|  |  |  |
| --- | --- | --- |
| Министерство образования и науки Российской Федерации | | |
| федеральное государственное бюджетное образовательное учреждение  высшего образования | | |
| «Иркутский государственный университет» | | |
| (ФГБОУ ВО «ИГУ») | | |
| Факультет бизнес-коммуникаций и информатики | | |
| Кафедра прикладной информатики и документоведения | | |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
| **ОТЧЕТ БАКАЛАВРА О ПРОХОЖДЕНИИ ПРАКТИКИ**  **Б2.В.03(Н). Научно-исследовательская работа**  **(получение первичных навыков научно-исследовательской работы)** | | |
|  | | |
|  | |  |
|  | |  |
|  | |  |
| Студент 3 курса,  ФИО Подставьте своё |  | |
| Группа Подставьте свою |  | |
|  |  | |
| Научный руководитель практики от кафедры |  | |
| д. и. н., профессор М. Д. Кушнарева \_\_\_\_\_\_\_\_\_\_ |  | |
|  | |  |
|  | |  |
| Работа защищена | |  |
| «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2024 г. | |  |
| С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_ | |  |
| Протокол № \_\_\_\_\_\_ | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
| **Иркутск, 2024** | | |

Содержание

[Введение 3](#_Toc170992638)

[Задачи практики 3](#_Toc170992639)

[Глава 1. Теоретико-методологическое обоснование объекта и предмета исследования 5](#_Toc170992640)

[Глава 2. Литературный обзор по теме научно-исследовательской работы 6](#_Toc170992641)

[Глава 3. Теоретический обзор по теме НИР 7](#_Toc170992642)

[Мошенники как угроза личности в цифровом пространстве 7](#_Toc170992643)

[Информационные ресурсы 8](#_Toc170992644)

[Нарушение приватности в современном информационном пространстве ..8](#_Toc170992645)

[Почему это угроза 9](#_Toc170992646)

[Трекеры 9](#_Toc170992647)

[Распространённость трекеров 11](#_Toc170992648)

[Утечки персональных данных 13](#_Toc170992649)

[Крупнейшие утечки за последние несколько лет 14](#_Toc170992650)

[Минимизация рисков 14](#_Toc170992651)

[Библиографический список по теме НИР 16](#_Toc170992652)

[Заключение 19](#_Toc170992653)

# Введение

Научно-исследовательская работа направления «**Прикладная информатика в управлении**» – один из важнейших этапов подготовки будущих специалистов в данной отрасли.

Цель научно-исследовательской работы: систематизация, расширение и закрепление профессиональных знаний, формирование навыков ведения самостоятельной научной работы, исследования и экспериментирования, подготовка к практическому самостоятельному проведению научных исследований, разработке оригинальных научных идей для подготовки выпускной квалификационной работы (ВКР) и представлению результатов научных исследований в различных формах отчетности.

## Задачи практики

* выявление и формулирование актуальных научных проблем;
* разработка программ научных исследований и разработок, организация их выполнения;
* разработка методов и инструментов проведения исследований и анализ их результатов;
* разработка организационно-управленческих моделей процессов, явлений и объектов, оценка и интерпретация результатов;
* поиск, сбор, обработка, анализ и систематизация информации по теме исследования;
* практическое участие в научно-исследовательской работе коллективов исследователей;
* подготовка научных обзоров, отчетов, публикаций.

В результате прохождения данной практики должны сформироваться следующие компетенции:

* Способность выполнять работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы (ПК-1);
* Способность осуществлять консультационно-техническую поддержку клиентов по вопросам технического обслуживания и обеспечения работоспособности инфокоммуникационных систем и (или) их составляющих (ПК-2);
* Способность управлять процессами технической поддержки инфокоммуникационных систем и (или) их составляющих (ПК-3);
* Способность создавать и редактировать информационные ресурсы (ПК-4);
* Способность управлять информационными ресурсами (ПК-5)

Практика отвечает следующим основным требованиям: соответствует профилю подготовки бакалавров; располагает квалифицированными кадрами для руководства практикой бакалавров; предоставляет бакалаврам возможность использования компьютеризированных рабочих мест, снабженных программным обеспечением и выходом в Интернет, в объеме, необходимом для выполнения задач практики.

# Глава 1. Теоретико-методологическое обоснование объекта и предмета исследования

**Тема НИР**: «Информационные угрозы для личности (физического лица)»

**Актуальность темы исследования** заключается в том, с распространением интернета и «умных» устройств, а также общей цифровизацией, уязвимость личной информации значительно увеличилась. Угрозы, такие как кражи личных данных, мошенничество, скрытый сбор и анализ информации, становятся всё более распространёнными и серьёзными, больше и больше требуя от людей понимания их сути и эффективных мер защиты.

**Цель НИР** — повышение осведомленности о потенциальных информационных угрозах для личности и разработка эффективных стратегий защиты от них.

**Для достижения цели определим задачи работы**:

1. Проанализировать современные информационные угрозы и их возможные последствия;
2. Определить материалы и методы исследования;
3. Провести анализ результатов исследования;
4. Разработать рекомендации по мерам защиты.

**Объект исследования** – цифровая личная информация и личные данные физического лица в онлайн-среде.

**Предмет исследования** – информационные угрозы личности, их возможные последствия и способы защиты.

**Методы исследования** - сбор, анализ, синтез, обобщение и систематизация информации.

# Глава 2. Литературный обзор по теме научно-исследовательской работы

Стоит сказать, что тема информационной безопасности личности пока что не успела собрать внушительное количество «серьёзной» научно-исследовательской литературы по причине своей новизны. Однако из имеющейся современной литературы всё же можно выделить труд[1] наших соотечественников Полякова В. П. и Романенко Ю. А., в котором они фокусируются на педагогическом аспекте проблемы, и книгу[2] Андрея Бирюкова, где он подробно описывает информационные угрозы и технические методы противодействия им. Из зарубежной литературы, где эта тема раскрыта несколько лучше ввиду того, что на западе цифровизация началась раньше, стоит обратиться к книге[3] американского криптографа Брюса Шнайера, которая содержит множество экспертных советов о том, как обезопасить себя в цифровом пространстве. Также стоит обратить внимание на книгу[4] Фреда Шнайдера и Макса Блюменталя о доверии в цифровом пространстве, которая хоть и вышла в 1998 году, но актуальна во всём мире и на сегодняшний день, потому что пусть техника за эти 26 лет изменилась, но люди и их доверчивость — нет.

Отдельно хочу заметить, что библиографический материал выше описывает базовые принципы информационной безопасности личности в целом, в которых, несомненно, необходимо разбираться. Однако сегодняшние технологии развиваются и сменяют друг друга так быстро, что издавать книги по ним нет смысла, ведь пока книга будет писаться, редактироваться и утверждаться, её материал перестанет быть актуальным. Поэтому все материалы по безопасности относительно технологий, появившихся недавно (таких как смартфоны и современный софт) существуют в основном в интернете, в виде статей, прямых технических инструкций и видеороликов. Например, статья[5] Дмитрия Сергеева и Алексея Малахова в деталях описывает различные мошеннические схемы и как на них не попасться. Есть и целые информационные порталы вроде «Кибрариума» от Сбера, который посвящён цифровой безопасности с точки зрения простого пользователя.

# Глава 3. Теоретический обзор по теме НИР

Сегодня интернет является неотъемлемой частью нашей жизни, предоставляя множество возможностей для общения, работы и развлечения. Однако, вместе с этим, он также открывает двери ряду угроз. Сегодняшний цифровой мир представляет собой сложную систему, в которой пользователи сталкиваются с различными рисками и опасностями. Главными угрозами пользователю в цифровом пространстве являются три вещи: мошенники, отслеживание и утечки данных.

## Мошенники как угроза личности в цифровом пространстве

Одной из таких угроз являются мошенники, которые активно используют интернет для обмана и извлечения выгод за счет пользователей. Фишинговые сайты и спам-рассылки постепенно уходят в прошлое — в наше время мошенники используют более изощрённые схемы обмана. Они могут притворяться организациями (например, банковскими или медицинскими), родственниками и друзьями, техподдержкой, использовать социально значимые события в стране и социальную инженерию, чтобы убедить пользователей отдать им деньги или выдать персональную информацию.

По данным[6] Сбера, в 2022 году мошенники сделали 1,5 миллиарда попыток позвонить клиентам банков с целью похищения денежных средств. В течение последнего полугодия только в Сбере такие попытки затронули более 65% клиентов. В день совершается около 5 миллионов звонков, в том числе, с помощью роботов. Через форму обратной связи в мобильном приложении банка клиенты пожаловались на 1,8 миллионов телефонных звонков от мошенников. По прогнозам, эти числа будут расти.

В современном мире, где технологии развиваются с каждым днем, мошенники адаптируются к новым условиям. Они совершенствуют свои методы, используя искусственный интеллект и автоматизацию для ещё большей эффективности и увеличения охвата потенциальных жертв. С развитием интернета вещей и распространением смартфонов, доступных для миллиардов пользователей по всему миру, мошеннические схемы становятся более сложными и трудноразличимыми для обычного пользователя.

Многие становятся жертвами мошенничества в первую очередь из-за своей недостаточной осведомленности о таких угрозах.

### Информационные ресурсы

Мошенническим схемам обмана и популяризации методов противодействия им посвящён целый раздел на портале по кибербезопасности «Кибрарий» от Сбера. К примеру, одно из их последних расследований посвящено противодействию схеме с поддельным биржевым брокером[7], которая является довольно распространённой ввиду свойственного человеческой натуре желания просто приумножить свои деньги.

Также на этом портале собраны и проанализированы самые распространённые и эффективные схемы обмана, такие как поддельные госсервисы[8], фейковые сотрудники известных компаний[9] и так далее. Конечно, кроме описания схем, ресурс предлагает множество способов защиты в виде памяток и статей. Этот материал хорошо подходит для образовательных целей всем возрастным и социальным группам, и при необходимости на советы оттуда можно ссылаться.

## Нарушение приватности в современном информационном пространстве

Современные мегакорпорации активно собирают огромные объемы информации о своих клиентах и пользователях, создавая их цифровые профили для самых разных целей.

### Почему это угроза

Не всем очевидно, почему

Пользователь, как правило, недостаточно информирован или не информирован вовсе о том, какие его данные собираются, как они собираются и что получается в результате анализа этих данных. В таких случаях недостаток контроля над своими данными приводит к недоверию в отношении цифровых технологий.

Такая глубокая слежка уже сейчас широко используется для рекламы и цензуры. Как писал Брюс Шнайер во вступлении к своей книге: «ваш оператор сотовой связи отслеживает ваше местоположение и знает, кто был с вами. Ваши покупки записываются и позволяют узнать, являетесь ли вы безработным, больным или беременной. Ваши контакты показывают ваш круг общения. Гугл знает, о чем вы думаете, потому что сохраняет ваши поисковые запросы. Фейсбук может определить вашу сексуальную ориентацию без вашего упоминания о ней»[10]. Так что, действительно, информация сегодня — главный ресурс.

### Трекеры

Трекер (от *to track* «отслеживать») — сборщик данных о пользователях программного обеспечения и веб-страниц. Как правило, они используются для построения цифрового профиля человека, и в последствие для создания более эффективной рекламы, а иногда и для цензуры и алгоритмического подбора «правильного» контента.

Существуют инструменты, позволяющие обнаружить трекеры. Например, Blacklight от независимой исследовательской группы The Markup можно использовать для обнаружения трекеров на веб-страницах. Технология Blacklight заключается в том, что он использует данные скриптов, базу данных *DuckDuckGo Tracker Radar* и анализ сетевых запросов для выполнения тестов. В результате он генерирует отчет для пользователя. Подробнее технологические принципы работы своего инструмента исследовательская группа описала в соответствующей статье[11].

Проведём эксперимент самостоятельно: найдём какой-нибудь случайный веб-сайт и посмотрим, какие трекеры на нём есть:

1. Введём в поисковик нейтральный запрос «как вырастить монгольский дуб»;
2. Скопируем первую ссылку и вставим её в Blacklight (themarkup.org/blacklight?url=https://stroy-podskazka.ru).

В результате мы получили, что на странице обычного сайта про садоводство *stroy-podskazka.ru* содержится:

* 3 рекламных трекера третьих лиц;
* 3 других отслеживающих компонента (куки третьих лиц);
* отслеживатель курсора и нажатых клавиш.

Стоит обратить внимание, что это не очень популярный сайт с нишевой тематикой. Если взять такой популярный в России ресурс как Pikabu.ru, там найдётся 5 трекеров и 8 отслеживающих куки третьих лиц, при этом на сайте есть скрипты, предназначенные для обхода блокировщиков рекламы и трекинга.

При этом в подавляющем большинстве случаев нигде на сайтах понятно и доступно для простого пользователя не обозначено то, какие данные собираются (и что они собираются вообще), куда они отправляются и что с ними потом делают. Такая ситуация в современном интернете повсеместна. Как показало исследование[12], многие владельцы сайтов и сами не подозревают, какие данные о пользователях в результате использования сервисов третьих лиц на сайте собираются этими самыми третьими лицами. К примеру, подключая к своему сайту сервиса комментариев Disqus, владелец сайта через куки третьих лиц собирает данные для трекеров 21 различных фирм! (рис.1)  
Изображение выглядит как текст, снимок экрана, Веб-сайт, веб-страница

Автоматически созданное описание

Рис. 1

### Распространённость трекеров

Согласно некоторым исследованиям[13], почти все популярные сайты и мобильные приложения содержат трекеры. В процессе исследования было проанализировано 5000 популярных сайтов, результат в виде графика трекеров и случаев их обнаружения представлен на рис.2:

Изображение выглядит как текст, снимок экрана, линия, Шрифт

Автоматически созданное описание

Рис. 2

Как видно, три самых распространённых рекламных трекера принадлежат соответственно корпорациям Google, Amazon (Doubleclick — их трекер) и Facebook. Проверим эти данные. Действительно, согласно общедоступной статистике[14], доходы Google от рекламы в 2023 составили 78% от всех остальных их доходов.

Исследования также приводит таблицу рейтинга распространённости трекеров (их родительских фирм) на сайтах и в мобильных приложениях (таблица 1):

|  |  |  |
| --- | --- | --- |
| **Фирма трекера** | **Ранг на сайтах** | **Ранг в мобильных приложениях** |
| Google | 1 | 1 |
| Twitter | 2 | 6 |
| Facebook | 3 | 3 |
| Microsoft | 5 | 26 |
| Paypal | 6 | 185 |
| Amazon | 15 | 2 |
| Tencent | 19 | 240 |
| Alibaba | 20 | 84 |
| Comscore | 25 | 4 |
| VK | 27 | 110 |
| Yandex | 28 | 49 |
| Mail.ru | 31 | 121 |

Таблица 1

Опять проведём эксперимент, но на этот раз с мобильным приложением. Например, сейчас почти у всех на смартфоне стоит приложение 2ГИС. Проверим его на трекеры с помощью утилиты Tracker Control. В результате получаем следующую информацию:

* Приложение отправляет информацию о пользователе в такие трекеры как Amplitude, AppsFlyer, Facebook, Google, Huawei, VK, Mail.Ru;
* Страны, куда приложение отправляет данные отслеживания: США, Британия, Россия;
* Все действия в интерфейсе приложения записываются.

Чтобы защититься от большей части трекеров и увеличить свою приватность, достаточно придерживаться достаточно простых правил:

1. Использовать преимущественно программы и сервисы с открытым исходным кодом;
2. Установить в браузер блокировщик рекламы, например Ublock Origin;
3. На телефоне установить блокировщик трекеров на уровне системы. Упомянутый ранее Tracker Control хорошо подходит для этой задачи, используя технологию Firewall для блокировки интернет-траффика, направленного в трекеры[15].
4. Стараться избегать продуктов и экосистем фирм, которые зарабатывают в основном на рекламе. Например, Google, Amazon, Facebook, Yandex
5. Как можно меньше вводить свои личные данные в интернете.

## Утечки персональных данных

Проблема утечек персональных данных остро стоит в современном мире, особенно в нашей стране, и представляют прямую угрозу пользователю как в информационном пространстве, так и в жизни. Вышеописанные две угрозы в виде роста количества мошенников, низкой степени приватности в сети и недостаточной осведомлённости о своих данных тесно связны с проблемой утечек и только усугубляют её.

Согласно данным Роскомнадзора, в 2022 году в сеть утекли 600 миллионов записей о россиянах, тогда ведомство зафиксировало более 140 утечек. В 2023 году Роскомнадзор зафиксировал 168 утечек персональных данных, в результате которых в открытый доступ попало более 300 миллионов записей[16]. А с начала 2024 года к одному лишь марту утекло 500 миллионов записей о россиянах[17].

### Крупнейшие утечки за последние несколько лет

* Яндекс.Еда: в 2022 году утекли такие данные, как имена и фамилии, номера телефонов, адреса доставки и заказы, которых в опубликованной базе данных было почти 50 миллионов[18].
* СДЭК: в 2022 году утекли номера телефонов, физические и электронные адреса клиентов. По словам фирмы, утечка затронула несколько десятков миллионов пользователей[18].
* AT&T: в 2023 году было опубликовано 73 миллиона персональных данных о клиентах. Данные включали в себя имена, номера телефонов и почтовые адреса. При этом AT&T до сих пор не знает, как произошла эта утечка данных[19].
* Различные фирмы малого бизнеса: в последние несколько нет хакеры стали фокусироваться не только на атаках больших корпораций, но и малого бизнеса. В текущем 2024 году злоумышленники выкладывали информацию преимущественно небольших компаний, так как они часто относятся к персональным данным менее серьёзно, чем большие. Например, в 2024 количество утёкших в сеть паролей (самого охраняемого компонента персональных данных) в России выросло в шест раз как раз по этой причине[20].

### Минимизация рисков

Сбер провёл исследование[21], где выявил основные тренды утечек (их количество действительно растёт), их источники, какие данные обычно утекают, где и за какую цену продаются (в основном в Телеграме, по 17 рублей за строчку из таблицы базы данных). Также в статье указаны способы минимизации риска в связи с угрозой утечки — увы, полностью в современном мире их избежать не удастся.

Основные их рекомендации по минимизации рисков от утечек повторяют выявленные мной выше рекомендации о противодействии мошенникам и отслеживанию, что подтверждает мой изначальный тезис о том, что проблема утечек персональных данных тесно связана с этими двумя угрозами.

# Библиографический список по теме НИР

1. Поляков Виктор Павлович, Романенко Юрий Александрович   
   «Педагогическое обеспечение информационной безопасности личности в цифровой информационно-образовательной среде» // Наука о человеке: гуманитарные исследования. 2020. №1.
2. Бирюков, А. А. «Информационная безопасность: защита и нападение». Москва, ДМК Пресс, 2017.
3. B. Schneier. “Secrets and Lies: Digital Security in a Networked World”. John Wiley & Sons, New York, 2000.
4. F.B. Schneider and M. Blumenthal, editor. “Trust in Cyberspace”. National Research Council, National Academy Press, 2101 Constitution Ave., Washington, D.C. 20418, 1998. Final report of the National Research Council Committee on Information Trustworthiness.
5. Дмитрий Сергеев, Алексей Малахов: «Виды мошенничесва в интернете. Как избежать мошенников и что делать, если вас обманули». Тинькоф-журнал, 2024 // https://journal.tinkoff.ru/wiki/fraud
6. Сбербанк. «Анализ мошеннических звонков из колл-центров на территории Украины», 2022 // https://sberbank.ru/ru/person/kibrary/investigations/analiz\_moshennicheskih\_zvonkov
7. Сбербанк. «Обман под маской биржевого брокера», 2024 // https://sberbank.ru/ru/person/kibrary/investigations/obman-pod-maskoj-birzhevogo-brokera
8. Сбербанк. «Схемы обмана: Поддельные госсервисы», 2021 // https://www.sberbank.ru/ru/person/kibrary/investigations/skhemy-obmana-poddelnye-gosservisy
9. Сбербанк. «Схемы обмана: Звонки фейковых сотрудников», 2024 // https://www.sberbank.ru/ru/person/kibrary/investigations/skhemy-obmana-poddelnye-gosservisy
10. Schneier B. “Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World”. New York: W. W. Norton & Company, 2015.
11. Surya Mattu, Aaron Sankin “How We Built a Real-time Privacy Inspector”. The Markup, 2020 // https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector
12. Surya Mattu, Aaron Sankin “The High Privacy Cost of a “Free” Website”. The Markup, 2020 // https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites
13. Reuben Binns, Jun Zhao, Max Van Kleek, Nigel Shadbold: “Measuring third party tracker power across web and mobile”. University of Oxford, Department of Computer Science, UK, 2018.
14. Tiago Bianchi: “Distribution of Google segment revenues from 2017 to 2023”. Statista, 2024 // https://statista.com/statistics/1093781/distribution-of-googles-revenues-by-segment
15. Konrad Kollnig: “TrackerControl for Android”, Github, 2023 // https://github.com/TrackerControl/tracker-control-android
16. «В 2023 году в сеть утекло более 300 млн записей о россиянах», ТАСС, 2024 // https://tass.ru/obschestvo/19693845
17. Татьяна Стекольникова, «Роскомнадзор сообщил об утечке 500 млн данных о россиянах за один раз», РБК, 2024 // https://rbc.ru/rbcfreenews/65d7ef3d9a7947d8608dbbb3
18. Анна Левочкина, «14 компаний, откуда утекли данные пользователей в 2022 году», Сравни.ру, 2022 // https://sravni.ru/text/14-kompanij-otkuda-utekli-dannye-polzovatelej-v-2022-godu
19. Аружан Дарибай, «Крупнейшие утечки данных с начала года», TENGRI NEWS, 2024 // https://tengrinews.kz/tech/nazvanyi-krupneyshie-utechki-dannyih-s-nachala-goda-539908
20. Лаборатория Касперского, «В 2024 году количество утёкших паролей в России выросло в шесть раз», 2024 // https://www.kaspersky.ru/about/press-releases/2024\_v-2024-godu-kolichestvo-utyokshih-parolej-v-rossii-vyroslo-v-shest-raz
21. Сбербанк. «Утечки персональных данных: теперь деньги — не главное», 2022 // https://www.sberbank.ru/ru/person/kibrary/investigations/utechki-personalnykh-dannykh

# Заключение

**Б2.В.03(Н). Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)** способствовала закреплению и углублению теоретической подготовки и приобретению практических навыков и компетенций в сфере профессиональной деятельности.

В результате прохождения производственной практики, были сформированы следующие компетенции:

* Способность выполнять работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы (ПК-1);
* Способность осуществлять консультационно-техническую поддержку клиентов по вопросам технического обслуживания и обеспечения работоспособности инфокоммуникационных систем и (или) их составляющих (ПК-2);
* Способность управлять процессами технической поддержки инфокоммуникационных систем и (или) их составляющих (ПК-3);
* Способность создавать и редактировать информационные ресурсы (ПК-4);
* Способность управлять информационными ресурсами (ПК-5)