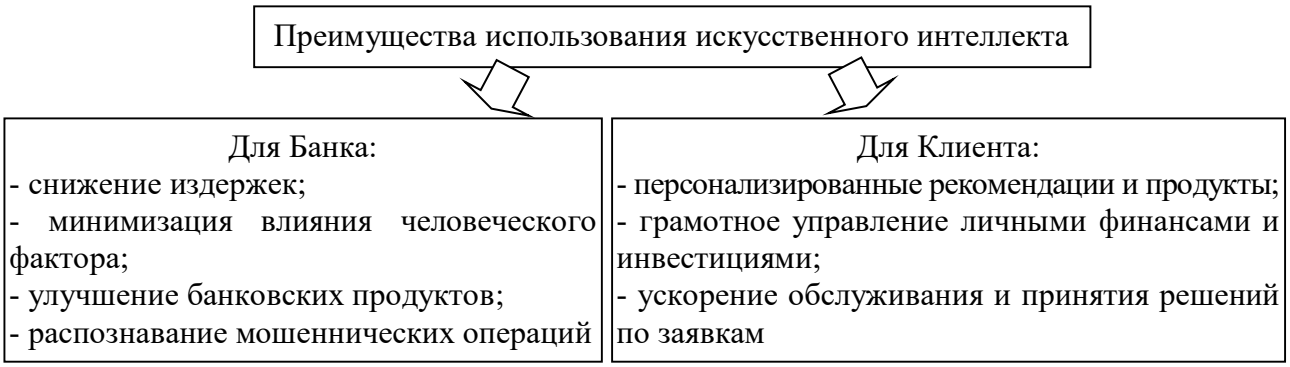

Рисунок 3. Преимущества использования искусственного интеллекта в банковской деятельности

Источник: составлено автором по данным [4]

В наше время все мошенничества (практически 90%) совершаются в киберпространстве, поэтому Сбербанк, будучи экосистемой, постоянно совершенствует процессы по обеспечению кибербезопасности.

Необходимо отметить, что значимым событием 2017 года стало получение Центром управления кибербезопасностью Сбербанка сертификата соответствия международному стандарту ISO/IEC 27001:2013. Сертифицированный Британским институтом стандартов (BSI), Сбербанк стал первым в России банком, обладающим подобного рода признанием международного уровня [3].

Формируя единую культуру кибербезопасности для Банка и клиентов, Сбербанк продвигается через дочернюю компанию «Бизон», на 100% принадлежащую Сбербанку, и реализующую проекты Fraud Monitoring as a Service (мониторинг финансовых транзакций с целью выявления мошеннических операций) и Threat Intelligence Platform (платформа по сбору и обработке технической информации, позволяющей заказчикам защищаться от кибератак и расследовать инциденты) [7].

Собственная система кибербезопасности с технологией Threat Intelligence представляет собой строго структурированную информацию (сведения), благодаря которой организация получает возможность отслеживать потенциальные киберугрозы. Другими словами, технология Threat Intelligence – это своего рода киберразведка, главной целью которой

является знание о вероятных нападениях со стороны кибермошенников. Полный цикл разведки киберугроз можно представить на рисунке 4.

Рисунок 4. Цикл технологии Threat Intelligence

Источник: [7]

Таким образом, процесс кибербразведки включает в себя 5 последовательных этапов, начинающихся планированием, где устанавливаются цели и расставляются приоритеты, и заканчивающихся доведением информации до конечных потребителей, в роли которых могут выступать как внешние потребители, так и собственные подразделения информационной безопасности в филиалах, дочерних и зависимых бизнес-единицах банка.

Следует подчеркнуть, что в мире огромный дефицит кадров в области кибербезопасности, и Россия, в том числе находится в дефицитной позиции, поскольку потребность в организации защиты от кибератак растет стремительными темпами. Встает вопрос, какими качествами должен обладать современный специалист по кибербезопасности. Это человек, который:

- знает толк в современных технологиях (без этого в современном мире обеспечить требуемый уровень защиты нельзя);

- разбирается в рисках, т.е. он понимает, какие неприятности могут случиться с пользователями той или иной технологии для того, чтобы обеспечить им защиту;

- познает психологию людей (с целью убедить человека делать то, что нужно с требуемым уровнем безопасности).

Так, «человеку будущего» в кибербезопасности должны быть присущи следующие навыки и способности:

- инновационность и digital-навыки;
- развитие команд и сотрудничество;
- системное мышление и решение проблем;
- управление результатами и ответственность;
- управление собой;
- клиентоцентричность;
- развитие новых компетенций и знаний;
- уникальный опыт.

Иными словами, специалист по кибербезопасности, как собирательный образ, сочетает в себе навыки программиста, специалиста в сфере информационных технологий, риск-менеджера, психолога.

На базе правил кибербезопасности, которые должен знать каждый сотрудник экосистемы Сбербанка, создана специальная программа под названием «Агент кибербезопасности». Это фактически игра, где сотрудник в соответствующей форме проходит обучающии модули и приобретает необходимые теоретические знания для их применения на практике. Фишинговые учения или киберучения – это следующий этап для того, чтобы сотрудник смог применить знания, которые он получил в результате обучения в реальной обстановке, максимально приближенной к боевой.

Сбербанк уже сейчас применяет такие технические способы защиты пользовательской информации, как технология SSL-шифрования данных (Secure Sockets Layer), биометрическая идентификация пользователя, аутентификация посредством одноразового случайно сгенерированного кода (пароля), использование электронной цифровой подписи и уникальных ключей, ограниченная длительность сессии клиента в системе интернет-банкинга, уведомления через SMS-сообщения об операциях в интернет-банкинге.

Таким образом, можно сделать вывод, что основополагающим инструментом развития бизнеса и роста капитализации для кредитных организаций становятся лайфстайл-экосистемы. Экосистема как нововведение, являясь большим технологическим проектом Сбербанка, влечет за собой неопределенности, трудности и риски, одним из которых является смена менталитета. Говоря о классической безопасности, акцент делается на конфиденциальности и изолированности поступающей информации и обеспечения ее защиты. Служба кибербезопасности Сбербанка является одной из самых лучших в России и продолжает наращивать международное взаимовыгодное сотрудничество среди государственных и частных корпораций, формирует необходимые условия для организации

постоянного обмена информацией, развивает новые услуги в сфере кибербезопасности для вывода их на рынок. Накопленные знания и данные, высокий уровень профессионализма специалистов по кибербезопасности экосистемы Сбербанка, применение инновационных технологий, а также непосредственное сотрудничество с правоохранительными органами помогают успешно пресекать деятельность кибермошеннических группировок на самых ранних этапах.

Библиографический список

1. Технологическая трансформация: [сайт]. 2018. URL: https://2017.report-sberbank.ru/ru/performance-overview/technology/transformation (дата обращения: 18.03.2021).

2. СберПро / Финансы: [сайт]. 2020. URL: https://sber.pro/topics/finance (дата обращения: 17.03.2021).

3. Лидерство в кибербезопасности: [сайт]. 2018. URL: https://2017.report-sberbank.ru/ru/performance-overview/technology/cybersecurity (дата обращения: 18.03.2021).

4. Лекторий ВШЭ и Сбербанка: «Кибербезопасность будущего»: [сайт]. [дата публ. 19.09.2017]. URL: https://newsvideo.su/education/video/175053 (дата обращения: 17.03.2021).

5. Зачем банку непрофильные сервисы: [сайт]. 2021. [дата публ. 12.11.2019]. URL: https://mcs.mail.ru/blog/multfilmy-produkty-vrachi-zachem-banku-neprofilnye-servisy (дата обращения: 17.03.2021).

6. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ // КонсультантПлюс: надежная правовая поддержка: [официальный сайт]. 1997-2021. URL: http://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 17.03.2021).

7. Караева Ю.А., Сайбель Н.Ю. Способы защиты информации в Сбербанке / Актуальные вопросы современной акономики. 2021. №2. С. 199-207.