



## Евгений Панков: Опасности и киберугрозы будут меняться вместе с технологиями

Фишинг, вредоносное ПО, атаки в мессенджерах и дипфейки — онлайн-угрозы становятся всё изощрённее. О новых рисках и о том, как сегодня защищена российская доменная инфраструктура, редакция журнала «Интернет изнутри» поговорила с аналитиком данных Координационного центра доменов .RU/.РФ Евгением Панковым.

### — Евгений, как вы оцениваете текущую ситуацию с кибербезопасностью в российских доменах?

— Вообще, борьба с мошенничеством и кибератаками — это постоянная гонка копы и брони: как только появляются новые инструменты защиты, мошенники придумывают способы их обойти. Но если говорить о российских доменах верхнего уровня, то ситуация здесь постепенно улучшается. На фоне многих других доменных зон национальные домены .ru и .rf выглядят достаточно защищёнными.

Не без гордости могу сказать, что в этом году нам удалось переломить тенденцию последних лет и остановить рост фишинга — самой массовой угрозы в доменном пространстве

России. По итогам девяти месяцев этого года число обращений по фишингу в проекте «Доменный патруль» снизилось на 16%. Кроме того, у нас в России среднее время от получения обращения до блокировки вредоносного домена составляет менее 14 часов — и это лучший показатель в мире. Стоит отметить, что свыше 70% всех сообщений обрабатываются в первые 12 часов.

Но это не значит, что теперь можно расслабляться — мошенники всё время ищут новые схемы, и наша задача — не просто держать планку, но и постоянно развивать системы обнаружения и внедрять новые методы защиты.

### — Какие виды мошенничества с использованием доменных имён встречаются чаще всего? Как пользователю понять, что перед ним поддельный сайт?

— Фишинг был и остаётся самым частым видом мошенничества: в топе — поддельные сайты популярных банков, маркетплейсов и мессенджеров.

Злоумышленники в подробностях копируют дизайн сайтов, чтобы усыпить бдительность пользователей и выманить у них логины, пароли и данные банковских карт. Чтобы от-

личить подделку, в первую очередь нужно внимательно смотреть на адрес сайта: мошенники часто используют визуально схожие адреса, изменив несколько букв/символов или зарегистрировав сайт в другой доменной зоне.

Также стоит обращать внимание на дату создания домена, наличие HTTPS-сертификата, ошибки в текстах, сбившуюся вёрстку, украденные или сгенерированные ИИ иллюстрации. И главный маркер: если вас торопят «срочно ввести данные» или обещают слишком выгодные цены — это наверняка мошенники. Чтобы не потерять свои данные и деньги, не переходите по подозрительным ссылкам, тщательно проверяйте адреса сайтов и используйте для авторизации и оплаты только официальные ресурсы.

**— Какие тенденции вы сейчас наблюдаете у злоумышленников? Почему многие из них в последнее время переключились на мессенджеры?**

— Злоумышленники всегда идут туда, где больше потенциальных жертв и где им проще работать. Если раньше активно использовались домены, то сейчас мы видим явный сдвиг в сторону мессенджеров.

Причина проста: в Рунете за последние годы заметно усилились и ускорились механизмы противодействия фишингу. А значит, фишинговые домены «живут» всё меньше, и мошенникам становится невыгодно их использовать. Поэтому мошенники переходят в мессенджеры: за первые восемь месяцев 2025 года число доменов, имитирующих Telegram, выросло почти в четыре раза, растущая динамика наблюдается и по WhatsApp.

Почему именно мессенджеры? Во-первых, это самые популярные каналы общения пользователей, и аудитория у них огромная. Во-вторых, зарегистрировать аккаунт очень просто, а распространять любые ссылки или сообщения можно мгновенно. В-третьих, взлом профиля пользователя открывает мошенникам доступ к контактам, фото и документам, которые затем используются для атак на его друзей и знакомых. И, наконец, меры противодействия со стороны платформ пока явно недостаточны. Всё вместе это создаёт идеальную среду для мошенничества.

Кроме того, в 2025 году мы наблюдаем ещё один тревожный тренд — рост атак с использованием вредоносного программного обеспечения (ВПО). За восемь месяцев этого года поступило более пяти тысяч жалоб на ВПО, что почти в три раза выше показателей аналогичного периода 2024 года. Мошенники

всё чаще используют связку фишинга с ВПО, которая позволяет получить полный контроль над устройством жертвы и не только похищать конфиденциальную информацию и деньги, но и автоматически распространять фишинговые ссылки новым адресатам.

**— Какие приёмы мошенников представляют наибольшую опасность для технических специалистов?**

— Технические специалисты, как правило, менее восприимчивы к классическим схемам — их не так легко обмануть фишинговым письмом или поддельным маркетплейсом. Но у них есть своя уязвимость: доверие к коллегам, профессиональным сервисам и внутренним коммуникациям. Этим и пользуются злоумышленники.

Когда человек работает в высоком темпе и рутине, внимание к мелочам снижается. Поэтому хакеры часто маскируют атаки под рабочие процессы: поддельные письма от коллеги или системного администратора, уведомления от сервисов для разработчиков или профессиональных сообществ, запросы «срочно обновить пароль» или «настроить доступ». Всё выглядит максимально правдоподобно, и именно здесь специалисты рискуют попасться.

**— Если говорить о бизнесе: какие атаки чаще всего нацелены именно на компании и их цифровую инфраструктуру? Что, по-вашему, важнее для компаний и пользователей: строить сильные защиты от атак или учиться минимизировать их последствия?**

— Для бизнеса самыми опасными являются ВЕС-атаки, атаки с использованием ВПО и социальная инженерия в мессенджерах.

Чаще всего злоумышленники маскируют вредоносные письма под деловую переписку: это могут быть «срочные» просьбы оплатить счёт, проверить вложение или перейти по ссылке. Переход по таким ссылкам нередко приводит к установке троянов вроде DarkWatchman RAT, которые дают





удалённый доступ к устройствам и позволяют собирать переписку, документы, пароли и другую чувствительную информацию.

Ещё одна схема — подделка коммуникаций от имени руководителей или партнёров. Здесь используются либо взломанные аккаунты корпоративной почты, либо похожие адреса, а всё чаще и дипфейки, когда сотрудник получает сообщение или звонок якобы от своего руководителя. Так злоумышленники выманивают деньги или получают доступ к внутренним системам.

Отдельно стоит упомянуть схему взлома панели управления доменом у регистратора. Это позволяет не только «угнать» домен, но и получить доступ к ключевой IT-инфраструктуре компании. Например, подменить настройки почтовых серверов, перехватывать переписку, перенаправлять пользователей на фишинговые сайты и даже создавать поддельные точки доступа в корпоративную сеть и собирать данные сотрудников.

Если говорить о стратегии защиты, то это не вопрос выбора: нужно выстраивать комплексную защиту, способную не только отразить угрозу, но и минимизировать последствия атаки. Эффективная система безопасности включает и своевременную настройку защитных механизмов, и регулярный аудит инфраструктуры, и обучение сотрудников, и мониторинг активности, и особое внимание к защите корпоративного домена.

**— Искусственный интеллект развивается стремительно, и вместе с ним появляются новые риски. Замечаете ли вы уже примеры атак с использованием ИИ?**

— Да, примеры атак с использованием искусственного интеллекта мы уже видим. Сегодня ИИ помогает злоумышленникам делать дипфейки и создавать более убедительные сценарии атак. Зачастую он используется для автоматизации процессов: от сканирования сетей и кражи данных до генерации персонализированных фишинговых писем. Также были случаи, когда вредоносные ссылки и ПО внедрялись прямо в диалоги с ИИ-чатами: человек задаёт обычный вопрос, а в ответ получает опасную ссылку, даже не подозревая об угрозе.

Очевидно, что искусственный интеллект будет и дальше развиваться, а это значит, что пользователям и специалистам по ИБ нужно учиться работать с новыми рисками: повышать цифровую грамотность, критически оценивать информацию и внедрять современные методы защиты.

**— Возможно ли заранее отследить и выявить фишинговый домен ещё на этапе регистрации? Какие инструменты для этого используются?**

— Да, сегодня в зонах .ru и .rf уже применяются проактивные методы, которые позволяют выявлять потенциально опасные домены на этапе регистрации.

Новые домены автоматически проходят проверку по ряду признаков: система отмечает подозрительные регистрации и передаёт их на дополнительную проверку компетентным

организациям. Это помогает предотвращать инциденты, не дожидаясь, пока домен начнёт использоваться для фишинга. Также мы активно изучаем возможности использования ИИ для обнаружения вредоносных регистраций и анализа угроз инфраструктуры DNS.

Важно понимать, что полная автоматическая блокировка фишинга невозможна: нужна дополнительная экспертиза, чтобы случайно не навредить добросовестным администраторам. Но сама связка проактивной разметки и работы «Доменного патруля» позволяет существенно сократить время обнаружения и сделать российское доменное пространство более безопасным.

#### — Какие шаги предпринимает Координационный центр для борьбы с вредоносными доменами?

— На сегодняшний день одним из самых эффективных механизмов борьбы с вредоносными доменами является проект «Доменный патруль». Он объединяет компетентные организации и регистраторов, что позволяет быстро выявлять и блокировать опасные ресурсы. Так, в 2024 году в отечественном доменном пространстве было заблокировано более 55 тысяч таких доменов, а с начала 2025 года — уже свыше 30 тысяч.

Кроме того, сейчас готовится законопроект о введении обязательной идентификации администраторов через ЕСИА (портал госуслуг). Это станет реальным барьером для поддельных данных и регистрации доменов под фишинг или другие противоправные действия. Технически система уже протестирована крупнейшими регистраторами и в ближайшее время станет отраслевым стандартом.

#### — И напоследок: какие практические рекомендации вы могли бы дать специалистам и владельцам бизнеса, чтобы надёжно защитить свои домены и цифровые ресурсы?

— Владельцам бизнеса я бы, в первую очередь, рекомендовал выбирать для своих сайтов и онлайн-проектов национальные зоны .ru, .rf и .su. Они являются одними из самых безопасных, а кроме того, полностью управляются внутри страны и не зависят от иностранных юрисдикций и платформ.

Отдельное внимание стоит уделить настройке корпоративной почты на домене. Это не только повышает уровень доверия со стороны клиентов и партнёров, но и позволяет выстраивать собственную систему защиты: подключать фильтры от спама и фишинга, настраивать двухфакторную аутентификацию, шифрование и резервное копирование.

Не менее важно обеспечить надёжную защиту серверов и регулярно обновлять системы, использовать антивирусы, внедрять мониторинг и аудит инфраструктуры. И, конечно, нужно учить сотрудников цифровой гигиене, знакомить с новыми видами атак и формировать чёткий план действий на случай возможных инцидентов.

Нужно понимать, что опасности и киберугрозы никуда не денутся — они будут меняться вместе с технологиями. Важно быть внимательными, учиться новому и не оставлять лазеек злоумышленникам. ■

