Минцифры России

Интеграл

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Федеральное государственное бюджетное учреждение «Научно-исследовательский институт «Интеграл»

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ОТЧЁТ ЗА 2023 ГОД

Результаты работы информационной системы «Антифишинг»

ФГБУ «НИИ «Интеграл»

Москва
2024

Содержание

ВВЕДЕНИЕ

В отчете представлены результаты анализа работы Информационной системы мониторинга фишинговых сайтов и утечки персональных данных (далее – ИС «Антифишинг»).

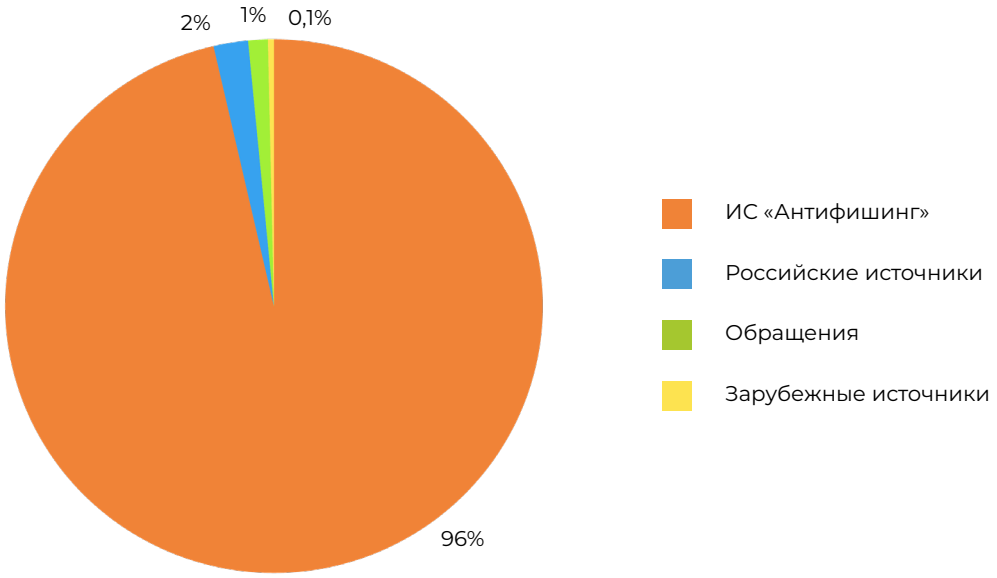
ИС «Антифишинг» обеспечивает выполнение следующих задач:

- мониторинг российского сегмента сети «Интернет»;
- поиск и обнаружение фишинговых ресурсов, запрещенного и деструктивного контента и утечек персональных данных;
- направление интернет-ресурсов заинтересованным сторонам (правоохранительным и уполномоченным органам, экспертным и другим организациям);
- подготовка данных по результатам работы ИС «Антифишинг» в органы власти (организации), а также информационно-аналитических отчетов по тенденциям и направлениям проведения фишинговых атак.

1. ОБЩИЕ РЕЗУЛЬТАТЫ РАБОТЫ В 2023 ГОДУ

За 2023 год ИС «Антифишинг» обработано порядка 3,5 млрд. ресурсов, зарегистрированных в более 300 доменных зонах сети «Интернет». В результате автоматизированного мониторинга сети «Интернет» и работы сотрудников, обслуживающих информационную систему, было выявлено 355459 фишинговых ресурсов, ресурсов с деструктивным и запрещенным контентом, а также с утечками персональных данных, ориентированными на российского пользователя, из которых 122056 ресурсов были заблокированы (разделегированы). Далее представлена более подробная информация о количестве ресурсов и способах получения информации о них:

- 342623 ресурса, поиск которых был выполнен с помощью ИС «Антифишинг»;
- 7382 ресурса, полученных из российских источников;
- 4190 ресурсов, указанных в обращениях органов государственной власти и граждан;
- 1264 ресурса, поступивших из зарубежных источников.



Основная информация об интернет-ресурсах поступает через ИС «Антифишинг» (97%). К российским источникам (2%) относятся фиды, предоставляемые российскими организациями. Сайты, полученные из зарубежных фидов, составляют менее одного процента от общего количества интернет-ресурсов, поступивших в информационную систему. Малый процент отбираемой системой из зарубежных источников обусловлен нацеленностью их в большей степени на пользователей из других стран и регионов. Также сведения о некоторых интернет-ресурсах исключается при проверке на дубликацию – информация о которых уже была ранее получена из других источников.

2. ОБЩАЯ ИНФОРМАЦИЯ О РЕСУРСАХ, ОБНАРУЖЕННЫХ В 2023 ГОДУ

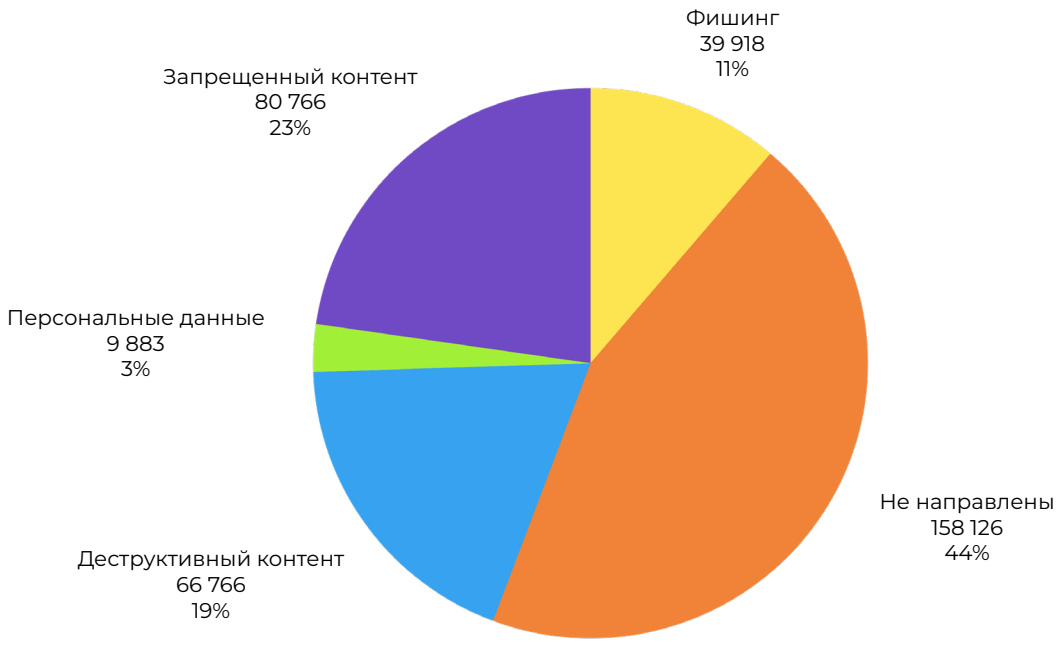
За 2023 год ИС «Антифишинг» было обнаружено около 355 тыс. интернет-ресурсов, среди которых:

1. Ресурсы, применяемые для получения конфиденциальных сведений за счет введения пользователей в заблуждение (фишинг);
2. Материалы, направленные на распространение недостоверной общественно значимой информации в сети «Интернет» (деструктивный контент);
3. Ресурсы, в материалах которых могут содержаться признаки других нарушений законодательства Российской Федерации: изготовление и оборот поддельных документов, незаконный сбыт наркотических веществ и др. (запрещенный контент);
4. Ресурсы, на которых размещены материалы, которые могут нарушать законодательство Российской Федерации в области персональных данных (продажа персональных или конфиденциальных данных, в том

числе получение их при помощи взлома ресурсов).

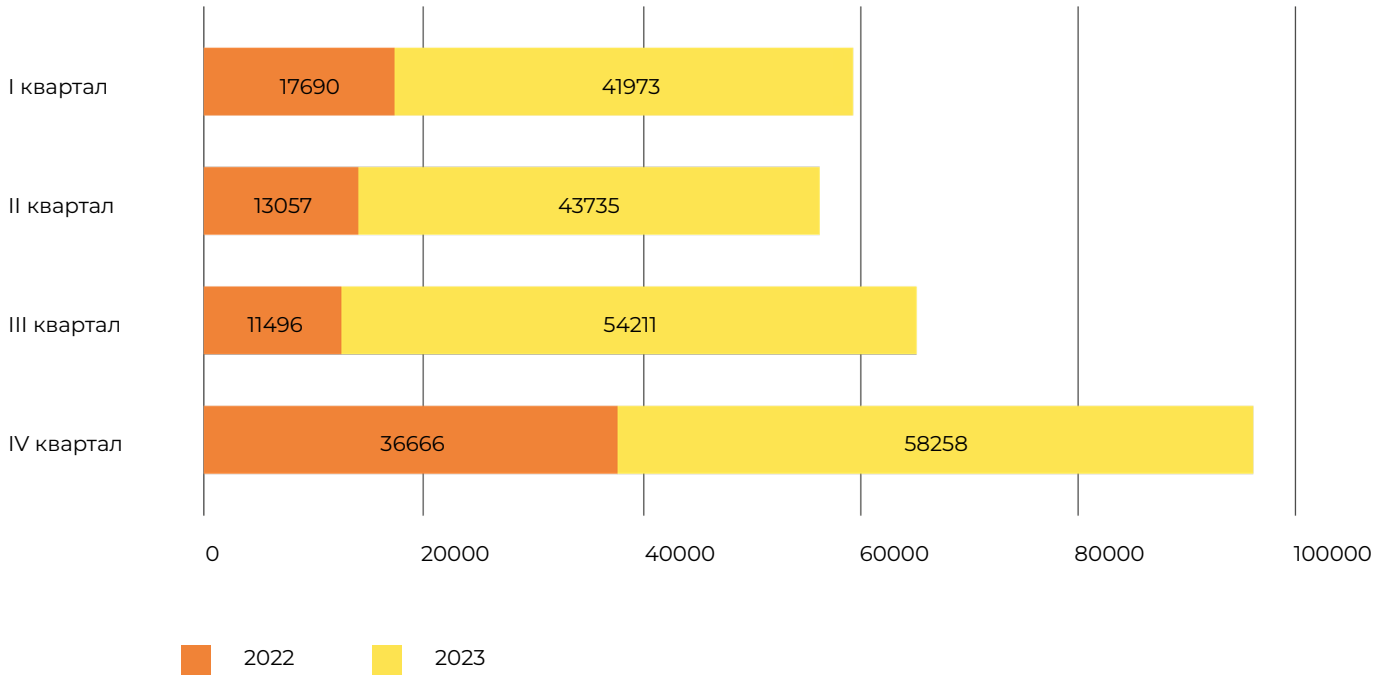
5. Выявленные и обработанные ресурсы, которые не были направлены заинтересованным сторонам по следующим причинам:
   - противоправная информация была удалена;
   - ресурс может вводить пользователей в заблуждение, но в настоящий момент не используется для сбора конфиденциальных сведений;
   - ресурс прекратил функционирование;
   - для оценки деятельности ресурса требуется проведение оперативно-розыскных мероприятий и другая деятельность, не входящая в компетенцию ФГБУ «НИИ «Интеграл».

Количество выявленных интернет-ресурсов



Из представленной информации видно, что наибольший процент от общего количества выявленных ресурсов составляют ресурсы с деструктивным и запрещенным контентом. Большое количество таких ресурсов связано с разжиганием русофобии в части европейских стран, а также созданием такого контента специальными подразделениями в этих странах и на Украине.

Общее количество выявленных интернет-ресурсов за I-IV кварталы 2022 и 2023 гг.



- за I квартал 2023 год количество выявленных ресурсов увеличилось на 58% по сравнению с I кварталом 2022 г.;
- за II квартал 2023 год количество выявленных ресурсов увеличилось на 71% по сравнению с II кварталом 2022 г.;
- за III квартал 2023 год количество выявленных ресурсов увеличилось на 79% по сравнению с III кварталом 2022 г.;
- за IV квартал 2023 год количество выявленных ресурсов увеличилось на 38% по сравнению с IV кварталом 2022 г.

Значительное увеличение выявляемых ИС «Антифишинг» ресурсов с разной противоправной информацией в 2023 году обусловлено следующими основными причинами:

- проведение информационной (пропагандистской) войны против Российской Федерации;
- переход многих криминальных структур из области прямого мошенничества в виртуальную, что пока позволяет проводить такие действия в ряде случаев безнаказанно;
- постоянное изменение и расширение ланшафта мошеннических схем;
- совершенствование методов и способов обнаружения ИС «Антифишинг» таких ресурсов.

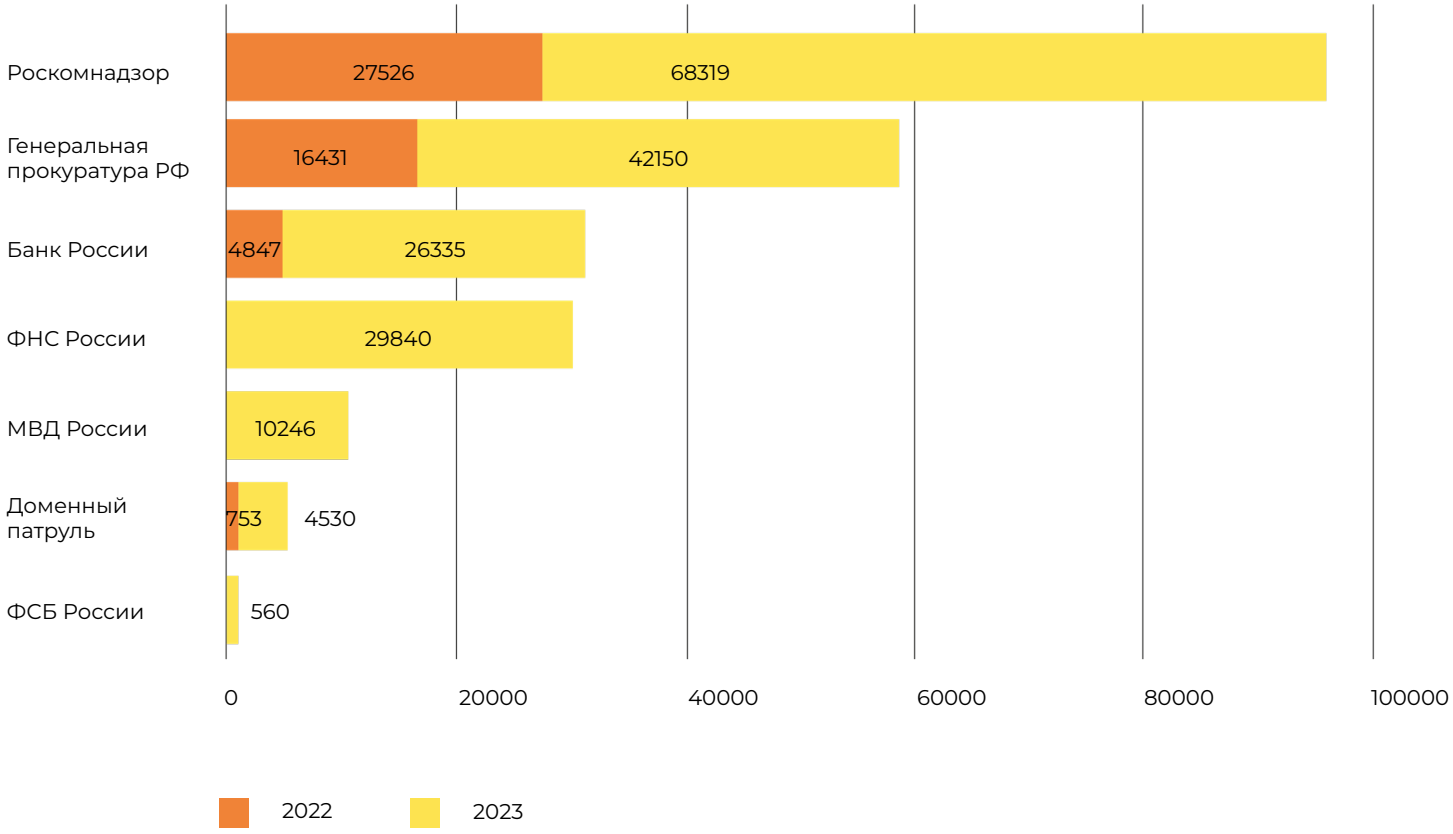
Для повышения эффективности борьбы с фишинговыми атаками, деструктивным и запрещенным контентом и утечкой персональных данных организовано информационное взаимодействие с органами государственной власти и организациями. Результатом информационного обмена с органами власти, в полномочия которых входит принятие решения об ограничении доступа к ресурсу на территории Российской Федерации или осуществление

прекращения делегирования доменного имени, является блокирование и прекращение делегирования 122056 ресурсов в 2023 году. В рамках информационного обмена с заинтересованными сторонами в 2023 году ресурсы направлялись следующим адресатам:

- Роскомнадзор – 68319 ресурсов;
- Генеральная прокуратура – 55903 ресурса;
- ФНС – 29840 ресурсов;
- ФСБ – 560 ресурса;
- МВД – 10246 ресурса;
- Координационный центр «Доменный патруль» – 4530 ресурсов;
- Банк России – 26335 ресурсов.

На графике отображена информация в сравнении количества интернет-ресурсов, направленных различным адресатам в 2022 и 2023 гг.

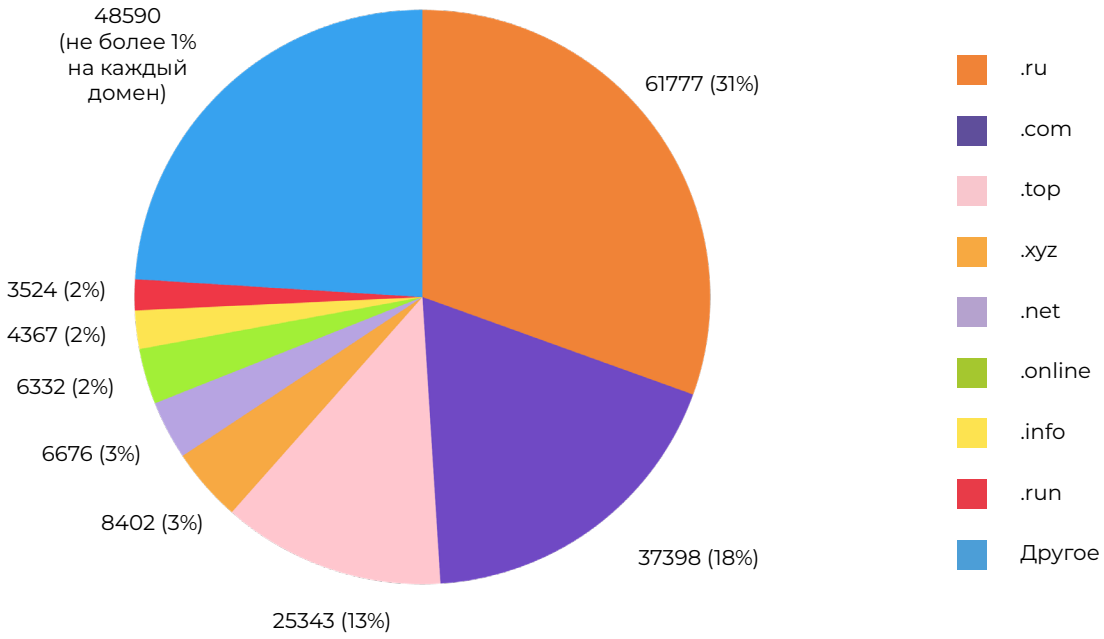
Количество направленных интернет-ресурсов (2022–2023 гг.)



Из представленной информации видно, что в 2023 году по сравнению с 2022 годом количество ресурсов, направленных заинтересованным сторонам, увеличилось в 3-4 раза. Основными получателями такой информации стали Роскомнадзор, Генеральная прокуратура Российской Федерации, Банк России и Федеральная налоговая служба. В 2023 году наблюдалось увеличение количества интернет-ресурсов, содержащих запрещенный и деструктивный контент, а также фишинговых интернет-ресурсов, целью которых является

компрометация данных банковских карт и другой информации, связанной с ведением финансовой деятельности. В топ-3 по количеству направленных ресурсов находятся заинтересованные стороны, в компетенцию которых входит анализ и/или блокирование данных интернет-ресурсов.

Количество выявленных интернет-ресурсов за 2023 год (домены верхнего уровня)

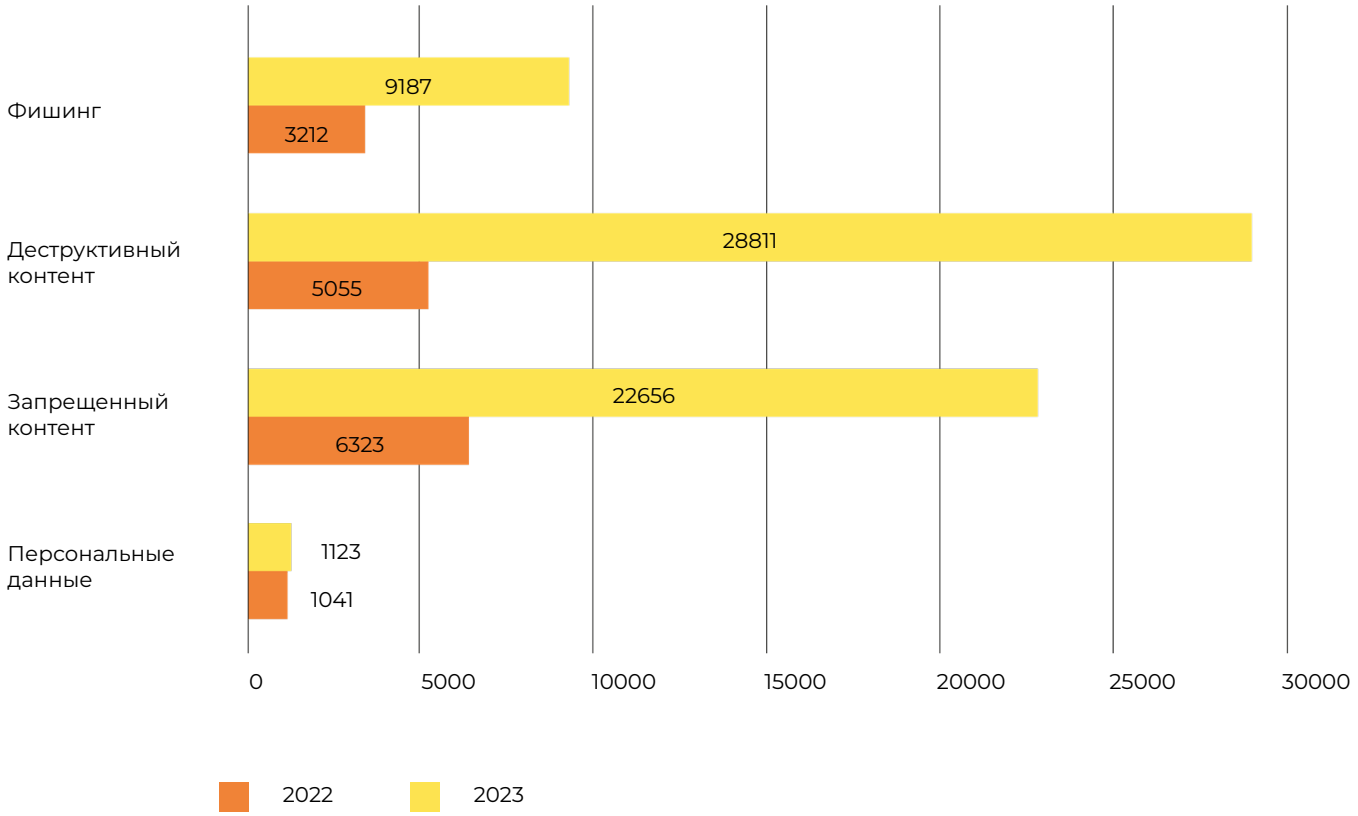


Наибольшее количество доменов, на которых была размещена противоправная информация, приходилось на доменную зону .ru (31%), на втором месте – .com (18%), на третьем месте – .top (13%), на четвертом месте – .xyz и .net (3%), на пятом месте – .online, .run, .info (2%). Оставшаяся доля распределилась между 321 доменами (доля каждого из которых составляет не более 1%).

Следует отметить, что домен .RU является единственной национальной доменной зоной, входящей в топ-5 по количеству обнаруженных интернет-ресурсов. Злоумышленники могут регистрировать доменные имена в зоне .RU с целью ввести пользователей в заблуждение. Пользователь может предположить, что ресурс, зарегистрированный в зоне .RU, является заслуживающим доверия. Также возможной причиной может быть сравнительно невысокая стоимость доменных имен в данной доменной зоне. Таким образом, злоумышленники могут создать большее количество ресурсов при меньших расходах, таким образом увеличивая количество потенциальных жертв.

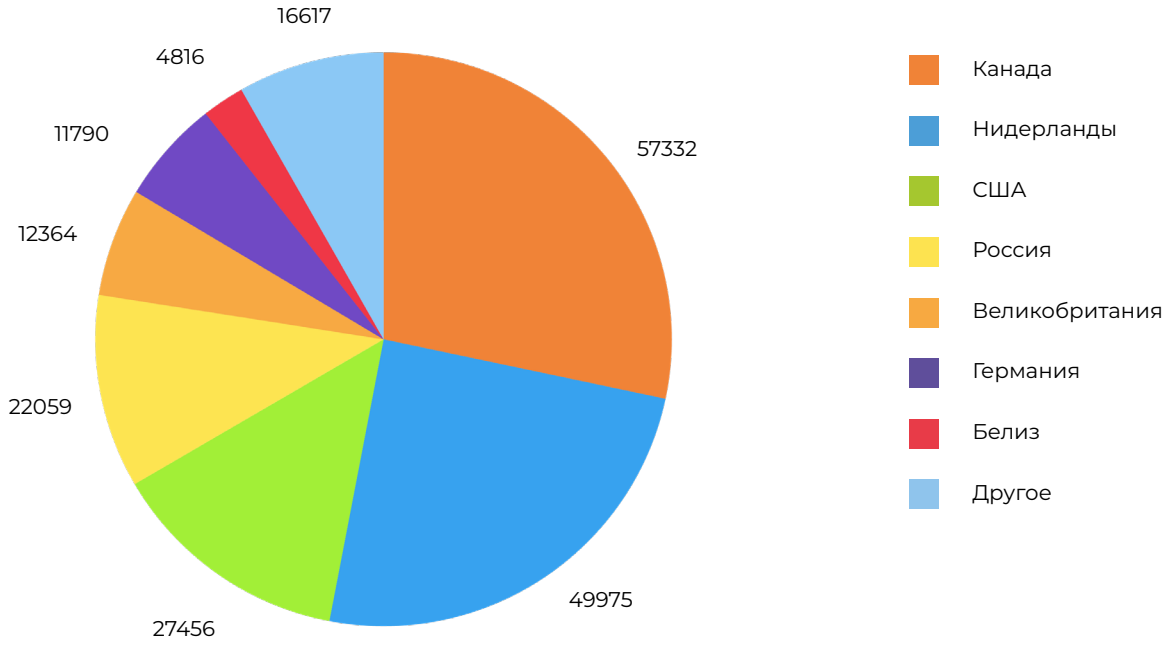
Более подробная информация, касающаяся домена .RU, представлена на следующем графике.

Сравнение количества интернет-ресурсов в 2022–2023 гг. (доменная зона .RU)



В 2023 году отмечается рост количества выявленных ресурсов, имеющих домен верхнего уровня .RU. Следует отметить, что по сравнению с 2022 годом отмечается значительное увеличение количества выявленных ресурсов практически по всем категориям и в особенности с деструктивным контентом. Данный факт связан с попыткой ряда западных стран и Украины осуществлять мероприятия по дискредитации Вооруженных сил Российской Федерации, проводящей специальную военную операцию путем распространения искаженной, неподтвержденной, ложной информации.

Количество выявленных интернет-ресурсов в 2023 г. (размещение серверов)



Из информации, представленной на графике, следует, что большинство обнаруженных интернет-ресурсов размещено на зарубежных серверах. Для более эффективного ухода от преследования правоохранительных органов в Российской Федерации, злоумышленники и нарушители законодательства страны размещают русскоязычные ресурсы на вычислительных мощностях в других странах. Наибольшее количество доменов размещено на серверах в Канаде (28%); на втором месте – Нидерланды (25%), на третьем месте – США (14%), на четвертом месте – Россия (11%), на пятом месте – Великобритания и Германия (6%), на шестом – Белиз (2%). Оставшаяся доля распределилась между 69 странами (доля каждой из которых составляет не более 1%). Возможно наибольшее количество размещаемых доменов в Канаде связано с тем, что в этой стране проживает самая большая украинская диаспора.

3. ФИШИНГОВЫЕ АТАКИ

По состоянию на конец декабря 2023 г. ФГБУ «НИИ «Интеграл» было обнаружено около 39 тыс. ресурсов, применяемых для получения конфиденциальных сведений за счет введения пользователей в заблуждение, что на 75 % больше чем в 2022 году.

3.1. Основные характеристики фишинговых ресурсов в 2023 году

При изучении ресурсов, обнаруженных в 2023 году, были выявлены следующие признаки, которые были неоднократно замечены на фишинговых ресурсах:

- **Тайпсквоттинг.** Использование доменного имени, схожего до степени смешения с доменным именем официального ресурса упоминаемой организации или содержащим название упоминаемой организации. Пользователь может открыть данный интернет-ресурс, к примеру, допустив опечатку при написании доменного имени официального интернет-ресурса.
- **Генерация случайных доменных имен.** Данная стратегия противоположна тайпсквоттингу, принцип которого описан выше; злоумышленники используют случайные доменные имена, не обладающие сходством с доменными именами известных интернет-ресурсов (официальных сайтов банков и т.д.).
- **SSL-сертификат.** Злоумышленники приобретают SSL-сертификаты для фишинговых ресурсов с целью введения пользователей в заблуждение. Пользователи ошибочно предполагают, что наличие SSL-сертификата гарантирует защиту от всех видов мошенничества.
- **Автоматизация процессов и продажа инструментов для проведения фишинговых атак.** Для создания большого количества фишинговых ресурсов в кратчайшие сроки используются конструкторы сайтов, для работы с которыми не требуется привлечение опытных разработчиков и дизайнеров. Злоумышленники используют готовые шаблоны для создания большого количества фишинговых ресурсов.
- **Защита от обнаружения (скрытое содержание).** Злоумышленники предпринимают меры для ограничения круга пользователей, имеющих доступ к содержимому фишинговых интернет-ресурсов. К примеру, отображение содержимого сайта с фальшивой платежной формой может состояться только в случае перехода с поддельного сайта, на котором пользователю предлагается приобрести билеты или забронировать место для проведения досуга. Также отображение вредоносного содержимого может осуществляться при условии использования URL-адреса с указанием конкретной страницы, которую потенциальная жертва может получить, к примеру, через рассылку писем на электронной почте.
- **Маскировка под официальный ресурс с помощью транслитерации юридического лица.** При просмотре информации о фишинговом домене можно увидеть, что он копирует ИНН целевой организации, а также путем транслитерации пытается замаскировать под нее и собственное наименование организации.

3.2. Виды фишинговых ресурсов

Наиболее популярными являются ресурсы, относящиеся к следующим тематическим группам:

1) банковский сектор;
2) социальные сети и мессенджеры;
3) маркетплейсы и онлайн-магазины;
4) инвестиционные платформы;

5) сервисы по продаже билетов и бронированию.

Далее приведена более подробная информация о ресурсах, входящих в перечисленные тематические группы.

3.2.1. Упоминание банков, маркетплейсов, онлайн магазинов, социальных сетей и мессенджеров как способ введения в заблуждение

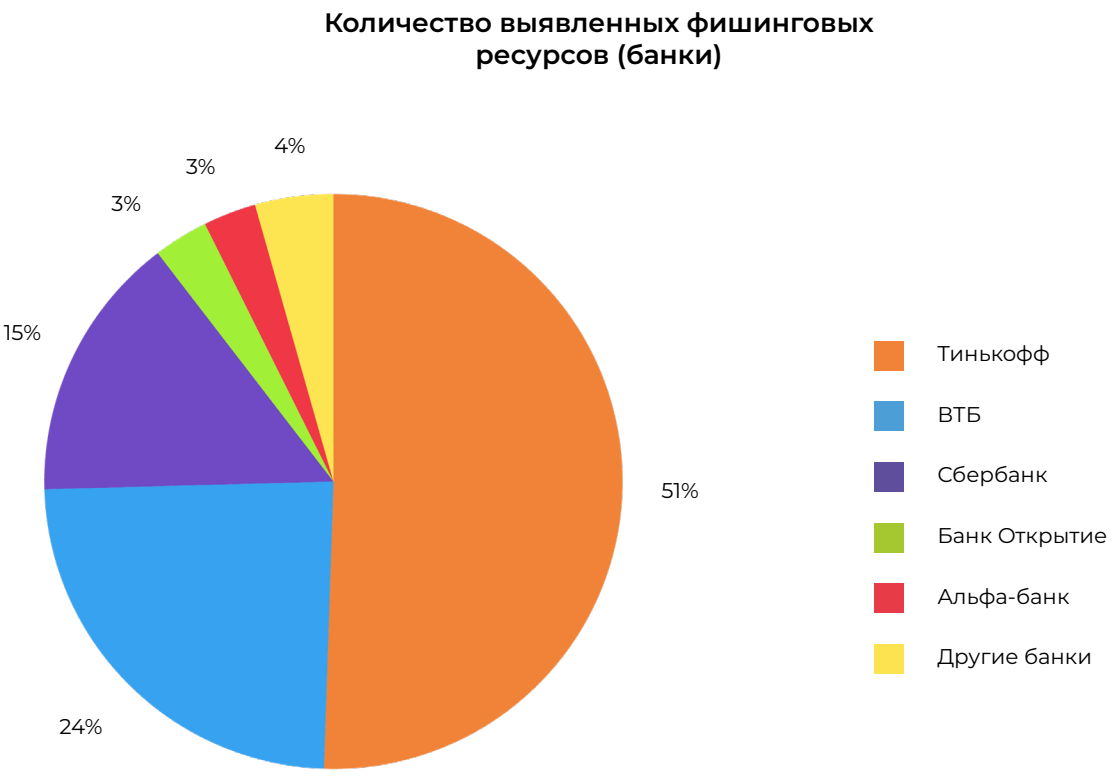
Получение денежных средств – одна из популярных целей злоумышленников. Тем не менее, они стремятся получить от своей жертвы как можно больше, не ограничиваясь однократным платежом. Для кражи сведений, позволяющих пользоваться личным кабинетом на сайте банка, банковской картой и т.д., активно используются фишинговые сайты.

Злоумышленники создают многочисленные интернет-ресурсы, якобы принадлежащие банкам, маркетплейсам, онлайн-магазинам, социальным сетям и мессенджерам. Представляется возможным выделить следующие разновидности данных ресурсов:

- имитации входа в личный кабинет на сайте банка, маркетплейса или онлайн-магазина, а также фальшивые страницы, якобы предназначенные для открытия учетной записи в социальной сети;
- инвестиционные платформы, якобы принадлежащие банкам;
- сайты с несуществующими розыгрышами, акциями и другими способами получения денежного вознаграждения от имени банков, маркетплейсов, онлайн-магазинов, социальных сетей и мессенджеров. Также мошенники могут создавать сайты несуществующих организаций, якобы проводящих розыгрыши, при использовании визуальных и текстовых материалов с нескольких безопасных для пользователей сайтов. За 2023 г. обнаружено около 3,5 тыс. подобных сайтов;
- интернет-ресурсы, якобы предназначенные для защиты платежной информации клиентов банков или предназначенные для консультирования клиентов банков в случае возникновения вопросов или проблем.

Самые популярные банки – Тинькофф (около 1350 ресурсов), ВТБ (около 640 ресурсов), Сбербанк (около 400 ресурсов).

Злоумышленники создают не только сайты-двойники реально существующих банков, но и сайты «лжебанков» – несуществующих кредитных организаций. Пользователю, посетившему сайт лжебанка, могут предложить оформление кредита или вклада. Таким образом, жертва может не только перевести денежные средства мошенникам, но и добровольно скомпрометировать персональные данные.

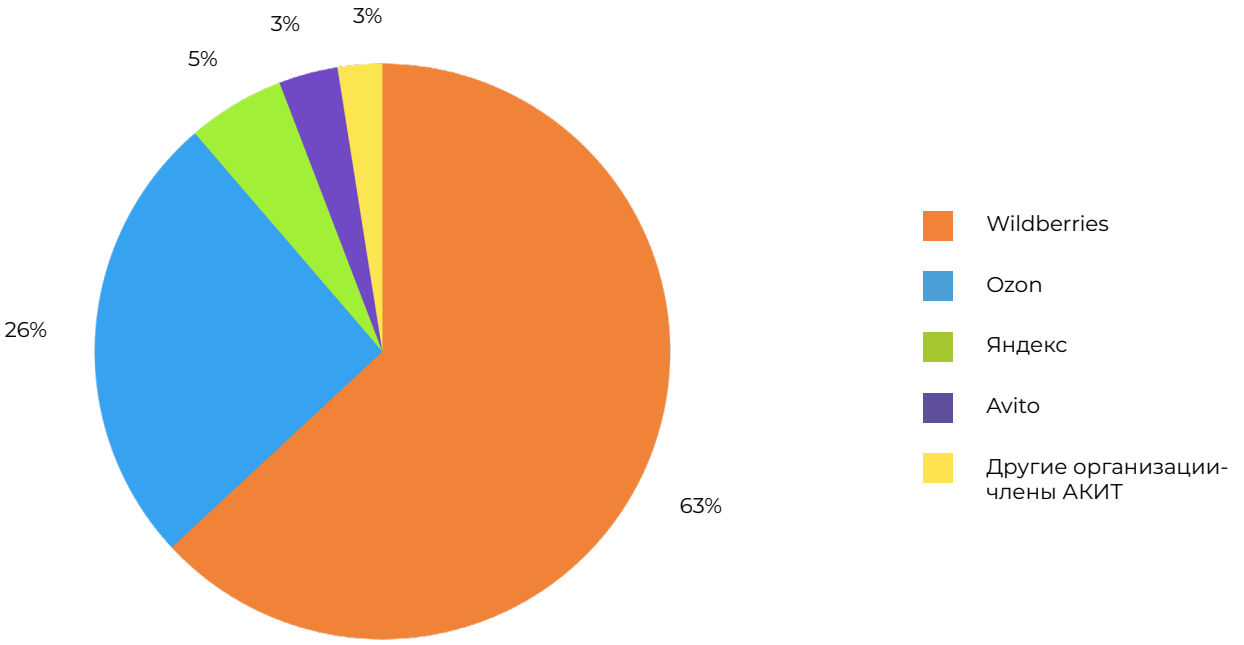


Активным направлением среди мошенников является сфера интернет-продаж. Лидеры среди упоминаемых организаций-членов АКИТ (Ассоциации компаний интернет торговли) – Wildberries (около 3320 ресурсов), Ozon (около 1350 ресурсов). Популярность маркетплейсов растет; кроме того, упомянутые организации широко известны среди русскоязычных пользователей. Указанные обстоятельства являются причиной высокого интереса злоумышленников к созданию сайтов, якобы принадлежащих Ozon и Wildberries.

Фишинговые ресурсы, мимикрирующие под официальные ресурсы организаций-членов Ассоциации компаний интернет-торговли, могут быть нацелены не только на покупателей. Некоторые фишинговые ресурсы нацелены на кражу данных пользователей, желающих стать партнерами организации-члена Ассоциации компаний интернет-торговли.

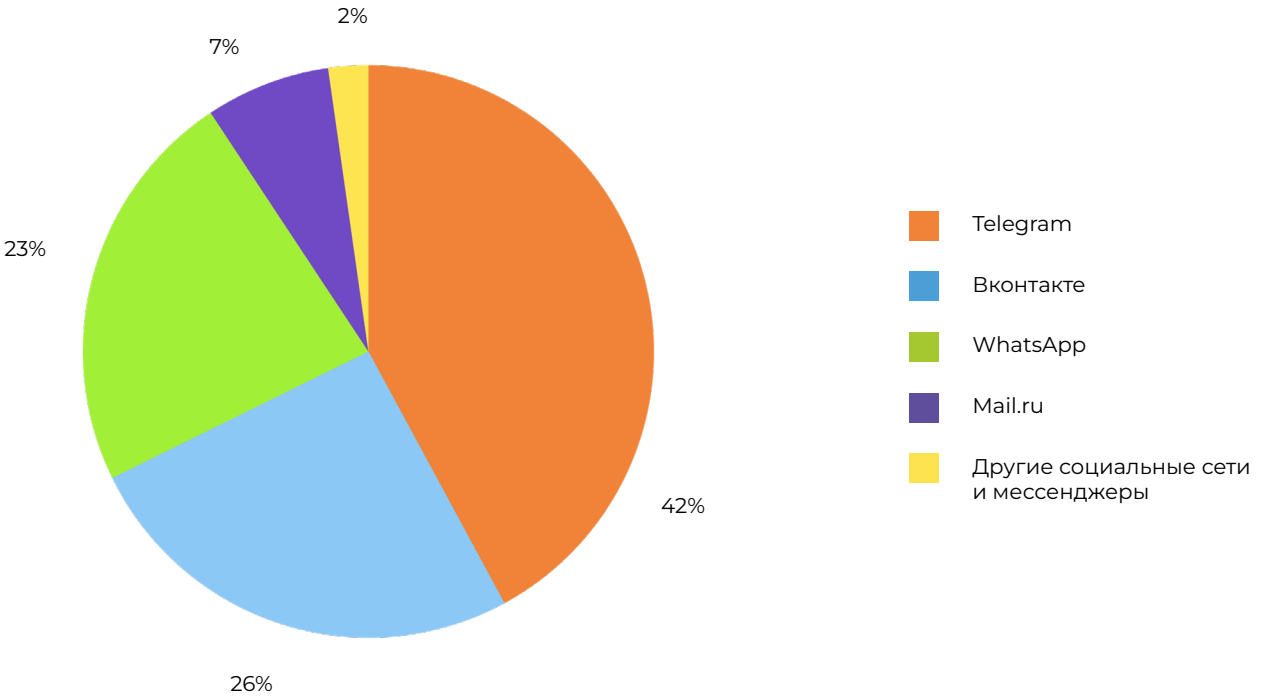
Более подробная информация о количестве ресурсов представлена на графике.

Количество выявленных фишинговых ресурсов (организации-члены АКИТ)



Чаще всего злоумышленники создают сайты, якобы связанные с мессенджерами Telegram, WhatsApp и корпорацией VK, с целью получения сведений, необходимых для входа в учетную запись. Высокий интерес к созданию подобных сайтов объясняется большой аудиторией людей, ежедневно пользующихся социальными сетями и мессенджерами. Указанные мессенджеры и социальные сети популярны среди русскоязычных пользователей. Более того, украденные данные могут использоваться для получения доступа к сервисам, привязанным к социальным сетям и мессенджерам. Также существуют сайты, одновременно нацеленные как на пользователей социальных сетей и мессенджеров, так и пользователей ресурсов организаций-членов АКИТ. К примеру, существуют ресурсы, на которых пользователю предлагается заполнить анкету для заключения партнерства с Wildberries, после чего предлагается завершить процедуру подачи заявки, выполнив вход в учетную запись мессенджера Telegram. На графике представлены данные по выявленным ресурсам в социальных сетях и мессенджерах, которые используют злоумышленники для обмана граждан.

Количество выявленных фишинговых ресурсов (социальные сети и мессенджеры)



3.2.2. Инвестиционные платформы как разновидность фишинга

На сайтах фальшивых инвестиционных проектов утверждается, что пользователь, зарегистрировавшийся на платформе, получит надежный источник дохода без приложения усилий. За 2023 год обнаружено около 17 тыс. ресурсов по «инвестиционным платформам».

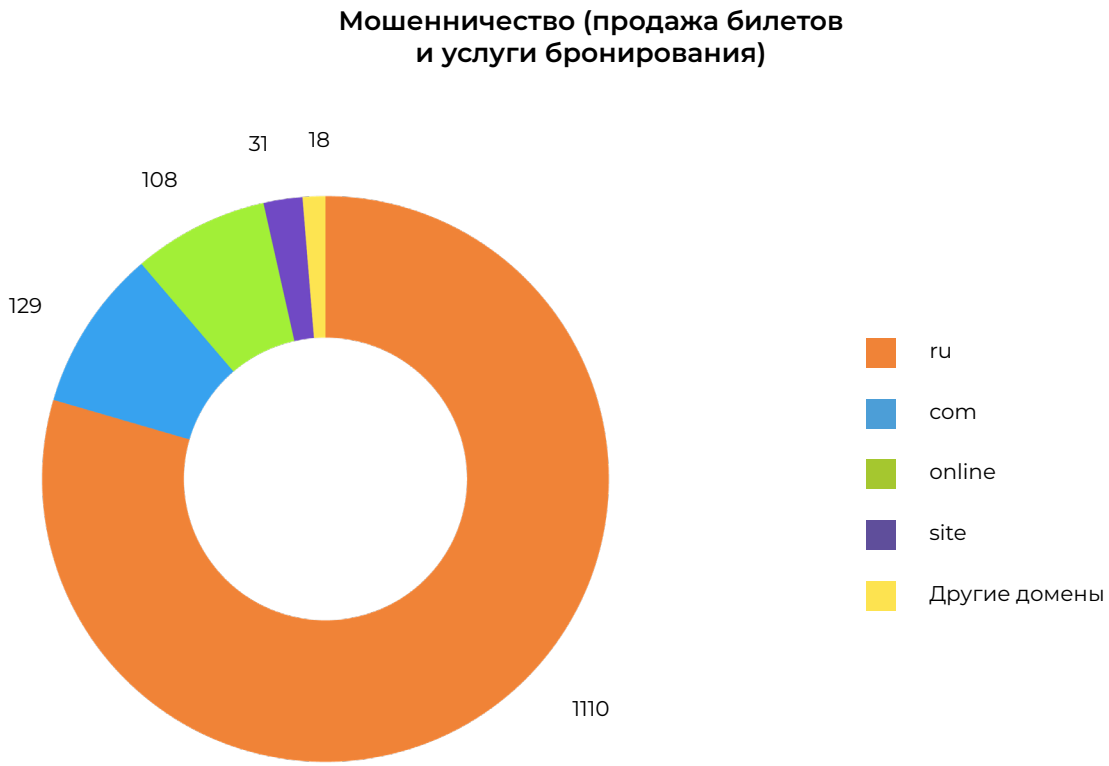
Для того, чтобы привлечь внимание пользователей и убедить их в том, что сайт является заслуживающим доверия, злоумышленники используют элементы оформления реально существующих организаций. Особенно часто используются упоминания названий и элементы оформления организаций, которые хорошо известны большинству пользователей. Отечественной компанией, наиболее часто упоминаемой мошенниками на сайтах инвестиционных платформ, является ПАО «Газпром» (приблизительно 4 тыс. ресурсов). Тем не менее, на русскоязычных фишинговых ресурсах часто упоминаются и известные зарубежные организации. Лидер среди упоминаемых зарубежных организаций – компании X Holdings Corp., принадлежащего Илону Маску (Tesla, X Corp. (бывш. Twitter) и др.), а также холдинговая компания Meta Platforms (признана экстремистской организацией на территории РФ).

3.2.3. Кража данных при помощи сайтов с предложениями по продаже билетов и услуг бронирования

Также представляется возможным выделение группы ресурсов, которые связаны с индустрией развлечений – сферой, представляющей особый интерес для мошенников. Ранее упоминалось, что создатели фишинговых ресурсов часто нацелены на получение доступа к денежным средствам и

банковским картам пользователей. Поддельные сайты с предложениями по продаже билетов и услугам бронирования создаются именно с этой целью. Злоумышленники вводят в заблуждение пользователей, желающих приобрести билеты в театр или забронировать место для свидания.

За 2023 год обнаружено около 2 тыс. подобных ресурсов. Более 50% обнаруженных ресурсов были размещены в зоне .RU. Неоднократно были замечены группы интернет-ресурсов со схожим содержанием и доменными именами. Как было упомянуто ранее, возможной причиной массового создания фишинговых ресурсов в зоне .RU может быть обусловлено сравнительно невысокой стоимостью доменного имени в данной зоне.



Для сбора денежных средств и конфиденциальной информации используются сайты-двойники, ориентированные на потенциальных посетителей существующих в действительности театров, стендап-шоу. Так, злоумышленники создают клоны сайта, осуществляющего продажу билетов на концерты StandUp Шоу «ТНТ». Также мошенники могут копировать оформление сайтов проектов, которые прекратили осуществление деятельности, или создавать сайты несуществующих учреждений культуры при использовании визуальных и текстовых материалов с нескольких сайтов театров или других учреждений. Следует отметить, что в данную категорию не входят сайты перекупщиков билетов – так называемых «консьерж-сервисов».

3.3. Способы введения пользователей в заблуждение

Отдельно следует рассмотреть способы, которые злоумышленники применяют для введения пользователей в заблуждение. Данные средства не

ограничены какой-либо тематической группой ресурсов:

- упоминание государственных праздников в качестве причины предоставления денежного вознаграждения и других благ. Так, в конце апреля 2023 года началось обнаружение сайтов, на которых пользователям обещалось получение выплат в честь Дня Победы, в мае 2023 года – в честь Дня России, в декабре 2023 года – к Новому году. Разработанные шаблоны продолжают использоваться злоумышленниками после того, как упоминаемое событие состоялось: к примеру, в августе 2023 года были выявлены мошеннические ресурсы, посвященные Дню России или продажа элитных продуктов к Новому году;
- создание ресурсов с предложениями, актуальными в определенный период времени (продажа билетов на самолет в летние месяцы и др.). К примеру, в июне-августе 2023 года увеличилось количество сайтов, на которых пользователи якобы могли купить билет на самолет; покупка билетов представляется актуальной в летние месяцы, когда многие пользователи оформляют отпуск;
- создание ресурсов, посвященных явлениям и событиям, активно обсуждаемым в СМИ. Один из примеров – инвестиционные платформы, на которых пользователям предлагается «заработать» на цифровом рубле. Введение цифрового рубля – значимое событие для российской экономики и общества, поэтому в 2023 году в средствах массовой информации неоднократно публиковались материалы, связанные с данной формой российской национальной валюты. Предполагается, что пользователь, посетивший сайт «инвестиционной платформы», знает о существовании понятия «цифровой рубль», но не осведомлен о его текущем статусе;
- имитация оформления официальных ресурсов СМИ. Отличия, на которые может обратить внимание пользователь – грамматические ошибки, а также лексические средства, нехарактерные для новостных заметок.

4. ДЕСТРУКТИВНЫЙ КОНТЕНТ

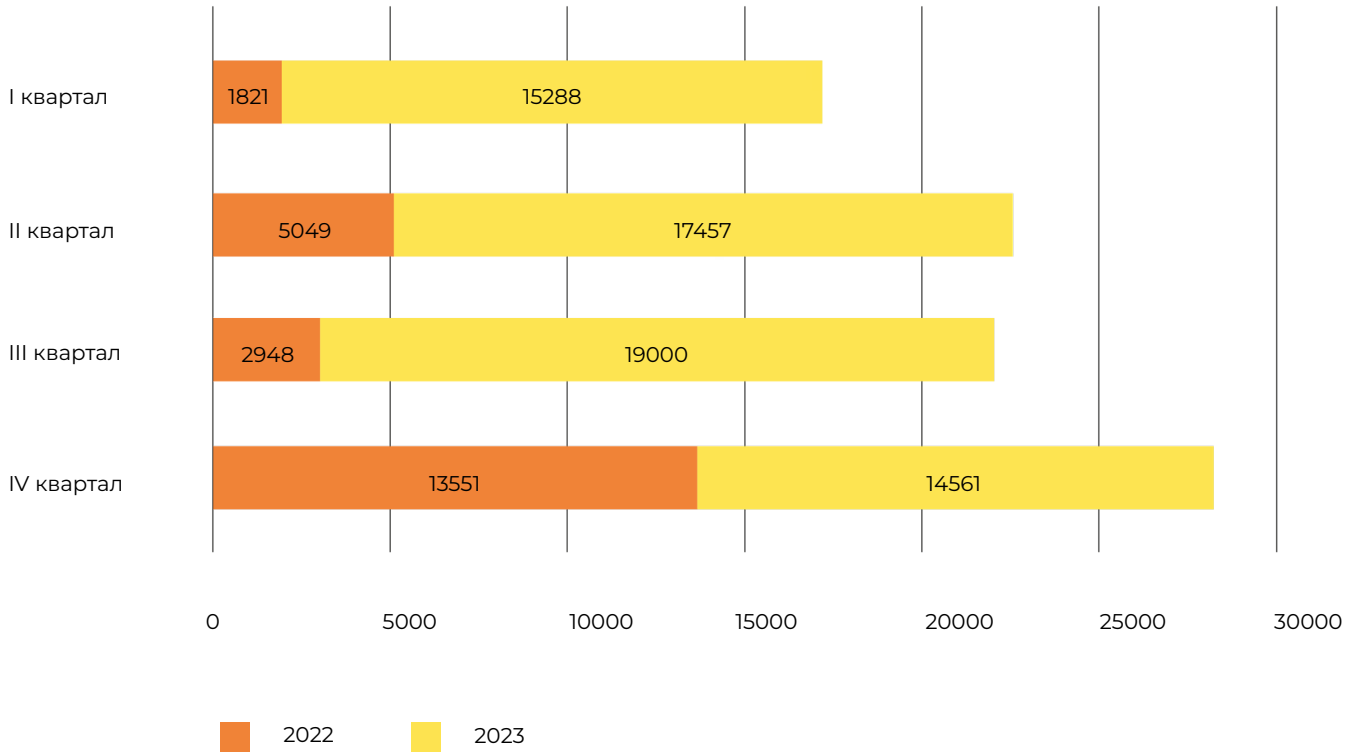
По состоянию на конец декабря 2023 года ИС «Антифишинг» было обнаружено около 66 тыс. ресурсов, применяемых для распространения недостоверной общественно значимой информации в сети «Интернет».

Основные характеристики деструктивного контента в 2023 г.:

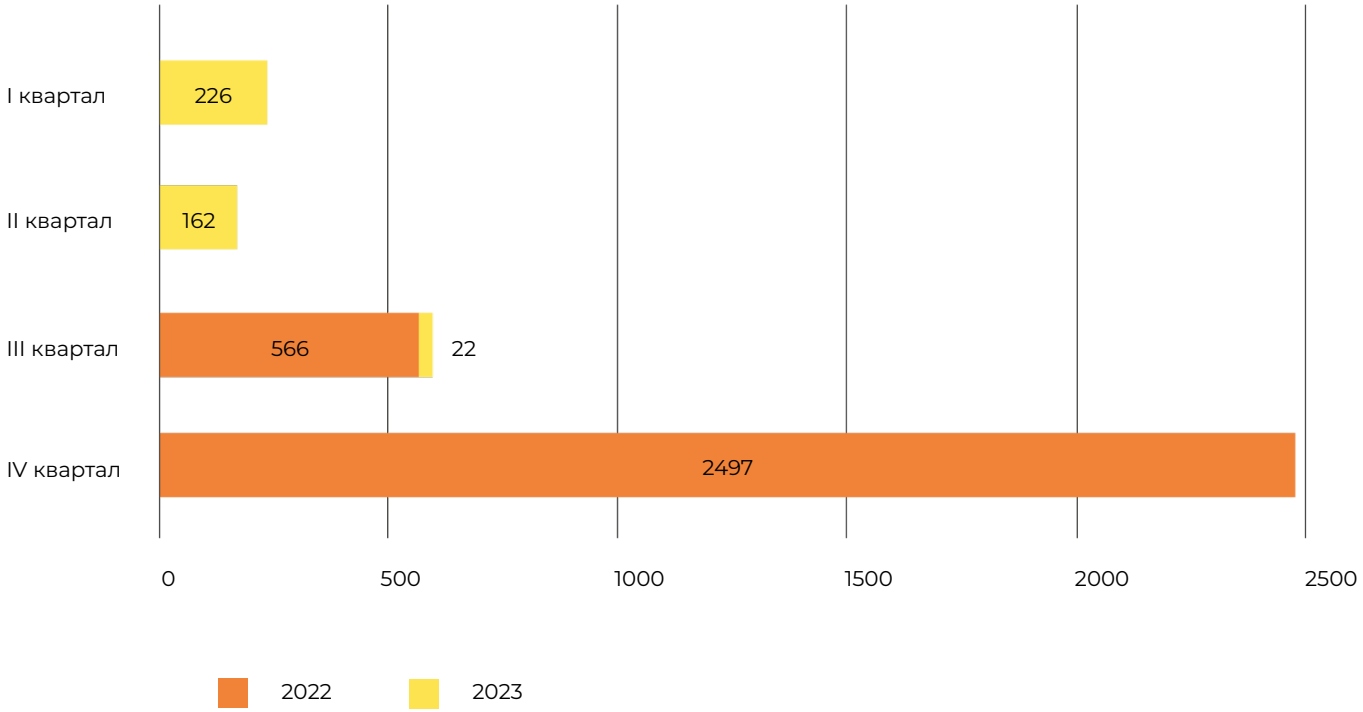
- **Распространение контента через социальные сети и мессенджеры.** Социальные сети, мессенджеры и платформы для размещения видеоматериалов используются в качестве канала массового распространения деструктивного контента;
- **Психологическое воздействие.** Для создания социальной напряженности распространяются материалы, цель которых – вызвать у потребителей информации такие эмоции, как гнев или страх (к примеру, потенциальными жертвами могут являться родственники военнослужащих, которым предлагается уточнить, является ли интересующий их гражданин военнопленным);

– **Распространение заведомо ложной информации.** Массовое распространение пропагандистских материалов, начатое в 2022 году, продолжается в 2023 году. Материалы распространяются в различных формах: в виде фотографий, видеороликов, записей и комментариев в социальных сетях, а также сайтов.

Сведения о количестве ресурсов с деструктивным контентом (СВО)



Сведения о количестве ресурсов с деструктивным контентом (Мобилизация)



Из информации, представленной на графиках, следует, что в 2023 году наблюдалось увеличение количества ресурсов с деструктивным контентом, тематически связанным с проведением специальной военной операции РФ.

Наибольшее количество интернет-ресурсов (2497 ресурсов), которые были посвящены мобилизации в РФ, было обнаружено в IV квартале 2022 года. Упомянутый «всплеск» связан с тем, что частичная мобилизация была объявлена в конце сентября 2022 года, что привлекло внимание создателей деструктивного контента. Повышенный интерес населения к вопросам, связанным с мобилизационными мероприятиями, был использован при попытках создания социальной напряженности на территории Российской Федерации. В 2023 году количество подобных ресурсов уменьшилось: общее количество обнаруженных за год ресурсов не превышает (410 ресурсов). За прошедший год у пользователей появилась возможность сбора разносторонней информации о мобилизационных мероприятиях, и связанный с ними деструктивный контент перестал использоваться вследствие падения эффективности психологического воздействия на потенциальных жертв.

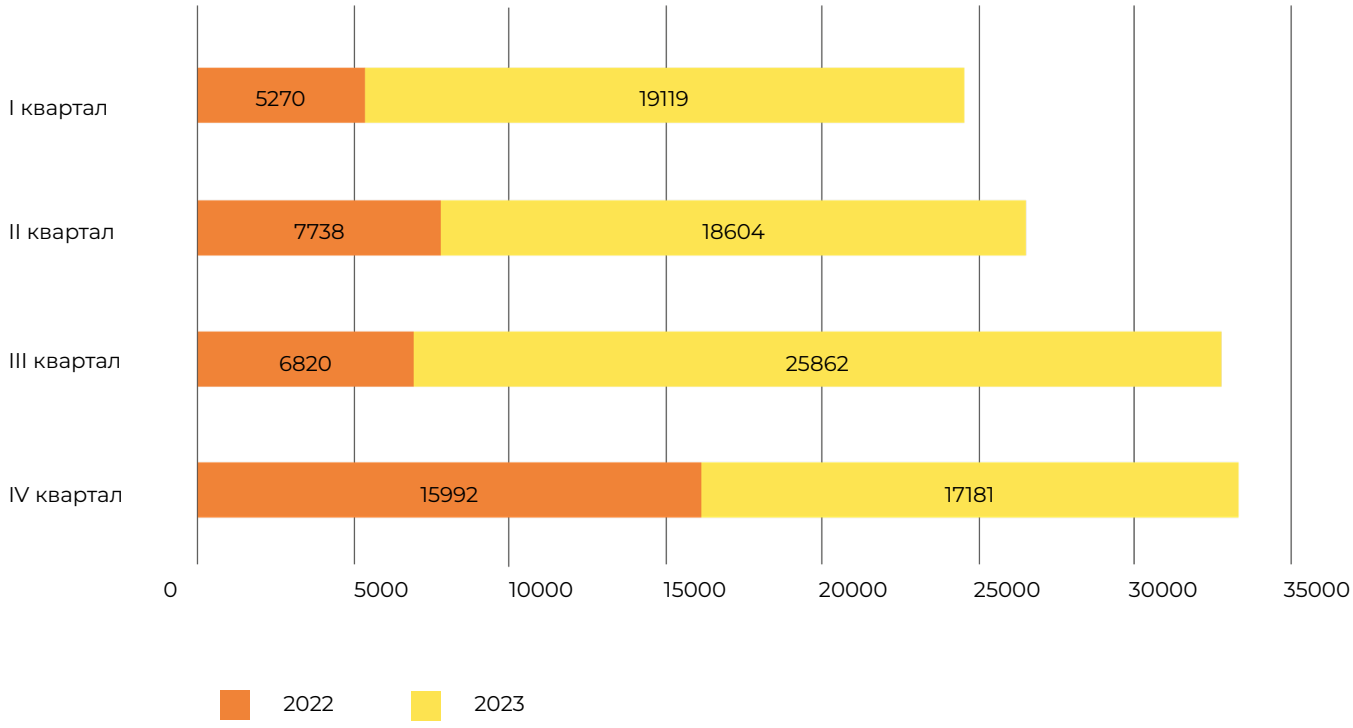
5. ЗАПРЕЩЕННЫЙ КОНТЕНТ

По состоянию на конец декабря 2023 года ФГБУ «НИИ «Интеграл» было обнаружено около 80 тыс. ресурсов, в материалах которых могут содержаться признаки нарушений законодательства Российской Федерации: изготовление и оборот поддельных документов, незаконный сбыт наркотических веществ и др.

Основные характеристики запрещенного контента в 2023 г.:

- **Распространение контента через форумы.** Незаконное приобретение и оборот поддельных документов, оружия и наркотических веществ зачастую происходит через различные теневые платформы и форумы.
- **Постоянное обновление третьего уровня домена.** Ресурсы с запрещенным контентом в большинстве случаев размещены на третьих уровнях доменного имени. После блокировки создатели подобных сайтов создают другой домен третьего уровня и продолжают нелегальную на территории РФ деятельность.
- **Упоминание способов теневой покупки.** На сайтах по приобретению нелегальной продукции могут быть размещены рекомендации по установке программного обеспечения и описания других способов, якобы позволяющим пользователям совершить противоправные действия без преследования со стороны правоохранительных органов.

Сведения о количестве ресурсов с запрещенным контентом



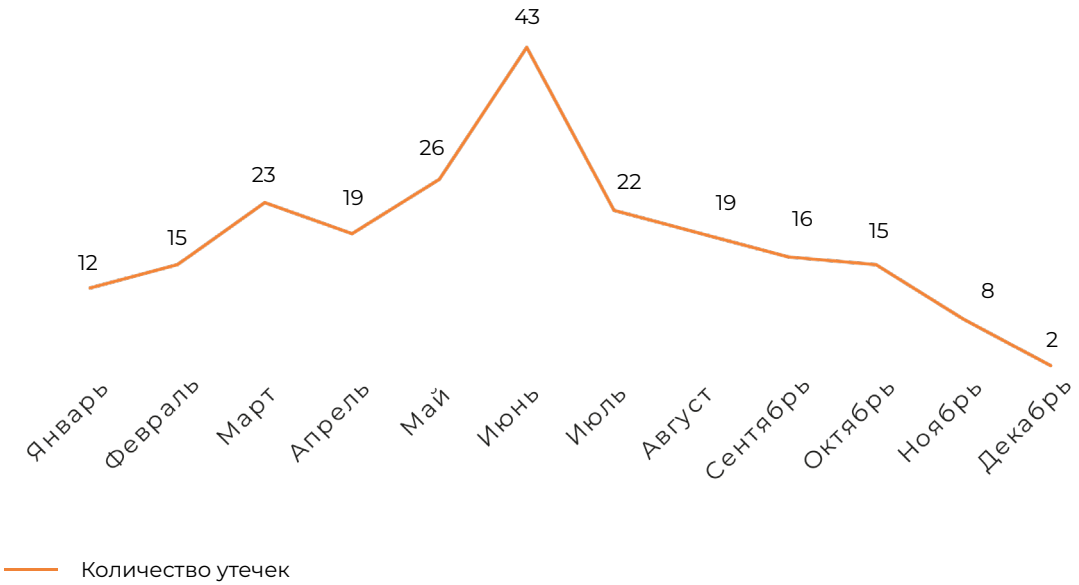
Следует отметить, что по сравнению с 2022 годом, в 2023 году отмечается увеличение количества выявленных ресурсов с запрещенным контентом в 3–4 раза.

Злоумышленники реагируют на происходящие в мире события. В случае, если событие или явление перестает играть важную роль для их потенциальных жертв, мошенники прекращают создание соответствующих интернет-ресурсов. Так, в 2023 году было обнаружено меньше ресурсов, тематически связанных с коронавирусной инфекцией, чем в 2022 году. Коронавирусная инфекция стала значительно реже упоминаться в русскоязычном информационном поле; кроме того, был снят ряд ограничений, которые были введены с целью предотвращения распространения коронавирусной инфекции. Представляется, что в силу указанных обстоятельств мошеннические интернет-ресурсы, содержащие упоминания коронавирусной инфекции, стали менее эффективным инструментом для злоумышленников.

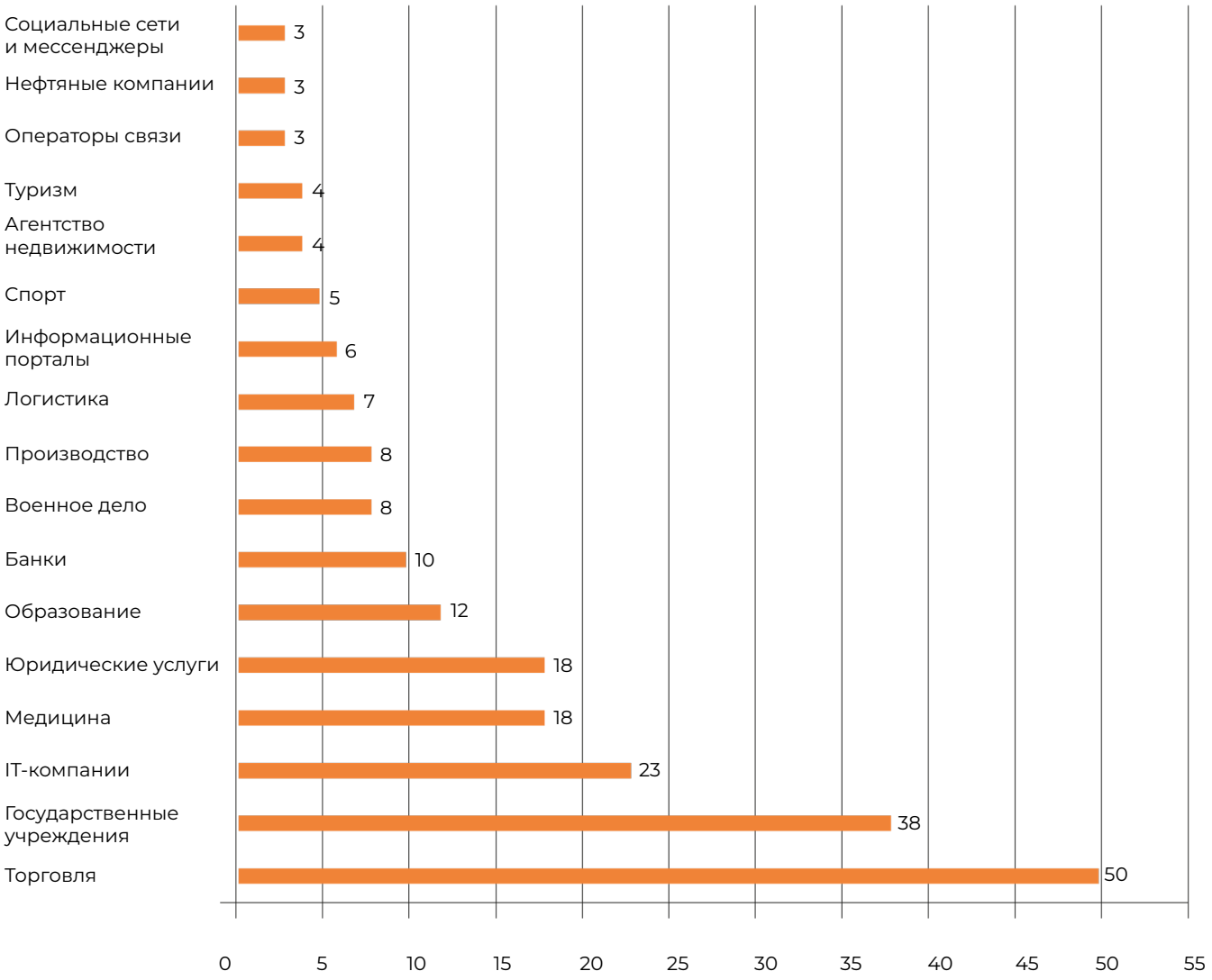
6. УТЕЧКИ ДАННЫХ

С января по декабрь 2023 года ФГБУ «НИИ «Интеграл» было обнаружено 200 утечек данных, касающихся граждан Российской Федерации. Общий объем опубликованных данных составил 230 гигабайт (при подсчете веса данные находились в сжатом состоянии). Наибольшее количество утечек данных выявлено в июне 2023 года.

Сведения о количестве обнаруженных утечек данных (2023 г.)



Распределение утечек по отраслям



Распределение утечек персональных данных по отраслям представлены на графике.

В 86% случаев произошла утечка баз данных. Оставшиеся 14% – это файлы и документы, в которых информация представлена в другой форме (к примеру, в виде изображения, таблицы и т.д.).

Утечка данных могла сопровождаться кибератакой, в ходе которой злоумышленники, получившие доступ к сайту пострадавшей организации, осуществляли замену содержимого страниц сайта (дефейс). Тем не менее, дефейс сайта совершался менее чем в 5% случаев.

Размещенные в публичном доступе базы данных за 2023 год содержат в общей сложности более 400 млн строк, в том числе 91,3 млн адресов электронной почты и 144,7 млн телефонных номеров.

ВЫВОДЫ

В 2023 году было обнаружено на 70% больше ресурсов, чем в 2022 году. Для введения пользователей в заблуждение пользователи не только создавали ресурсы-двойники официальных сайтов организаций, но и сайты несуществующих организаций и проектов (к примеру, учреждений культуры и кредитных организаций). Цель создателей фишинговых ресурсов, как правило, было получение доступа к учетной записи жертвы (в социальных сетях, на сайтах реально существующих организаций и т.д.), а также компрометация данных банковской карты пользователя.

Количество фишинговых ресурсов постоянно увеличивается: автоматизация процессов создания сайтов позволяет злоумышленникам использовать множество однотипных ресурсов для введения пользователей в заблуждение. Кроме того, шаблоны фишинговых ресурсов могут быть использованы злоумышленниками, не являющимися высококвалифицированными дизайнерами и разработчиками. Указанные обстоятельства также могут привести к увеличению количества пользователей-жертв. Кроме того, для распространения как фишинговых ресурсов, так и других представляющих угрозу для пользователей ресурсов и сведений используются социальные сети и мессенджеры. Распространение информации в различных формах и через несколько каналов связи также может привести к увеличению количества случаев введения пользователей в заблуждение и совершения противоправных действий.

Особую обеспокоенность вызывают попытки злоумышленников сделать ресурс доступным только для потенциальных жертв, скрывая содержимое от сторонних пользователей. Кроме того, создатели фишинговых ресурсов стремятся избежать обнаружения ресурсов специалистами по информационной безопасности (к примеру, при помощи генерации произвольных доменных имен, тематически не связанных с содержимым ресурса). Представляется, что в 2024 году злоумышленники будут разрабатывать новые способы, позволяющие избежать обнаружения ресурсов, используемых для совершения противоправной деятельности, лицами, способными оказать содействие в прекращении делегирования доменного имени или ограничения доступа.

В 2023 году было обнаружено 200 утечек данных. Лидером по количеству жертв, у которых были похищены данные организаций и граждан, стала сфера торговли. Злоумышленники проявляют интерес к данной сфере не только при создании фишинговых ресурсов, но и выборе жертв для массовой кражи данных. Повышенный интерес к сфере торговли объясняется растущей популярностью заказов товаров и услуг онлайн, в результате чего пользователи добровольно предоставляют компаниям информацию о себе. На втором месте находятся государственные учреждения, на третьем – организации, ведущие деятельность в сфере информационных технологий. Государственные учреждения – одна из приоритетных целей западных и украинских хакеров; кража подобных данных используется как возможное доказательство некомпетентности лиц, работающих в органах государственной власти. Для компаний, деятельность которых связана с информационными технологиями, утечка данных может нести существенные репутационные риски: граждане могут избегать прибегать к услугам компании, которая не способна защитить данные своих клиентов.

По сравнению с 2022 годом было обнаружено в 7-8 раз больше ресурсов с деструктивным и запрещенным контентом. Создатели ресурсов заинтересованы в продаже товаров и оказании услуг, запрещенных на территории Российской Федерации: продаже наркотических веществ, оружия, поддельных документов и персональных данных. Лица, создающие деструктивный контент, реагируют на происходящие на территории Российской Федерации и за рубежом события, создавая новые материалы с недостоверной информацией. Наибольший интерес для злоумышленников представляют события и сферы жизни, упоминание которых может быть эффективно использовано для оказания психологического воздействия на пользователя (провоцирование таких эмоций, как страх или гнев).

минцифры_

Интеграл

ФГБУ «НИИ «Интеграл»

111024, г. Москва, ул. Авиамоторная, д. 26
тел. +7(495) 673-40-30 факс +7(495) 673-18-32
e-mail: integral@indepo.ru

Москва
2024