Садыков Р.Р. Социальная инженерия: атаки с использованием синтетических личностей и дипфейков // Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 1(63) с. 52–61

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056.5:316.6

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: АТАКИ С ИСПОЛЬЗОВАНИЕМ СИНТЕТИЧЕСКИХ ЛИЧНОСТЕЙ И ДИПФЕЙКОВ

Садыков Р.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: rasilstudent@yandex.ru

В данной работе рассматривается анализ методов социальной инженерии, основанных на создании и эксплуатации синтетических личностей в сети Интернет, а также дипфейков, созданных с помощью искусственного интеллекта. Исследование будет опираться на сформированное описание цифрового профиля злоумышленника, что включает в себя поведенческие и коммуникативные характеристики. Подобный анализ позволит оценить уязвимость пользователей к различным формам поддельной айдентики. Показано, что без строгой категоризации уровней пользовательской осведомлённости и сценариев цифрового взаимодействия вероятность успеха реализации атак с участием ИИ-имперсонации и/или дипфейков оказывается существенно завышенной. В работе также представлена типология жертв и сценариев, основанных на использовании методов синтетических личностей и дипфейков, схема методического воздействия злоумышленника на жертву, а также статистические данные, основывающиеся на вышеперечисленных методиках мошенничества. Рассмотрен пример случая мошенничества с использованием искусственного интеллекта и обоснована приоритетность адаптивных стратегий защиты, ориентированных на динамическое выявление подозрительного поведения цифровых субъектов.

Ключевые слова: Искусственный интеллект, социальная инженерия, модель жертвы, синтетическая личность, фишинг, психологическая атака, адаптивные стратегии, информационная безопасность.

SOCIAL ENGINEERING: SYNTHETIC IDENTITY AND DEEPFAKE ATTACKS

Sadykov R.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: rasilstudent@yandex.ru

The article develops an approach to analyzing the techniques of social engineering based on the creation and exploitation of synthetic identities on the Internet, as well as impersonation via AI-generated deepfakes. The proposed approach relies on a formal description of an attacker's digital profile, which includes behavioral and communicative characteristics. This enables the assessment of users' vulnerability to various forms of synthetic identity manipulation. It is shown that, without formalizing user awareness levels and scenarios of digital interaction, the likelihood of successful attacks involving these methods is significantly higher. The article also presents a typology of victims and attack scenarios based on the use of synthetic identities and deepfakes, along with a graphical model of the attacker's methodological influence on the victim, supplemented with statistical data on the aforementioned method of fraud. An example of a fraud case involving the use of artificial intelligence is also presented, and the priority of adaptive defense strategies focused on dynamically detecting suspicious behavior of digital entities is substantiated.

Keywords: Artificial intelligence, social engineering, victim model, synthetic identity, phishing, psychological attack, adaptive strategies, information security.

Современное информационное общество характеризуется тенденцией к расширению области сбора и многоступенчатой обработки персональных данных, что обуславливается стремительным развитием информационных технологий и ростом важности персональных данных как стратегического, в том или ином понимании, ресурса. На фоне развития технологического прогресса и усиленного внедрения информационных технологий в бытовую жизнь человека, в том числе искусственного интеллекта (ИИ), всё более очевидной становится уязвимость со стороны человеческого фактора, которая остаётся фундаментальной основой всех действий злоумышленников. Социальная инженерия, в свою очередь, формируется как совокупность методов психологического воздействия на человека, направленных на изучение его модели поведения и на психо-когнитивное воздействие соответственно, с целью получения доступа к какой-либо чувствительной и/или конфиденциальной информации, ресурсам или инфраструктуре ограниченного доступа. Изучение механизмов подобных воздействий приобретает первостепенную значимость, поскольку именно человек в любом случае остаётся наиболее слабым звеном в цепочке информационной безопасности.

Целью работы является разработка аналитического подхода к оценке уязвимости пользователей к атакам социальной инженерии, основанным на синтетических цифровых личностях и дипфейках, с учетом уровней пользовательской осведомлённости и контекста взаимодействия.

Социальная инженерия, главным образом, состоит из нескольких аспектов. Основными из них являются: разведка (reconnaissanse), легенда (pretexting), взаимодействие/коммуникация (engagement), психологические приемы (psychological methods). Каждый аспект имеет свою основную роль. Так, разведка позволяет собрать информацию о цели: ее положении/роли в обществе/компании, ее контактах, профилях в социальных сетях, структуре организации (при условии атаки на корпоративную личность). Совокупность всего вышеперечисленного зачастую объединяют в понятие OSINT. Ролевая легенда, в свою очередь, позволяет создать ситуационную обстановку и работать над вызовом доверия у жертвы. Психологические приемы позволяют манипулировать эмоциями и чувствами цели для достижения целей, задуманных злоумышленниками.

Взаимодействие с жертвой осуществляется через каналы атак, такими как: электронная почта и социальные сети (phishing), физический (тейлгейтинг, сталкинг), взаимодействие с устройствами (зараженные накопители, устройства).

Как отмечается в работе *Бириха Э.В. «Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPv6»:*

«злоумышленники активно используют уязвимости современных протоколов связи и методы динамического построения сетей, что позволяет им адаптироваться к защитным мерам компаний. Если раньше социальная инженерия сводилась к относительно примитивным формам фишинга или телефонному выманиванию данных, то сегодня она превратилась в целый комплекс взаимосвязанных стратегий, подкреплённых анализом больших данных, искусственным интеллектом и глубоким знанием поведенческих паттернов целевых аудиторий» [1].

Учитывая стремительное развитие искусственного интеллекта, стоит особенно отметить такие способ социальной инженерии, как «синтетическая цифровая личность» и «дипфейки»

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. [2][3]

Дипфейк — это форма медиаконтента, например фото или видео, созданного искусственным интеллектом (ИИ) для изображения реальных или несуществующих людей, выполняющих действия, которые они никогда не совершали. [4]

Если говорить о данных методе более обобщенно – подобные атаки, осуществляемые посредством «синтетической цифровой личности» или «дипфейка» можно расценивать как кражу личности. Злоумышленники зачастую подделывают профили известных в обществе людей, устанавливая контакт с фальшивых профилей в социальных сетях с пользователями, не идентифицирующими угрозу, и отправляя им, как пример, те самые «дипфейки» для повышения уровня доверия в их диалогах. Стоит также упомянуть, что не все данные синтетического профиля могут быть сфабрикованными. Некоторые данные вполне могут быть настоящими, например, ИНН (идентификационный номер налогоплательщика), но при этом необязательно соответствовать личности, коей предоставляется злоумышленник, что позволяет ему эффективнее замести следы своих действий/

Формализованная типология жертв атак социальной инженерии с использованием ИИ

В рамках данной работы жертва рассматривается как цифровой субъект, характеристики которого могут быть формализованы и использованы в аналитических моделях риска.

Модель жертвы (формальное описание)

Предлагается описывать пользователей, попавших на влияние мошенников, в виде вектора параметров:

V = ⟨L, A, C, E, R⟩

где:

- **L (Literacy)** — уровень цифровой и ИИ-осведомлённости;
- **A (Authority sensitivity)** — чувствительность к социальному иерархическому давлению;
- **C (Context)** — контекст взаимодействия;
- **E (Emotional state)** — эмоциональное состояние в момент атаки;
- **R (Resources access)** — уровень доступа в инфраструктуре

Данная модель позволяет перейти от субъективных характеристик жертвы к сравнимым параметрам.

Параметры модели жертвы

Таблица 1 - Уровень цифровой осведомлённости (L)

Уровень	Характеристика
L1	Пользователь не осознаёт существования дипфейков и синтетических личностей
L2	Пользователь неполноценно осведомлён теоретически, отсутствие возможности распознания в практических случаях
L3	Пользователь обладает практическими навыками верификации, способен распознать данные виды мошенничества

При L_1 вероятность успешной атаки с использованием ИИ-имперсонации стремится к максимуму: таких пользователей легче всего ввести в заблуждение.

Таблица 2 - Чувствительность к социальному иерархическому давлению (A)

Уровень	Характеристика
A1	Высокая восприимчивость к социальному давлению: высокая подверженность лицам, стоящим выше в социальной иерархии
A2	Умеренная восприимчивость к социальному давлению
A3	Критическое отношение к источнику информации, верификация подлинности сведений

ИИ-дипфейки усиливают воздействие на пользователей уровня A_1, создавая впечатление авторитарности предоставляемой информации, имитируя визуальные и голосовые признаки.

Таблица 3 - Контекст взаимодействия (C) (Таблица 3)

Уровень	Характеристика
C1	Личное общение (близкие люди: родственные связи, друзья и знакомые)
C2	Корпоративная среда
C3	Публичная или анонимная среда (зачастую, незнакомые лица)

Атаки с дипфейками наиболее эффективны в контекстах C_1 и C_2, где запросы выглядят легитимными, т.к. поступают из более доверенных кругов общения пользователя.

Таблица 4 - Эмоциональное состояние (E)

Уровень	Характеристика
E1	Преобладание негативных эмоций: общее стрессовое состояние, страх, ощущение срочности, тревожность
E2	Нейтральный эмоциональный спектр
E3	Хладнокровие и частично повышенная настороженность

Большинство успешных атак происходят при E_1. При E3 могут возникать эмоции разных степеней, которые, тем не менее, не позволяют пользователю стать жертвой мошенничества.

Таблица 5 - Уровень доступа в инфраструктуре (R)

Уровень	Характеристика
R1	Ограниченный
R2	Финансовый
R3	Корпоративный / административный

Максимальная ценность атак достигается при воздействии на субъектов с уровнями доступа R_2–R_3, что приводит к целенаправленному выбору злоумышленниками ролей, связанных с управлением финансовыми и информационными ресурсами.

Типология жертв (сводная классификация)

На основе параметров выделяются типы пользвателей (Таблица 6)

Таблица 6 -Типы пользователей

Тип	Профиль	Описание
V_1	$\langle L_1, A_1, C_1, E_1, R\rangle$	Пользователи с низкой цифровой осведомлённостью
V_2	$\langle L_2, A_1, C_2, E_1, R_2\text{-}R_3\rangle$	Пользователи корпоративных инфраструктур
V_3	$\langle L_3, A_2, C, E_2\text{-}E_3, R\rangle$	Пользователи с высокой цифровой компетентностью

Вероятность успешной атаки

Вероятность успеха атаки может быть представлена как условная функция:

$$\mathbf{P_s = f(V, A_a, T)}$$

где:

- **V** — параметры жертвы;
- $\mathbf{A_a}$ — профиль атакующего;
- **T** — используемые ИИ-технологии (дипфейк, синтетическая личность, голосовая имитация).

При сочетании (L_1, A_1, E_1) вероятность $P_s \rightarrow \max$.

Вероятность успешной атаки с использованием искусственного интеллекта определяется совокупным влиянием параметров жертвы (V), характеристик атакующего (A_a) и применяемых ИИ-технологий (T). В рамках настоящей работы данная зависимость рассматривается не как строго вычисляемая вероятность, а как качественная функция риска, позволяющая сопоставлять различные сценарии атак между собой.

Анализ же, в свою очередь, показывает, что наибольшая вероятность успешной атаки наблюдается при сочетании низкого уровня цифровой осведомлённости жертвы, высокой чувствительности к социально-иерархическому фактору и повышенного эмоционального давления (L_1, A_1, E_1).

Примерная схема взаимодействия представлена на Рисунке 1.

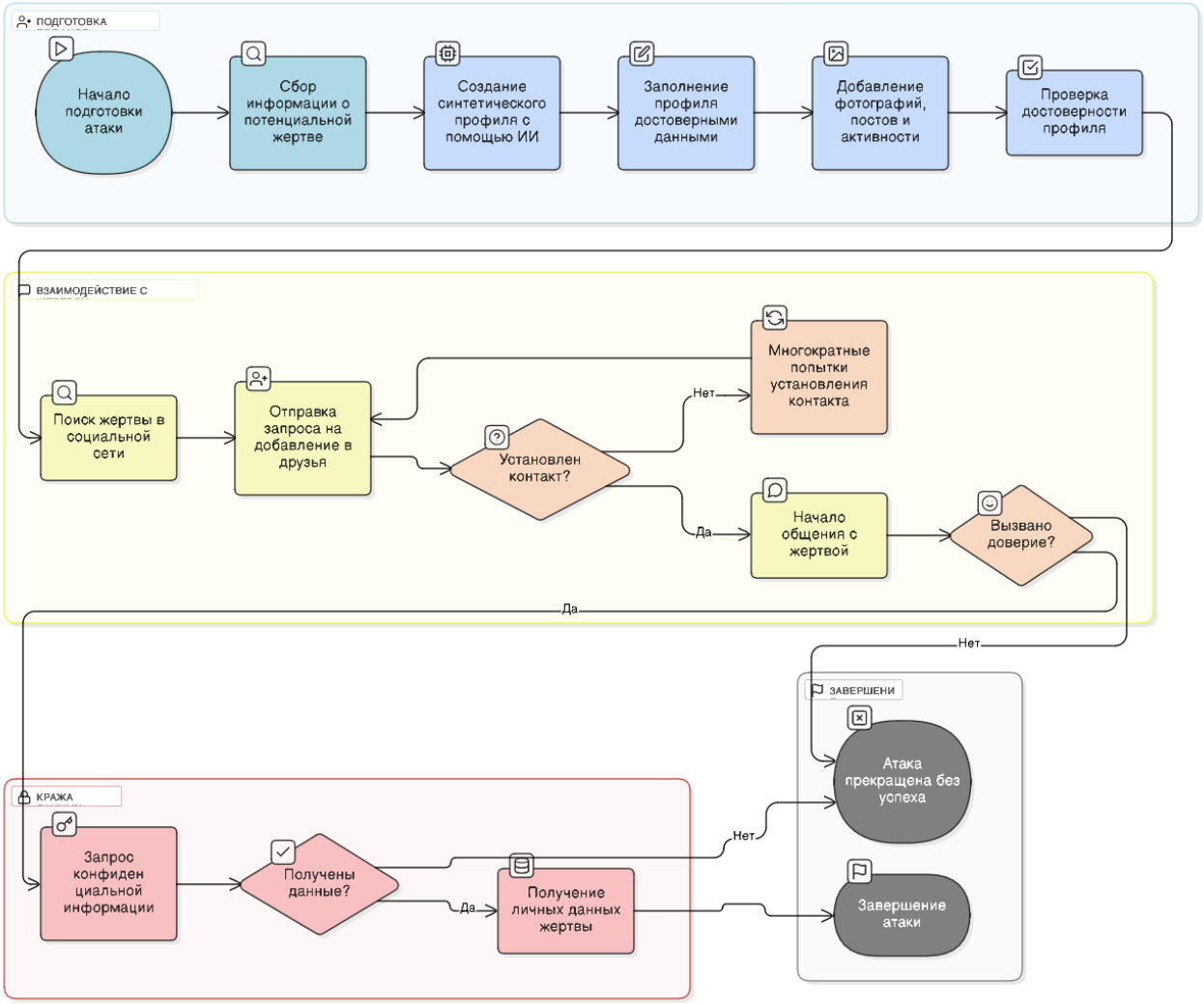

Рисунок 1 – Схема взаимодействия злоумышленника с жертвой

Говоря о поддельных (синтетических) личностях, их можно определить по следующим пунктам:

1. Фотографии, аватар профиля

Синтетические цифровые учетные записи имеют фотографии/рисунки, сгенерированные искусственным интеллектом. Рисунки, например, имеют характерное размытие диффузии: мягкие границы объектов, «заплывшие» текстуры, нечеткость деталей. До сей поры нейросети могут ошибаться и в анатомии: лишние пальцы, неправдоподобные изгибы конечностей и их сращивание, неверные пропорции. Некоторые модели нейросетевых технологий уже обучены работе с фотореалистичными изображениями и большинство подобных ошибок встречаются реже.

2. Биография профиля, данные о человеке

Зачастую, подобные данные будут также сгенерированы при помощи нейросети, с возможностью ручного редактирования.

3. История записей в социальных сетях

Злоумышленнику нужно создать имитацию социальной жизни, из-за чего создается череда публикаций, комментариев и различных репостов. Зачастую данные публикации не имеют глубокого контекста и четкой связи между собой.

4. Список контактов/друзей

Зачастую список друзей подобных личностей состоит из аналогичных профилей, специализированных ботов, а в крайних случаях – из взломанных аккаунтов настоящих людей.

5. Поведение

В зависимости от типа технологий нейросетей можно проследить паттерн имитации поведения: ответы одного стиля, излишне формальные и вежливые приветствия, «моментальные» ответы в точную секунду отправки жертвой собственного сообщения, и так далее.

Если же говорить о дипфейках, то создаются они либо с помощью GAN (Generative Adversarial Network), либо с использованием автокодировщика. [4]. Дипфейки же имеют гораздо более широкую область использования, и, соответственно, влияния. Они могут использоваться для следующих целей:

1. Дезинформационные кампании

Широкое распространение дезинформационных кампаний происходит в социальных сетях, особенно во время каких-либо важных общественных событий (выборы, катастрофы, резонансные события), для воздействия на широкий слой общественности.

2. Шантаж

Шантаж является одной из ключевых целей использования дипфейков. Если противостоять «краже личности», где примером выступает случай когда на контакт с пользователем выходит личность, широко известная в различных кругах, или некое государственное лицо – достаточно просто, то при подделке личности самой жертвы ситуация осложняется. Шантажисты могут «наложить» лицо человека на любое фото либо видео, чем и угрожают жертве, грозясь разослать этот контент его близким людям и родственникам, требуя выкуп.

3. Фишинг

Нечто похожее на шантаж, но подделывается личность близкого жертве человека. Зачастую это просьба о помощи в реальном времени, просьба перечислить денежные средства, либо получить какие-либо иные конфиденциальные данные.

Если говорить о признаках дипфейка и компрометации видео-контента, можно отметить следующие пункты:

1. Мимика лица

Так как нейросети все еще обучаются, они, как уже было указано ранее, могут допускать ошибки в анатомии лица в фотографиях, и «не успевать» за видеорядом в вопросе рендера лица. Изображение может быть дерганым, взгляд может быть «стеклянным», а кожа лица максимально гладкой.

2. Обстановка и освещение

Зачастую, визуальные артефакты происходят и на заднем фоне. Смазанные надписи, «дергающиеся» объекты, характерная искусственному интеллекту «рябь».

По реальным случаям можно привести пример того, как еще в 2023 году сотрудник из финансового отдела компании Arup, предоставляющей профессиональные услуги в области проектирования, архитектуры, планирования и консалтинга, филиал которой базировался в

Гонконге, перечислил злоумышленникам $25.000.000 после приглашения на видеозвонок якобы «старшим менеджером» компании. В видеозвонке также была симуляция других сотрудников и финансового директора компании, что сделало обстановку еще более убедительной для сотрудника. [6][7]

Чтобы защититься от подобных методов, достаточно быть осведомленным об отличительных особенностях сгенерированного контента и синтетических личностей, которые уже были описаны в тексте ранее, а также перепроверять подлинность предоставляемых людьми данных.

В корпоративных же сетях, взяв как пример ту же защиту баз данных, можно существуют дополнительные средства защиты информации помимо основных, что привязано к отдельно разработанной системе безопасности [8]. Подобные методы защиты подбираются компаниями соответственно.

Для вычисления вероятности успешной атаки и калькуляции ее факторов в работе были приведены характеристики, а также соответствующая им формула.

Таким образом, угроза мошенничества с использованием искусственного интеллекта в нынешнее время является в высшей степени актуальной. Предполагается, что с дальнейшим развитием информационных технологий и нейросетей всецелом возрастет и количество случаев мошенничества с использованием ИИ. Рекомендуется усилить комплекс мер по предотвращению подобных преступлений: повысить цифровую грамотность населения, развить технологии аутентификации, а также внести соответствующие законопроекты.

Список литературы

1. Бирих Э.В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPv6 / Э.В. Бирих // Вестник Санкт-Петербургского государственного университета телекоммуникаций. – 2024. – № 1. – С. 45-53.
2. Кузьмин А.М., Свичкарь Д.А., Хенкин П.В. Мошенничество с использованием синтетических цифровых личностей / Современные информационные технологии и ИТ-образование, [S.l.], v. 19, n. 2, p. 251-261, june 2023. ISSN 2411-1473.
3. Кузьмин А.М., Свичкарь Д.А., Хенкин П.В. Синтезированные цифровые личности / Сбер. – URL: https://www.sberbank.ru/ru/person/kibrary/experts/sintezirovannye-cifrovye-lichnosti
4. Как защищаться от дипфейков / Kaspersky. – URL: https://www.kaspersky.ru/resource-center/threats/protect-yourself-from-deep-fake
5. Ashley D’Andrea, Kaylee Palak, Darren Guccione. What are deepfakes? / Keeper. URL - https://www.keepersecurity.com/blog/ru/2024/09/19/what-are-deepfakes/
6. Heather Chen, Kathleen Magramo / CNN. – URL: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
7. Cheng Leng, Chan Ho-him. Arup lost $25mn in Hong Kong deepfake video conference scam / Financial Times. – URL: https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea?\
8. Защита информации в базах данных / Э. В. Бирих, Л. А. Виткова, В. В. Гореленко, Д. Б. Казаков // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной научно-технической и

научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 89-92. – EDN YRQKPJ.

9. Методология формирования модели угроз безопасности информационных систем / Э. В. Бирих, Е. Ю. Рябов, Д. В. Сахаров // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 103-107. – EDN NSLUFH.
10. Развитие стандартов и руководств в сфере облачных технологий / Э. В. Бирих, Л. А. Виткова, М. В. Левин, М. В. Чмутов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 92-95. – EDN YRPZWJ.
11. Выбор инструментов динамического анализа безопасности web-приложений для задач цифровой экономики / Э. В. Бирих, А. С. Груздев, А. О. Камалова, Д. В. Сахаров // Защита информации. Инсайд. – 2024. – № 1(115). – С. 42-46. – EDN RLNHWK.
12. Исследование способов повышения безопасности корпоративных сетей / Н. Ф. Махмутова, Э. В. Бирих, Д. В. Сахаров [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – Т. 51, № 3. – С. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.

References

1. Birikh E.V. Modeling a Secure Scalable Enterprise Network with Dynamic Routing Based on IPv6 / E.V. Birikh // Bulletin of the St. Petersburg State University of Telecommunications. - 2024. - No. 1. - pp. 45-53.
2. Kuzmin A.M., Svichkar D.A., Henkin P.V. Fraud Using Synthetic Digital Identities / Modern Information Technologies and IT Education, [S.l.], v. 19, n. 2, pp. 251-261, June 2023. ISSN 2411-1473.
3. Kuzmin A.M., Svichkar D.A., Henkin P.V. Synthesized Digital Identities / Sber. – URL: https://www.sberbank.ru/ru/person/kibrary/experts/sintezirovannye-cifrovye-lichnosti
4. How to protect yourself from deepfakes / Kaspersky. – URL: https://www.kaspersky.ru/resource-center/threats/protect-yourself-from-deep-fake
5. Ashley D’Andrea, Kaylee Palak, Darren Guccione. What are deepfakes? / Keeper. URL - https://www.keepersecurity.com/blog/ru/2024/09/19/what-are-deepfakes/
6. Heather Chen, Kathleen Magramo / CNN. – URL: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
7. Cheng Leng, Chan Ho-him. Arup lost $25mn in Hong Kong deepfake video conference scam / Financial Times. – URL: https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea?\

8. Information security in databases / E. V. Birikh, L. A. Vitkova, V. V. Gorelenko, D. B. Kazakov // Actual problems of infotelecommunications in science and education (APINO 2017): Collection of scientific articles of the VI International scientific-technical and scientific-methodical conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S.V. Bachevsky. Volume 2. – St. Petersburg: Saint Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2017. – pp. 89–92. – EDN YRQKPJ.
9. Methodology for Forming a Model of Information System Security Threats / E.V. Birikh, E.Yu. Ryabov, D.V. Sakharov // Actual Problems of Infotelecommunications in Science and Education (APINO 2017): Collection of scientific articles from the VI International Scientific, Technical and Scientific-Methodological Conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S.V. Bachevsky. Volume 2. – St. Petersburg: Saint Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2017. – pp. 103-107. – EDN NSLUFH.
10. Development of standards and guidelines in the field of cloud technologies / E. V. Birikh, L. A. Vitkova, M. V. Levin, M. V. Chmutov // Actual problems of infotelecommunications in science and education (APINO 2017): Collection of scientific articles of the VI International scientific-technical and scientific-methodical conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S. V. Bachevsky. Volume 2. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2017. – pp. 92-95. – EDN YRPZWJ.
11. Selection of tools for dynamic analysis of web application security for digital economy tasks / E. V. Birikh, A. S. Gruzdev, A. O. Kamalova, D. V. Sakharov // Information Security. Inside. - 2024. - No. 1 (115). - Pp. 42-46. - EDN RLNHWK.
12. Research of ways to improve the security of corporate networks / N. F. Makhmutova, E. V. Birikh, D. V. Sakharov [et al.] // Bulletin of the Dagestan State Technical University. Technical sciences. - 2024. - Vol. 51, No. 3. - pp. 110-116. - DOI 10.21822/2073-6185-2024-51-3-110-116. - EDN HDGBOY.