ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2024-51-3-130-144 Обзорная статья/ Review article

Исследование методом расширенного систематического обзора литературы E-SLR проблемы обеспечения безопасности персональных данных при использовании OSINT

Н.Н. Романова[1], В.В. Грызунов[2]
Петербургский государственный университет путей сообщения Императора Александра I,
[1]190031, г. Санкт-Петербург, Московский пр-т., 9, Россия,
[2]Санкт-Петербургский университет ГПС МЧС России,
[2]196105, г. Санкт-Петербург, Московский пр-т., 149, Россия

Резюме. Цель. Количество персональных данных в открытых источниках увеличивается с каждым днем, что позволяет получить доступ к ним с помощью методов разведки по открытым источникам (OSINT) третьим лицам, которые могут использовать их в злонамеренных целях. Целью данной работы является идентификация угроз и существующих методов и средств обеспечения безопасности персональных данных пользователя и его репутации при использовании злоумышленниками OSINT, а также идентификация основных проблем при защите ПД пользователя с учетом OSINT. **Метод.** Для исследования используется расширенный метод систематического обзора литературы (e-SLR), представляющий систематический обзор литературы (SLR), дополненный ответами нейросетей ChatGPT, GigaCHAT, YndexGPT. **Результат.** Получен 41 источник для анализа проблемы, на основании которых определены угрозы для персональных данных:нарушение конфиденциальности персональных данных, нарушение работы информационных систем, целевые атаки с использованием социальной инженерии, раскрытие паролей, шпионаж; средства защиты:обработка данных перед публикацией, анонимизация и деперсонафикация, ограничение персональных данных, выбор сайтов, защита с помощью OSINT, создание сложных паролей, использование средств защиты, организационные меры; проблемы при разработке средств защиты: работа с большими данными, недостоверность информации и источников, трудоемкость анализа данных, технические ограничения, предвзятость, этический и юридический аспекты. **Вывод.** Полученные результаты можно использовать для разработки моделей защиты персональных данных в открытых источниках, методов и средств обнаружения и предотвращения нарушения их защищенности.

Ключевые слова: OSINT, систематической обзор литературы, информационная безопасность, персональные данные, искусственный интеллект, методы защиты информации

Для цитирования: Н.Н. Романова, В.В. Грызунов. Исследование методом расширенного систематического обзора литературы E-SLR проблемы обеспечения безопасности персональных данных при использовании OSINT. Вестник Дагестанского государственного технического университета. Технические науки. 2024;51(3):130-144. DOI:10.21822/2073-6185-2024-51-3-130-144

Research by the method of an extended systematical literature review E-SLR the problem of ensuring the security of personal data when using OSINT

N.N. Romanova[1], V.V. Gryzunov[2]
[1]Emperor Alexander I St. Petersburg State Transport University,
[1]9 Moskovsky Ave., Saint Petersburg 190031, Russia,
[2]Saint Petersburg University of State Fire Service of Emercom of Russia,
[2]149 Moskovsky Ave., Saint Petersburg 196105, Russia

Abstract. Objective. The amount of personal data in open sources increases, which makes it possible for third parties to access it using open source intelligence (OSINT) methods, which can be used for malicious purposes. The aim of the work is to identify threats and existing

methods and means of ensuring the security of a user's personal data and his reputation when using OSINT by intruders, as well as to identify the main problems in protecting user PD taking into account OSINT. **Method.** The study uses an extended method of systematic literature review (e-SLR), which is a systematic literature review (SLR) supplemented by responses from ChatGPT, GigaCHAT, YndexGPT neural networks. **Result.** 41 sources were received for the analysis of the problem, on the basis of which threats to personal data were identified: violation of the confidentiality of personal data and the operation of information systems, targeted attacks using social engineering, password disclosure, espionage; protection tools: data processing before publication, anonymization and depersonalization, limitation of personal data, selection of sites, protection using OSINT, creation of complex passwords, use of protection tools, organizational measures; problems in the development of protection tools: working with big data, unreliability of information and sources, labor-intensiveness of data analysis, technical limitations, bias, ethical and legal aspects. **Conclusion.** The results were used to develop models for protecting personal data in open sources, methods and means for detecting and preventing violations of their security.

Keywords: OSINT, systematic literature review, information security, personal data, artificial intelligence, information security methods

For citation: N.N. Romanova, V.V. Gryzunov. Research by the method of an extended systematical literature review E-SLR the problem of ensuring the security of personal data when using OSINT. Herald of Daghestan State Technical University. Technical Sciences. 2024; 51(3):130-144. DOI:10.21822/2073-6185-2024-51-3-130-144

Введение. С каждым днем в сети Интернет появляется все большее количество данных, к которым относятся и персональные. Это происходит по разным причинам: размещение данных пользователем самостоятельно или в результате применения злоумышленником методов социальной инженерии [1], в ходе интеграции информационных систем [2], нарушение правил безопасной разработки приложений [3] и т.п.

Разрозненные персональные данные собираются в единую картину злоумышленниками [4] посредством разведки по открытым источникам (OSINT) [5]. Наиболее ценные для злоумышленника источники – разнообразные места публичного общения: чаты, форумы, социальные сети и мессенджеры.

Применение OSINT к открытым геоинформационным системам может представлять отдельную угрозу, потому что позволяет установить местоположение объекта разведки в реальном мире [6]. OSINT часто используется ввиду своих преимуществ [7]: сбор данных осуществляется быстро и в режиме реального времени, получение данных легально и безопасно для разведчика, данный способ прост в использовании, а благодаря существующему программному обеспечению (ПО) еще и удобен, процесс разведки бесплатен или стоит недорого.

При этом классические методы обеспечения информационной безопасности практически бессильны против OSINT, так как находятся за пределами модели нарушителя, на основе которой действуют средства защиты информации [8]. В руках злоумышленника OSINT представляет следующие угрозы: осуществление целевых атак (фишинг, атаки с использованием социальной инженерии), шантаж/вымогательство на основе полученных данных, мошенничество с использованием полученных персональных данных, кража личности, нарушение конфиденциальности (раскрытие/продажа данных третьим лицам).

Постановка задачи. Исследование проблемы обеспечения безопасности персональных данных при использовании злоумышленниками OSINT является актуальным.

Целью данной работы является идентификация угроз и существующих методов и средств обеспечения безопасности персональных данных пользователя и его репутации при использовании злоумышленниками OSINT, а также идентификация основных проблем при защите ПД пользователя с учетом OSINT.

Методы исследования. Метод систематического обзора литературы является видом научного исследования, в котором объектом изучения служат результаты ряда оригинальных исследований [9].

При использовании данного метода уменьшается возможность появления систематических и случайных ошибок за счет переработки и обобщения результатов этих исследований. Метод систематического обзора литературы включает этапы исследования:

1. **Постановка исследовательского вопроса.** Необходимо определить цель и объем исследования, в соответствии с которыми будут сформированы границы исследования и основные исследовательские вопросы. Для изучения проблемы обеспечения безопасности персональных данных (ПД) при использовании злоумышленниками OSINT была поставлена цель: идентификация угроз и существующих методов и средств обеспечения безопасности персональных данных пользователя и его репутации при использовании злоумышленниками OSINT, идентификация основных проблем при защите ПД пользователя с учетом OSINT.

   В соответствии с целью сформулированы исследовательские вопросы:

– Какие существуют угрозы для безопасности ПД пользователя и его репутации при использовании злоумышленниками OSINT?
– Какие существуют методы и средства обеспечения безопасности ПД противодействующие OSINT?
– Какие возникают проблемы при разработке методов и средств защиты ПД, противодействующих OSINT?

2. **Процесс поиска источников.** На данном этапе определяется основная стратегия поиска, состоящая из следующих шагов:

2.1. Определение цифровых библиотек. Необходимо определить критерии, которым должны соответствовать библиотеки для поиска источников, и конкретные базы данных, соответствующие критериям. Были определены следующие критерии для подбора цифровых библиотек для поиска: содержит материалы русских авторов; содержит материалы зарубежных авторов; обновляемые; содержит материалы на тему «информационная безопасность».

Для поиска были выбраны две системы: eLIBRARY и Google Scholar, потому что они способны проводить поиск по заданному фильтру и индексируют статьи журналов из перечня ВАК и международной базы данных SCOPUS.

2.2. Формирование поисковых запросов. Определяются поисковые запросы для каждого исследовательского вопроса. Для составления запросов можно использовать ключевые слова, синонимы, логические связки.

Для проводимого исследования были определены следующие поисковые запросы:

– (персональные данные | репутация) & (угрозы | уязвимости | риски) & OSINT;
– (средства защиты | методы защиты | способы защиты) & (персональные данные | репутация) & (против | противодействующих) & OSINT;
– (проблемы | риски | трудности) & (разработка | создание | проектирование) & (средства защиты | методы защиты | меры защиты | способы защиты) & (против | противодействующих) & OSINT.

2.3. Промежуточный поиск. На данном этапе производится непосредственный поиск по библиотекам, определенным на шаге 2.1, по запросам, определенным на шаге 2.2. На данном этапе были получены количественные результаты (табл.1).

3.Отбор на основании критериев включения и исключения. Необходимо сформулировать критерии, на основании которых будет получено однозначное решение включения или исключения для каждого источника, полученного на предыдущем шаге. Отбор проводится в два этапа:первый – по названиям, ключевым словам, году издания и другим свойствам источника, второй – изучение аннотаций и полных текстов.

Таблица 1. Результаты поисковых запросов
Table 1. Search query results

№ поискового запроса Search query number	Количество найденных исследований в eLIBRARY Number of studies found in eLIBRARY	Количество найденных исследований в Google Scholar Number of studies found in Google Scholar
ПЗ1	136	184
ПЗ2	196	315
ПЗ3	79	445
Итого	1355	

Для отбора публикаций были определены следующие критерии исключения и включения:

3.1.Первый этап отбора – отбор по названиям, ключевым словам:

- Исключаются обзоры литературы. В исследование попадают только собственные исследования авторов, которые включают новые подтвержденные данные.
- Исключаются статьи, которые опубликованы в ненаучных журналах или подготовлены для семинара. В исследование попадают статьи научных журналов и конференций.
- Исключаются статьи, написанные до 2020 года.
- Исключаются статьи, которые описывают не техническую составляющую процесса.

3.2. Второй этап отбора – отбор по аннотациям, полным текстам:

- (Включение) В исследовании рассматриваются угрозы безопасности ПД, возникающие при использовании злоумышленниками OSINT.
- (Включение) В исследовании рассматриваются способы защиты ПД от OSINT.
- (Включение) В исследовании рассматриваются проблемы, возникающие при защите ПД против OSINT.

После отбора было получено 93 результата (табл.2).

Таблица 2. Результаты поисковых запросов после отбора
Table 2. Results of search queries after selection

№ поискового запроса Search query number	Количество найденных исследований в eLIBRARY Number of studies found in eLIBRARY	Количество найденных исследований в Google Scholar Number of studies found in Google Scholar
Первый этап отбора		
ПЗ1	16	55
ПЗ2	7	143
ПЗ3	7	185
Итого	413	
Без дубликатов	228	
Второй этап отбора		
Итого	93	

4. Отбор на основании оценки качества. На данном этапе формулируются вопросы для оценки качества каждого оставшегося источника. Для ответов на вопросы устанавливаются числовые коэффициенты: «Да» = 1, «Частично» = 0.5, «Нет» = 0. Коэффициенты ответа на каждый вопрос суммируются и дают оценку качества источника. Исследователь должен определить какая минимальная оценка приемлема для включения источника в исследование и отбросить все источники, имеющих меньшую оценку. Для оценки качества были сформулированы следующие вопросы:

1. Ясно ли сформулированы цели и задачи исследования?
2. Сравнивается ли исследование со связанными работами?
3. Имеют ли выводы четкое изложение и теоретическую поддержку?
4. Описываются ли возможности будущего применения полученных данных?
5. Учтены ли ограничения исследования?
6. Журнал публикации статьи входит в перечень ВАК?
7. Журнал публикации статьи входит в перечень Scopus?

Для каждого вопроса, кроме 6, предусмотрены три варианта ответа и числовые коэффициенты: «Да» = 1, «Частично» = 0.5, «Нет» = 0. После ответа на все вопросы для каждого результата была получена количественная оценка качества. 52 исследования, получившие оценку 3 и меньше были отброшены. Для дальнейшего анализа взят 41 источник.

5. Сбор и анализ данных. Все результаты отбора заносились в электронную таблицу Excel. В ней сохранялись полные ссылки источников для последующего цитирования, также отдельно были вынесены тип публикации, год, вопросы оценки качества и конечная оценка качества каждого источника. Краткое описание систематического обзора литературы с полученными результатами представлено на (рис. 1).

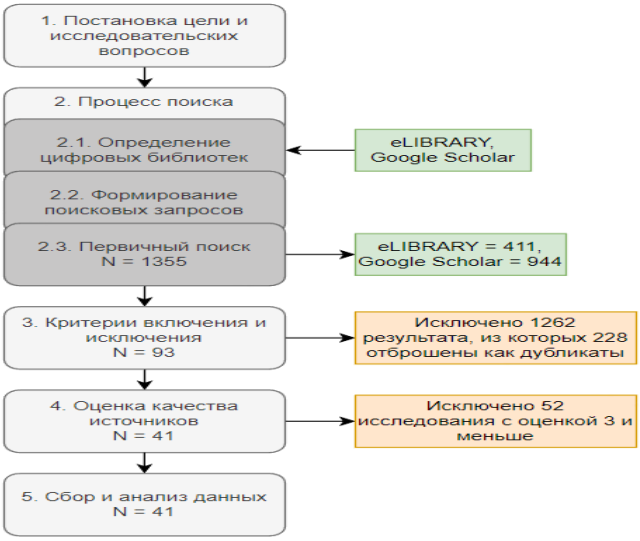

Рис. 1. Процесс систематического обзора литературы
Fig. 1. The systematic literature review process

Обсуждение результатов. Какие существуют угрозы для безопасности персональных данных (ПД) пользователя и его репутации при использовании злоумышленниками OSINT?

1. **Нарушение конфиденциальности персональных данных**

С помощью OSINT злоумышленник может получить незаконный доступ к персональным данным пользователей открытых источников, таких как, социальные сети, форумы, веб-приложения [10, 11]. Важный этап OSINT - анализ полученных персональных данных [7], поскольку, например, отдельный номер телефона или адрес электронной почты не определяет пользователя однозначно, следовательно, необходимо выстроить связи между разрозненными ПД для получения целого “портрета” пользователя. Собранные персональные данные могут быть выложены на специализированные сайты бесплатно для предоставления большему кругу людей и дальнейшего незаконного использования, а также могут быть проданы в виде подробных баз персональных данных [12].

Проведение разведки по открытым источникам может иметь личный характер и осуществляться в целях мести [10, 13], шантажа, вымогательства, нанесения ущерба репутации [5], а также может привести к киберзапугиванию, кибersплетням или киберагрессии [14]. Одно из преимуществ OSINT для злоумышленника - простота [7, 15]. С развитием технологий получить персональные данные легко даже для обычного пользователя компьютера, например, через telegram-каналы или боты можно получить персональные данные интересующего человека за небольшую плату [16]. Более продвинутый пользователь сети Интернет может обратиться к открытым данным государственных органов, например, налоговой или судебных приставов, и получить персональные данные жертвы [17], в качестве источников данных могут быть использованы также электронные копии сайтов из веб-архивов; страницы, кэшированные поисковыми системами; новостные порталы [18]. Существуют специальные инструменты, которые позволяют упростить и ускорить поиск персональных данных [19], например, операторы расширенного поиска Google или

Yandex, расширения для браузеров (Fast Advanced Google Search, OSINT.support, EXIF Viewer Pro и др.).

2. **Нарушение работы информационных систем**. Злоумышленники перед атакой проверяют целевой информационный ресурс различными способами, в том числе и с помощью OSINT [20]. Используя разведку по открытым источникам можно обнаружить слабые места в системе защиты потенциальной жертвы [5, 10, 13, 18], а также другую полезные данные, например, блок используемых IP-адресов, данные программного и аппаратного обеспечения, конфигурацию хостов, топологию сети, физическое местонахождение, структуру управления организации, персональные данные сотрудников и др. На основании этих данных можно определить конкретную уязвимость и совершить более успешную атаку [20 - 23]. Для сканирования информационных ресурсов с помощью OSINT используются бесплатные приложения, например, Maltego, The Harvester, Mosint.

3. **Целевые атаки с использованием социальной инженерии**. На основе полученных данных из разведки по открытым источникам злоумышленники определяют цель атаки, её интересы, наиболее уязвимые места [10, 13], на основании которых определяют более подходящие и эффективные методы воздействия [24]. Один из популярных видов подобных атак - целевой фишинг [25 - 27] для осуществления, которого сначала проводится разведка по открытым источникам для получения контекстной информации о жертвах, например, об их хобби, семье, работе или отпуске, которая потом может быть использована для создания сценария атаки [28].

4. **Раскрытие паролей пользователей**. В результате OSINT могут быть получены сведения о жизни жертвы, которые можно использовать для подбора пароля к устройствам, аккаунтам социальных сетей и др [29]. В исследованиях [25, 29] рассматривается процесс создания пользователями паролей, особенно, повторение паролей для разных сайтов и использование личных данных для создания лучше запоминающихся паролей. Данная проблема приводит к утечке персональных данных, финансовым потерям или даже краже личности [7], например, социальная кража личности – получив персональные данные жертвы злоумышленники создают поддельный идентичный профиль в социальных сетях, через который выдавая себя за жертву, общаются с ее коллегами, родственниками, друзьями для получения денежной выгоды, распространения ложной информации; финансовая кража – имея персональные данные пользователя можно получить доступ к банковскому счету, кредитным картам и другим финансовым источникам жертвы для получения финансовой выгоды. Часть пользователей создают мнемонические пароли на фразах, которые можно найти в Интернете, что создает проблемы, связанные с надежностью создаваемого пароля, особенно если такой мнемонический словарь включен в инструменты взлома паролей [29]. Пароль подбирается на основании сферы интересов жертвы, выявленных с помощью OSINT [30].

5. **Шпионаж.** Данный тип разведки может осуществляться как вручную, так и с помощью автоматизированных средств. К средствам слежки можно отнести: сервисы слежки и сбора данных (Maltego, Babel X, PhoneInfoga, TinEye, Sleeping Time) с сотни тысяч веб-сайтов, блогов и аккаунтов, которые позволяют строить графы коммуникации между людьми, анализируя и прогнозируя информационно-сетевые события; внедрение в устройства эксплойты, вирусы, руткиты, трояны, использующие уязвимости программной среды; программы-шпионы и программные закладки; перехват и анализ интернет-трафика и другие [31].

Какие существуют методы и средства обеспечения безопасности ПД, противодействующие OSINT?

1. **Обработка данных перед публикацией в сети**. Для противодействия методам OSINT рекомендуется обрабатывать данные перед выставлением в общий доступ: из файлов фото и видео удалять метаданные (данные геолокации, дата, время и др.), для усложнения сопоставления личных цифровых данных применять обфускацию (маскировка/подмена данных подмешиванием отвлекающих или вводящих в заблуждение дан-

ных в профиль), синтез данных (так, фото с «зашумлением» усложняет задачу машинного распознавания и поиска по соцсетям)) [31].

2. **Анонимизация и деперсонификация**. В исследовании [17] рассматривается организационно-технический протокол анонимизации наборов данных для их публикации в открытых источниках, протокол обеспечивает итерационную процедуру полной анонимизации в зависимости от уровня конфиденциальности обрабатываемых данных. К методам анонимизации относятся: маскировка данных (замена чувствительных данных вымышленными или частично вымышленными данными, что делает невозможной идентификацию исходных данных), токенизация (замена чувствительных данных токеном или нечувствительным значением, уникальным для исходных данных), агрегирование данных (объединение или группировка данных вместе для сокрытия индивидуальных значений или идентификационных данных).

3. **Ограничение выставляемых данных**. Один из методов защиты от OSINT - правильно дозировать персональные данные выставляемые в своих социальных сетях, но данная ответственность лежит на самом пользователе, ведь только он решает, нужно ли совершенно различным людям знать, где вы живете, в какое время уходить на работу и т.д [32]. Для распространения данных, которые потом могут быть использованы для атаки, рекомендуется использовать личные сообщения, зашифрованные чаты. Также для защиты от опознавания по лицу алгоритмами искусственного интеллекта (ИИ) рекомендуется выставлять фото со спины, с боку, с недостаточным освещением и другими способами, позволяющими затруднить распознавание лица.

4. **Выбор сайтов, которым передавать свои персональные данные**. В наше время почти каждый сайт требует пройти процедуру регистрации для получения данных, однако большая часть требует еще и дополнительные данные кроме логина и пароля, например, ФИО, дата рождения, почта, номер телефона и др., а сайты предоставляющие услуги купли-продажи получают еще и банковские данные пользователя. В данном случае необходимо понимать куда мы предоставляем наши персональные и насколько этому сайту/приложению можно их доверить, ведь именно с незащищенных и ненадежных ресурсов происходят утечки данных или они сами их продают для получения прибыли [32]. Перед тем, как выкладывать свои персональные данные на сайт, рекомендуется ознакомиться с его политикой конфиденциальности. Если ваши данные были размещены на сайте без вашего согласия, то можно запросить их удаление через электронную почту модерации сайта.

5. **Использование OSINT против OSINT**. Огромное количество данных, получаемых посредством OSINT, позволяет специалистам по информационной безопасности узнать о тенденциях в области уязвимостей и расстановки сил в хакерских группировках, что позволяет предотвратить киберпреступления [33]. Идея проведения анализа защищенности этими методами все больше накладывается на существующие рекомендации регуляторов, так как большая их часть связана с анализом открытых источников и внешних ресурсов организации [18]. Проводя разведку по открытым источникам, специалист может выявить наличие доступных уязвимостей сети своей организации [21]. На основании собранных данных можно проводить оценку риска для безопасности организации и принимать решения о дальнейших действиях [25]. Правоохранительные органы также используют OSINT, чтобы выявить преступные намерения на ранней стадии и оперативно обнаружить противоправные действия [14]. OSINT используют в целях расследования преступлений и инцидентов информационной безопасности [34], установления виновности в кибератаках, для сбора данных о киберугрозах [35, 36]. К основным потребителям данных из открытых источниках являются платформы анализа угроз (TIP).

Например, ThreatQ, Threatstream, EclecticlQ, которые помогают организациям объединять, сопоставлять и анализировать данные об угрозах из нескольких источников в режиме реального времени для поддержки защитных действий [37]. В исследовании рассматривается процесс интеграции между методами OSINT и стандартом ISO 27001 для

дополнительной безопасности [38]. В исследовании [23] выявлены особенности обеспечения информационной безопасности организации с помощью средств OSINT, которые можно использовать в разработке тактических и стратегических рекомендаций организациям по формированию более надежных политик информационной безопасности, выявлению уязвимостей и снижению рисков. В исследовании [39] разработана концепция OSINT, для его использования в мониторинге безопасности. Использование OSINT позволяет специалистам по информационной безопасности получить более глубокое представление о APT-группировках: обнаружить вредоносные домены и IP-адреса, которыми пользуются APT-группировки, отследить упоминания участников угроз и их цели [40]. Использование OSINT является важной частью анализа угроз, включая тестирование на проникновение и реагирование на инциденты. Данные, полученные в результате интернет-разведки OSINT, о злоумышленнике и совершенном им преступлении, является важным фактором для успешного расследования. Она помогает выдвинуть версию, выбрать правильные тактические приемы при проведении следственных действий, спланировать и организовать подготовку к проведению тактических операций и правильно выстроить алгоритм действий на разных этапах расследования уголовного дела [41].

6. **Создание сложных паролей и ограничение попыток неправильного набора**. В исследовании [29] предлагаются методы усиления паролей, самые простые из которых, являются негибкие правила в отношении длины пароля и типа используемых символов, а также определенный допуск к количеству раз, когда учетные данные могут быть введены неправильно. В исследовании [21] также предлагается ограничивать количество попыток ввода пароля, а также использовать двухфакторную аутентификацию для входа в аккаунт. В исследовании [42] описывается новый метод оценки паролей, который использует учетные записи человека в социальных сетях для повышения точности оценки пароля путем создания собственных списков слов, сравнения пароля со словами, найденными в социальных сетях человека, и поиска в большой базе данных утекших или взломанных паролей.

7. **Использование средств защиты информации**. Для организаций рекомендуется использовать системы обнаружения/предотвращения вторжений и межсетевые экраны [16] для сканирования сети и обнаружения подозрительного трафика, также предлагается установить обманную систему для изучения и фиксации интереса злоумышленника к организации [21]. Также советуется подключать двухфакторную аутентификацию для защиты в случае компрометации паролей, а выход в сеть осуществлять посредством VPN [16], для обеспечения анонимного выхода в сеть и сокрытия своего местоположения, поведения в сети. Для защиты сервера предлагается использовать SSH-ключ вместо пароля, а также настроить резервное копирование для восстановления данных в случае потери или изменения. Для соединения с сервером по сети Интернет рекомендуется использовать протокол TLS для криптографически безопасного соединения. Он дает возможность клиентам проводить проверку подлинности серверов и наоборот.

8. **Организационные меры**. Необходимо проводить регулярное обучение сотрудников распознаванию методов социальной инженерии и фишинга, а также оповещать их о новых видах атак, также необходимо уведомлять сотрудников о необходимости фильтрации контента, размещенного ими и имеющего непосредственное отношение к трудовой деятельности [21]. Если у пользователей есть знания по аспектам безопасности в киберпространстве, то количество персональных данных полученных с помощью OSINT может быть значительно меньше, чем у беспечных пользователей. Должны быть четко прописаны обязанности каждого сотрудника, доступные ему данные, границы их распространения, также по возможности обработка персональных данных должна производится на рабочих, а не личных устройствах [11].

Какие возникают проблемы при разработке методов и средств защиты ПД, противодействующих OSINT?

1. **Работа с Big Data**. Количество персональных данных, получаемых посредством OSINT, может достигать огромных размеров, а сам процесс сбора представляет сложную по времени задачу [7, 33, 43]. Применение средств автоматизации не решает полностью проблему обработки больших данных [44]. Значительных ресурсов требует фильтрация и анализ полученных данных [14], что ставит перед специалистами по информационной безопасности задачу по усовершенствованию существующих и разработке новых более эффективных методов обработки данных, нахождения связей между ними и интерпретации полученных результатов.

2. **Недостоверность информации и ненадежность источников.** Зачастую данные, размещенные в открытых источниках недостоверны или субъективны [45]. Из всего набора данных, полученного посредством OSINT, сложнее вывести достоверные данные, а для обнаружения ложной информации и отбора достоверных данных требуется много времени и усилий [7, 33, 43], что, с одной стороны, осложняет злоумышленнику подготовку к атаке, а с другой, мешает специалистам по защите устанавливать необходимость их защиты, приводит к ложным выводам [35]. Субъективные и ложные данные позволяют создать информационный «шум» в ПД, который может снизить вероятность успешности атаки или увеличить усилия и затраты атакующего, что сделает атаку не выгодной. На данный момент нет инструментов зашумления персональных данных для публикации в открытых источниках, что является еще одной задачей для специалистов по защите. Также для изучения остаются вопросы: как именно и в каких случаях следует применять данный метод? При работе с персональными данными необходимо проводить проверку надежности источников, поскольку выбор ресурса также может привести к ошибочным выводам и неправильным результатам [43]. К наиболее субъективным и требующим дополнительной проверки относятся онлайн СМИ и социальные сети [14]. Сложность в разработке мер и средств защиты персональных данных также определяется затратами ресурсов на выявление относительно небольшой подгруппы ценных источников из всего множества открытых ресурсов [20].

3. **Трудоемкость анализа данных.** Полученный, в результате разведки по открытым источникам, объем данных необходимо проанализировать, отфильтровать, классифицировать, сравнить с секретными, что требует квалифицированных кадров и времени [43]. Кроме того, важен корректный учет формализованных связей между данными, содержащимися в публикуемом пользователем контенте, и результатами, полученными с помощью разработанных инструментов оценки ряда идентификационных параметров личности нарушителя [13], такие как идентификатор страницы в социальных сетях, персональные данные со страницы, список друзей и подписок и др. Отдельную ценность имеют информация о процессе обработки данных, сохраненные массивы еще необработанных данных, отчеты и сводки для последующего использования, что облегчает поиск и позволяет сократить использование ресурсов при повторном использовании данных [46].

По мере увеличения количества источников и типов приложений объем данных OSINT растет в геометрической прогрессии, что требует новых аналитических методов для получения значимой информации [47]. Искусственный интеллект является одним из способов решения этой задачи [14, 37]. Инструменты искусственного интеллекта, машинного обучения и автоматизации способны сканировать огромные объемы данных и коммуникаций, умело выявляя связи и риски, требующие дальнейшего изучения [14]. Анализ полученных данных необходим для установки закономерностей между разрозненными персональными данными для разработки методов защиты.

4. **Технические ограничения**. При разработке средств защиты необходимо решать проблемы, связанные со спецификой совместного использования программно-аппаратных средств: расширений веб-браузера, ограничений, накладываемых разработчи-

ками и других [13]. Некоторые данные, получаемые в ходе разведки по открытым источникам, могут быть представлены в нечитаемом или сложно читаемом видах, что существенно снижает возможность дальнейшей работы с ними [45].

5. **Неоцененность технологии**. В организационной культуре разведывательных агентств ценность данных, собранных OSINT, недооценивается, а важность данных иногда не учитывается, поскольку любой может получить к ним доступ и использовать их [33].

6. **Этический и юридический аспект**. С увеличением возможностей OSINT появляются вопросы относительно обеспечения защиты интересов граждан и надлежащего уровня защиты персональных данных. Согласно ФЗ №152 «О персональных данных», собирать, обрабатывать и хранить ПД людей можно только с их согласия. Однако, многие сайты, в том числе социальные сети, принимают за согласие факт регистрации пользователя или само использование ресурса, что приводит к выбору - либо передавать свои ПД, либо не пользоваться ресурсом [35].

Обсуждение результатов. OSINT общедоступен и имеет право раскрывать данные, которые размещены неявно [14], однако к ним могут относиться ПД из специальной категории, например, расовая, национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимной жизни, что не допускается без прямого согласия пользователя. Основная сложность состоит в том, что эти данные можно получить путем анализа открытых данных пользователя - фото, посты, список друзей и др. На данный момент отсутствуют единые стандарты открытости информации, подходов к использованию таких данных и инструментов их обработки [34, 45, 48]. Авторами предложено расширение метода SLR с применением искусственного интеллекта. Используемый классический метод SLR базируется на квалификации эксперта и, значит, несёт в себе признаки субъективного подхода. Данный недостаток нейтрализуется путём применения для задач поиска искусственного интеллекта. Расширенный таким образом метод SLR предлагается назвать e-SLR.

Суть расширения в том, что п.2.2 метода SLR дополняется ответами нейросетей.

В исследовании использованы 3 нейросети:

1. **ChatGPT** (англ. Generative Pre-trained Transformer «генеративный предварительно обученный трансформер»). Данная нейросеть представляет собой большую языковую модель, представленную американской компанией OpenAI 30 ноября 2022г. Функциональные возможности: ответы на вопросы пользователей, поиск информации (подобно поисковым системам), написание кода, перевод текста, пересказ и перефразирование текста, распознавание и генерация голоса, распознавание изображений. Сервис заблокирован в России на момент написания статьи. Доступ возможен через VPN и иностранные номера телефонов, чат-ботов посредников.

2. **YandexGPT** – нейросеть, выпущенная компанией Яндекс в мае 2023. Работает по аналогии с языковой моделью GPT компании Open AI. Функциональные возможности: ответы на вопросы, генерация текста, генерация изображений по текстовому описанию, написание простого кода, пересказ, форматирование текста.

3. **GigaCHAT.** Данная нейросеть выпущена Сбером в апреле 2023. Неросеть основана на ансамбле NeONKA (NEural Omnimodal Network with Knowledge-Awareness), включающей в себя модели ruGPT-3.5 с 13 млрд параметров, Kandinsky 2.1, ruCLIP и FRED-T5. Функциональные возможности: ответы на вопросы, генерация текста, генерация изображений по текстовому описанию, перевод, написание простого кода, анализ данных. В результате опроса нейросетей были получены следующие дополнительные данные, отвечающие на исследовательские вопросы:

1. Какие существуют угрозы для безопасности персональных данных (ПД) пользователя и его репутации при использовании злоумышленниками OSINT? Ответы соответствуют данным, полученным в результате анализа литературы, представленных в п. Результаты систематического обзора литературы.

2. Какие существуют методы и средства обеспечения безопасности ПД противодействующие OSINT?

Прокси-серверы и серверы аутентификации. Они обеспечивают дополнительный уровень безопасности, скрывая IP-адрес пользователя и проверяя подлинность его учетных данных [GigaCHAT].

Настройка приватности. Ограничение физического и логического доступа к персональным данным помогает предотвратить утечку и неправомерное использование информации [YandexGPT]. Проверьте и регулярно обновляйте настройки приватности на своих социальных медиа-аккаунтах. Ограничьте доступ к вашей личной информации, такой как адрес электронной почты, номер телефона и местоположение, только для доверенных контактов [ChatGPT].

3. Какие возникают проблемы при разработке методов и средств защиты ПД, противодействующих OSINT?

Постоянное развитие технологий. Злоумышленники постоянно разрабатывают новые методы и техники для получения доступа к данным и обхода систем безопасности. Поэтому необходимо постоянно обновлять и улучшать методы и средства защиты [GigaCHAT]. Методы и средства защиты ПД должны постоянно развиваться и адаптироваться к новым угрозам и технологиям. Это требует регулярного мониторинга и обновления системы защиты [ChatGPT].

Недостаток ресурсов. Разработка и внедрение эффективных методов и средств защиты требует значительных финансовых и временных ресурсов. Некоторые компании и организации могут не иметь достаточных ресурсов для внедрения современных мер безопасности [GigaCHAT]. Разработке и внедрению новых систем безопасности может потребоваться значительное количество времени, денег и человеческих ресурсов [YandexGPT].

Сложность обнаружения. Определить все возможные угрозы и способы их реализации может быть сложно, что затрудняет создание универсальных систем защиты [YandexGPT]. Одной из проблем является сложность обнаружения персональных данных, которые могут быть доступны через OSINT-исследования. Ведь ПД могут быть разбросаны в различных источниках, их агрегирование может потребовать времени и ресурсов [ChatGPT].

Противоречия между защитой и доступностью. Баланс между защитой ПД и обеспечением доступности может стать вызовом. Всеобъемлющая защита может ограничить доступ к информации, которая может быть полезна для различных операций и исследований [ChatGPT].

Стратегическое планирование. Разработка эффективных методов защиты ПД требует стратегического планирования. Важно определить, какие именно данные нуждаются в защите, и какие методы и средства будут наиболее эффективны для противодействия OSINT [ChatGPT].

Вывод. В данной статье методом e-SLR изучена проблема обеспечения безопасности персональных данных при использовании злоумышленниками OSINT на основе анализа 48 источников литературы и применении искусственного интеллекта.

В результате обзора обнаружены следующие угрозы для безопасности персональных данных при использовании злоумышленниками OSINT: сбор информации /обнаружение конфиденциальной информации; социальная инженерия; нарушение конфиденциальности; кибершпионаж; фишинг; утечка данных; обнаружение уязвимостей информационных систем.

Определены средства защиты для персональных данных пользователя от атак с использованием OSINT: межсетевые экраны (файрволлы); средства мониторинга сети; средства обнаружения попыток несанкционированного доступа (вторжения); нейронные сети; организационные методы; настройка приватности; сильные пароли и двухфакторная

аутентификация; шифрование данных; использование VPN; резервное копирование данных.

Рассмотрены сложности при создании средств защиты для персональных данных пользователя от атак с использованием OSINT: огромный объем информации; недостоверность информации; трудоемкость анализа информации; ненадежность источников данных; сложность интеграции / технические вызовы; ограничения законодательства; недостаточная осведомленность пользователей.

Предложенный в статье метод e-SLR является более эффективным, чем классический SLR, потому что выявил дополнительные средства защиты: прокси-серверы и серверы аутентификации, и сложности разработки средств защиты: постоянное развитие технологий, недостаток ресурсов, сложность обнаружения, противоречия между защитой и доступностью, стратегическое планирование.

Практическое применение настоящего исследования видится следующим образом:

1. Повышение осведомленности пользователей и организаций для принятия необходимых мер защиты своих данных и обучению своих сотрудников и пользователей правилам безопасности для предотвращения киберугроз.
2. Разработка предупредительных мер и средств защиты. Исследование позволяет лучше понять техники и инструменты, которые могут использоваться злоумышленниками при сборе и анализе открытой информации, что позволяет разработать соответствующие меры и средства защиты данных.
3. Обнаружение тенденций. Выявлены тренды и новые методы, которые злоумышленники используют для доступа к чувствительной информации, что позволяет развивать новые технологии обнаружения и защиты для опережения киберугроз.

Библиографический список:

1. Грызунов, В. В. Особенности применения технологических методов в социальной инженерии / В. В. Грызунов, О. С. Шкреба // Технико-технологические проблемы сервиса. – 2018. – № 4(46). – С. 90-94.
2. Выбор моделей доверия при интеграции распределенных информационных систем критического применения / В. В. Грызунов, А. А. Корниенко, М. Л. Глухарев, А. С. Крюков // Проблемы информационной безопасности. Компьютерные системы. – 2021. – № 4. – С. 79-90. – DOI 10.48612/jisp/ev3e-fmtu-x25h.
3. Романова, Н. Н. Особенности организации безопасной разработки приложений при использовании методов экстремального программирования / Н. Н. Романова, В. В. Грызунов // Информационные технологии и системы: управление, экономика, транспорт, право. – 2022. – №4(44). – С. 78-86.
4. Грызунов, В. В. Модель целенаправленных агрессивных действий на информационно-вычислительную систему // Человеческий фактор в сложных технических системах и средах (Эрго-2018):Труды Третьей международной науч.-практ. конф., Санкт-Петербург, 07 июля 2018 г. Под ред. А. Н. Анохина, А. А. Обознова, П. И. Падерно, С. Ф. Сергеева. – Санкт-Петербург: Межрегиональная общественная организация "Эргономическая ассоциация", 2018. С. 300-305.
5. Дворянкин О. А. OSINT, Pentest и нетсталкинг-информационные технологии интернета // Национальная ассоциация ученых. – 2022. – №. 84-2. – С. 6-13.
6. Грызунов, В. В. Концептуальная модель адаптивного управления геоинформационной системой в условиях дестабилизации // Проблемы информационной безопасности. Компьютерные системы. – 2021. – № 1. – С. 102-108.
7. Hwang Y. W. et al. Current status and security trend of osint //Wireless Communications and Mobile Computing. – 2022. – Т. 2022.
8. Грызунов, В. В. Структурно-функциональный синтез модели системы предотвращения вторжений // Проблемы информационной безопасности. Компьютерные системы. – 2006. – № 2. – С. 31-38.
9. Унгуряну Т.Н., Жамалиева Л.М., Гржибовский А.М. Краткие рекомендации по подготовке систематических обзоров к публикации // West Kazakhstan Medical Journal. 2019. №1 (61)., URL: https://cyberleninka.ru/article/n/kratkie-rekomendatsii-po-podgotovke-sistematicheskih-obzorov-k-publikatsii (дата обращения: 21.11.2023).
10. Современные технологии поиска информации в открытых источниках Дворянкин О.А., Клочкова Е.Н. В сборнике: Информационная безопасность: вчера, сегодня, завтра. Сборник статей по материалам VI Всероссийской научно-практической конференции. Москва, 2023. С. 64-68.
11. Şandor A. An Intelligence Perspective on Privacy and Data Protection Risks in Social Media // International conference knowledge-based organization. – 2020. – Т. 26. – №. 1. – С. 151-156.
12. Колосов Д. В. Разработка системы поиска информации о физических лицах, на основе открытых данных с использованием технологий искусственного интеллекта // 38.03. 05 Бизнес-информатика. – 2021.
13. Идентификация источников угроз информационной безопасности государственных информационных систем на основе открытых данных в интернете Гладнев В.В., Малый М.В., Стойчин К.Л., Пономарева О.А. Идентификация источников угроз информационной безопасности государственных информационных систем на основе открытых данных в интернете, В сборнике: Безопасность информационного пространства. дополне-

ние к сборнику научных трудов XXI Всероссийской науч.-практ. конференции студентов, аспирантов и молодых ученых. Екатеринбург, 2023. С. 31-34.
14. Pastor-Galindo J. et al. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends // IEEE Access. – 2020. – Т. 8. – С. 10282-10304.
15. Абрамова А. Г. Современные проблемы осуществления защиты персональных данных в сети: основополагающие принципы защиты персональных данных // Регион и мир. – 2020. – №. 4. – С. 21-25.
16. Коломыцев А. С., Вердиев О. Р. Как предотвратить утечку персональных данных // StudNet. – 2022. – Т. 5. – №. 7. – С. 7857-7864.
17. Борисов Р. С., Ефименко А. А. Протокол анонимизации наборов данных для публикации в открытых источниках // Правовая информатика - 2023 - №2.
18. Воложанина Д. Н. Пересмотр процедуры оценки защищенности методами OSINT в условиях нестабильной международной политической обстановки //Актуальные проблемы авиации и космонавтики. – 2022. – С. 261-264.
19. Evangelista J. R. G. et al. Systematic literature review to investigate the application of open source intelligence (OSINT) with artificial intelligence // Journal of Applied Security Research. – 2021. – Т. 16. – №. 3. – С. 345-369.
20. Tundis A., Ruppert S., Mühlhäuser M. A feature-driven method for automating the assessment of OSINT cyber threat sources // Computers & Security. – 2022. – Т. 113. – С. 102576.
21. Stodelov D., Miloslavskaya N. Open Source INTelligence Tools // Procedia Computer Science. – 2022. – Т. 213. – С. 83-88.
22. Bryushinin A. O., Dushkin A. V., Melshiyan M. A. Automation of the Information Collection Process by Osint Methods for Penetration Testing During Information Security Audit // 2022, Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). – IEEE, 2022. – С. 242-246.
23. Обеспечение информационной безопасности с помощью разведки по открытым источникам (OSINT) Шармаев В.И., Андреева Я.А., Василевский К.А. Вопросы защиты информации. 2022. № 2 (137). С. 45-50.
24. Годунов Д. А., Гунаев А. И. Информационная безопасность в сети, способы ведения кибер-разведки и защиты от неё // Научный аспект. – 2021. – Т. 2. – №. 2. – С. 179-189.
25. Oleksii Kuchmai T. S. Using open source intelligence (OSINT) as one of the effective and legitimate ways to avoid threats to the corporation // Scientific and practical cyber security journal. – 2021.
26. Даниленко, В. П. Использование открытых данных (OSINT) в целевых атаках / В. П. Даниленко // Автоматизация в промышленности. – 2023. – № 7. – С. 30-31. – EDN ZYYLQS.
27. Обнаружение целенаправленных атак веб-ориентированной обманной системой, основанной на алгоритме антиклассификации. Вишневский А.С., Ключарев П.Г. Нейрокомпьютеры: разработка, применение. 2020. Т. 22. № 3. С. 5-17.
28. Матецкий М. А. Инструменты противодейсвия безопасности данных организации // Школа молодых новаторов. – 2023. – С. 80-83.
29. Kanta A., Coisel I., Scanlon M. A survey exploring open source Intelligence for smarter password cracking // Forensic Science International: Digital Investigation. – 2020. – Т. 35. – С. 301075.
30. Kanta A., Coisel I., Scanlon M. Smarter password guessing techniques leveraging contextual information and OSINT // 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, 2020. – С. 1-2.
31. Миронова Н. Г. Арсенал технологий и методов информационного противодействия //Актуальные аспекты развития науки и общества в эпоху цифровой трансформации. – 2023. – С. 120-128.
32. Репетий, Е. О. Способы защиты персональных данных в интернете / Е. О. Репетий // Научный аспект. – 2023. – Т. 8, № 3. – С. 963-968. – EDN OBQRJH.
33. Сидорова, М. Е. Разведка по открытым источникам данных и ее применение для решения задач кибербезопасности / М. Е. Сидорова, А. Р. Кузьмин // Вестник Российского нового университета., Серия: Сложные системы: модели, анализ и управление. – 2023. – № 1. – С. 61-74. – DOI 10.18137/RNU.V9187.23.01.P.61. – EDN KKCSVG.
34. Kassim S. R. B. M., Li S., Arief B. How national CSIRTs leverage public data, OSINT and free tools in operational practices: An empirical study // Cyber Security: A Peer-Reviewed Journal. – 2022. – Т. 5. – №. 3. – С. 251-276.
35. Riebe T. et al. Values and Value Conflicts in the Context of OSINT Technologies for Cybersecurity Incident Response: A Value Sensitive Design Perspective //Computer Supported Cooperative Work (CSCW). – 2023. – С. 1-47.
36. Govardhan D. et al. Key Challenges and Limitations of the OSINT Framework in the Context of Cybersecurity // 2023 2nd International Conference on Edge Computing and Applications (ICECAA). – IEEE, 2023. – С. 236-243.
37. González-Granadillo G. et al. ETIP: An Enriched Threat Intelligence Platform for improving OSINT correlation, analysis, visualization and sharing capabilities // Journal of Information Security and Applications. – 2021. – Т. 58. – С. 102715.
38. AlKilani H., Qusef A. OSINT techniques integration with risk assessment ISO/IEC 27001 // International Conference on Data Science, E-Learning and Information Systems 2021. – 2021. – С. 82-86.
39. Lee D., Lee H. K. Study on OSINT-Based Security Control Monitoring Utilization Plan // International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/, Distributed Computing. – Cham: Springer International Publishing, 2022. – С. 161-172.
40. Использование OSINT для мониторинга угроз Жулев А.С. В книге: Вопросы информационной безопасности в современных условиях. Материалы студенческой научно-практической конференции. Самара, 2022. С. 8.
41. Иванов В. Ю. Использование OSINT в раскрытии и расследовании преступлений // Вестник Уральского юридического института МВД России. – 2023. – №. 1 (37). – С. 62-66.
42. Hubbard J., Bendiab G., Shiaeles S. IPASS: A Novel Open-Source Intelligence Password Scoring System // 2022 IEEE International Conference on Cyber Security and Resilience (CSR). – IEEE, 2022. – С. 90-95.
43. Тараканджи М. Я., Ортис С., Паюсова Т. И. Обеспечение защиты данных от утечек через открытые источники // Математическое и информационное моделирование. – 2023. – С. 388-399.
44. Характеристика OSINT и эффективность его использования Бондаренко Н.А., Гусева Т.М. В сборнике: Проблемы проектирования, применения и безопасности информационных систем в условиях цифровой экономики., Материалы XXII Международной научно-практической конференции. Ростов-на-Дону, 2022. С. 322-327.

45. Качалов, А. Г. Подготовка специалистов по работе с открытыми данными в сети интернет (OSINT) в гражданских и ведомственных вузах / А. Г. Качалов, М. М. Лантаев // Юридическая наука: история и современность. – 2021. – № 9. – С. 98-106. – EDN MXKJOE.
46. Khan S., Wallom D. A system for organizing, collecting, and presenting open-source intelligence // Journal of Data, Information and Management. – 2022. – Т. 4. – №. 2. – С. 107-117.
47. Филатова Д. К., Обласов А. А. Роль искусственного интеллекта в разведке с открытым исходным кодом (OSINT) // Наука, инновации и технологии: от идей к внедрению. – 2022. – С. 297-299.
48. Suryotrisongko H. et al. Robust botnet DGA detection: Blending XAI and OSINT for cyber threat intelligence sharing // IEEE Access. – 2022. – Т. 10. – С. 34613-34624.

References:

1. Gryzunov V. V. Features of the application of technological methods in social engineering. V. V. Gryzunov, O. S. Shkreba. *Technical and technological problems of service*. 2018:4 (46): 90-94. (In Russ)
2. Selection of trust models in the integration of distributed information systems of critical application.V. V. Gryzunov, A. A. Kornienko, M. L. Glukharev, A. S. Kryukov. *Problems of information security. Computer systems*. 2021; 4:. 79-90. - DOI 10.48612/jisp/ev3e-fmtu-x25h. (In Russ)
3. Romanova, N. N., V. V. Gryzunov Features of the organization of safe application development using extreme programming methods. *Information technologies and systems: management, economics, transport, law.* 2022;4 (44): 78-86. (In Russ)
4. Gryzunov, V. V. Model of targeted aggressive actions on the information and computing system / V. V. Gryzunov // The human factor in complex technical systems and environments (Ergo-2018): Proceedings of the Third international scientific and practical conference, St. Petersburg, July 07, 2018 / Edited by A. N. Anokhin, A. A. Oboznov, P. I. Paderno, S. F. Sergeev. - St. Petersburg: Interregional public organization "Ergonomic Association", 2018; 300-305. (In Russ)
5. Dvoryankin O. A. OSINT, Pentest and Netstalking Information *Technologies of the Internet. National Association of Scientists.* 2022; 84-2: 6-13. (In Russ)
6. Gryzunov, V. V. Conceptual Model of Adaptive Control of a Geoinformation System in the Context of Destabilization. *Problems of Information Security. Computer Systems.* 2021;1: 102-108. (In Russ)
7. Hwang Y. W. et al. Current Status and Security Trends of OSINT. *Wireless Communications and Mobile Computing*. 2022; 2022.
8. Gryzunov, V. V. Structural and Functional Synthesis of an Intrusion Prevention System Model. Problems of Information Security. Computer Systems. 2006; 2:31-38. (In Russ)
9. Unguryanu T.N., Zhamalieva L.M., Grzhibovsky A.M. Brief recommendations for preparing systematic reviews for publication. *West Kazakhstan Medical Journal*. 2019. No. 1 (61)., URL: https://cyberleninka.ru/article/n/kratkie-rekomendatsii-po-podgotovke-sistematicheskih-obzorov-k-publikatsii (date of access: 21.11.2023).
10. Modern technologies for searching information in open sources Dvoryankin O.A., Klochkova E.N. In the collection: Information security: yesterday, today, tomorrow. *Collection of articles based on the materials of the VI All-Russian scientific and practical conference.* Moscow, 2023; 64-68. (In Russ)
11. Şandor A. An Intelligence Perspective on Privacy and Data Protection Risks in Social Media*. International confer-ence knowledge-based organization.* 2020; 26(1): 151-156.
12. Kolosov D. V. Development of a system for searching for information about individuals based on open data using artificial intelligence technologies. 38.03. 05 Business Informatics. 2021. (In Russ)
13. Identification of sources of threats to the information security of state information systems based on open data on the Internet Gladnev V.V., Maly M.V., Stoychin K.L., Ponomareva O.A. Identification of sources of threats to the information security of state information systems based on open data on the Internet. In the collection: Security of information space. Supplement to the collection of scientific papers of the XXI All-Russian scientific and practical conference of students, graduate students and young scientists. Ekaterinburg, 2023;31-34. (In Russ)
14. Pastor-Galindo J. et al. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends // IEEE Access. 2020; 8:10282-10304.
15. Abramova A. G. Modern problems of implementing personal data protection on the network: fundamental principles of personal data protection. *Region and the World*. 2020;4:21-25. (In Russ)
16. Kolomytsev A. S., Verdiev O. R. How to prevent personal data leakage. StudNet. 2022; 5.(7): 7857-7864. (In Russ)
17. Borisov R. S., Efimenko A. A. Protocol for anonymizing data sets for publication in open sources. Legal informatics. 2023; 2. (In Russ)
18. Volozhanina D. N. Revision of the procedure for assessing security using OSINT methods in an unstable international political situation. *Actual problems of aviation and cosmonautics*. 2022; 261-264. (In Russ)
19. Evangelista J. R. G. et al. Systematic literature review to investigate the application of open source intelligence (OSINT) with artificial intelligence. *Journal of Applied Security Research*. 2021; 16(3): 345-369.
20. Tundis A., Ruppert S., Mühlhäuser M. A feature-driven method for automating the assessment of OSINT cyber threat sources // Computers & Security. 2022; 113: 102576.
21. Stodelov D., Miloslavskaya N. Open Source INTelligence Tools.*Procedia Computer Science*. 2022; 213: 83-88.
22. Bryushinin A. O., Dushkin A. V., Melshiyan M. A. Automation of the Information Collection Process by Osint Methods for Penetration Testing During Inf.
23. Ensuring Information Security Using Open Source Intelligence (OSINT) Sharmaev V.I., Andreeva Ya.A., Vasilevsky K.A. Information Security Issues. 2022; 2 (137): 45-50. (In Russ)
24. Godunov D.A., Gunaev A.I. Information Security on the Network, Methods of Conducting Cyber Intelligence and Protecting Against It. *Scientific Aspect*. 2021; 2(2):179-189. (In Russ)
25. Oleksii Kuchmai T.S. Using open source intelligence (OSINT) as one of the effective and legitimate ways to avoid threats to the corporation // Scientific and practical cyber security journal. 2021.
26. Danilenko, V. P. Using open data (OSINT) in targeted attacks. *Automation in industry*. 2023;7:30-31. (In Russ)

27. Detection of targeted attacks by a web-oriented deception system based on the anti-classification algorithm Vishnevsky A.S., Klyucharev P.G. Neurocomputers: development, application. 2020; 22(3): 5-17. (In Russ)
28. Matetsky M.A.Tools for counteracting organizational data security. *School of Young Innovators*. 2023:80-83(In Russ)
29. Kanta A., Coisel I., Scanlon M. A survey exploring open source Intelligence for smarter password cracking. *Forensic Science International: Digital Investigation*. 2020: 35: 301075.
30. Kanta A., Coisel I., Scanlon M. Smarter password guessing techniques leveraging contextual information and OSINT. 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, 2020; 1-2.
31. Mironova N. G. Arsenal of technologies and methods of information counteraction. Current aspects of the development of science and society in the era of digital transformation. 2023;120-128. (In Russ)
32. Repetiy, E.O. Ways to protect personal data on the Internet. *Scientific aspect.* 2023; 8(3): 963-968. (In Russ)
33. Sidorova, M. E. Open source intelligence and its application to solving cybersecurity problems / M. E. Sidorova, A. R. Kuzmin // Bulletin of the Russian New University., Series: Complex systems: models, analysis and management. 2023; 1:61-74. – DOI 10.18137/RNU.V9187.23.01.P.61. – EDN KKCSVG. (In Russ)
34. Kassim S. R. B. M., Li S., Arief B. How national CSIRTs leverage public data, OSINT and free tools in operational practices: An empirical study. *Cyber Security: A Peer-Reviewed Journal.* 2022;5(3):251-276.
35. Riebe T. et al. Values and Value Conflicts in the Context of OSINT Technologies for Cybersecurity Incident Re-sponse: A Value Sensitive Design Perspective.*Computer Supported Cooperative Work* (CSCW). 2023;1-47.
36. Govardhan D. et al. Key Challenges and Limitations of the OSINT Framework in the Context of Cybersecurity // 2023 2nd International Conference on Edge Computing and Applications (ICECAA). – IEEE, 2023;236-243.
37. González-Granadillo G. et al. ETIP: An Enriched Threat Intelligence Platform for improving OSINT correlation, analysis, visualization and sharing capabilities. *Journal of Information Security and Applications.* 2021;58:102715.
38. AlKilani H., Qusef A. OSINT techniques integration with risk assessment ISO/IEC 27001.*International Conference on Data Science, E-Learning and Information Systems* 2021; 2021: 82-86.
39. Lee D., Lee H. K. Study on OSINT-Based Security Control Monitoring Utilization Plan.*International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel, Distributed Computing*. Cham: Springer International Publishing, 2022; 161-172.
40. Using OSINT to Monitor Threats Zhulev A.S. In the book: Information Security Issues in Modern Conditions. Proceedings of the Student Scientific and Practical Conference. Samara, 2022;8. (In Russ)
41. Ivanov V. Yu. Using OSINT in Detecting and Investigating Crimes. Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia. 2023;1(37):62-66. (In Russ)
42. Hubbard J., Bendiab G., Shiaeles S. IPASS: A Novel Open-Source Intelligence Password Scoring System // 2022 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, 2022; 90-95.
43. Tarakdzhi M. Ya., Ortiz S., Payusova T. I. Ensuring data protection from leaks through open sources // Mathematical and information modeling. 2023; 388-399. (In Russ)
44. Characteristics of OSINT and the effectiveness of its use Bondarenko N.A., Guseva T.M. In the collection: Problems of design, application and security of information systems in the digital economy., Proceedings of the XXII International Scientific and Practical Conference. Rostov-on-Don. 2022;322-327. (In Russ)
45. Kachalov, A. G. Training of specialists in working with open data on the Internet (OSINT) in civil and departmental universities / A. G. Kachalov, M. M. Lantaev. *Legal science: history and modernity*. 2021;9: 98-106. – EDN MXKJOE.
46. Khan S., Wallom D. A system for organizing, collecting, and presenting open-source intelligence. *Journal of Data, Information and Management.* 2022; 4(2): 107-117.
47. Filatova D.K., Oblasov A.A. The Role of Artificial Intelligence in Open Source Intelligence (OSINT) // Science, Innovation and Technology: from Ideas to Implementation. 2022: 297-299. (In Russ)
48. Suryotrisongko H. et al. Robust botnet DGA detection: Blending XAI and OSINT for cyber threat intelligence shar-ing. *IEEE Access*. 2022; 10: 34613-34624.

Сведения об авторах:

Романова Надежда Николаевна, аспирант кафедры информатики и информационной безопасности; romanova.nadezhda.00@mail.ru

Грызунов Виталий Владимирович, доктор технических наук, доцент, профессор кафедры прикладной информатики и информационных технологий; viv1313r@mail.ru ORCID 0000-0003-4866-217X

Information about authors:

Nadezhda N. Romanova, Postgraduate student, Department of Computer Science and Information Security; romanova.nadezhda.00@mail

Vitaly V. Gryzunov, Dr. Sci. (Eng), Assoc. Prof., Prof., Department of Applied Computer Science and Information Technology; viv1313r@mail.ru ORCID 0000-0003-4866-217X

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 01.03.2024.

Одобрена после рецензирования / Reviced 30.03.2024.

Принята в печать /Accepted for publication 30.03.2024.