УДК 004.056
DOI: 10.25559/SITITO.18.202202.383-390

Научная статья

Инновационные технологии в сфере кибербезопасности

С. В. Лебедь
ПАО «Сбербанк России», г. Москва, Российская Федерация
Адрес: 117997, Российская Федерация, г. Москва, ул. Вавилова, д. 19
SVLebed@sberbank.ru

Аннотация

Цифровая трансформация любой организации должна включать вопросы кибербезопасности, без соблюдения требований которой невозможно выстроить надёжную информационную систему. Сегодня многие существующие программные продукты, средства защиты и ИТ-системы не соответствуют новым условиям, в которых им предстоит выполнять свои функции. После ухода зарубежных поставщиков программного обеспечения, Президентом России было принято решение о развитии программы импортозамещения и установлен срок перехода на отечественные средства защиты до 1 января 2025 года. В том числе, был введён запрет на использование любого иностранного софта на объектах критической информационной инфраструктуры России. В связи с текущей геополитической обстановкой и современной картиной киберугроз необходима разработка собственных решений в области информационной безопасности. Сбербанк активно занимается импортозамещением средств защиты информации с использованием инновационных технологий. Банк успешно преодолевает зависимость от западных поставщиков и от западных моделей и методик, меняет устаревшие подходы к оценке и управлению рисками, что помогает результативно решать задачи замены средств киберзащиты как для текущих задач, так и для работы в условиях возрастающей киберагрессии.

Ключевые слова: кибербезопасность, цифровая трансформация, инновационные технологии, антифрод, защита объектов критической информационной инфраструктуры, киберугрозы, противодействие мошенничеству, импортозамещение средств защиты информации, технологическая независимость

Автор заявляет об отсутствии конфликта интересов.

Для цитирования: Лебедь С. В. Инновационные технологии в сфере кибербезопасности // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 2. С. 383-390. doi: https://doi.org/10.25559/SITITO.18.202202.383-390

© Лебедь С. В., 2022

Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.

Original article

Innovative Technologies in Cybersecurity

S. V. Lebed
PJSC "Sberbank of Russia", Moscow, Russian Federation
Address: 19 Vavilov St., Moscow 117997, Russian Federation
SVLebed@sberbank.ru

Abstract

The digital transformation of any organization must include cybersecurity, without which it is impossible to build a reliable information system. Today, many existing software products, security tools, and IT systems do not match the new environment in which they will have to perform their functions. After the departure of foreign software suppliers, the President of Russia made a decision on the development of the import substitution program and set a deadline for the transition to domestic means of protection until January 1, 2025. In particular, a ban on the use of any foreign software at the facilities of Russia's critical information infrastructure was introduced. Given the current geopolitical situation and the current situation of cyber-threats, there is a need to develop indigenous solutions in the area of information security. Sberbank is actively engaged in import substitution of information security tools using innovative technologies. Sberbank successfully overcomes dependence on Western suppliers and on Western models and methods, changes outdated approaches to risk assessment and management, which helps to effectively address the challenges of replacing cybersecurity tools both for current tasks, and to work in the face of increasing cyber aggression.

Keywords: cybersecurity, digital transformation, innovative technologies, anti-fraud, protection of critical information infrastructure, cyber threats, fraud prevention, import substitution of information security tools, technological independence

The authors declare no conflict of interest.

For citation: Lebed S.V. Innovative Technologies in Cybersecurity. *Sovremennye informacionnye tehnologii i IT-obrazovanie = Modern Information Technologies and IT-Education*. 2022; 18(2):383-390. doi: https://doi.org/10.25559/SITITO.18.202202.383-390

1. Введение

Включение вопросов кибербезопасности в стратегии цифровой трансформации любой организации в качестве обязательного элемента, вовлечение первых лиц компаний в определение недопустимых для бизнеса киберугроз и фокус на импортонезависимые цифровые решения – главные факторы безопасной цифровой трансформации в условиях возросших рисков. Многие организации сталкиваются с тем, что существующие архитектуры, программные продукты, средства защиты и ИТ-системы уже не соответствуют тем требованиям, которые перед ними ставят современные реалии [1]-[3].

Как крупнейший финансовый институт, имеющий системообразующее федеральное значение, Сбербанк находится под пристальным вниманием хакерских группировок, а клиенты банка подвергаются атакам мошенников.

Многолетний и разносторонний опыт противостояния угрозам безопасности разного масштаба позволяет Сбербанку эффективно разрабатывать и внедрять передовые технологии. Более того, исследования и разработки – основа развития бизнеса, один из приоритетов Сбербанка и непременное условие для конкурентоспособности на рынке и создания лучших продуктов для клиентов. Высокую ценность научно-исследовательских работ подтверждает 367 патентов, полученных Сбербанком. Из них 75 зарегистрированы только за третий квартал 2022 года. Количество патентов, получаемых за год, динамично растет.

За первое полугодие 2022 года сотрудники Сбербанка опубликовали 23 статьи в изданиях, индексируемых Scopus и/или WoS, выступили с 17 докладами на конференциях A/A*. Сбербанк активно взаимодействует с вузами, в том числе по кибербезопасности: запущен трек Летней цифровой школы Сбербанка для преподавателей профильных вузов страны, в рамках которого обучено 530 преподавателей из 136 вузов (70% от общего числа профильных вузов) в 81 городе России. Обучение проводили эксперты Департамента кибербезопасности Сбербанка, которые разработали более 90 академических часа учебного контента.

Во всех направлениях работы эксперты кибербезопасности Сбербанка учитывают актуальные тенденции как в информационном, так и технологическом пространстве. Рассмотрим, как научные наработки и практический опыт Сбербанка используются в инновационном развитии сферы кибербезопасности [4].

2. Актуальный ландшафт киберугроз как среда развития технологий в сфере кибербезопасности

Традиционно кибербезопасность организации строилась по вероятностным моделям, когда средства защиты в первую очередь используются для закрытия тех рисков, вероятность наступления которых наиболее высока. Риски с низкой долей вероятности могут оставаться без внимания, либо вне контура управления рисками. Сегодня такой подход уже не работает – даже одна незакрытая уязвимость может привести к блокированию работы целой компании. Организации уже не могут использовать те методы, которые предлагаются руководящими документами регуляторов и учебниками по информационной безопасности, так как они не коррелируют с быстро меняющейся картиной киберугроз[1]. В текущих условиях должна действовать нулевая толерантность к любой уязвимости или угрозе, даже если она имеет совсем небольшую вероятность.

Термин «черный лебедь» означает маловероятное событие огромной разрушительной силы, как раз такой «черный лебедь» для многих экспертов в области кибербезопасности случился в феврале 2022 года, когда началась специальная военная операция (СВО) и, как следствие, полномасштабная кибервойна против России. Этот фактор является источником большинства современных вызовов, определяющих актуальный ландшафт киберугроз. Против российских организаций работает более 1 млн хакеров, в ходе кибервойны злоумышленники используют все доступные им средства, включая мощные DDoS-атаки, взломы сайтов, кражи данных, фишинг, информационные атаки[2]. Возрастает сложность атак, они становятся более многоуровневыми, глубокими и хорошо подготовленными [5]-[7]. Пример: на подготовку одной из самых сложных атак против Сбербанка (DDoS-атака в октябре 2022 года на все сервисы) злоумышленники потратили две недели, провели более 1000 разведывательных сканирований инфраструктуры. Гигантский скачок роста DDoS-атак пришелся на март, когда было отражено более 200 DDoS-атак, а количество одновременных атак составляло порядка 50. 95% крупнейших бот-сетей были арендованы для проведения DDoS-атак на российские компании.

Резко выросло количество фишинговых сайтов с использованием бренда Сбербанка. В среднем в неделю банк выявляет и инициирует блокировку 1800 доменных имен, имитирующих ресурсы Сбербанка: количество фишинговых ресурсов с начала года выросло в 4,8 раза.

С учетом социальной повестки сегодня преступники спекулируют на актуальной теме мобилизации: создают мошеннические ресурсы, якобы предлагающие услуги по пересечению границы, военторги или сайты помощи военнослужащим.

Таким образом, СВО стала лакмусовой бумагой уровня кибербезопасности каждой организации. Несмотря на то, что в целом Российская Федерация довольно успешно противостояла глобальной кампании, направленной против страны, результаты трудно назвать полностью удовлетворительными:

- 95% крупных компаний не справились эффективно с отражением кибератак;
- скомпрометировано 350 млн персональных записей граждан России (данные 65 млн граждан России).

В контексте анализа актуального ландшафта киберугроз также важно оценить текущий характер и уровень телефонного мошенничества, направленного против граждан Рос-

[1] Кибербезопасность в условиях электронного банкинга / А. А. Бердюгин, А. Б. Дудка, С. В. Конявская [и др.] ; Под ред. П. В. Ревенкова. М.: Прометей, 2020. 522 с. URL: https://www.elibrary.ru/item.asp?id=46576776 (дата обращения: 20.06.2022).

[2] Лебедь С. В. Уроки кибервойны: делаем выводы и готовим стратегию [Электронный ресурс] // Forbes. 08.06.2022. URL: https://promo.sber.ru/kibrary#/investigation (дата обращения: 20.06.2022).

сии. Темы, которые используют мошенники, не изменились («безопасный счет», «помощь в расследовании», «оформление кредита»), но преступники в поиске возможности обойти технические препятствия в виде антиспам-фильтрации или антифрод-сервисов стали чаще выбирать новые каналы коммуникаций, например, звонки в мессенджеры. В отличие от мобильной связи, они бесплатны, в них нет встроенной блокировки спама и определителей номеров. Кроме того, в мессенджере можно установить аватар с официальным логотипом организации или компании, что повышает доверие жертвы к входящему звонку [8]-[11]. За последнее время доля таких коммуникаций увеличилась в 2,7 раза.

Телефонное мошенничество становится более навязчивым и продуманным, в 2022 году был зафиксирован рекорд по украденной сумме у одного клиента – 150 млн руб. В 2021 году мошенники украли у клиентов банков (по данным Банка России) 13,5 млрд рублей, при этом в первом полугодии 2022 года 83% россиян столкнулись с телефонным мошенничеством (ВЦИОМ).

Для проактивного противодействия мошенничеству в Сбербанке используются AI-модели: real-time скоринг транзакций (оценка риска транзакций с задержкой не более 100 мс.); графовая аналитика (связи между клиентами и другими сущностями, оценка близости, кластеризация мошеннических групп); выявление нетипичных геолокационных паттернов перемещений, аномальных скоростей передвижений с помощью гео-моделей; скоринги сущностей (оценка различных сущностей – физических и юридических лиц, телефонов, устройств – по различным негативным аспектам); повышение качества данных (классификация обращений клиентов для фильтрации бытового мошенничества, ошибочных обращений и пр.) [12].

Достаточно свежий тренд – атаки на юридическое лицо посредством телефонного мошенничества. Под воздействием социальной инженерии бухгалтер или другой материально ответственный сотрудник совершает перевод или снимает деньги и передает их мошенникам.

Основным центром мошенничества по-прежнему остается Украина. Благодаря детальному расследованию деятельности одного из мошеннических кол-центров нам удалось выявить сценарии, скрипты, изучить инструкции, по которым работали мошенники[3].

3. Влияние зарубежных санкций на российский рынок информационных технологий

Сбербанк, как и многие российские компании, активно использовал продукты ведущих мировых производителей средств защиты информации (СЗИ). Но после начала СВО и введения санкций зарубежные поставщики программного обеспечения покинули рынок и прекратили поддержку и обновление своих продуктов на территории Российской Федерации.

В ответ на действия зарубежных поставщиков Президентом России принято решение о развитии программы импортозамещения и установлен срок перехода на отечественные средства защиты до 1 января 2025 года. В том числе вводится запрет на использование любого иностранного софта на объектах критической информационной инфраструктуры России[4].

Геополитические изменения сделали импортозамещение средств защиты информации жизненно необходимым. В настоящее время для компаний малого и среднего бизнеса существует возможность практически полной замены ушедших с рынка средств защиты на отечественные решения.

Исследования состояния отечественного рынка средств киберзащиты показали недостаточную зрелость представленных продуктов или их неспособность работать в масштабах инфраструктур крупных организаций. Основные проблемы – это нехватка решений для защиты высоконагруженных инфраструктур и ограниченность аналитической информации об угрозах кибербезопасности [13]-[15].

В связи с таким положением возникают вызовы в области кибербезопасности, которые встают не только перед крупными банками, но и перед другими организациями и госструктурами: зависимость от западных поставщиков и от западных моделей и методик, устаревшие подходы к оценке и управлению рисками, экспоненциальный рост объемов данных, которые необходимо обрабатывать в реальном времени. Чтобы преодолеть эти вызовы в кратчайшие сроки, в научном сообществе должны проводиться исследования с целью выработки предложений по решению перечисленных проблем и внедрению их в прикладной плоскости.

4. Собственные технологии Сбербанка – фундамент для технологической независимости

Сбербанк активно применяет agile – гибкую методологию разработки. Более 4 000 команд, в которые входят сотрудники из IT и бизнеса, совместно разрабатывают продукты, соответствующие строгим требованиям кибербезопасности. Имея успешный опыт создания высокотехнологичных и кибербезопасных продуктов и сервисов, Сбербанк результативно решает задачи импортозамещения средств киберзащиты.

Чтобы и в дальнейшем справляться с возрастающими киберугрозами, Сбербанк апробирует и внедряет инновационные технологии в продуктах собственной разработки. У банка есть несколько различных лабораторий, в том числе собственная лаборатория кибербезопасности, где тестируются самые смелые и передовые технологические решения. Среди продуктов Сбербанка, укрепляющих технологическую независимость: Платформа фрод-мониторинга (решение для защиты клиентов от мошенничества), RTCE (высокопроизводительная система корреляции событий), SberIRM (решение для обеспе-

[3] Кузнецов С. Атаки телефонных мошенников на россиян координируются на международном уровне [Электронный ресурс] // ПЛАС. 2022. № 7(293). URL: https://plusworld.ru/journal/2022/plus-7-2022/stanislav-kuznetsov-ataki-telefonnyh-moshennikov-na-rossiyan-koordiniruyutsya-na-mezhdunarodnom-urovne (дата обращения: 20.06.2022); Галицкий Х. Клиенты «Сбера» надежно защищены [Электронный ресурс] // Известия. 15.06.2022. URL: https://iz.ru/1349588/khariton-galitckii/klienty-sbera-nadezhno-zashchishcheny (дата обращения: 20.06.2022).

[4] О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации: Указ Президента Российской Федерации от 30.03.2022 № 166 [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202203300001 (дата обращения: 20.06.2022).

чения конфиденциальности данных), NBA (мониторинг сети и выявление аномалий), SOWA (шлюз безопасности прикладного уровня), SberNAC (решение по контролю доступа к проводной и беспроводной сети), TIP (система анализа киберугроз), ПКБ (Платформа кибербезопасности для обработки данных кибербезопасности)[5].

4.1. Платформа кибербезопасности Сбербанка

У Сбербанка более 100 млн клиентов (физических и юридических лиц), которые совершают миллионы транзакций в день. Работают 200 000 серверов и 350 000 рабочих станций, почти 20 000 офисов, распределенных по всей стране. Каждый объект информационной инфраструктуры, банковский процесс, действия сотрудников банка и клиентов генерируют огромный поток событий. В день на анализ в Security Operations Center банка поступает более 300 млрд событий. Чтобы их собрать, нормализовать, а затем провести интеллектуальный анализ данных (для некоторых задач в реальном времени) – необходимо использовать технологии BigData и AI (искусственного интеллекта)[6].

Именно на основе этих технологий разработана собственная Платформа кибербезопасности, которая решает задачи сбора данных со всех источников, их обогащения, обработки различными моделями искусственного интеллекта. Платформа кибербезопасности Сбербанка собирает информацию из более чем 250 источников, хранит уже 57 Тб данных, объем которых динамично увеличивается.

4.2. Экспоненциальный рост размерности расчетов

В масштабах инфраструктуры Сбербанка необходимо анализировать и оценивать миллионы уязвимостей и рисков по нескольким десяткам параметров. В связи с этим разработаны методы снижения размерности задач при оценках уязвимостей, угроз, рисков при современных масштабах инфраструктуры [16]. Одна из задач высокой вычислительной сложности: выявление промышленных данных в анализируемой базе данных (например, подготовленной для тестирования или разработки, или для передачи внешнему подрядчику – и не предполагающей содержания промышленных данных).

База данных может содержать миллиарды строк. Чтобы не анализировать их все, используется вероятностная оценка наличия промышленных данных в базе данных. Исходя из представленного подхода, например, чтобы обеспечить уверенность в 97±3%, достаточно проверить всего чуть более тысячи случайно выбранных (и не пустых) строк.

Данный подход был запатентован и используется для нескольких задач в банке. В том числе это изобретение позволило сократить время проверки отсутствия критических данных в тестовых базах данных с 10 дней до 1 часа, что стало одним из ключевых факторов в реализации крупнейшей программы банка по переезду на единую среду разработки и тестирования, для выполнения которой были проверены десятки тысяч баз данных.

4.3. Система автоматической приемки релизов на основе AI-моделей

Как было отмечено ранее в банке работают 4000 agile-команд, которые выпускают 6000 релизов в месяц. Необходимо обеспечить проверку релизов продуктов на безопасность, убедиться в том, что они не содержат угроз. Для этого была разработана и внедрена Система автоматической приемки релизов на основе AI-моделей, использующая Ансамблевый алгоритм определения безопасности релиза [17].

Собственное решение с применением AI-методов, разработанное специально для производственного процесса Сбербанка:

- near-real-time режим обработки;
- «легкое» дообучение модели в runtime;
- время жизни до переобучения - 1 квартал;
- контроль правильности решений на 5% выборке с помощью механизма автовалидации;
- возможность точечного корректирования работы модели с помощью системы правил;

Эффект:

- не менее 55% плановых релизов и до 80% релизов hotfix проходят приемо-сдаточные испытания в полностью автоматическом режиме;
- более 30 тыс. часов в квартал экономят команды и эксперты кибербезопасности за счет принятия автоматических решений.

4.4. Подход нейросетевого распознавания Deep Fake

Лицо человека является уникальным и удобным фактором для идентификации личности, поэтому банки активно используют биометрические технологии в процессах взаимодействия с клиентами для их идентификации и подтверждения финансовых операций. Практически на каждом этапе жизненного цикла биометрического распознавания может быть совершена атака на технологию. Кроме того, сам результат работы биометрии носит вероятностный характер и допускает ошибки, баланс между которыми достигается настройками характеристик той или иной реализации. Для успешного противостояния атакам на биометрию необходимо разработать методы и средства их обнаружения [18]-[24].

Отдельный тип атаки, набирающей популярность и степень угрозы в связи с развитием вычислительных мощностей и искусственного интеллекта, – это обман биометрии с помощью Deep Fake. При использовании Deep Fake злоумышленник пытается сгенерировать проверяемый образ (звук, фото, видео), который позволит обмануть биометрию и получить доступ к атакуемой системе.

Лабораторией кибербезопасности Сбербанка предложен новый подход нейросетевого распознавания Deep Fake: Geometric-Temporal Features, который позволяет достигнуть точности распознавания Deep Fake в 99%. Для сравнения: лучший алгоритм в 2021 году показывал результат в 91%.

[5] Сбербанк защищает граждан от злоумышленников [Электронный ресурс] // Сбербанк: Кибрарий. 30.11.2021. URL: https://promo.sber.ru/kibrary#/investigation (дата обращения: 20.06.2022); Сбер первым в России внедрил виртуальный ситуационный центр [Электронный ресурс] // Сбербанк. 30.11.2021. URL: https://www.sberbank.com/ru/news-and-media/press-releases/article?newsID=3944fae5-26fa-4469-80fb-e6427cf1e031&blockID=7&regionID=77&lang=ru&type=NEWS (дата обращения: 20.06.2022).

[6] Гарбузов Г., Теренин А., Бабак Н. Использование технологий искусственного интеллекта в построении режима коммерческой тайны на предприятии [Электронный ресурс] // Кибрарий, 2022. URL: https://promo.sber.ru/kibrary#/experts-opinion/opinion9 (дата обращения: 20.06.2022).

4.5. Открытая библиотека знаний о кибербезопасности «Кибрарий»

Сбербанк не только развивает собственные технологии и продукты, но и считает крайне необходимым делиться с экспертами кибербезопасности, а также гражданами России полезной аналитикой, советами, обучающими курсами в области кибербезопасности. Для этого был создан общедоступный ресурс «Кибрарий».

На портале представлено более 150 полезных материалов для повышения киберграмотности (памятки, статьи, тесты, советы и рекомендации экспертов Сбербанка), расследования, полезная информация, видеоматериалы по схемам мошенничества. Ресурс посещают более 20 000 пользователей в месяц, он продолжает наполняться полезными материалами.

5. Заключение

Несмотря на недоступность для использования средств защиты информации зарубежных поставщиков и нарастающую кибератрессию, Сбербанк не только успешно справляется с текущими проблемами и противостоит киберугрозам, но и развивает собственные технологические решения, не имеющие аналогов в мире. Тем не менее в будущем перед любой компанией и всей страной встанут ещё более серьезные вызовы в области обеспечения и повышения эффективности кибербезопасности.

Для их решения потребуются не только исследования, но и квалифицированные кадры [25]. Потребность в специалистах кибербезопасности в Российской Федерации существенно выросла: с 30 000 человек в 2021 году до 100 000 в 2022 году.

В ближайшем будущем среди экспертов кибербезопасности, по оценкам Сбербанка, будут востребованы специалисты по противодействию кибермошенничеству, кибербезопасности облачных сред, защите персональных данных и анализу угроз, а также исследователи уязвимостей и киберследователи. Им предстоит принимать вызовы и решать задачи в области мошенничества с цифровой валютой, угроз для умных устройств и искусственного интеллекта в сфере цифровой медицины и правосудия.

Список использованных источников

[1] Добродеев А. Ю. Кибербезопасность в Российской Федерации. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века // Вопросы кибербезопасности. 2021. № 4(44). С. 61-72. doi: https://doi.org/10.21681/2311-3456-2021-4-61-72

[2] Закалкин П. В. Эволюция систем управления киберпространством // Вопросы кибербезопасности. 2022. № 1(47). С. 76-86. doi: https://doi.org/10.21681/2311-3456-2012-1-76-86

[3] Савонин А. П. Экономическая безопасность в условиях цифровой экономики // Финансовая экономика. 2021. № 4. С. 82-84. URL: https://www.elibrary.ru/item.asp?id=45676973 (дата обращения: 20.06.2022).

[4] Коряковский Д., Теренин А. ИИ на страже банковских данных: опыт Сбербанка // BIS Journal – Информационная безопасность банков. 2020. № 2(37). С. 42-48. URL: https://ib-bank.ru/bisjournal/post/1319 (дата обращения: 20.06.2022).

[5] Ревенков П. В., Ошманкевич К. Р., Бердюгин А. А. Фишинговые схемы в банковской сфере: рекомендации пользователям интернета по защите и разработка задач регулирования // Финансы: теория и практика. 2021. Т. 25, № 6. С. 212-226. doi: https://doi.org/10.26794/2587-5671-2021-25-6-212-226

[6] Афанасьева Н. С., Елизаров Д. А., Мызникова Т. А. Классификация фишинговых атак и меры противодействия им // Инженерный вестник Дона. 2022. № 5(89). С. 169-182. URL: https://www.elibrary.ru/item.asp?id=48925602 (дата обращения: 20.06.2022).

[7] Ревенков П. В., Бердюгин А. А. Количественный подход к оценке риска воздействия кибератак при использовании технологии электронного банкинга // Защита информации. Инсайд. 2020. № 2(92). С. 36-42. URL: https://www.elibrary.ru/item.asp?id=42615396 (дата обращения: 20.06.2022).

[8] Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce / N. Ameen [и др.] // Computers in Human Behavior. 2021. Vol. 114. Article number: 106531. doi: https://doi.org/10.1016/j.chb.2020.106531

[9] Li Y., Saxunová D. A perspective on categorizing Personal and Sensitive Data and the analysis of practical protection regulations // Procedia Computer Science. 2020. Vol. 170. P. 1110-1115. doi: https://doi.org/10.1016/j.procs.2020.03.060

[10] Choi J. P., Jeon D.-S., Kim B.-C. Privacy and personal data collection with information externalities // Journal of Public Economics. 2019. Vol. 173. P. 113-124. doi: https://doi.org/10.1016/j.jpubeco.2019.02.001

[11] Иванов К. В., Балякин А. А., Малышев А. С. Технологии больших данных как инструмент обеспечения национальной безопасности // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. 2020. Т. 13, № 1. С. 7-19. doi: https://doi.org/10.18721/JE.13101

[12] Ларионова С. Л., Ряховский Е. Э. Организация противодействия финансовым операциям без согласия клиента // Финансовые рынки и банки. 2021. № 6. С. 60-67. URL: https://www.elibrary.ru/item.asp?id=46287383 (дата обращения: 20.06.2022).

[13] Гущина Е. А., Макаренко Г. И., Сергин М. Ю. Обеспечение информационно-технологического суверенитета государства в условиях развития цифровой экономики // Право.by. 2018. № 6(56). С. 59-63. URL: https://www.elibrary.ru/item.asp?id=36983674 (дата обращения: 20.06.2022).

[14] Ромашкина Н. П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. № 1(29). С. 2-9. doi: https://doi.org/10.21681/2311-3456-2019-1-2-9

[15] Марков А. С., Шеремет И. А. Безопасность программного обеспечения в контексте стратегической стабильности // Вестник Академии военных наук. 2019. № 2(67). С. 82-90. URL: https://www.elibrary.ru/item.asp?id=41590117 (дата обращения: 20.06.2022).
[16] Анализ существующих методов снижения размерности входных данных / С. Д. Ерохин, Б. Б. Борисенко, И. Д. Мартишин, А. С. Фадеев // T-Comm: Телекоммуникации и транспорт. 2022. Т. 16, № 1. С. 30-37. doi: https://doi.org/10.36724/2072-8735-2022-16-1-30-37
[17] Альсова О. К., Стубарев И. М. Неоднородный ансамблевый алгоритм классификации разнотипных данных // Известия Самарского научного центра Российской академии наук. 2017. Т. 19, № 6. С. 118-123. URL: https://www.elibrary.ru/item.asp?id=34964637 (дата обращения: 20.06.2022).
[18] Киселев А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2021. № 3. С. 54-64. doi: https://doi.org/10.18384/2310-6794-2021-3-54-64
[19] Local Relation Learning for Face Forgery Detection / S. Chen [и др.] // Proceedings of the AAAI Conference on Artificial Intelligence. 2021. Vol. 35, no. 2. P. 1081-1088. doi: https://doi.org/10.1609/aaai.v35i2.16193
[20] DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection / R. Tolosana [и др.] // Information Fusion. 2020. Vol. 64. P. 131-148. doi: https://doi.org/10.1016/j.inffus.2020.06.014
[21] Video Face Manipulation Detection Through Ensemble of CNNs / N. Bonettini [и др.] // 2020 25th International Conference on Pattern Recognition (ICPR). IEEE Computer Society, 2021. P. 5012-5019. doi: https://doi.org/10.1109/ICPR48806.2021.9412711
[22] What Makes Fake Images Detectable? Understanding Properties that Generalize / L. Chai, D. Bau, S. N. Lim, P. Isola // Computer Vision – ECCV 2020. ECCV 2020. Lecture Notes in Computer Science ; ed. by A. Vedaldi, H. Bischof, T. Brox, J. M. Frahm. Vol. 12371. Springer, Cham, 2020. P. 103-120. doi: https://doi.org/10.1007/978-3-030-58574-7_7
[23] Клюева А. А., Белов Д. А. Актуальное правовое исследование deepfake-технологий и новые вызовы для Российской правовой системы // Вопросы российской юстиции. 2021. № 14. С. 601-609. URL: https://www.elibrary.ru/item.asp?id=46458856 (дата обращения: 20.06.2022).
[24] Свирщ А. О., Олейникова П. А. Развитие технологии deepfake // Modern Science. 2021. № 12-4. С. 309-320. URL: https://www.elibrary.ru/item.asp?id=47460071 (дата обращения: 20.06.2022).
[25] Нечай А. А. Использование инновационных методов и современных технологий для повышения квалификации в области кибербезопасности // Азимут научных исследований: педагогика и психология. 2020. Т. 9, № 3(32). С. 193-196. doi: https://doi.org/10.26140/anip-2020-0903-0043

Поступила 20.06.2022; одобрена после рецензирования 10.07.2022; принята к публикации 14.07.2022.

Об авторе:
Лебедь Сергей Васильевич, вице-президент, директор Департамента кибербезопасности, ПАО «Сбербанк России» (117997, Российская Федерация, г. Москва, ул. Вавилова, д. 19), кандидат технических наук, **ORCID: https://orcid.org/0000-0001-6913-761X,** SVLebed@sberbank.ru

Автор прочитал и одобрил окончательный вариант рукописи.

References

[1] Dobrodeev A.Yu. Cybersecurity in Russian Federation. A trendy term or the priority technologic area of enhancing national and international security of the XXI century. *Voprosy kiberbezopasnosti* = Cybersecurity issues. 2021; (4):61-72. (In Russ., abstract in Eng.) doi: https://doi.org/10.21681/2311-3456-2021-4-61-72
[2] Zakalkin P.V. Evolution of Cyberspace Management Systems. *Voprosy kiberbezopasnosti* = Cybersecurity issues. 2022; (1):76-86. (In Russ., abstract in Eng.) doi: https://doi.org/10.21681/2311-3456-2012-1-76-86
[3] Savonin A.P. Economic Security in the Conditions of the Digital Economy. *Finansovaja jekonomika* = Financial Economics. 2021; (4):82-84. Available at: https://www.elibrary.ru/item.asp?id=45676973 (accessed 20.06.2022). (In Russ., abstract in Eng.)
[4] Koryakovsky D., Terenin A. *Iskusstvennyj intellekt na strazhe bankovskih dannyh: opyt Sberbanka* [Artificial Intelligence on guard of banking data: Sberbank's experience]. *BIS Journal – Information Security of Banks.* 2020; (2):42-48. Available at: https://ib-bank.ru/bisjournal/post/1319 (accessed 20.06.2022). (In Russ.)
[5] Revenkov P.V., Oshmankevich K. R., Berdyugin A. A. Phishing schemes in the banking sector: Recommendations to Internet users on protection and development of regulatory tasks. *Finance: Theory and Practice.* 2021; 25(6):212-226. (In Russ., abstract in Eng.) doi: https://doi.org/10.26794/2587-5671-2021-25-6-212-226
[6] Afanaseva N.S., Elizarov D.A., Myznikova T.A. Classifying and countering phishing attacks. *Engineering journal of Don.* 2022; (5):169-182. Available at: https://www.elibrary.ru/item.asp?id=48925602 (accessed 20.06.2022). (In Russ., abstract in Eng.)
[7] Revenkov P.V., Berdyugin A.A. Quantitative approach to assessing the risk of cyberattacks in using electronic banking technology. *Zašita informacii. Inside.* 2020; (2):36-42. Available at: https://www.elibrary.ru/item.asp?id=42615396 (accessed 20.06.2022). (In Russ., abstract in Eng.)

[8] Ameen N., Tarhini A., Shah M.H., Madichie N., Paul J., Choudrie J. Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior.* 2021; 114:106531. (In Eng.) doi: https://doi.org/10.1016/j.chb.2020.106531

[9] Li Y., Saxunová D. A perspective on categorizing Personal and Sensitive Data and the analysis of practical protection regulations. *Procedia Computer Science*. 2020; 170:1110-1115. (In Eng.) doi: https://doi.org/10.1016/j.procs.2020.03.060

[10] Choi J.P., Jeon D.-S., Kim B.-C. Privacy and personal data collection with information externalities. *Journal of Public Economics*. 2019; 173:113-124. (In Eng.) doi: https://doi.org/10.1016/j.jpubeco.2019.02.001

[11] Ivanov K.V., Balyakin A.A., Malyshev A.S. Big Data Technologies as a National Security Instrument. *St. Petersburg State Polytechnical University Journal. Economics.* 2020; 13(1):7-19. (In Russ., abstract in Eng.) doi: https://doi.org/10.18721/JE.13101

[12] Larionova S.L., Ryakhovski E.E. Organization of counteraction to financial transactions without the client's consent. *Financial Markets and Banks.* 2021; (6):60-67. Available at: https://www.elibrary.ru/item.asp?id=46287383 (accessed 20.06.2022). (In Russ., abstract in Eng.)

[13] Gushchina E.A., Makarenko G.I., Sergin M.Y. Ensuring information and technological sovereignty of the state under the conditions of development of digital economy. *Pravo.bu.* 2018; (6):59-63. Available at: https://www.elibrary.ru/item.asp?id=36983674 (accessed 20.06.2022). (In Russ., abstract in Eng.)

[14] Romashkina N.P. Global military political problems in international informational security: trends, threats and prospects. *Voprosy kiberbezopasnosti* = Cybersecurity issues. 2019; (1):2-9. (In Russ., abstract in Eng.) doi: https://doi.org/10.21681/2311-3456-2019-1-2-9

[15] Markov A.S., Sheremet I.A. Software Safety in the Context of Strategic Stability. *Vestnik Akademii voennyh nauk*. 2019; (2):82-90. Available at: https://www.elibrary.ru/item.asp?id=41590117 (accessed 20.06.2022). (In Russ.)

[16] Erokhin S.D., Borisenko B.B., Martishin I.D., Fadeev A.S. Analysis of existing methods to reduce the dimensionality of input data. *T-Comm.* 2022; 16(1):30-37. (In Russ., abstract in Eng.) doi: https://doi.org/10.36724/2072-8735-2022-16-1-30-37

[17] Alsova O.K., Stubarev I.M. Heterogeneous ensemble algorithm for classification of different types of data. *Izvestia of Samara Scientific Center of the Russian Academy of Sciences.* 2017; 19(6):118-123. Available at: https://www.elibrary.ru/item.asp?id=34964637 (accessed 20.06.2022). (In Russ., abstract in Eng.)

[18] Kiselev A.S. On the Expansion of Legal Regulation in the Field of Artifi cial Intelligence: Deepfake as a Threat to National Security. *Bulletin of Moscow Region State University. Series: Jurisprudence*. 2021; (3):54-64. (In Russ., abstract in Eng.) doi: https://doi.org/10.18384/2310-6794-2021-3-54-64–

[19] Chen S., Yao T., Chen Y., Ding S., Li J., Ji R. Local Relation Learning for Face Forgery Detection. *Proceedings of the AAAI Conference on Artificial Intelligence.* 2021; 35(2):1081-1088. (In Eng.) doi: https://doi.org/10.1609/aaai.v35i2.16193

[20] Tolosana R., Vera-Rodriguez R., Fierrez J., Morales A., Ortega-Garcia J. DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection. *Information Fusion.* 2020; 64:131-148. (In Eng.) doi: https://doi.org/10.1016/j.inffus.2020.06.014

[21] Bonettini N., Cannas E.D., Mandelli S., Bondi L., Bestagini P., Tubaro S. Video Face Manipulation Detection Through Ensemble of CNNs. *2020 25th International Conference on Pattern Recognition (ICPR).* IEEE Computer Society; 2021. p. 5012-5019. (In Eng.) doi: https://doi.org/10.1109/ICPR48806.2021.9412711

[22] Chai L., Bau D., Lim S.N., Isola P. What Makes Fake Images Detectable? Understanding Properties that Generalize. In: Vedaldi A., Bischof H., Brox T., Frahm J.M. (eds.) *Computer Vision – ECCV 2020. ECCV 2020. Lecture Notes in Computer Science.* Vol. 12371. Springer, Cham; 2020. p. 103-120. (In Eng.) doi: https://doi.org/10.1007/978-3-030-58574-7_7

[23] Klyueva A.A., Belov D.A. Current legal research of deepfake technologies and new challenges for the Russian legal system. *Voprosy rossijskoj justicii.* 2021; (14):601-609. Available at: https://www.elibrary.ru/item.asp?id=46458856 (accessed 20.06.2022). (In Russ., abstract in Eng.)

[24] Svirsh A.O., Oleinikova P.A. *Razvitie tehnologii deepfake* [Development of deepfake technology]. *Modern Science*. 2021; (12-4):309-320. Available at: https://www.elibrary.ru/item.asp?id=47460071 (accessed 20.06.2022). (In Russ.)

[25] Nechai A.A. Use of Innovative Methods and Modern Technologies for Advanced Training in Cybersecurity. *Azimut nauchnyh issledovanij: pedagogika i psihologija* = Azimuth of Scientific Research: Pedagogy and Psychology. 2020; 9(3):193-196. (In Russ., abstract in Eng.) doi: https://doi.org/10.26140/anip-2020-0903-0043

Submitted 20.06.2022; approved after reviewing 10.07.2022; accepted for publication 14.07.2022.

About the author:

Sergey V. Lebed, Vice President, Director of the Cybersecurity Department, PJSC "Sberbank of Russia" (19 Vavilov St., Moscow 117997, Russian Federation), Cand.Sci. (Eng.), **ORCID: https://orcid.org/0000-0001-6913-761X,** SVLebed@sberbank.ru

The author has read and approved the final manuscript.