Кировское областное государственное общеобразовательное бюджетное учреждение «Средняя школа с углубленным изучением отдельных предметов г.Кирс Верхнекамского района» Кировской области

**ИССЛЕДОВАТЕЛЬСКИЙ ПРОЕКТ**

**«Интернет-мошенничество»**

Проект подготовил: Половников Тимофей,

ученик 9 Г класса

Руководитель проекта: Конышев Алексей Сергеевич, учитель информатики

Кирс,

2022 год

# Содержание

[1. Введение 3](#_Toc100598600)

[2. Обзор литературы 5](#_Toc100598601)

[2.1. Что такое интернет мошенничество? 5](#_Toc100598602)

[2.1.1.Интернет-мошенничество 5](#_Toc100598603)

[2.1.2. Социальная инженерия 5](#_Toc100598604)

[2.2. История распространения интернет-мошенничества 6](#_Toc100598605)

[2.3. Основные виды интернет мошенничества: 7](#_Toc100598606)

[2.3.1.Фишинг 7](#_Toc100598607)

[2.3.2.Фарминг 11](#_Toc100598608)

[2.3.3.Претекстинг 12](#_Toc100598609)

[2.3.4. Интернет-магазины 13](#_Toc100598610)

[2.3.5. Нигерийские письма 14](#_Toc100598611)

2.3.6. [Киберскво́ттинг 15](#_Toc100598612)

2.3.7. [Тайпскво́ттинг 15](#_Toc100598613)

[2.4. Меры предосторожности 15](#_Toc100598614)

[3. Практическая часть 18](#_Toc100598615)

[3.1. Опрос учащихся 18](#_Toc100598616)

[3.2. Разбор конкретного примера мошенничества в сети 19](#_Toc100598617)

[3.3. Что грозит за мошенничество в интернете? 20](#_Toc100598618)

4. [Заключение 22](#_Toc100598619)

5. [Литература 23](#_Toc100598620)

6. [Приложение 24](#_Toc100598621)

# 1. Введение

Мошенничество в сети интернет стало одним из самых распространённых видов мошенничества. Дело в том, что одновременно с прогрессом, на два шага вперед развиваются способы обмана обычных пользователей. Это достаточно обширная проблема, ведь Интернет - это огромная паутина захватившая весь мир. И в ней можно оставаться анонимным, поэтому процент раскрытия преступлений очень невелик. Чаще всего на обман ведутся люди, которые не осведомлены о уловках злоумышленника – это пожилые и дети. Однако благодаря хорошему информированию о новых способах мошенничества, становиться все меньше и меньше жертв.

**Актуальность**

Интернет всё больше проникает в нашу жизнь. Сложно представить обычного школьника без телефона и интернета. По интернету мы общаемся, совершаем покупки и ищем какую-либо информацию. С широким распространением интернета появилось интернет-мошенничество, которое развивается быстрыми темпами. Поэтому я считаю, что эта проблема актуальна в наши дни.

**Проблема:**

Мошенничество в сети интернет стало одним из самых распространённых видов мошенничества.

**Гипотеза:**

Можно избежать обмана в сети интернет, если люди будут больше знать об его угрозах. Необходимо соблюдать правила, чтобы не попасться на уловки мошенников в Интернете.

**Цели:**

Ознакомить сверстников с правилами поведения в интернете и перестать вестись на обман.

**Задачи:**

1. Изучить виды мошенничества

2. Изучить меры предосторожности

3. Провести и проанализировать опрос учащихся

4. Разобрать конкретный пример мошенничества в сети

**Методы исследования:**

Поиск, анализ, обобщение информации в интернете, опрос учащихся.

# 2. Обзор литературы

## 2.1. Что такое интернет мошенничество?

### 2.1.1.Интернет-мошенничество

**Интернет-мошенничество** (Электронное мошенничество) — вид [мошенничества](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE) с использованием [Интернета](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82). Оно может включать в себя скрытие информации или предоставление неверной информации с целью вымогательства у жертв денег, имущества и наследства. Интернет-мошенничество не считается отдельным преступлением, а включает ряд незаконных действий, совершаемых в [киберпространстве](https://ru.wikipedia.org/wiki/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D1%81%D1%82%D0%B2%D0%BE). Однако оно отличается от [кражи](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B0%D0%B6%D0%B0), поскольку в этом случае жертва добровольно и сознательно предоставляет преступнику информацию, деньги или имущество. Оно также отличается тем, что в нём участвуют правонарушители, разделенные во времени и пространстве.

Согласно отчёту [ФБР](https://ru.wikipedia.org/wiki/%D0%A4%D0%91%D0%A0) о преступлениях в Интернете за 2019 год, Центр жалоб о преступлениях в Интернете получил более 467 тысяч жалоб. Жертвы потеряли более 3,5 млрд долларов из-за онлайн-мошенничества в 2019 году. Согласно исследованию, проведённому Центром стратегических и международных исследований и [McAfee](https://ru.wikipedia.org/wiki/McAfee" \o "McAfee), [киберпреступность](https://ru.wikipedia.org/wiki/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C" \o "Киберпреступность) обходится мировой экономике в 600 млрд долларов, что составляет 0,8 % от общего мирового [ВВП](https://ru.wikipedia.org/wiki/%D0%92%D0%92%D0%9F). Мошенничество в Интернете проявляется во многих формах: от почтового спама до онлайн-жульничества.

### 2.1.2. Социальная инженерия

**Социальная инженерия** — в контексте [информационной безопасности](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C) — психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации. Следует отличать от понятия [социальной инженерии](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D1%8F_(%D1%81%D0%BE%D1%86%D0%B8%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F)) в социальных науках — которое не касается разглашения конфиденциальной

информации. Совокупность уловок с целью сбора информации, подделки

или несанкционированного доступа от традиционного «мошенничества» отличается тем, что часто является одним из многих шагов в более сложной схеме мошенничества.

Мошенники изыскивают все новые и новые варианты «заработка». Я опишу наиболее распространенные из них, но читатели должны понимать, что только внимание к деталям и ответственное отношение к деньгам может по-настоящему защитить от уловок непорядочных людей. Итак, давайте приступим к детальному изучению вопроса, какие есть виды мошенничества в интернете.

## 2.2. История распространения интернет-мошенничества

Интернет-мошенничество появилось во времена, когда интернет стал

массово входить в каждый дом. В 90-х годах прошлого столетия, с появлением доступа к персональным компьютерам и внедрения Интернета в широкие массы населения, появилась не только положительная сторона в быстром получении информации, но и угроза, вызванная действиями интернет-мошенниками (смотреть приложение. Рис 1). Как правило в этот период мошенники завоевывали незаконным путем личные данные пользователей Интернет:

* логины и пароли для подключения к сети Интернет по средствам Dial-up (телефонные линии), для его использования за счет своих жертв;
* логины и пароли от почтовых ящиков, для хищения информации из электронных писем.

В 2000-е годы с массовым внедрением банковских карт и способностьюих онлайн оплаты, появилось экономическое мошенничество, ее целью является хищение информации о банковской

карте (номер карты, срок действия, фамилии и имени держателя, а также секретного кода CVC) жертвы, для осуществления платежа или перевода денежных средств в карманмошеннику.С появлением интернет-магазинов, а также различных площадок с объявлениями в Интернете, мошенники так же нашли способ обманывать своих жертв продавая отличный от описания, либо несоответствующего качество, в других случаях и вовсе несуществующий товар. Массовая регистрация и пользование социальными сетями, так же нашло применение для корыстных целей мошенников. Злоумышленники стали пользоваться чувствами людей, такими как жалость и доверчивость. В социальных сетях публикуются объявления о помощи больным детям и письма с просьбой о помощи от родственников, знакомых, вместо которых сидит мошенник и просит деньги в виде перевода на карту или иную банковскую систему.

## 2.3. Основные виды интернет мошенничества:

### 2.3.1.Фишинг

**Фи́шинг** — вид [интернет-мошенничества](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE_%D0%B2_%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5), целью которого является получение [доступа к конфиденциальным данным](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D1%81%D0%B0%D0%BD%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF) [пользователей](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C) — [логинам](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%B3%D0%B8%D0%BD_(%D1%83%D1%87%D1%91%D1%82%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D1%8C)) и паролям. Это достигается путём проведения [массовых рассылок](https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B0%D0%BC) [электронных писем](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%87%D1%82%D0%B0) от имени популярных [брендов](https://ru.wikipedia.org/wiki/%D0%91%D1%80%D0%B5%D0%BD%D0%B4), а также личных сообщений внутри различных сервисов, например, от имени банков или внутри [социальных сетей](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C_(%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)). В письме часто содержится прямая ссылка на [сайт](https://ru.wikipedia.org/wiki/%D0%A1%D0%B0%D0%B9%D1%82), внешне неотличимый от настоящего, либо на сайт с [редиректом](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%BD%D0%B0%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_URL" \o "Перенаправление URL). После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к [аккаунтам](https://ru.wikipedia.org/wiki/%D0%90%D0%BA%D0%BA%D0%B0%D1%83%D0%BD%D1%82) и банковским счетам. Фишинг — одна из разновидностей [социальной инженерии](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D1%8F), основанная на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее.

Для защиты от фишинга производители основных интернет-[браузеров](https://ru.wikipedia.org/wiki/%D0%91%D1%80%D0%B0%D1%83%D0%B7%D0%B5%D1%80" \o "Браузер) договорились о применении одинаковых способов информирования пользователей о том, что они открыли подозрительный сайт, который может принадлежать мошенникам. Новые версии браузеров уже обладают такой возможностью, которая соответственно именуется «антифишинг».

**Борьба с фишингом. Обучение пользователей**

Один из методов борьбы с фишингом заключается в том, чтобы научить людей различать фишинг и бороться с ним. Люди могут снизить угрозу фишинга, немного изменив своё поведение. Так, в ответ на письмо с просьбой «подтверждения» учётной записи (или любой другой обычной просьбой фишеров) специалисты советуют связаться с компанией, от имени которой отправлено сообщение, для проверки его подлинности. Кроме того, эксперты рекомендуют самостоятельно вводить веб-адрес организации в адресную строку браузера вместо использования любых [гиперссылок](https://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%BF%D0%B5%D1%80%D1%81%D1%81%D1%8B%D0%BB%D0%BA%D0%B0) в подозрительном сообщении.

Практически все подлинные сообщения организаций содержат в себе упоминание некой информации, недоступной для фишеров. Некоторые, например, [PayPal](https://ru.wikipedia.org/wiki/PayPal" \o "PayPal), всегда обращаются к своим адресатам по именам, а письмо с общим обращением «Уважаемый клиент PayPal» может расцениваться как попытка фишинга. Письма от банков и кредитных учреждений часто содержат в себе часть номера счёта. Однако недавние исследования показали, что люди не различают появление первых цифр счёта или последних цифр, в то время как первые цифры могут быть одинаковы для всех клиентов финансового учреждения. Людям можно

объяснить, что подозрительны любые письма, не содержащие какой-либо конкретной личной информации. Но фишинговые атаки начала 2006 года содержали подобную [персональную информацию](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5), следовательно, наличие подобной информации не гарантирует безопасность сообщения. Кроме того, по результатам другого исследования было выяснено, что присутствие личной информации существенно не изменяет процент успеха фишинговых атак, что свидетельствует о том, что большинство людей вообще не обращает внимания на подобные детали.

**Технические методы**

**Браузеры, предупреждающие об угрозе фишинга**

Другим направлением борьбы с фишингом является создание списка фишинговых сайтов и последующая сверка с ним. Подобная система существует в браузерах [InternetExplorer](https://ru.wikipedia.org/wiki/Internet_Explorer), [MozillaFirefox](https://ru.wikipedia.org/wiki/Mozilla_Firefox), [GoogleChrome](https://ru.wikipedia.org/wiki/Google_Chrome), [Safari](https://ru.wikipedia.org/wiki/Safari) и [Opera](https://ru.wikipedia.org/wiki/Opera). Firefox использует антифишинговую систему [Google](https://ru.wikipedia.org/wiki/Google_(%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F)" \o "Google (компания)). Opera использует чёрные списки [PhishTank](https://ru.wikipedia.org/wiki/PhishTank" \o "PhishTank) и [GeoTrust](https://ru.wikipedia.org/w/index.php?title=GeoTrust&action=edit&redlink=1" \o "GeoTrust (страница отсутствует)) и списки исключений GeoTrust. По результатам независимого исследования 2006 года Firefox был признан более эффективным в обнаружении фишинговых сайтов, чем InternetExplorer. В 2006 году появилась методика использования специальных [DNS](https://ru.wikipedia.org/wiki/DNS)-сервисов, фильтрующих известные фишинговые адреса: этот метод работает при любом браузере и близок использованию [hosts](https://ru.wikipedia.org/wiki/Hosts)-файла для блокировки рекламы.

**Усложнение процедуры авторизации**

Сайт [BankofAmerica](https://ru.wikipedia.org/wiki/Bank_of_America" \o "Bank of America) предлагает пользователям выбрать личное изображение и показывает это выбранное пользователем изображение с каждой формой ввода пароля. И пользователям банковских услуг следует

вводить пароль лишь тогда, когда они видят выбранное изображение. Однако недавнее исследование показало, что отсутствие изображения не останавливает большинство пользователей при вводе пароля.

**Борьба с фишингом в почтовых сообщениях**

Специализированные [спам-фильтры](https://ru.wikipedia.org/wiki/E-mail_%D1%84%D0%B8%D0%BB%D1%8C%D1%82%D1%80%D0%B0%D1%86%D0%B8%D1%8F) могут уменьшить число фишинговых электронных сообщений, получаемых пользователями. Эта методика основывается на [машинном обучении](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%88%D0%B8%D0%BD%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) и [обработке естественного языка](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%BA%D0%B0_%D0%B5%D1%81%D1%82%D0%B5%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE_%D1%8F%D0%B7%D1%8B%D0%BA%D0%B0) при анализе фишинговых писем.

**Услуги мониторинга**

Некоторые компании предлагают банкам и прочим организациям, потенциально подверженным фишинговым атакам, услуги круглосуточного контроля, анализа и помощи в закрытии фишинговых сайтов. [Физические лица](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%B7%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B5_%D0%BB%D0%B8%D1%86%D0%BE) могут помогать подобным группам, сообщая о случаях фишинга.

Юридические меры

26 января 2004 года Федеральная комиссия по торговле США подала первый иск против подозреваемого в фишинге. Ответчик, подросток из [Калифорнии](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BB%D0%B8%D1%84%D0%BE%D1%80%D0%BD%D0%B8%D1%8F), обвинялся в создании веб-страницы, внешне схожей с сайтом [AOL](https://ru.wikipedia.org/wiki/AOL), и краже данных кредитных карт. Другие страны последовали этому примеру и начали искать и арестовывать фишеров. Так, в [Бразилии](https://ru.wikipedia.org/wiki/%D0%91%D1%80%D0%B0%D0%B7%D0%B8%D0%BB%D0%B8%D1%8F) был арестован Вальдир Пауло де Альмейда, глава одной из крупнейших фишинговых [преступных группировок](https://ru.wikipedia.org/wiki/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C), в течение двух лет укравшей от 18 до 37 миллионов долларов США. В июне 2005 года власти [Великобритании](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%BE%D0%B1%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D1%8F) осудили двух участников интернет-мошенничества. В 2006 году японской полицией было задержано восемь человек по подозрению в фишинге и краже 100 миллионов иен. Аресты продолжались в 2006 году — в ходе спецоперации [ФБР](https://ru.wikipedia.org/wiki/%D0%A4%D0%91%D0%A0) задержало банду из шестнадцати участников в Европе и США.

В Соединённых Штатах Америки 1 марта 2005 года [сенатор](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D0%BD%D0%B0%D1%82%D0%BE%D1%80_%D0%A1%D0%A8%D0%90) [Патрик Лехи](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%82%D1%80%D0%B8%D0%BA_%D0%9B%D0%B5%D1%85%D0%B8) представил [Конгрессу](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D0%B3%D1%80%D0%B5%D1%81%D1%81_%D0%A1%D0%A8%D0%90) проект Антифишингового закона. Если бы этот

законопроект был принят, то преступники, создающие фальшивые веб-сайты и рассылающие поддельную электронную почту, подвергались бы штрафу до 250 тысяч долларов и лишению свободы сроком до пяти лет. В

Великобритании был принят Закон о мошенничестве 2006 года, предусматривающий ответственность за [мошенничество](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE) в виде тюремного заключения сроком до 10 лет, а также запрещающий владение или разработку фишинговых инструментов для совершения мошенничества.

### 2.3.2.Фарминг

В классическом [фишинге](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3" \o "Фишинг) злоумышленник распространяет письма электронной почты среди пользователей [социальных сетей](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C), онлайн-банкинга, почтовых веб-сервисов, заманивая на поддельные сайты пользователей, ставших жертвой обмана, с целью получения их логинов и паролей. Многие пользователи, активно использующие современные веб-сервисы, не раз сталкивались с подобными случаями фишинга и проявляют осторожность к подозрительным сообщениям. В схеме классического фишинга основным «слабым» звеном, определяющим эффективность всей схемы, является зависимость от пользователя — поверит он фишеру или нет. При этом с течением времени повышается информированность пользователей о фишинговых атаках. Банки, социальные сети, прочие веб-службы предупреждают о разнообразных мошеннических приемах с использованием методов социальной инженерии. Все это снижает количество откликов в фишинговой схеме — все меньше пользователей удается завлечь обманным путём на поддельный сайт. Поэтому злоумышленники придумали механизм скрытого перенаправления пользователей на фишинговые сайты, получивший название фарминга. Злоумышленник распространяет на компьютеры пользователей специальные вредоносные программы, которые после запуска на компьютере перенаправляют обращения к заданным сайтам на поддельные сайты. Таким образом, обеспечивается высокая скрытность атаки, а участие пользователя сведено к минимуму — достаточно дождаться, когда пользователь решит посетить интересующие злоумышленника сайты.

Вредоносные программы, реализующие фарминг-атаку, используют два основных приема для скрытного перенаправления на поддельные сайты — манипулирование файлом HOSTS или изменением информации DNS.

**Способы защиты:**

Способов абсолютной защиты от фарминг-атак не существует, поэтому необходимо использовать профилактические меры:

- Использовать и регулярно обновлять лицензионное антивирусное программное обеспечение.

- Использовать защиту электронного почтового ящика (отключить предварительный просмотр).

- Не открывать и не загружать вложения электронных писем от незнакомых и сомнительных адресатов.

### 2.3.3.Претекстинг

**Претекстинг**— атака, в которой злоумышленник представляется другим человеком и по заранее подготовленному сценарию узнает конфиденциальную информацию. Эта атака подразумевает должную подготовку, как то: день рождения, ИНН, номер паспорта либо последние цифры счета, для того, чтобы не вызвать подозрений у жертвы. Обычно реализуется через телефон или электронную почту.

**2.3.3.1. Квид про кво**

**Квид про кво** - вид атаки подразумевает обращение злоумышленника в компанию по корпоративному телефону (используя [актёрское мастерство](https://ru.wikipedia.org/wiki/%D0%90%D0%BA%D1%82%D1%91%D1%80%D1%81%D0%BA%D0%BE%D0%B5_%D0%B8%D1%81%D0%BA%D1%83%D1%81%D1%81%D1%82%D0%B2%D0%BE)) или электронной почте. Зачастую злоумышленник представляется сотрудником технической поддержки, который сообщает о возникновении технических проблем на рабочем месте сотрудника и предлагает помощь в их устранении. В процессе «решения» технических проблем злоумышленник вынуждает цель атаки совершать действия, позволяющие атакующему запускать команды или устанавливать различное программное обеспечение на компьютере жертвы.

Проведенное в [2003 году](https://ru.wikipedia.org/wiki/2003_%D0%B3%D0%BE%D0%B4) исследование в рамках программы [Информационная безопасность](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C) показало, что 90 % офисных работников готовы разгласить конфиденциальную информацию, например свои пароли, за какую-либо услугу или вознаграждение.

### 2.3.4. Интернет-магазины

Мошенничество в Интернете довольно часто начинается с интернет-магазинов. На сайте какого-либо магазинчика вам будет предложено купить товар по низким ценам. Особенно привлекательно это тогда, когда Вы можете купить эксклюзивный товар по заниженной стоимости. Далее существует несколько видов обмана. Первый и самый откровенный — это оплата покупки полностью или предоплата до получения. После того как вы перечислите деньги на счет мошенника, он просто исчезает и не выходит на связь. Любые попытки связаться с администрацией терпят неудачу. Второй исход менее неприятный. Вы оплачиваете покупку, а взамен получаете или подделку, или какую-нибудь ерунду, которую вы и вовсе не заказывали. И снова все попытки связаться с продавцом терпят неудачи.

### 2.3.5. Нигерийские письма

**«Нигери́йские пи́сьма»**  — распространённый вид [мошенничества](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE), типа [писем счастья](https://ru.wikipedia.org/wiki/%D0%9F%D0%B8%D1%81%D1%8C%D0%BC%D0%B0_%D1%81%D1%87%D0%B0%D1%81%D1%82%D1%8C%D1%8F), получивший наибольшее развитие с появлением массовых рассылок по [электронной почте](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%87%D1%82%D0%B0) ([спама](https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B0%D0%BC)). Письма названы так потому, что особое распространение этот вид мошенничества получил в [Нигерии](https://ru.wikipedia.org/wiki/%D0%9D%D0%B8%D0%B3%D0%B5%D1%80%D0%B8%D1%8F), причём ещё до распространения [Интернета](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82), когда такие письма распространялись по обычной почте. Однако нигерийские письма приходят и из других африканских стран, а также из городов с большой нигерийской диаспорой ([Лондон](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BD%D0%B4%D0%BE%D0%BD), [Амстердам](https://ru.wikipedia.org/wiki/%D0%90%D0%BC%D1%81%D1%82%D0%B5%D1%80%D0%B4%D0%B0%D0%BC), [Мадрид](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D0%B4%D1%80%D0%B8%D0%B4), [Дубай](https://ru.wikipedia.org/wiki/%D0%94%D1%83%D0%B1%D0%B0%D0%B9_(%D0%B3%D0%BE%D1%80%D0%BE%D0%B4))). Рассылка писем началась в середине [1980-х](https://ru.wikipedia.org/wiki/1980-%D0%B5) гг.

Как правило, мошенники просят у получателя письма помощи в многомиллионных денежных операциях, обещая солидные проценты с сумм. Если получатель согласится участвовать, у него постепенно выманиваются всё более крупные суммы денег якобы на оформление сделок, уплату сборов, взятки чиновникам, и т. П.

Нигерийские письма — один из самых распространённых видов мошенничества в интернете.

### 2.3.6. Киберскво́ттинг

**Киберскво́ттинг** — регистрация [доменных имён](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B5%D0%BD%D0%BD%D0%BE%D0%B5_%D0%B8%D0%BC%D1%8F), содержащих торговую марку, принадлежащую другому лицу, с целью их дальнейшей перепродажи или недобросовестного использования. Люди, практикующие такие действия, называются киберскво́ттерами.

В СМИ часто путают киберсквоттинг с [домейнингом](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B5%D0%B9%D0%BD%D0%B8%D0%BD%D0%B3" \o "Домейнинг) (регистрация доменных имён, не содержащих торговую марку, с целью дальнейшей перепродажи).

### 2.3.7. Тайпскво́ттинг

**Тайпскво́ттинг** — регистрация [доменных имён](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B5%D0%BD%D0%BD%D0%BE%D0%B5_%D0%B8%D0%BC%D1%8F), близких по написанию с адресами популярных сайтов в расчёте на [ошибку](https://ru.wikipedia.org/wiki/%D0%9E%D1%88%D0%B8%D0%B1%D0%BA%D0%B0) части [пользователей](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C). Например, «wwwsite.example» в расчёте на пользователя, который хотел попасть на «www.site.example».

При близости к очень популярным доменам тайпосквоттер может собрать на своём [сайте](https://ru.wikipedia.org/wiki/%D0%A1%D0%B0%D0%B9%D1%82) достаточно большой [процент](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%86%D0%B5%D0%BD%D1%82) «промахнувшихся» посетителей и заработать за счёт показа [рекламы](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%BA%D0%BB%D0%B0%D0%BC%D0%B0). Или, если пользователь собрался ввести логин и пароль на оригинальном сайте, а [ввёл их на подложном](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3), то тайпосквоттер-злоумышленник может получить эти данные для дальнейшего несанкционированного доступа к чужой информации. В большинстве развитых стран тайпсквоттинг [торговых марок](https://ru.wikipedia.org/wiki/%D0%A2%D0%BE%D0%B2%D0%B0%D1%80%D0%BD%D1%8B%D0%B9_%D0%B7%D0%BD%D0%B0%D0%BA), как и их [киберсквоттинг](https://ru.wikipedia.org/wiki/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D1%81%D0%BA%D0%B2%D0%BE%D1%82%D1%82%D0%B8%D0%BD%D0%B3" \o "Киберсквоттинг), является незаконной деятельностью и запрещается различными постановлениями и законами о продажах.

## 2.4. Меры предосторожности

Основными признаками мошенничества являются:

- навязчивая реклама, обещающая огромный доход без вложения знаний и большого труда;

- требование ввода ваших персональных данных на сомнительных ресурсах;

- требование отправки смс;

- заманчивые предложения, приходящие через почту от незнакомых людей. Как правило, это спам разосланный многим с цель на ком-нибудь поживиться.

5 предлогов для обмана:

* Заработок.
* Помощь страдающим.
* Разблокировки опций программ, приложений.
* Выгодное приобретение товаров.
* Розыгрыш ценных призов.

Рекомендации по безопасному использованию ресурсов сети Интернет:

- Не отправляйте СМС на короткие номера, не узнав прежде их реальную стоимость!

- Не оставляйте номер своего мобильного на сомнительных сайтах!

- Всегда проверяйте контактные данные, представленные на сайте компании или частного лица, с которыми планируете иметь дело.

- Проверьте регистрационные данные самого сайта, на какую компанию или частное лицо было зарегистрировано доменное имя и как давно.

- Если Вам предлагают работу, то платить должны Вам, а не Вы.

- Не отправляйте деньги за регистрацию, за почтовые расходы, как залог за комплектующие, с которыми Вам предстоит работать и т. п.

- Почитайте отзывы других пользователей сети об этой компании, сайте или частном лице.

- Не открывайте файлы, которые прислали неизвестные Вам люди. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.

- Не добавляйте незнакомых людей в свой контакт (ICQ, MSN messenger и т.д.)

- Ни под каким предлогом не выдавай незнакомым людям свои личные

данные (домашний адрес, номер телефона и т.д.) и пароли.

- Старайся не нажимать на рекламные баннеры, даже если они кажутся тебе очень заманчивыми.

- Не оставлять своих персональных данных на открытых ресурсах.

- Не проходи по ссылкам в спамовых письмах.

# 3. Практическая часть

## 3.1. Опрос учащихся

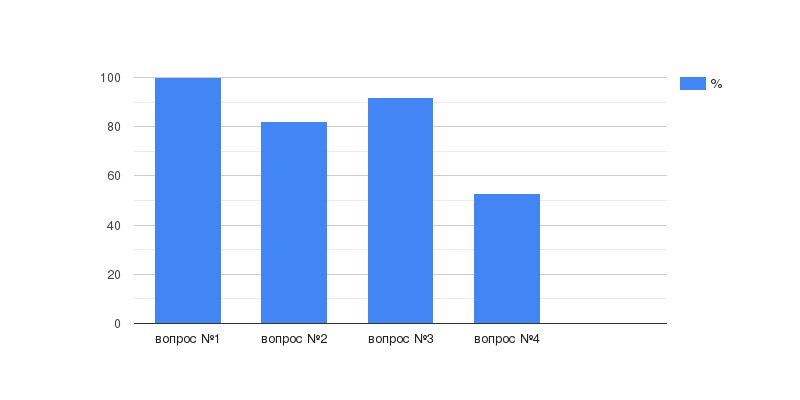
Меня заинтересовал ряд вопросов:

* №1 какой процент знает, что такое интернет мошенничество?
* №2 какой процент сверстников подвергались обману в сети интернет?
* №3 знают ли они меры предосторожности?
* №4 знают ли они, какие наказания следуют за мошенничество?
* №5 как часто они сталкивались с ним?
* №6 с чем именно они чаще всего сталкивались?

Я провёл опрос своего класса в количестве 18 человек, а также в социальной сети ВКонтакте в количестве 23 человек. Всего в опросе приняли участие 41 человек (всем опрошенным было 15-16 лет).

По результатам опроса я сделал выводы:

* все учащиеся знают, что такое мошенничество в интернете;
* многие сталкивались с ним;
* чаще всего сталкивались с кражей логинов и паролей;
* практически все знают меры предосторожности;
* половина учеников знают, какие наказания следуют за мошенничество в сети;
* по периодичности они очень редко сталкиваются с мошенничеством снова;
* несмотря на такие положительные результаты опроса, всё равно многие попадаются на обман злоумышленников.



## 3.2. Разбор конкретного примера мошенничества в сети

Пользователь Авито давно пользуется данным сервисом, много покупает и продаёт. Знает про все различные схемы обмана при личной встрече перед покупкой/продажей. Человек очень внимательный и дотошный. История, рассказанная далее, произошла с опытным продавцом, а не с тем, кто первый день на Авито.

У автора очередная продажа, покупатель просит отправить товар Авито. Доставкой. Иван упаковывает товар, делает фотографию посылки и уходит с Почты России. Покупатель принимает товар и по каким-то причинам отказывается от него. Иван ждёт обратную доставку, а затем снова идёт на почту. При получении посылки он снимает процесс распаковки и получения товара на видео и вместо условного смартфона он видит там упаковку от телефона и запиханные в неё конфеты. Иван не теряется, просит на почте оформить акт приёма с описанием всего, что пришло. Вместе с этим актом, видео упаковки и видео распаковки он отправляется в Авито. Поддержку, где его раз за разом просят подождать. Спустя несколько месяцев он получает отказ в компенсации, так как нет видео, где видно, что это покупатель подменил заказ. Из этого примера видно, что даже если вы постараетесь, соберете все доказательства и хорошенько подготовитесь, вы всё равно рискуете оказаться жертвой мошенников.

Почему так происходит?

При оформлении Авито.Доставки, покупатель оплачивает покупку сразу, но сервис держит деньги у себя до тех пор, пока покупатель не подтвердит, что товар пришёл и с ним всё в порядке. Однако товар доставляется Почтой России или Боксберри, где сотрудникам всё равно, что покупатель делает с посылкой в период проверки.

Как это можно было бы решить?

Либо договориться с Почтой России и Боксберри о том, что их сотрудники специально следят за покупателями во время проверки и включить эту работу в комиссию сервиса при доставке, либо же организовать собственные пункты самовывоза, где уже сотрудники самого Авито будут проверять, чтобы не было никаких подмен.

Третий вариант — передавать деньги покупателю только после того, как продавец подтвердит, что с посылкой всё в порядке (хотя этот вариант может спровоцировать новые виды мошенничества).

## 3.3. Что грозит за мошенничество в интернете?

На данный момент большинство мошенников остаются безнаказанными, ведь в сети интернет можно быть полностью анонимным. Существует ряд стаей, карающих за мошенничество в интернете. Основной статьёй считается - 159 УК РФ “Мошенничество”, но также злоумышленника можно привлечь к ответственности ещё по нескольким статьям, такие как: Статья 272 УК РФ – Неправомерный доступ к компьютерной информации, статья 273 УК РФ – Создание, использование и распространение вредоносных программ, Статья 274 УК РФ – Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно - телекоммуникационных сетей.

Наказание по статье 159 УК РФ:

- штраф в размере до ста двадцати тысяч рублей;

- заработная плата или иного дохода осужденного за период до одного года;

- обязательные работы на срок до трехсот шестидесяти часов;

- исправительные работы на срок до одного года;

- ограничение свободы на срок до двух лет;

- принудительные работы на срок до двух лет;

- арест на срок до четырех месяцев;

- лишение свободы на срок до двух лет.

Как видим, практически каждый из видов интернет - мошенничества может быть наказан с помощью не одной, а нескольких статей Уголовного Кодекса.

Исследование глобальных экономических преступлений, проведенное с участием деловых кругов в 78 странах, выяснило, что интернет - мошенничество занимает четвертое место в мире по частоте совершения.

В 2017 году на российские информационные ресурсы было совершено свыше 70 миллионов компьютерных атак, что почти втрое больше, чем годом ранее. Потери российской экономики из-за атак киберпреступников в 2017 году составили более 600 млрд рублей. «Эта цифра превышает примерно в два раза ущерб от всех других экономических преступлений» и превышает 200% от финансовой поддержки СМИ из бюджета РФ в 2017 году, а также почти 50% расходов на здравоохранение.

# Заключение

Таким образом, я могу сделать вывод, что многие пользователи интернета знают о проблеме, но всё равно ведутся на обман. Не попадаться на уловки злоумышленника, на самом деле не так сложно, как ликвидировать его последствия. Для этого достаточно иметь хороший антивирус, регулярно проверять компьютер на наличие вирусов, не переходить по подозрительным ссылкам, бережнее относиться к деньгам и конфиденциальной информации.

При работе с исследовательским проектом были выполнены все поставленные задачи:

1. Изучить виды мошенничества

2. Изучить меры предосторожности

Цель работы была выполнена. Гипотеза доказана. Мы приобрели новые ценные знания, которыми можно будет делиться с другими и применять самим.

# Литература

1. <https://ru.wikipedia.org/wiki/Фишинг#:~:text=Фи́шинг%20—%20вид%20интернет-мошенничества%2C%20целью,либо%20на%20сайт%20с%20редиректом>
2. <https://ru.wikipedia.org/wiki/Социальная_инженерия>
3. <https://ru.wikipedia.org/wiki/Интернет-мошенничество>
4. <https://sudact.ru/law/uk-rf/osobennaia-chast/razdel-viii/glava-21/statia-159/>
5. <https://stykrf.ru/273>
6. <https://stykrf.ru/272>
7. <https://stykrf.ru/274>
8. <https://ru.wikipedia.org/wiki/Фарминг>
9. <https://www.iphones.ru/iNotes/user-posts/avito-pyat-istoriy-pro-bespomoshchnuyu-sluzhbu-podderzhki-11-17-2020>
10. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/

# Приложение

**Статистические данные**



Рисунок. 1 – рост преступлений за 7 лет, совершаемых через интернет

Количество инцидентов в I квартале 2021 года в сравнении с аналогичным периодом 2020 года увеличилось на 17%, а относительно IV квартала 2020 прирост составил 1,2%.

На организации были направлены 88% атак. Чаще всего злоумышленники атаковали госучреждения, промышленные компании и организации в сфере науки и образования.

Основным мотивом в атаках как на организации, так и на частных лиц остается получение данных.

Главными целями злоумышленников являются персональные и учетные данные, а при атаках на организации к ним добавляется еще и коммерческая тайна.

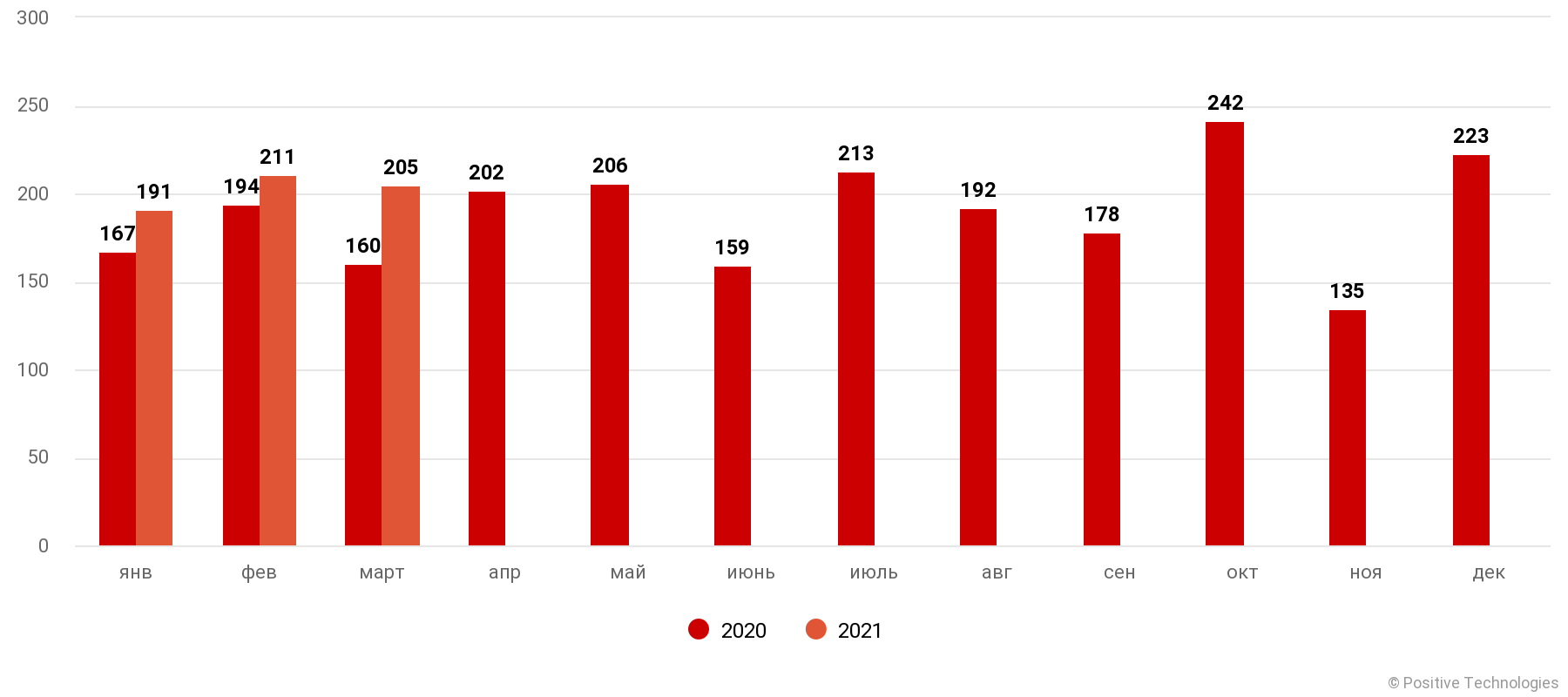


Рисунок 2. Количество инцидентов в 2020 и 2021 годах (по месяцам)

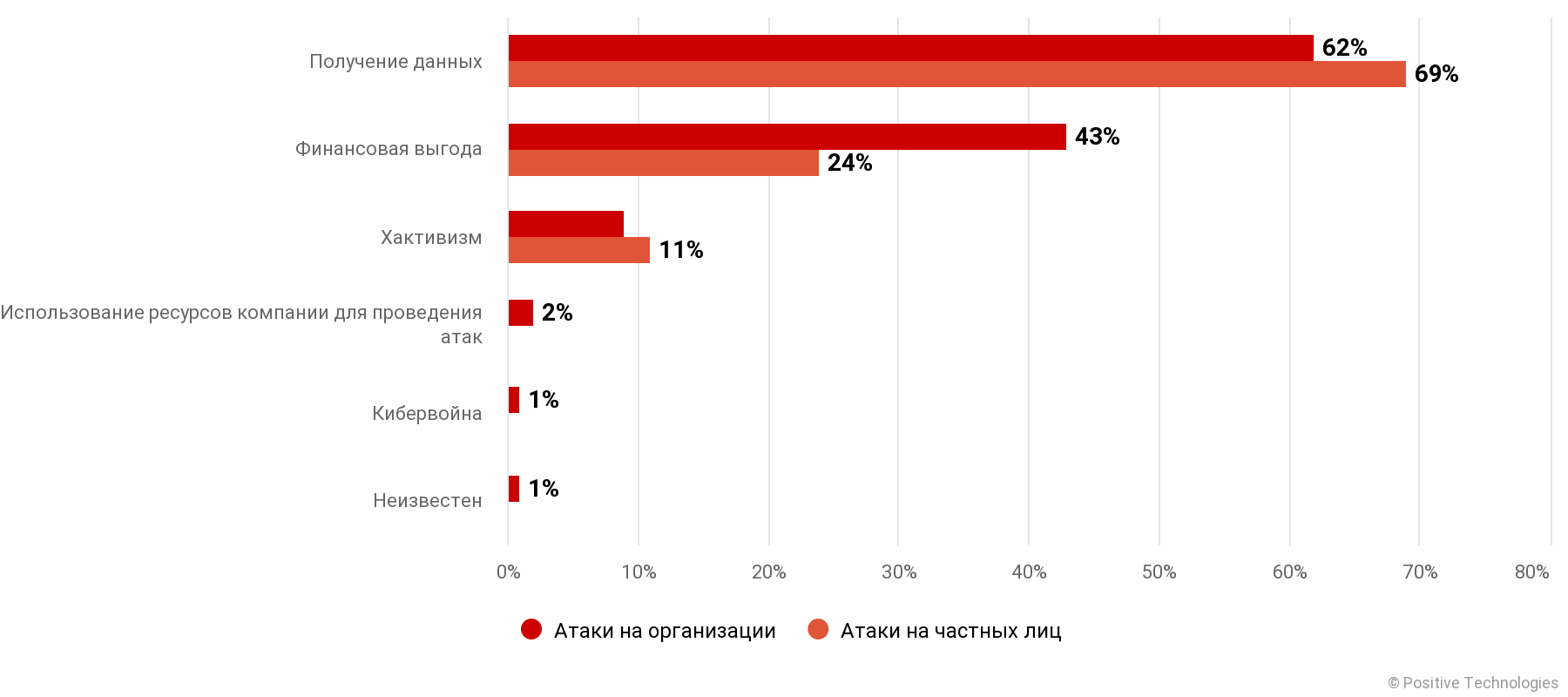


Рисунок 3. Мотивы злоумышленников (доля атак)

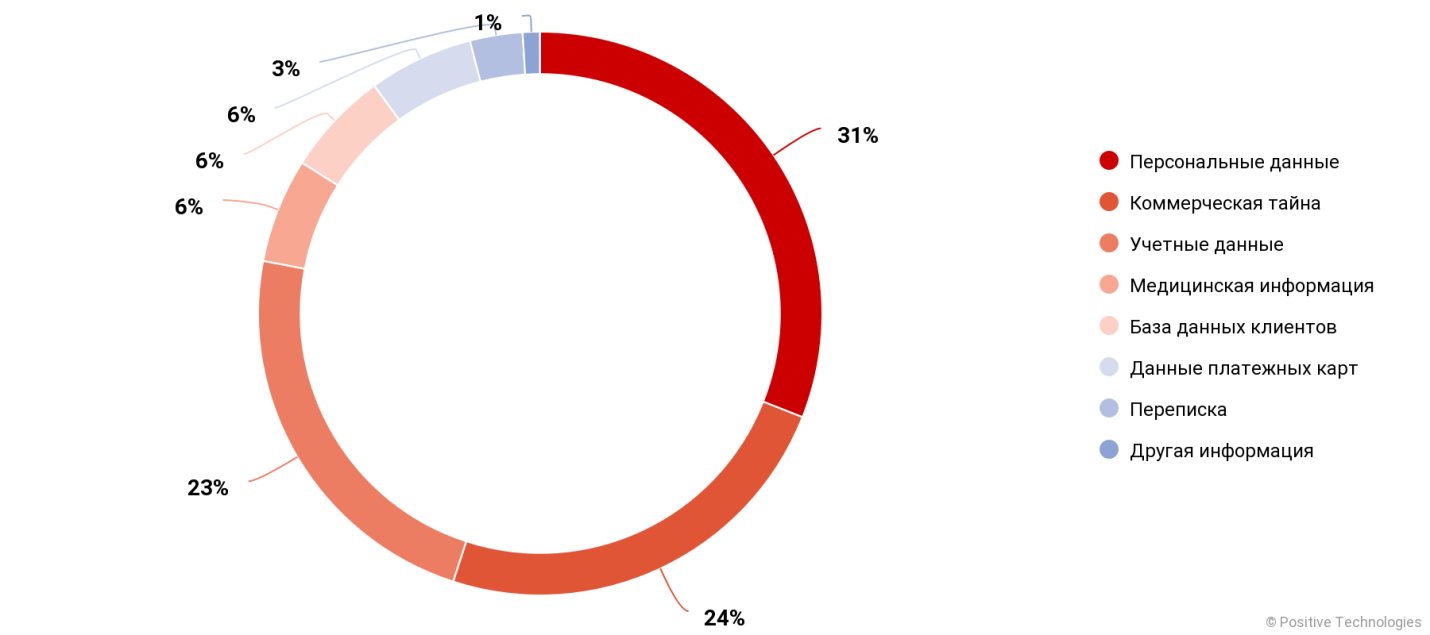


Рисунок 4. Типы украденных данных (в атаках на организации)

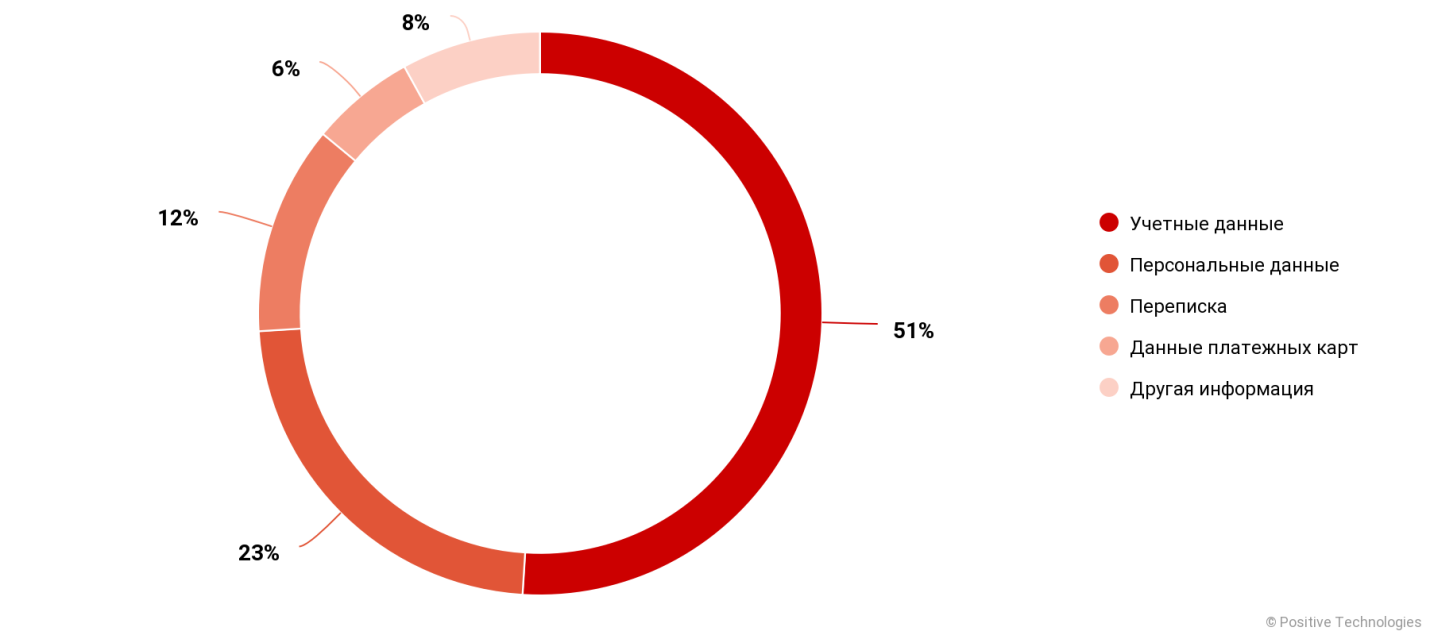


Рисунок 5. Типы украденных данных (в атаках на частных лиц)

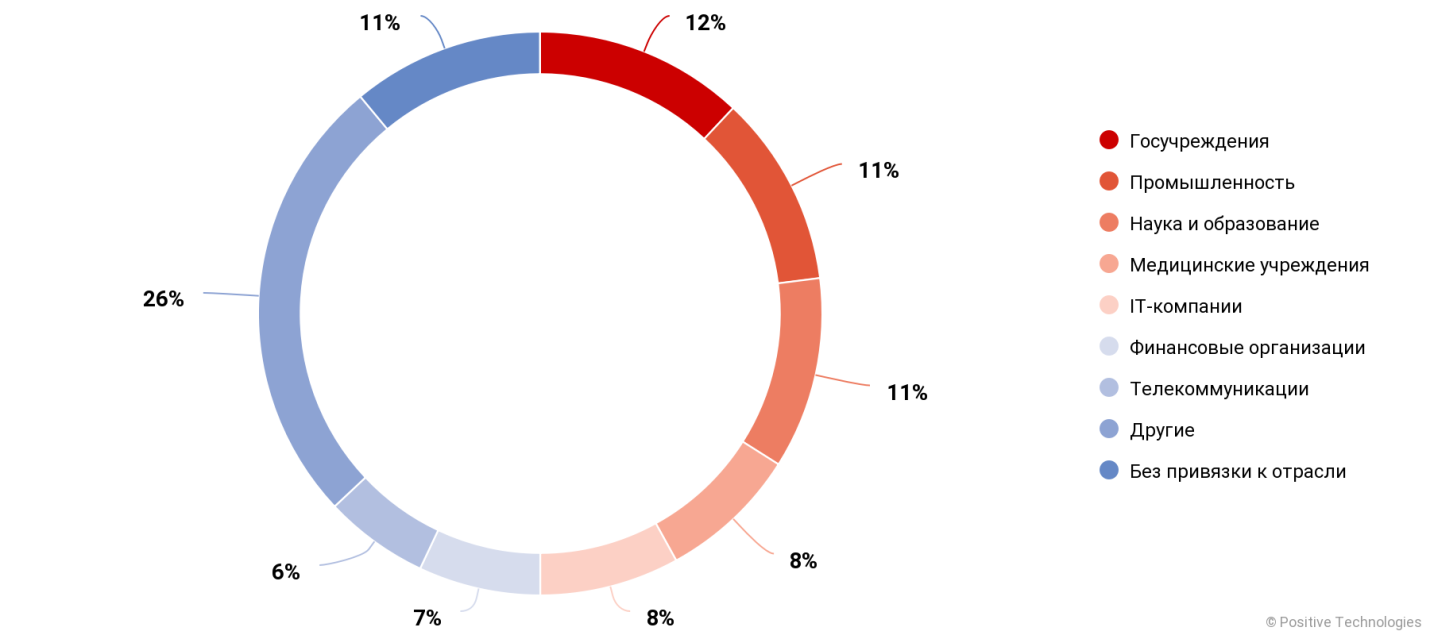


Рисунок 6. Категории жертв среди организаций

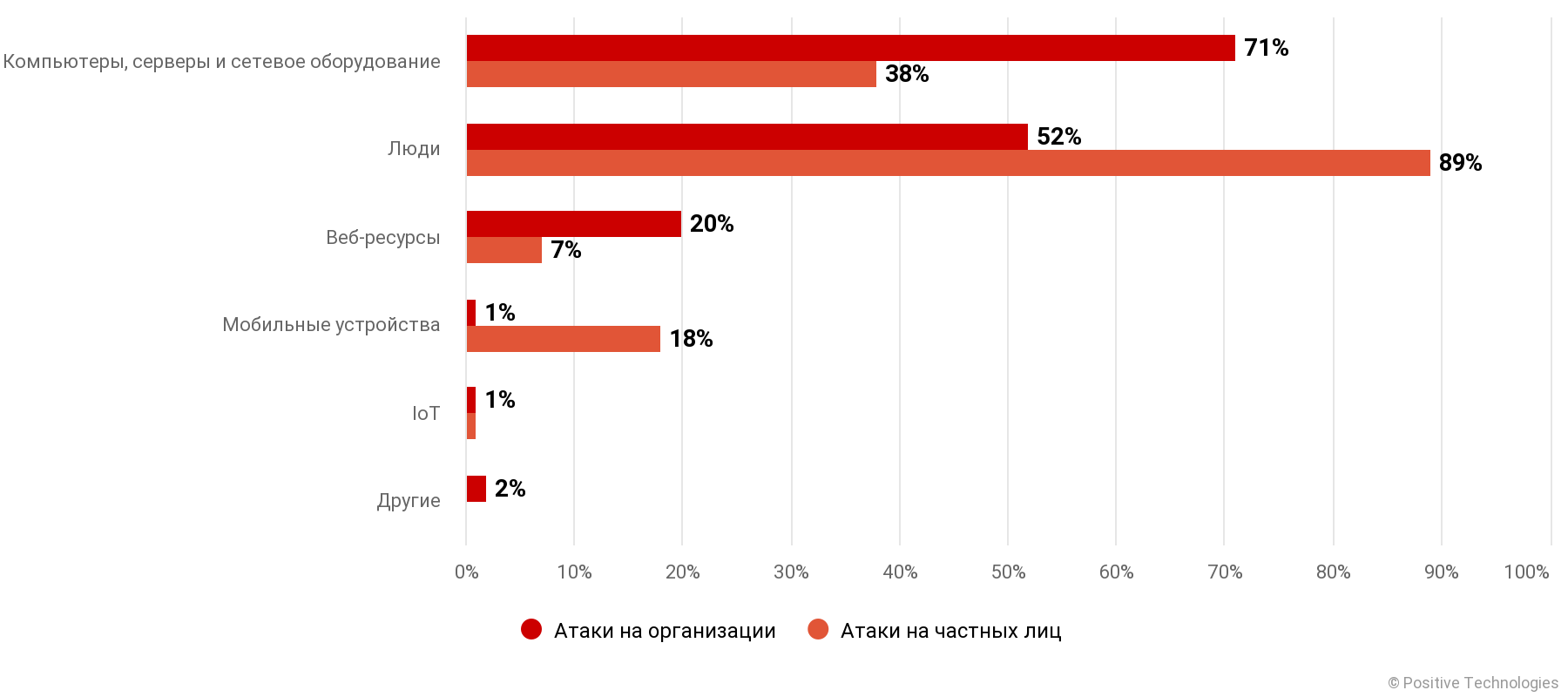


Рисунок 7. Объекты атак (доля атак)

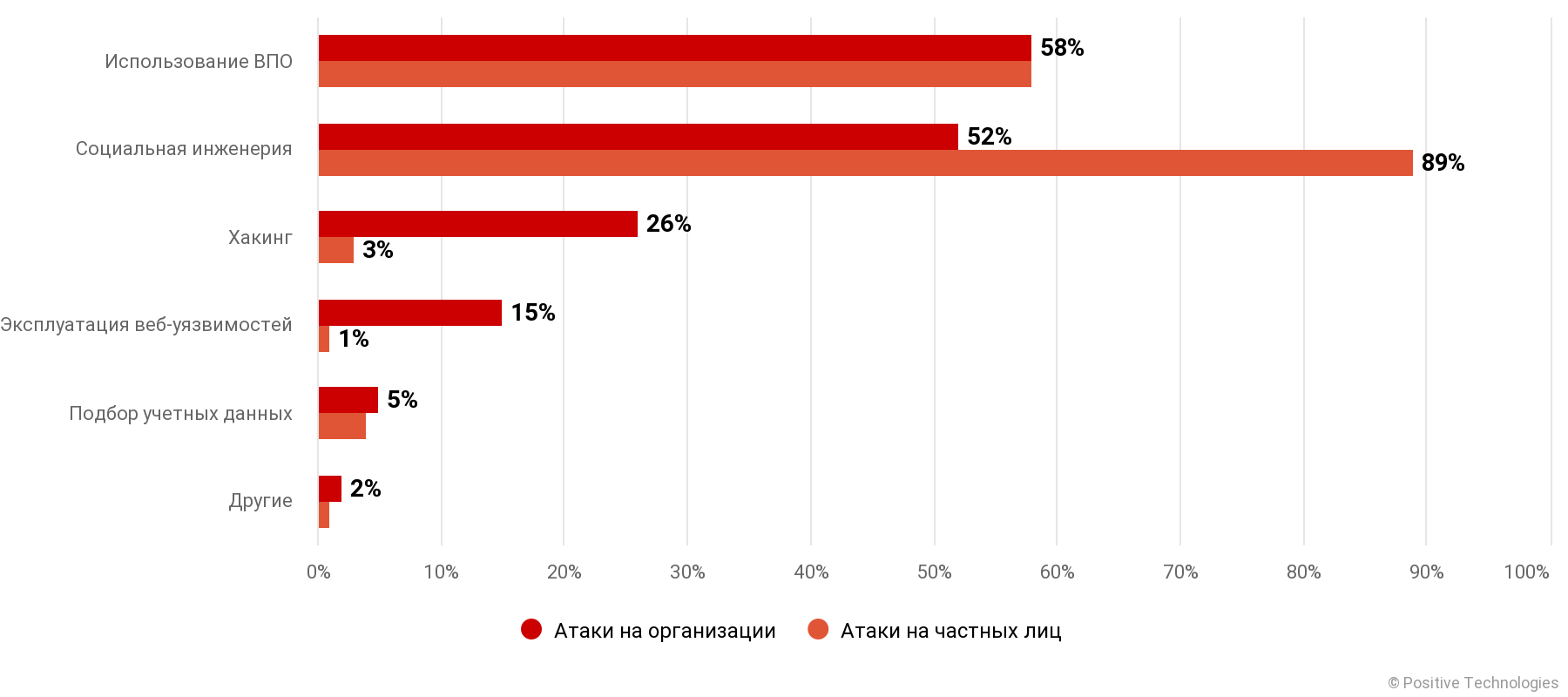


Рисунок 8. Методы атак (доля атак)

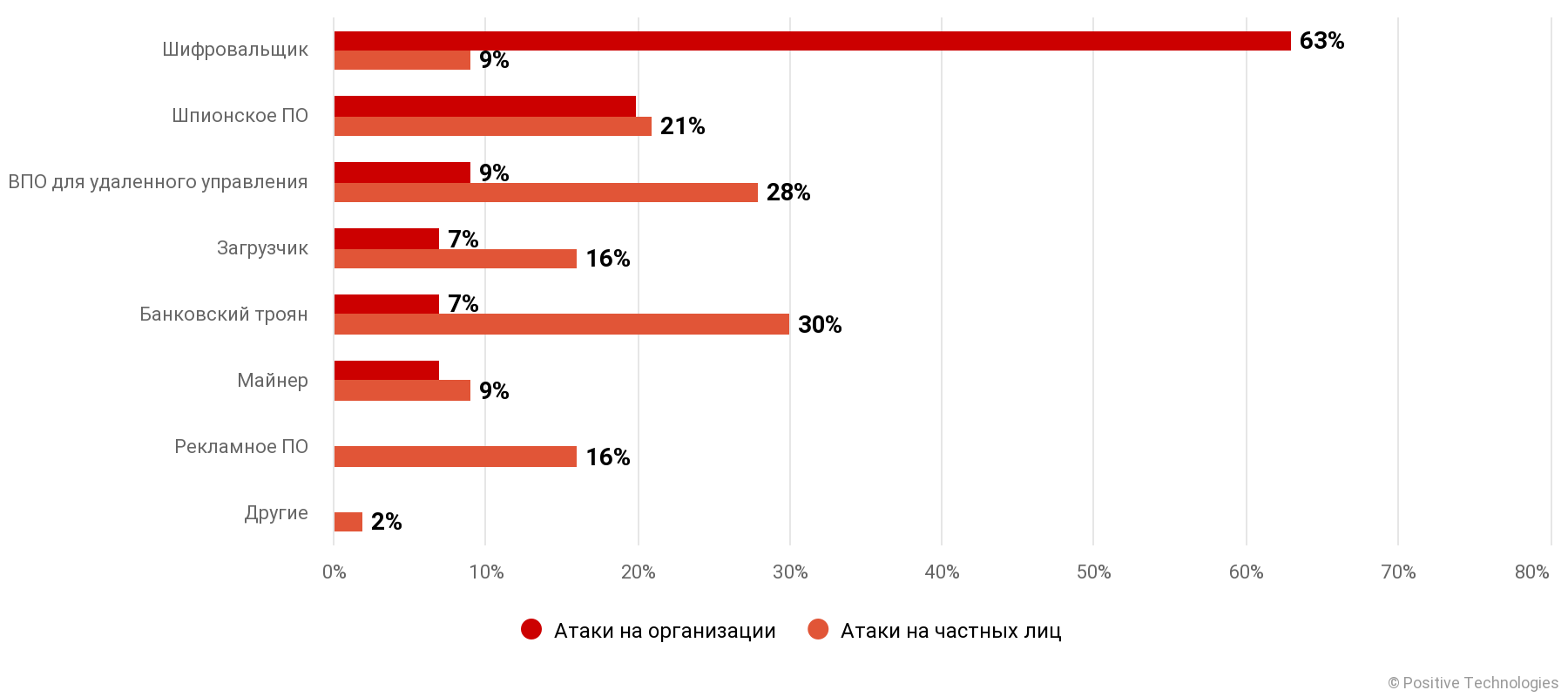


Рисунок 9. Типы вредоносного ПО (доля атак с использованием ВПО)