УДК 004.931.056+57.087.1:004.056.5
DOI: 10.25559/SITITO.019.202302.251-261

Оригинальная статья

Мошенничество с использованием синтетических цифровых личностей

А. М. Кузьмин, Д. А. Свичкарь*, П. В. Хенкин
ПАО «Сбербанк России», г. Москва, Российская Федерация
Адрес: 117312, Российская Федерация, г. Москва, ул. Вавилова, д. 19
*DASvichkar@sberbank.ru

Аннотация
Синтетическая цифровая личность – это цифровая запись о некоторой личности (персоне), содержащая стандартные атрибуты личности (имя, телефон, адрес и т.д.), значения которых полностью сфабрикованы или скомпилированы из реальных и вымышленных данных. С развитием цифровизации в мире и, в частности, услуг по предоставлению удаленной идентификации клиентов, онлайн-банкинг и бизнес подвергаются атакам с использованием все более сложных схем мошенничества с задействованием таких синтетических персон. Например, в США вместо использования украденной кредитной карты или удостоверения личности (ID) многие мошенники теперь используют фиктивные, искусственные удостоверения личности для получения кредита. По многим оценкам, мошенничество с искусственными идентификационными данными является самым быстрорастущим видом финансовых преступлений в Соединенных Штатах, на долю которого приходится от 10 до 15 процентов списаний в типичном портфеле необеспеченных кредитов. Еще более тревожным является то, что за этими идентификаторами накапливаются гораздо большие потери, что превращает их в скрытые бомбы замедленного действия. Определить фиктивные данные может оказаться весьма сложной задачей. Для машинного обучения, например, отличия фиктивный данных от настоящих могут быть очень незначительными. Углубленный анализ данных, оставленных реальными людьми, может помочь банкам определить, являются ли их клиенты реальными или нет, и предотвратить убытки от этого быстро растущего вида финансовых преступлений. В работе рассматриваются вопросы создания таких данных, подходы к их выявлению и схемы угроз с их использованием, проведена оценка масштабируемости угрозы синтетических цифровых личностей на территории Российской Федерации и предложена терминология на русском языке для описания области синтетических цифровых личностей.

Ключевые слова: синтетическая цифровая личность (СЦЛ), генерация цифровой личности, тиражирование личностей, вирализация синтетических личностей

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Кузьмин А. М., Свичкарь Д. А., Хенкин П. В. Мошенничество с использованием синтетических цифровых личностей // Современные информационные технологии и ИТ-образование. 2023. Т. 19, № 2. С. 251-261. doi: https://doi.org/10.25559/SITITO.019.202302.251-261

© Кузьмин А. М., Свичкарь Д. А., Хенкин П. В., 2023

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

Original article

Synthetic Identity Fraud

A. M. Kuzmin, D. A. Svichkar*, P. V. Khenkin
PJSC "Sberbank of Russia", Moscow, Russian Federation
Address: 19 Vavilova St., Moscow 117312, Russian Federation
* DASvichkar@sberbank.ru

Abstract

A synthetic digital identity is a digital record about a certain person (person), containing standard identity attributes (name, phone, address, etc.), and the values of these attributes are fabricated or compiled from real and fictitious data. With the development of digitalization and, in particular, services for providing remote customer identification, online banking and business are being attacked using increasingly complex fraud schemes involving synthetic personas. For example, in the USA, instead of using a stolen credit card or identification card (ID), many scammers now use fictitious, artificial IDs to obtain credit. By many estimates, Synthetic Identity Fraud is the fastest-growing type of financial crime in the United States, accounting for 10 to 15 percent of charge-offs on a typical unsecured loan portfolio. Even more worrisome is the fact that these IDs accumulate far greater losses, turning them into hidden time bombs. Identifying fictitious data can be quite challenging. For machine learning, for example, the differences between fictitious data and real data can be very insignificant. In-depth analysis of data left by real people could help banks determine whether their customers are real or not and prevent losses from this fast-growing type of financial crime. The article discusses the issues of creating such data, approaches to their identification and threat patterns, assesses the scalability of the threat of synthetic digital identities on the territory of the Russian Federation and proposes terminology in Russian to describe the field of synthetic digital identities.

Keywords: synthetic digital identity (SDI), digital identity generation, replication of identities, viralization of synthetic identities

Conflict of interests: The authors declare no conflict of interest.

For citation: Kuzmin A.M., Svichkar D.A., Khenkin P.V. Synthetic Identity Fraud. *Modern Information Technologies and IT-Education.* 2023;19(2):251-261. doi: https://doi.org/10.25559/SITITO.019.202302.251-261

Введение

С развитием цифровизации в мире и в частности услуг по предоставлению удаленной регистрации и идентификации пользователей, бизнес подвергается атакам с использованием все более сложных схем мошенничества. Одним из перспективных методов мошенничества становится синтетическая генерация данных несуществующих людей с целью их регистрации в системе организации и последующих мошеннических действий под учетной записью несуществующего в реальности человека. Организации по всему миру обеспокоены данной уязвимостью при открытии удаленного доступа к системам, но до сих пор не разработаны эффективные механизмы выявления данного вида мошенничества. Кроме того, мало внимания уделяется выявлению синтетических личностей в уже имеющейся клиентской базе. Данный вид мошенничества может долгое время оставаться незамеченным, что и приносит достаточно большой ущерб и трудности при расследовании инцидентов.
Синтетические цифровые личности используются для совершения преступлений на разных уровнях мошеннической активности: от мошенничества с частными переводами денег до финансирования глобальных террористических операций. Несмотря на то, что банки и финтех-компании еще не полностью осознают вред от синтетических личностей, регуляторы и правительственные группы активно изучают эту проблему, что означает скорую необходимость изменений в нормативно-правовом регулировании.

Мировой опыт

По результатам анализа мирового опыта в данной сфере выяснилось, что наибольший рост данного вида мошенничества пришелся на США. К 2020 году объем потерь от данного вида мошенничества оценивался в 20 млрд долларов США. На проблему уже обратили внимание регуляторы, правоохранительные органы и финансовые организации США, на которые приходится порядка 50% потерь от данного вида мошенничества. Глобальная пандемия, в дополнение к ее влиянию на жизнь и здоровье людей и экономическую активность, сильно ускорила рост киберпреступности. В ответ на экономические сложности, вызванные пандемией, правительство США разработало стимулирующие адресные программы, чтобы быстро помочь нуждающимся. Эти программы были оперативно запущены с пониманием того, что они будут более уязвимы для мошенничества, чем уже устоявшиеся с хорошо проработанными защитными механизмами, и преступники тут же воспользовались такой соблазнительной возможностью. Количество мошенничеств с получением помощи от государства во время пандемии выросло с 23242 зарегистрированных случаев в 2019 до 407512 и 395948 случаев в 2020 и 2021 году соответственно, то есть почти в 20 раз!

Всплеск мошенничества с СЦЛ именно в США связан с исторической зависимостью граждан страны от номера социального страхования (SSN).SSN не был создан для учета граждан, поэтому неудивительно, что это не идеальный источник данных для верификации личности. Администрация социального обеспечения США перешла к рандомизированным номерам SSN в 2011, также убрав зависимость между первыми тремя цифрами в номере и штатом проживания человека, упростив задачу мошенникам, которые могут просто придумать SSN, что они и делают в 40% случаев. Запуск сервиса электронной верификации SSN (eCBSV) в июле 2021 года позволила повысить надежность SNN в качестве идентификатора личности[1]. Допущенные к сервису банки теперь могут проводить проверку соответствия даты рождения, SSN и имени, но это не закрыло проблему полностью. Финансовые организации не могут проводить проверку для заявителей за пределами США, что дает злоумышленникам возможность подавать заявки из-за рубежа или же использовать VPN, чтобы достичь того же эффекта.
Хотя количество украденных или раскрытых персональных данных уменьшается от года к году, так как киберпреступники смещают свое внимание с частных лиц на бизнес, мошенникам все равно есть с чем работать. На протяжении только последних трех лет в утечках было раскрыто более 1,4 млрд элементов персональных данных. Огромный объем украденных персональных данных сделал их доступными, преступники могут приобрести существующий SSN всего за 1 доллар США, а водительское удостоверение – за 20 долларов США.
Covid-19 ускорил переход к онлайн банкингу, особенно среди более консервативного старшего поколения, где 90% людей старше 60 впервые воспользовались онлайн банкингом в 2020 году. Одновременно с этим банки в США сокращают офлайн-присутствие: количество отделений сократилось на 14824 за последние 5 лет. Чтобы удовлетворить возросший спрос на онлайн-услуги финансовые организации были вынуждены ускорить свою цифровую трансформацию. И выявление мошенничества оказалось одной из отстающих областей. Традиционные системы верификации личности, хорошо выявляющие обычную кражу личности, оказались в большинстве своем беспомощными перед лицом новой угрозы и пропускают 85-95% потенциально синтетических цифровых личностей.
По другим странам подробную статистику реализации данного вида мошенничества найти не удалось. По всей видимости, это связано с тем, что в других странах цифровые услуги распространены в меньшей степени, и нет такой сильной зависимости граждан от номера социального страхования.
Реализация мошенничества с использованием синтетических цифровых личностей в Российской Федерации затруднена благодаря принятым в финансовых организациях практикам «Знай своего клиента» – KYC (англ. know your customer)[2], а также пункта 5 статьи 7 федерального закона № 115-ФЗ «О

[1] The State of Synthetic Fraud: Evolution, Trends, and How We Will Eradicate It By 2026. Nevada, US : Socure, 2023 [Электронный ресурс]. URL: https://offers.socure.com/the-state-of-synthetic-fraud.html (дата обращения: 23.06.2023).

[2] Директива Европейского Парламента и Совета Европейского Союза 2015/849 от 20 мая 2015 г. «О предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма, об изменении Регламента (ЕС) 648/2012 Европейского Парламента и Совета ЕС и об отмене Директивы 2005/60/ЕС Европейского Парламента и Совета ЕС и Директивы 2006/70/ЕС Европейской Комиссии» [Электронный ресурс] // European Union, 2023. URL: https://eur-lex.europa.eu/eli/dir/2015/849/oj/eng (дата обращения: 23.06.2023).

противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[3], так как требует личного присутствия клиента или его представителя для проведения его идентификации. В случае же открытия счета без личного присутствия клиента или его представителя (например, при открытии счета юридического лица) требуется подпись электронного документа квалифицированной цифровой подписью, для получения которой необходимо пройти идентификацию в удостоверяющем центре. При надлежащем проведении процедуры идентификации со стороны финансовой организации или удостоверяющего центра, возможность открытия счета или получения услуг для синтетической личности на данный момент сильно ограничены, однако и у нас в стране есть подобные примеры.

Примеры мошенничества примеры мошенничества[4]

В США:

- в 2013 году Департамент Юстиции США обвинил 18 человек в соучастии в одной из самых крупных и сложных схем мошенничества с использованием банковских карт. Преступная группировка создала сеть из более чем 7000 синтетических личностей и незаконно получила на них более 25000 кредитных карт. Используя пиггибэкинг, группировка поддерживала функционирование более 1800 дроп-адресов, получала тысячи кредитных крат с небольшим кредитным лимитом и исправно вносила платежи по кредитам. Группировка также использовала юридические лица для улучшения кредитной истории синтетических личностей, получая значительную прибыль от своих операций. Однако точный размер ущерба сложно определить из-за сложности схем и давности преступлений;
- В 2013 году двое мошенников создали более 750 синтетических личностей, часть из которых использовалась для неправомерного получения миллионов долларов США в виде выплат по программе займов в случае чрезвычайных обстоятельств. Мошенники начали выращивать СЦЛ еще в 2015 году и использовали их для основания подставных компаний и открытия счетов в финансовых учреждениях. Они использовали данные компании для подачи заявлений по программе займов в случае чрезвычайных обстоятельств, создавая фальшивые личности с помощью, украденной SSN и других ключевых данных. Три подставные компании были созданы с использованием СЦЛ. Затем мошенники использовали данные компании для подачи заявлений на займ в размере 75 000 долларов США, запрашивая 50 сотрудников компании, все из которых были синтетическими личностями. Заявления были одобрены в тот же день. Все эти СЦЛ находились в «спящем» состоянии в течение многих лет, прежде чем были использованы для подачи заявок на займ, что может служить примером масштаба подобных атак, реализуемых во время значимых мировых событий;
- мошенник приобрел в даркнет SSN (по $5 за каждый), принадлежавшие мужчинам с высоким доходом и положительной кредитной историей, что позволяло бы ему претендовать на большую сумму кредита. Он использовал реальные имена и даты рождения, но создал новые e-mail адреса. Далее он заключил контракты с тремя разными операторами сотовой связи и подал заявки на кредит в различных организациях. После чего выбрал организацию, которая предложила наибольший кредит – $ 150 000. После чего заказал поддельные водительские права в даркнете и осуществил мошенничество;
- преступник выручил более $ 200 000 наличными в результате незаконной продажи оружия. Понимая, что внесение крупной суммы на счет может вызвать подозрения, он решил использовать множество синтетических личностей для открытия счетов в различных банках, которые затем можно было использовать для внесения денег и совершения новых закупок. Были приобретены 30 SSN в даркнет, затем созданы синтетические личности, используя имена своих контактов в социальных сетях, а также свой реальный адрес и телефон, после чего подал 30 заявок на открытие счетов в финансовых организациях (все заявки были одобрены). После чего внёс деньги на счета и использовал для покупки оружия.

В Российской Федерации:

- в Таганроге злоумышленница почти 14 лет (с 2008 по 2022 год) получала выплаты на несуществующих детей. У женщины по документам было 7 детей, но только 3 из них были настоящими. Остальные были зарегистрированы после домашних родов на основании заявления свидетеля. Размер нанесенного ущерба составил около 2,5 млн рублей[5];
- в Красноярске в 2019 году было зафиксировано порядка 20 случаев регистрации детей после родов на дому на основании заявления свидетеля. Как впоследствии выяснили правоохранительные органы, во всех случаях в качестве свидетеля выступала одна и та же женщина, которая и придумала мошенническую схему и реализовывала ее в сговоре с другими женщинами, выступавшими в качестве матерей регистрируемых несуществующих детей[6];
- в Хабаровском крае с января 2020 года по ноябрь 2021 действовала организованная преступная группа, состоящая из 23 женщин, заявивших о фиктивных родах на дому и получивших свидетельства о рождении на основании заявления свидетеля. В результате действий мошенников был нанесен ущерб государству в размере более 19 миллионов рублей[7].

---

[3] О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма : федер. закон Рос. Федерации от 07.08.2011 № 115-ФЗ (последняя редакция) : принят Государственной Думой 13 июля 2001 г. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_32834 (дата обращения: 23.06.2023).

[4] The Federal Reserve. Synthetic Identity Fraud Use Cases. Federal Reserve Banks, 2023. [Электронный ресурс]. URL: https://fedpaymentsimprovement.org/synthetic-identity-fraud-mitigation-toolkit/when-synthetics-become-a-reality (дата обращения: 23.06.2023).

[5] Шиляева А. Многодетная мама с одним классом образования провернула многомиллионную аферу [Электронный ресурс] // Комсомольская правда. 9 января 2023. URL:https://www.rostov.kp.ru/daily/27450/4703659 (дата обращения: 23.06.2023).

[6] Ильченко Н., Серебровская Е. В Красноярске цыганки массово регистрировали в ЗАГСе несуществующих детей для получения маткапитала [Электронный ресурс] // Комсомольская правда. 14 августа 2019. URL: https://www.krsk.kp.ru/daily/27016.4/4078047 (дата обращения: 23.06.2023).

[7] Фалхвадзе Е. Домашние роды и выдуманные дети: банда мамочек из Хабаровска «выцыганила» 19 миллионов рублей на пособия [Электронный ресурс] // Комсомольская правда. 1 ноября 2022. URL: https://www.hab.kp.ru/daily/27465/4670725 (дата обращения: 23.06.2023).

Эффект влияния на различные сферы экономики

В то время как атаки с использованием синтетических личностей ведут к финансовым потерям, средний размер потерь и общее количество счетов, понесших финансовые потери в результате мошенничества, значительно отличаются в зависимости от отрасли. На примере США – наибольшие потери наблюдаются в секторе автокредитования и кредитных карт – в среднем около 17000 и 14000 долларов США соответственно. Наименьшие потери фиксируются банками по текущим и сберегательным счетам – в среднем менее 400 долларов США на 1 инцидент. При этом для цифровых банков характерен более высокий процент синтетических счетов относительно общего количества счетов, чем у традиционных банков.

Из-за низкого уровня регистрируемых и выявляемых потерь и относительной новизны проблемы, банковская индустрия пока еще не применяет продвинутые методы выявления синтетических личностей в момент открытия счета. Также лишь небольшое количество банков пытается выявлять синтетические личности среди существующей клиентской базы. Банки зачастую не могут отличить атаки с применением синтетических личностей от обычной задолженности по выплатам и списывают потери на падение платежеспособности клиента или обычное мошенничество. При этом на банковский сектор приходится почти 50% от общего количества атак с применением синтетических личностей.

Синтетические личности могут быть использованы для совершения всевозможных вредоносных действий, в том числе для отмывания денег, торговли людьми или наркотиками, мошенничества с платежами и даже террористической деятельности.

Рост числа мошеничеств

Синтетические цифровые личности используются в сравнительно небольшом количестве клиентских счетов, но при этом ответственны за огромный объем потерь. По оценкам FiVerify Cyber Fraud Network[8] потери от СЦЛ в США достигли 20 млрд долларов в 2020 году.

Финансовые организации, обнаруживающие активные поддельные аккаунты, закрывают их, а потери зачастую объясняются плохим андеррайтингом[9]. По оценкам FiVerity за 12 месяцев с момента открытия счетов СЦЛ имеют возможность похитить около 90000 долларов США. Эта сумма не включает периодически применяемую мошенниками тактику заявить себя жертвой кражи личности, чтобы удвоить сумму хищения.

Проблемы противодействия

- Противодействие мошенничеству с использованием синтетических цифровых личностей затруднено рядом факторов:
  - Сложность выявления синтетических цифровых личностей как при прохождении KYC новым клиентом, так и в существующей клиентской базе.
  - Отсутствие пострадавших лиц, способных заявить о факте мошенничества (как в случае с другими видами мошенничества).
  - Сложность с отделением мошенничества с использованием синтетических цифровых личностей от других видов мошенничества или случаев реальной неплатёжеспособности клиента.
  - При этом мошенники способны быстро создавать целые армии из синтетических личностей и оперативно масштабировать свои мошеннические операции, что видно из стремительного растущего объема потерь от данного вида мошенничества (с 6 млрд долларов США в 2016 году до 20 млрд долларов США в 2020 году). Развитие технологий deepfake и генеративных искусственных нейронных сетей (GAN) [1], и рост доступности инструментов для их создания синтетических изображений лица вносит дополнительные сложности в выявление синтетических цифровых личностей. Предлагаемые в современных исследованиях методы синтеза изображений лиц, такие как ExFaceGAN [2], SynFace [3], SFace [4], DigiFace-1M [5], USynthFace [6], IDnet [7], GAN-control [8] и других подобных, уже сейчас позволяют синтезировать изображения одного и того же лица в разных условиях, под разными углами и с разными выражениями лица. Это дает злоумышленникам возможность для создания реалистичных профилей синтетических цифровых в социальных сетях и наполнять его реалистичными фотографиями, тем самым подкреплять уверенность в существовании личностей и затруднять процесс их выявления и проверки.
  - Дальнейшее развитие технологий в сторону синтеза реалистичного видео способно еще сильнее усугубить ситуацию, так как позволит синтетическим цифровым личностям проходить KYC-проверки в удаленном режиме, участвовать в видеозвонках и онлайн-встречах. В настоящее время данное направление активно исследуется и развивается целый ряд подходов, позволяющих осуществлять «пересадку» лиц на видео или генерировать полностью синтетические видео с реалистичными лицами людей, например, Live Speech Portraits [9], Mobile Face Swap [10], GHOST [11], DeepFaceLab [12], AP-GAN [13], Style FaceV [14], Styleheat [15], AnifaceGAN [16], Head2Head [17]. Для работы большинства из этих подходов достаточно предоставить лишь одно изображение целевого лица и получаемый результат перцептивно неотличим от реально существующего лица, а небольшие возникающие при генерации артефакты могут быть интерпретированы собеседником как помехи в канале видеосвязи. При сочетании вышеописанных подходов с методами синтеза голоса, такими как Hifi-GAN [18], Naturalspeech [19], FastDiff [20] и возможностями больших языковых моделей, например,

[8] Buzzard J., Kitten T. 2021 Identity Fraud Report. FiVerity, 2023. [Электронный ресурс]. URL: https://www.fiverity.com/resources/sif-report-2021 (дата обращения: 23.06.2023).

[9] 2021 Consumer Sentinel Network Data Book: Federal Trade Commission February. Independently published, 2022. 90 p. [Электронный ресурс]. URL: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2021 (дата обращения: 23.06.2023).

GPT-3 [21], Llama [22] или Bloom [23] в руках злоумышленников могут оказаться полностью автономные, мультимодальные интеллектуальные боты, способные самостоятельно вести разумный диалог и проходить верификацию личности и другие проверки по видео- и аудиосвязи без участия человека. Все это может позволить злоумышленникам легко масштабировать атаки с использованием СЦЛ до невиданных ранее масштабов.

- Синтетические личности несут не только угрозы финансовых потерь для банков и других организаций. Они также могут быть использованы в преступных схемах по отмыванию денег, торговле наркотиками и оружием и даже финансированию террористической деятельности.
- Для противодействия этому растущему виду мошенничества финансовые регуляторы США вместе с группой отраслевых экспертов разработали ряд рекомендаций для финансовых и других организаций по выявлению синтетических цифровых личностей при регистрации новых клиентов, а также в существующей клиентской базе.
- В качестве первого шага в борьбе с мошенничеством с использованием синтетических личностей Федеральный Резервная система США в апреле 2021 года разработала его определение:
- Мошенничество с использованием синтетической личности (*Synthetic Identity Fraud*) – использование персональных данных для фабрикации личности или сущности для совершения противоправных действий с целью извлечения личной или финансовой выгоды.
- Несмотря на довольно простое определение, процесс создания профиля синтетической цифровой личности может быть довольно сложным технологически, и включать использование автоматизации и машинного обучения.

Определение синтетической цифровой личности

По своей сути синтетическая цифровая личность – это несуществующая цифровая личность, состоящая из набора данных, таких как, имя, фамилия, телефон, адрес и т.д. сфабрикованных из вымышленных данных или скомпилированных из реальных и вымышленных данных (далее – СЦЛ)[10].

Главным отличием и соответственно опасностью для атакуемой организации является отсутствие пострадавшего. В случае традиционного мошенничества злоумышленник использует реальные данные существующего человека и таким образом наносит ущерб конкретному человеку. Жертва обнаруживает мошеннические действия и обращается в организацию и правоохранительные органы, что зачастую позволяет оперативно расследовать инцидент. В случае мошенничества с использованием СЦЛ жертва, в традиционном понимании, отсутствует, что не позволяет оперативно установить факт преступления и жертвой в данном случае становится сама организация.

Используемые для создания синтетической цифровой личности элементы можно разделить на 2 категории:

основные – элементы личности, которые в комбинации как правило уникальны и однозначно идентифицируют личность. В эту категорию входят ФИО, дата рождения, и уникальные номера официальных документов (SSN, номер паспорта);

дополнительные – элементы, которые могут подкрепить идентификацию личности, но которые не могут подтвердить личность сами по себе (почтовый адрес, номер телефона, IP-адрес, ID устройства).

В зависимости от реальности используемых элементов выделяется три метода создания синтетической цифровой личности:

Фабрикация – личность создается из полностью вымышленных элементов, без использования похищенных или скомпрометированных данных.

Манипуляция – личность создается путем частичных изменений элементов реально существующей личности (например, имя и дата рождения остаются прежними, изменяется только номер паспорта или SSN).

Компиляция – личность создается из комбинации реальных и вымышленных элементов.

Этапы создания СЦЛ

Типичные шаги, предпринимаемые мошенниками для создания синтетической цифровой личности[11]:

Шаг 1. Мошенник создает личность используя украденные или сфабрикованные персональные данные

Для многих мошенников процесс создания синтетической личности начинается в даркнет, где они могут приобрести персональные данные и другую личную информацию, раскрытую в результате сливов, социальной инженерии или краулинга социальных сетей. Также мошенники часто фабрикуют всю информацию, которую они используют для подачи заявки на кредит. Если используется реальный номер социального страхования (SSN), то как правило он принадлежит ребенку, пожилому человеку или бездомному, так как эти группы людей редко используют или проверяют свою кредитную историю.

Шаг 2. Мошенник подает заявку на кредит используя синтетическую личность

По данным компании ID Analytics более 50% мошенников подают заявку на получение кредита онлайн. При этом некоторое количество мошенников, использующих СЦЛ также лично приходят в финансовые учреждения, предоставляя ложную информацию для подтверждения своей личности. После приема заявки финансовое учреждение подает запрос в одно или несколько бюро кредитных историй, откуда приходит ответ об отсутствии кредитной истории у данной персоны. В таком случае, как правило, финансовое учреждение отказывает в выдаче кредита. Но, согласно закону, подобный запрос приводит к созданию кредитного профиля нового клиента, даже несмо-

[10] Uncovering Synthetic Identity Fraud. LexisNexis [Электронный ресурс]. URL: https://risk.lexisnexis.com/insights-resources/article/synthetic-identity-fraud (дата обращения: 23.06.2023); Synthetic Identity Fraud: A Costly Challenge. Information Security Media Group, Corp., 2022. [Электронный ресурс]. URL: https://www.databreachtoday.com/whitepapers/synthetic-identity-fraud-costly-challenge-w-10873 (дата обращения: 23.06.2023).

[11] Synthetic Identity Fraud in the U.S. Payment System: A Review of Causes and Contributing Factors. Payments Fraud Insights. The Federal Reserve, 2019. [Электронный ресурс]. URL: https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf (дата обращения: 23.06.2023).

тря на то, что в кредите ему было отказано.

Шаг 3. Мошенник повторно подает заявку на кредит, пока она не будет одобрена

Мошенник продолжает подавать заявки на выдачу кредита в различные финансовые организации, пока одна из них не одобряет ему кредит. Далее мошенник использует предоставленную кредитную линию, исправно внося платежи без просрочек, чтобы получить доступ к более щедрым кредитным лимитам. Этот процесс может занять от нескольких месяцев до года, особенно если реальный владелец SNN не проявляет кредитной активности.

Шаг 4. Мошенник ускоряет формирование положительной кредитной истории

Мошенник может ускорить процесс формирования положительной кредитной истории за счет тактики «пиггибэкинга» – добавления СЦЛ как авторизованного пользователя к аккаунту с хорошей кредитной историей. Таким аккаунтом может быть другая СЦЛ, которая была создана ранее и уже сформировала себе хорошую кредитную историю. По данным ID Analytics почти 50% СЦЛ используют пиггибэкинг для формирования кредитной линии.

Мошенники используют различные тактики для того, чтобы СЦЛ выглядела реалистично и могла претендовать на большие кредитные линии. Эти тактики могут включать создание фальшивых документов, удостоверяющих личность, ведение аккаунтов в социальных сетях, использование дроп-адресов (например, абонентских ящиков, адресов пустующих зданий либо домов отдыха), что позволяет мошенникам получать письма и посылки или перенаправлять их по другим адресам. Мошенники также используют СЦЛ для учреждения юридических лиц, на которые можно получить POS-терминалы для проведения мошеннических карточных транзакций и другой противоправной деятельности.

Шаг 5. Мошенник совершает преступление

По мере того, как кредитный рейтинг СЦЛ повышается, мошенник получает доступ ко все более и более крупным кредитам, пока в конце концов мошенник не совершает кражу. Для этого он максимально использует доступную ему кредитную линию и исчезает. Кроме этого, мошенник может удвоить выплату по каждой кредитной линии, заявив о краже личности чтобы аннулировать платежи, заявленным им как мошеннические. Затем мошенник может создать новую СЦЛ и повторить процесс.

Особенности мошенничества с использованием СЦЛ

Хотя мошенничество с СЦЛ похоже на традиционную кражу личность, его развитие, реализация и последствия совершенно не похожи на предыдущие поколения финансовых преступлений:

Масштабируемость – благодаря отличной масштабируемости мошенничество с СЦЛ стало самым быстрорастущим видом финансовых преступлений в США. Преступники используют автоматизацию для сбора элементов личности и создают миллионы синтетических профилей.

Скрытность – благодаря глубокому пониманию принципов работы платежной системы и использованию специально разработанного ПО преступники имеют возможность создавать синтетические профили, которые очень сложно выявить. В отличие от кражи реальной личности, в данном случае нет пострадавшего, который может заметить мошенническую транзакцию в своей истории транзакций и обратиться в банк.

Виральность – как только синтетическая личность получает достаточно высокий кредитный рейтинг, она быстро открывает в среднем пять кредитных линий, как правило в разных банках. Подключая дополнительные синтетические профили к счету уже авторизованного пользователя, преступники имеют возможность оперативно подготавливать следующую волну синтетических личностей для дальнейших преступлений.

Хотя мошенничество с СЦЛ, скорее всего, существовало в каком-то виде на протяжении десятилетий, наличие системных проблем в безопасности, развитие технологий и массовое внедрение цифровых услуг спровоцировало резкий рост этого вида мошенничества.

Опыт противодействия мошенничеству с применениемСЦЛ

Государственные регуляторы и правоохранительные органы в США уже несколько лет озабочены проблемой противодействия мошенничеству с применением синтетических цифровых личностей.

Экспертным сообществом был разработан ряд методов эффективного выявления СЦЛ. Они разбиты на две группы в зависимости от этапа жизненного цикла. Данные рекомендации в первую очередь направлены на финансовую сферу, где проблема синтетических цифровых личностей стоит особо остро[12].

Выявление СЦЛ при открытии счета

Очевидной и лучшей стратегий снижения риска мошенничества является идентификация синтетической личности до начала деловых отношений[13]. Если СЦЛ никогда не станут клиентами компании, вероятность негативного воздействия будет минимальна. После установления отношений с клиентом выявить синтетическую личность становится сложнее, так как транзакции СЛЦ зачастую имитируют действия легитимного клиента. Например, действия по кредитной карте, скорее всего, будут выглядеть как нормальные, так как периодически производятся списания и погашение долга будет происходить вовремя.

Для выявления СЦЛ при открытии счета рекомендуется более

[12] Detecting Synthetic Identity Fraud in the U.S. Payment System. Payments Fraud Insights. The Federal Reserve, 2019. [Электронный ресурс]. URL: https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-october-2019.pdf (дата обращения: 23.06.2023); Mitigating SyntheticIdentity Fraud in theU.S. Payment System. Payments Fraud Insights. The Federal Reserve, 2020. [Электронный ресурс]. URL: https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2020.pdf (дата обращения: 23.06.2023).

[13] HorswellS., et al. Identity FraudReport 2023. Onfido, 2023. [Электронный ресурс]. URL: https://onfido.com/wp-content/uploads/2022/12/identity-fraud-report-2023.pdf (дата обращения: 23.06.2023).

тщательно подходить к процессу проверки личности и использовать различные инструменты для этого[14]:
сторонние данные – чем больше сторонних источников будет использовано для верификации, тем больше шансов, что личность реально существует. Данные реальных людей согласуются между собой, в то время как данные синтетических личностей, как правило, содержат несостыковки. Например, заявитель может уже иметь банковский счет, студенческий займ, текущий и предыдущий адрес, номер телефона и адрес электронной почты. Эти элементы данных о личности должны совпадать в различных источниках;
данные государственных информационных систем (ГИС) и публичные данные – эти данные могут помочь в подтверждении личности заявителя. Например, проверка адреса заявителя в ГИС или публичных данных может показать, что данный адрес связан с другим лицом или же является офисным, а не жилым зданием;
сравнение данных[15] – мошенники часто переиспользуют элементы данных при создании СЦЛ, перемешивая номера документов, имена, даты рождения и адреса в разных комбинациях. В связи с этим выявление СЦЛ возможно при сравнении подаваемых заявителем данных с информацией, используемой в уже выявленных случаях мошенничества;
технологические решения – на рынке уже существует ряд IT-решений, способных помочь с выявлением СЦЛ в процессе открытия счета. Эти решения используют данные из различных источников, как открытых, так и проприетарных, для анализа информации в заявлении на предмет вероятности того, что данная личность является синтетической. Среди производителей подобных решений на данный момент выделяются компании Socure, FiVerify и ряд других.

Выявление СЦЛ среди существующих пользователей

С точки зрения транзакционной активности СЦЛ не отличаются от реальных клиентов: они точно также совершают различные покупки и своевременно вносят платежи, стремясь увеличить свою кредитную линию. До самого момента хищения денег и прекращения погашения кредита выявить СЛЦ на основании транзакционной активности крайне затруднительно. Экспертная группа Федеральной резервной системы дает следующие высокоуровневые рекомендации для выявления СЛЦ среди существующих клиентов[16]:
проводите регулярный анализ и сравнение данных клиентов, чтобы выявить пересечения в данных – этот подход считается эффективным, так как мошенники часто переиспользуют одни и те же синтетические данные, используют данные другого человека или осуществляют доступ к счету с одного устройства или IP-адреса;
анализируйте детали транзакций на предмет потенциальных критериев для выявления СЛЦ – построение профиля для выявления СЦЛ как правило базируется на подтвержденных случаях мошенничества и их деталях (короткая или отсутствующая история, добавление новых авторизованных пользователей к счету, объемы и тип транзакций и т.п.);
используйте дополнительные данные для сравнения и подтверждения данных клиентов – для выявления синтетических личностей рекомендуется использовать дополнительные источники данных: данные поставщиков решений по противодействию мошенничеству, данные из государственных информационных систем, данные о цифровом следе в сети Интернет.
В части анализа транзакций, в научных публикациях исследуется ряд подходов с применением глубоких нейронных сетей и графовых сетей, направленных на выявление СЦЛ, например, в работах [24-26].

Угроза СЦЛ в Российской Федерации

Как уже было сказано выше, российское законодательство, требования регуляторов и обязательная проверка данных клиентов затрудняют реализацию мошенничества с использованием СЦЛ. Но такие риски до сих пор остаются, особенно в случае сговора с должностным лицом организации. В случае сговора с сотрудником ИТ-подразделения возможно добавление записи о счете СЦЛ непосредственно в базу данных АС с использованием административных полномочий данного сотрудника.
На горизонте в 5 лет при внедрении единой биометрической системы (ЕБС) для прохождения идентификации с помощью биометрических данных, таких как изображение лица или отпечатки пальцев (в случае добавления данного фактора в ЕБС в будущем), возможности использования СЦЛ для противоправных действий расширяются, так как не требуется личное присутствие в офисе финансовой организации для прохождения идентификации. Технологии генерации изображений и видео с помощью искусственного интеллекта могут помочь злоумышленникам создать правдоподобный deepfake-образ[17] для прохождения удаленных проверок по видеосвязи, а также сгенерировать правдоподобные изображения отпечатков пальцев [27] для прохождения биометрической проверки.
В целом, можно выделить следующие факторы, облегчающие реализацию угроз с применением СЦЛ:
1. Сговор с сотрудником финансовой организации или удостоверяющего центра. В данном случае существует риск пропуска или ненадлежащего проведения ряда проверок.
2. Использование иностранных документов, удостоверяющих личность (ДУЛ). Возможности проведения проверок иностранных ДУЛ ограничены, по сравнению с ДУЛ РФ.

[14] Richardson B., Waldron D. Fighting back against synthetic identity fraud. McKinsey & Company, 2019. [Электронный ресурс]. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/fighting-back-against-synthetic-identity-fraud (дата обращения: 23.06.2023).

[15] 2022 Global State of Fraud and Identity Report. LexisNexis, 2022. [Электронный ресурс]. URL: https://risk.lexisnexis.com/insights-resources/research/global-state-of-fraud-and-identity (дата обращения: 23.06.2023).

[16] Insights and resources [Электронный ресурс] // KPMGLLP, 2023. URL: https://advisory.kpmg.us/blog/2022/detecting-undetectable.html (датаобращения: 23.06.2023).

[17] Deep Face Live // GitHub, 2023. [Электронный ресурс]. URL: https://github.com/iperov/DeepFaceLive (дата обращения: 23.06.2023).

3. Использование ДУЛ без фото (например, свидетельство о рождении). Отсутствие фото затрудняет возможность удостоверения личности.
4. Удаленное открытие счета для туристов без прохождения идентификации в РФ. Данная инициатива прорабатывается Минэкономразвития для развития въездного туризма в РФ и подразумевает открытие карты удаленно до фактического приезда иностранного туриста в РФ, что может затруднять надлежащее проведение проверок[18].

В таблице 1 приведены возможные меры противодействия угрозам СЦЛ при проведении идентификации для разных типов используемые СЦЛ.

Таблица 1. **Возможные меры противодействия использованию СЦЛ**
Table 1. **Possible measures to counter the use of SDP**

Тип СЦЛ	Характерные особенности	Меры противодействия
СЛЦ, полученная путем фабрикации	Номер и данные ДУЛ являются вымышленными	Проверка номера ДУЛ на действительность
СЦЛ, полученная путем манипуляции	Номер ДУЛ и другие данные документа принадлежат одному лицу, а фото в ДУЛ - другому	Проверка взаимного соответствия фото и данных ДУЛ (при наличии фото в ДУЛ)
СЦЛ, полученная путем компиляции	Номер ДУЛ принадлежит одному лицу, другие персональные данные, указанные в документе – другому лицу или ряду лиц	Перекрестная проверка соответствия номера ДУЛ, ФИО, даты рождения и других данных ДУЛ

Источник: здесь и далее в статье все таблицы составлены авторами.
Source: Hereinafter in this article all tables were made by the authors.

При оценке угрозы СЦЛ в РФ также важно учесть, что помимо банковских организаций, где существующие законы и предписываемые ими процедуры идентификации снижают к минимуму возможность применения СЦЛ, существует еще ряд сфер и организаций, где применение СЦЛ для достижения целей злоумышленников (как правило, хищение или незаконное получение денежных средств) также целесообразно. Примеры наиболее вероятных целей для мошенничества с использованием СЛЦ приводятся в таблице 2.

Таблица 2. **Вероятные цели для мошенничества с применением СЦЛ помимо банковских организаций**
Table 2. **Possible targets for Synthetic Identity Fraud other than banking organizations**

Организации	Цель злоумышленника
Микрофинансовые организации	Получение кредитов или займов
Страховые организации	Получение страховых выплат
Нотариальные организации	Оформление нотариальных доверенностей, нотариально заверенных копий, удостоверение сделок с использованием документов СЦЛ
Государственные органы социальной защиты	Получение социальных выплат или льгот
Прочие организации	Трудоустройство СЦЛ с целью промышленного шпионажа, хищения интеллектуальной собственности, материальных ценностей или денежных средств

В случае сговора злоумышленника с сотрудником организации реализации мошеннической схемы существенно упрощается, так как позволяет пропускать целый ряд проверок, призванных противодействовать мошенничеству. Но даже в случае отсутствия сговора возможна реализация ряда мошеннических схем с использованием фальшивых документов и подставных лиц для представления СЦЛ при очной подаче документов. Степень сложности реализации мошеннической схемы напрямую зависит от количества и качества проверок, а также предоставляемых документов.

Заключение

На основании вышеизложенного можно сделать вывод, что проблема и масштаб роста мошенничества с использованием СЦЛ наиболее остро стоит в США, что прежде всего, связано с историческими факторами, такими как использование номера социального страхования (SSN) в качестве основного идентификатора и высокого уровня цифровизации бизнеса без своевременного внедрения механизмов и проверок, препятствующих мошенничеству, а наибольшее количество потерь (порядка 50%) приходится на банковскую сферу.

В других странах, в том числе Европы и Азии, мошенничество с СЦЛ не выделено в отдельную категорию, и отдельный учет потерь и масштабов подобного мошенничества не ведется, в том числе и потому, что данный вид мошенничества довольно сложно выявить и отличить от случаев реальной неплатежеспособности или плохого андеррайтинга при выдаче кредитов.

В Российской Федерации в силу принятых законов и выработанных процедур в финансовых организациях проверки персональных данных клиентов аналогичные мошеннические

[18] Буйлов М. Туристам подготовили карту [Электронный ресурс] // Коммерсантъ. № 243 от 29 декабря 2022. С. 5. URL: https://www.kommersant.ru/doc/5748545 (дата обращения: 23.06.2023); The Stark Reality of Synthetic ID Fraud. Equifax, 2022. [Электронный ресурс]. URL: https://www.equifax.com/resource/-/asset/white-paper/stark-reality-synthetic-id-fraud (дата обращения: 23.06.2023).

схемы с применением СЦЛ реализовать гораздо сложнее, но в случае сговора с сотрудником финансовой или другой организации такое становится возможным.

Государственные органы социальной защиты в России также подвержены риску мошенничества с СЦЛ. Некоторые случаи были зафиксированы на протяжении последних 10 лет. Ряд других организаций также может быть подвержен данному виду мошенничества, но пока подобные случаи не выделены в отдельную категорию и не ведется статистика потерь, поэтому оценить текущий уровень потерь в России от мошенничества с СЦЛ не представляется возможным.

Таким образом, организациям требуется уделить внимание вышеизложенным методам создания и интеграции СЦЛ в автоматизированные системы, а также применить описанные методы для поиска и выявления СЦЛ.

References

[1] Goodfellow I., Pouget-Abadie J., Mirza M., Xu B., Warde-Farley D., Ozair S., Courville A., Bengio Y. Generative adversarial networks. *Communications of the ACM*. 2020;63(11):139-144. doi: https://doi.org/10.1145/3422622

[2] Boutros F. et al. ExFaceGAN: Exploring Identity Directions in GAN's Learned Latent Space for Synthetic Identity Generation. arXiv:2307.05151. 2023. Available at: https://arxiv.org/abs/2307.05151 (accessed 23.06.2023).

[3] Qiu H., Yu B., Gong D., Li Z., Liu W., Tao D. SynFace: Face Recognition with Synthetic Data. In: 2021 IEEE/CVF International Conference on Computer Vision (ICCV). Montreal, QC, Canada: IEEE Computer Society; 2021. p. 10860-10870. doi: https://doi.org/10.1109/ICCV48922.2021.01070

[4] Boutros F., Huber M., Siebke P., Rieber T., Damer N. SFace: Privacy-friendly and Accurate Face Recognition using Synthetic Data. In: 2022 IEEE International Joint Conference on Biometrics (IJCB). Abu Dhabi, United Arab Emirates: IEEE Computer Society; 2022. p. 1-11. doi: https://doi.org/10.1109/IJCB54206.2022.10007961

[5] Bae G. et al. DigiFace-1M: 1 Million Digital Face Images for Face Recognition. In: 2023 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV). Waikoloa, HI, USA: IEEE Computer Society; 2023. p. 3515-3524. doi: https://doi.org/10.1109/WACV56688.2023.00352

[6] Boutros F., Klemt M., Fang M., Kuijper A., Damer N. Unsupervised Face Recognition using Unlabeled Synthetic Data. In: 2023 IEEE 17th International Conference on Automatic Face and Gesture Recognition (FG). Waikoloa Beach, HI, USA: IEEE Computer Society; 2023. p. 1-8. doi: https://doi.org/10.1109/FG57933.2023.10042627

[7] Kolf J.N., Rieber T., Elliesen J., Boutros F., Kuijper A., Damer N. Identity-driven Three-Player Generative Adversarial Network for Synthetic-based Face Recognition. In: 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). Vancouver, BC, Canada: IEEE Computer Society; 2023. p. 806-816. doi: https://doi.org/10.1109/CVPRW59228.2023.00088

[8] Shoshan A., Bhonker N., Kviatkovsky I., Medioni G. GAN-Control: Explicitly Controllable GANs. In: 2021 IEEE/CVF International Conference on Computer Vision (ICCV). Montreal, QC, Canada: IEEE Computer Society; 2021. p. 14063-14073. doi: https://doi.org/10.1109/ICCV48922.2021.01382

[9] Lu Y., Chai J., Cao X. Live speech portraits: real-time photorealistic talking-head animation. *ACM Transactions on Graphics*. 2021;40(6):220. doi: https://doi.org/10.1145/3478513.3480484

[10] Xu Z., Hong Z., Ding C., Zhu Z., Han J., Liu J., Ding E. MobileFaceSwap: A Lightweight Framework for Video Face Swapping. *Proceedings of the AAAI Conference on Artificial Intelligence*. 2022;36(3):2973-2981. doi: https://doi.org/10.1609/aaai.v36i3.20203

[11] Groshev A., Maltseva A., Chesakov D., Kuznetsov A., Dimitrov D. GHOST – A New Face Swap Approach for Image and Video Domains. *IEEE Access.* 2022;10:83452-83462. doi: https://doi.org/10.1109/ACCESS.2022.3196668

[12] Jia F., Yang S. Video face swap with DeepFaceLab. In: Proceedings of SPIE 12168, International Conference on Computer Graphics, Artificial Intelligence, and Data Processing (ICCAID 2021). SPIE; 2022. Article number: 121681H. doi: https://doi.org/10.1117/12.2631297

[13] Zhang L., Yang H., Qiu T., Li L. AP-GAN: Improving Attribute Preservation in Video Face Swapping. *IEEE Transactions on Circuits and Systems for Video Technology*. 2022;32(4):2226-2237. doi: https://doi.org/10.1109/TCSVT.2021.3089724

[14] Qiu H., Jiang H., Zhou H., Wu W., Liu Z. StyleFaceV: Face Video Generation via Decomposing and Recomposing Pretrained StyleGAN3. arXiv:2208.07862 2022. doi: https://doi.org/10.48550/arXiv.2208.07862

[15] Yin F. et al. StyleHEAT: One-Shot High-Resolution Editable Talking Face Generation via Pre-trained StyleGAN. In: Avidan S., Brostow G., Cissé M., Farinella G.M., Hassner T. (eds.) Computer Vision – ECCV 2022. ECCV 2022. Lecture Notes in Computer Science. Vol. 13677. Cham: Springer; 2022. p. 85-101. doi: https://doi.org/10.1007/978-3-031-19790-1_6

[16] Wu Y. et al. AniFaceGAN: Animatable 3D-Aware Face Image Generation for Video Avatars. In: Advances in Neural Information Processing Systems (NeurIPS 2022). 2022;35:36188-36201. Available at: https://proceedings.neurips.cc/paper_files/paper/2022/hash/eae78bf2712f222f101bd7d12f875a57-Abstract-Conference.html (accessed 23.06.2023).

[17] Koujan M.R., Doukas M.C., Roussos A., Zafeiriou S. Head2Head: Video-based Neural Head Synthesis. In: 2020 15th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2020). Buenos Aires, Argentina: IEEE Computer Society; 2020. p. 16-23. doi: https://doi.org/10.1109/FG47880.2020.00048

[18] Kong J., Kim J., Bae J. HiFi-GAN: generative adversarial networks for efficient and high fidelity speech synthesis. In: Proceedings of the 34th International Conference on Neural Information Processing Systems (NIPS'20). Article number: 1428. Red Hook, NY, USA: Curran Associates Inc.; 2020. p. 17022-17033. Available at: https://dl.acm.org/doi/pdf/10.5555/3495724.3497152 (accessed 23.06.2023).

[19] Tan X. et al. Naturalspeech: End-to-end text to speech synthesis with human-level quality. arXiv:2205.04421v2. 2022. doi: https://doi.org/10.48550/arXiv.2205.04421

[20] Huang R. et al. FastDiff: A Fast Conditional Diffusion Model for High-Quality Speech Synthesis. In: Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence Main Track. Pages 4157-4163.

[21] Dale R. GPT-3: What's it good for? *Natural Language Engineering*. 2021;27(1):113-118. doi: https://doi.org/10.1017/S1351324920000601

[22] Touvron H. et al. LLaMA: Open and Efficient Foundation Language Models. arXiv:2302.13971. 2023. doi: https://doi.org/10.48550/arXiv.2302.13971

[23] Scao T. L. et al. Bloom: A 176B-Parameter Open-Access Multilingual Language Model. arXiv:2211.05100. 2022. doi: https://doi.org/10.48550/arXiv.2211.05100

[24] Khan I., Bokhari M.U., Hanafi B., Zeyauddin M. Synthetic Identity Detection using Inductive Graph Convolutional Networks. In: 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom). New Delhi, India: IEEE Computer Society; 2023. p. 973-978.

[25] Liang C. Z. et al. Credit Monitoring Application: Protect Children from Child Identity Theft. *International Journal of Data Science and Advanced Analytics*. 2022;4:77-83. Available at: http://www.ijdsaa.com/index.php/welcome/article/view/146 (accessed 23.06.2023).

[26] Srivastava S., Singh A.K. Fraud detection in the distributed graph database. *Cluster Computing*. 2023;26(1):515-537. doi: https://doi.org/10.1007/s10586-022-03540-3

[27] Minaee S., Abdolrashidi A. Finger-GAN: Generating Realistic Fingerprint Images Using Connectivity Imposed GAN. arXiv:1812.10482. 2018. doi: https://doi.org/10.48550/arXiv.1812.10482

Поступила 19.06.2023; одобрена после рецензирования 23.06.2023; принята к публикации 27.06.2023.
Submitted 19.06.2023; approved after reviewing 23.06.2023; accepted for publication 27.06.2023.

Об авторах:

Кузьмин Александр Михайлович, исполнительный директор Лаборатории кибербезопасности, ПАО «Сбербанк России» (117312, Российская Федерация, г. Москва, ул. Вавилова, д. 19), **ORCID: https://orcid.org/0000-0001-8352-5811,** kuzmin.a.mikhaylo@sberbank.ru

Свичкарь Денис Анатольевич, руководитель направления отдела оценки защищенности технологий И\А Управления криптографии, аутентификации и идентификации Департамента кибербезопасности, ПАО «Сбербанк России» (117312, Российская Федерация, г. Москва, ул. Вавилова, д. 19), **ORCID: https://orcid.org/0000-0002-0158-1682,** DASvichkar@sberbank.ru

Хенкин Павел Владимирович, исполнительный директор-начальник отдела оценки защищенности технологий И\А Управления криптографии, аутентификации и идентификации Департамента кибербезопасности, ПАО «Сбербанк России» (117312, Российская Федерация, г. Москва, ул. Вавилова, д. 19), **ORCID: https://orcid.org/0000-0001-6141-9970,** pvkhenkin@sberbank.ru

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the authors:

Alexander M. Kuzmin, Executive Director of the Cybersecurity Lab, PJSC "Sberbank of Russia" (19 Vavilova St., Moscow 117312, Russian Federation), **ORCID: https://orcid.org/0000-0001-8352-5811,** kuzmin.a.mikhaylo@sberbank.ru

Denis A. Svichkar, Head of the I\A Technology Security Assessment Department of the Cryptography, Authentication and Identification Department of the Cybersecurity Department, PJSC "Sberbank of Russia" (19 Vavilova St., Moscow 117312, Russian Federation), **ORCID: https://orcid.org/0000-0002-0158-1682,** DASvichkar@sberbank.ru

Petr V. Khenkin, Executive Director-Head of the I\A Technology Security Assessment Department of the Cryptography, Authentication and Identification Department of the Cybersecurity Department, PJSC "Sberbank of Russia" (19 Vavilova St., Moscow 117312, Russian Federation), **ORCID: https://orcid.org/0000-0001-6141-9970,** pvkhenkin@sberbank.ru

All authors have read and approved the final manuscript.