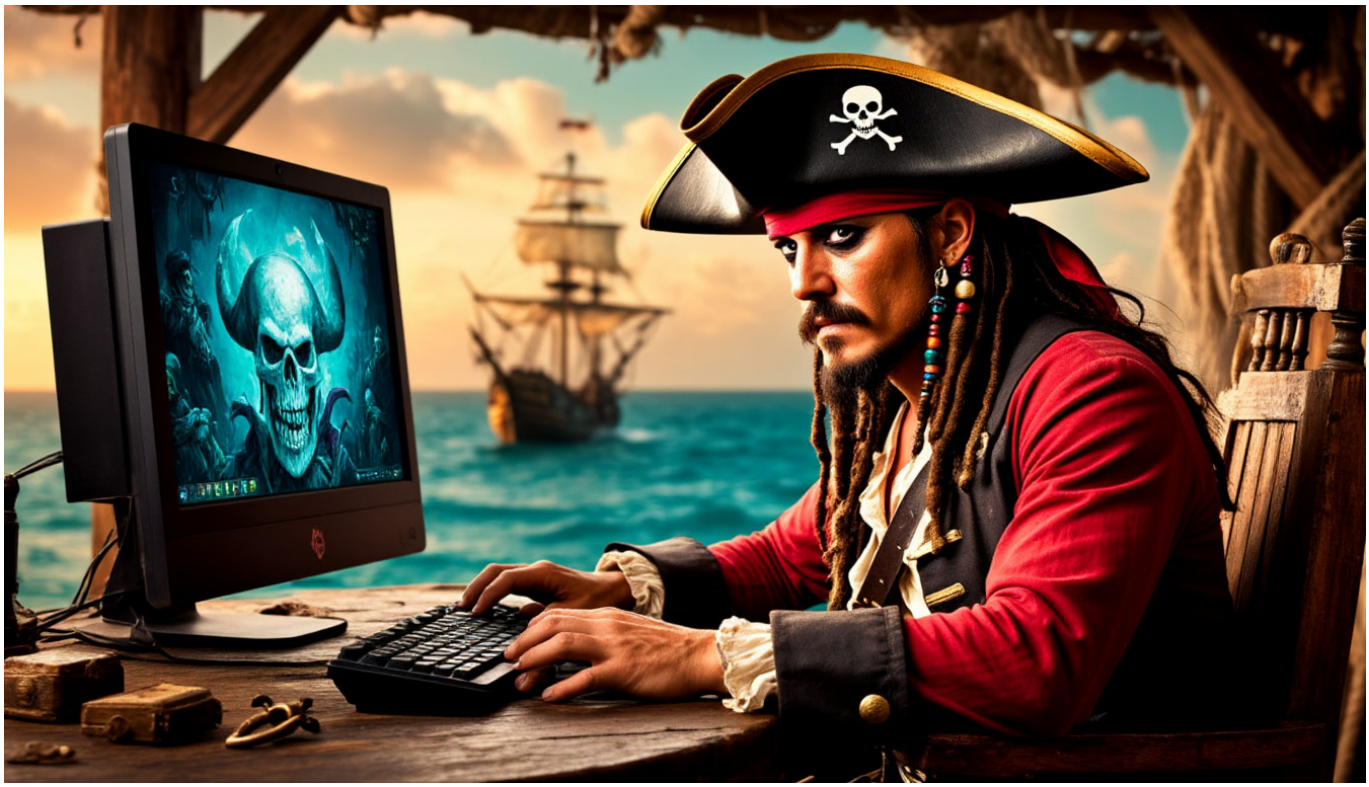
Международный пиратский день и цифровое пиратство

19.09.2025



Праздник с юмором или серьёзный подтекст?

19 сентября во многих странах отмечают Международный пиратский день. История этого необычного праздника началась в 1995 году в американском городке Олбани, штат Орегон. Два друга ради шутки стали разговаривать, вставляя в речь «пиратские словечки». Затея оказалась настолько удачной, что они решили повторять её ежегодно. С годами праздник обрёл популярность.

Однако за весёлой романтикой «пиратской жизни» стоит иная, куда более серьёзная сторона — цифровое пиратство. В XXI веке «пират» — это не человек с повязкой на глазу, а тот, кто скачивает или распространяет фильмы, игры, музыку, книги или программы без разрешения правообладателя. Этот феномен стал частью интернет-культуры и одновременно вызовом для экономики, права и безопасности.

Россия и цифровое пиратство — что говорят цифры?

В последние годы рынок нелегального видеоконтента в России начал сокращаться, чему способствовали развитие онлайн-кинотеатров, доступные подписки и ужесточение мер контроля. По данным Forbes, в первом полугодии 2024 года рынок пиратских фильмов и сериалов заметно уменьшился, что свидетельствует о переходе части аудитории в легальное поле.

Однако в игровых сегментах ситуация иная. В 2024 году российские пользователи скачали пиратских видеоигр на сумму около 190 миллиардов рублей. Более двух

третей геймеров признают, что хотя бы раз пользовались нелегальными копиями, а каждый пятый скачивал десятки тайтлов.

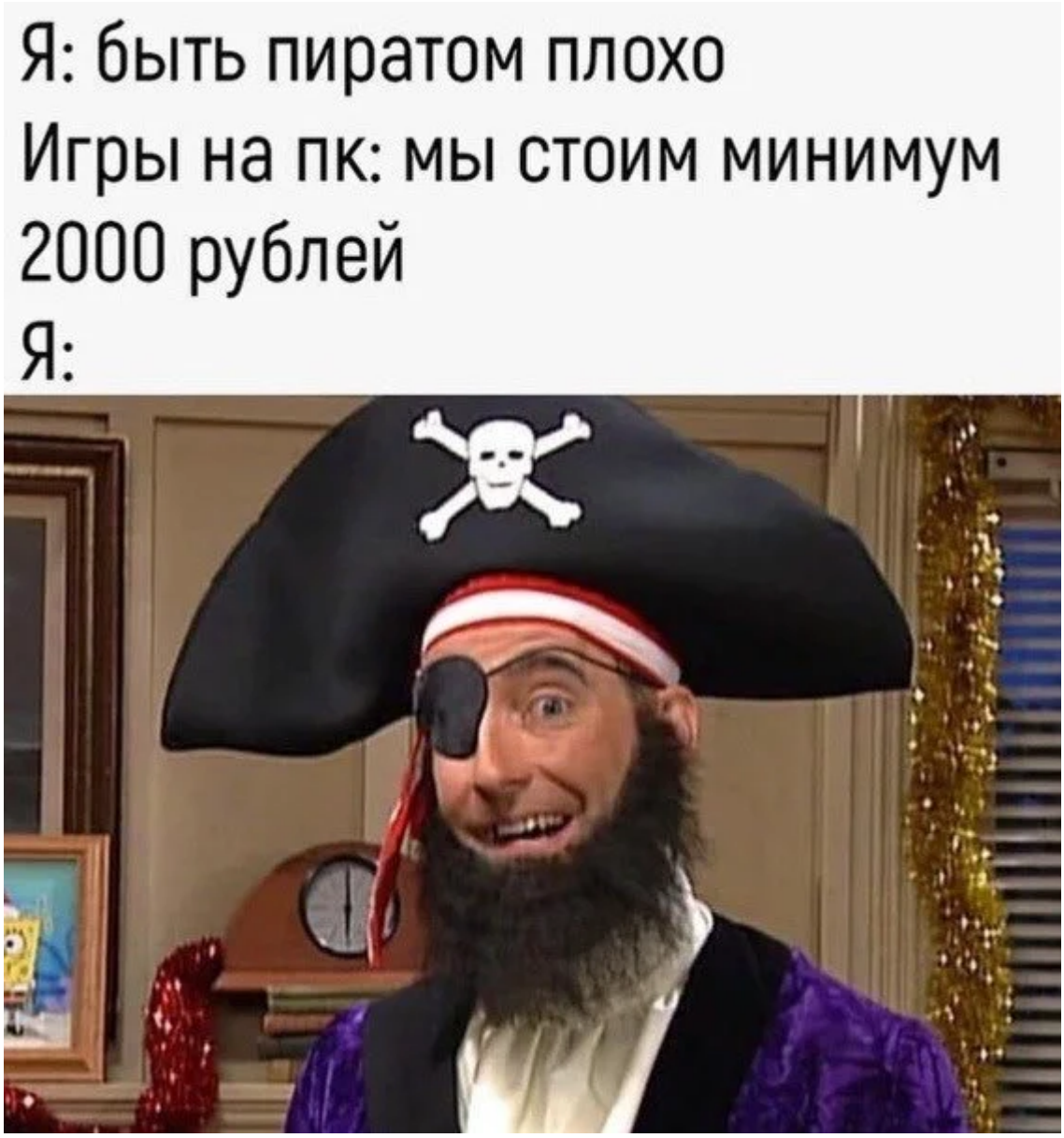


Фото: pikabu.ru

Новосибирская область — а что у нас?

Если перейти от общероссийской картины к локальной, то в Новосибирской области ситуация имеет свои особенности. Прямых исследований о том, сколько именно фильмов или игр скачивают жители региона нелегально, пока нет. Но можно опираться на косвенные данные.

> «По итогам прошлого года в Новосибирской области было зарегистрировано свыше 13,4 тыс. преступлений, совершённых с использованием информационно-телекоммуникационных технологий. По сравнению с предыдущим годом, их число снизилось на 6,5%», — писали наши коллеги из РБК ещё в апреле этого года, ссылаясь на пресс-службу ГУ МВД по региону. При этом, выросла и сумма — более 3,8 миллиардов рублей.

Меняется и характер юридической практики. Если ещё несколько лет назад возбуждались уголовные дела за использование контрафактного ПО, то к 2023 году их количество сократилось практически до нуля. Об этом писали всё в том же РБК со ссылкой на СУ СКР по региону: «В Новосибирской области резко снизилось число уголовных дел по статье о нарушении авторских прав. При этом блокировки сайтов и административные меры усилились».

Наконец, в медиа и вовсе заговорили о штрафах для пользователей за поиск контента. Так, в июле 2025 года, в СМИ зашумели о том, что Госдума рассматривает поправки, которые введут административную ответственность за целенаправленный поиск запрещённых материалов в интернете.

Не высказался и не прокомментировал разве что ленивый. Однако судя по бурной реакции, в целом тема пиратства, будь то скачивание контента или просто поиск «запрещёнки», воспринимается уже не как «шутка», а как серьёзная угроза.

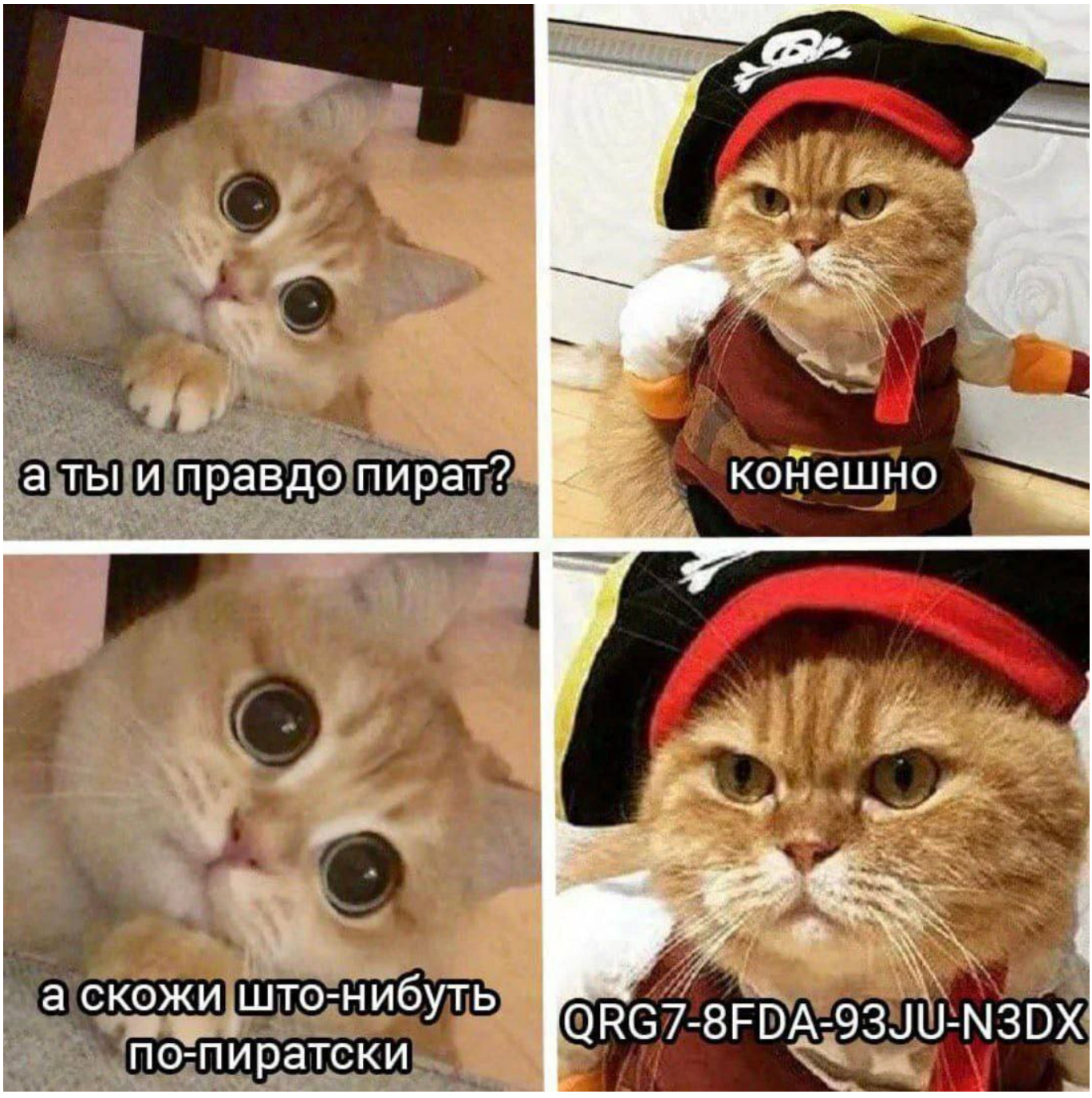


Фото: pikabu.ru

Как себя обезопасить от кражи данных — советы эксперта

Для обычного пользователя пиратство кажется безобидным способом сэкономить. Но в действительности жители Новосибирской области сталкиваются с теми же угрозами, что и пользователи по всему миру.

Как рассказал, Иван Никрошкин, руководитель Молодёжной лаборатории исследования безопасности кода отечественного ПО и компьютерной криминалистики НГТУ НЭТИ, старший преподаватель кафедры защиты информации НГТУ НЭТИ, пиратский контент часто, если не сказать повально, маскирует вредоносное ПО. Люди думают, что скачивают фильм или книгу, а на деле передают доступ к своим паролям и банковским данным.

> «Наиболее частые „экземпляры“ — это, конечно, рекламное вредоносное программное обеспечение и майнеры криптовалюты, если мы говорим о пользовательском сегменте. Если говорить о корпоративном сегменте, то тут, разумеется, применяются более сложные и дорогостоящие технологии, шпионское ПО, например. Такие операции корпоративного уровня злоумышленники обычно проворачивают целенаправленно — на организации конкретной отрасли или конкретную организацию, так что пользователям прямого противостояния с высококвалифицированным злодеем в реальном времени стоит опасаться меньше всего.
> Для пользователей же особенно неприятны разного рода „массовое“ ВПО — то, что штампуется для неконтролируемого распространения через ссылки в почте, вложения в мессенджерах, и, конечно, пиратский контент из любых источников», — рассказал Иван Никрошкин нашему изданию.

По словам эксперта, массовое вредоносное программное обеспечение не так критично и опасно в масштабе урона в целом, но персонально для человека может обернуться кошмаром в виде похищенных платёжных данных, учётных записей и паролей, уничтоженной информации и выходом системы из строя.

> «Распознать ВПО без применения антивирусных систем достаточно сложно, но возможно, если мы говорим о майнерах — это внезапный рост потребления ресурсов компьютера, подвисания и так далее. Самый простой и примитивный, но при этом рабочий способ — обратить внимание на шум системы охлаждения и почаще заглядывать в диспетчер задач.
> Если же говорить о ВПО, целью которого стоит хищение данных, то тут всё значительно сложнее. Безусловно какую-то активность могут уловить встроенные в систему средства защиты, но на практике такое происходит в одном случае из ста, злоумышленникам не составляет труда их обойти, а в момент непосредственной передачи данных пользователя делать всё достаточно „бесшумно“. Только на этапе, когда данные уже похищены и проданы, пользователь начнёт получать уведомления от сервисов и платёжных систем о подозрительных

> попытках входа и транзакциях, но только если создатели сервиса позаботились о таком функционале», — предупреждает Иван Никрошкин.

По его словам, стандартные рекламные ВПО видно сразу — в виде рекламных баннеров на рабочем столе и в окнах приложений. Зачастую любое отклонение от нормального поведения устройства или его системы может говорить о заражении вредоносной программой. К счастью, сейчас системы научились оповещать пользователя об использовании микрофона и камеры, так что шпионское ПО низкого качества пользователь тоже заметит сразу.

Однако, по словам руководителя Молодёжной лаборатории исследования безопасности кода отечественного ПО и компьютерной криминалистики НГТУ НЭТИ, первое, самое базовое и самое главное — установить антивирусную систему. На отечественном рынке представлены варианты на любой вкус, а эффективность такого «базового слоя» защиты даст огромный прирост в защищённости ваших данных.

> «Второе — безусловно критически смотреть на содержимое страниц и ссылок, по которым вы планируете что-либо загружать или просто переходить. Сейчас отечественные браузеры предоставляют возможность посмотреть рейтинг конкретной посещаемой страницы, что в значительной мере упрощает задачу. Если говорить о содержимом — внимательно следите за тем, по какой ссылке кликаете, часто злоумышленники умело маскируют одну ошибку в длинной ссылке, обнаружить ее при беглом осмотре практически невозможно, а по ту сторону вас поджидает фишинговый сайт или загрузка ВПО. С содержимым страниц примерно та же история — оценивайте содержимое очень критично, при малейшем подозрении на подделку — покиньте страницу.
> Третье — отключите автоматическую загрузку. Зачастую злоумышленники играют на том, что мы не успеваем задуматься, скачивая и открывая файл. Добавьте себе пару секунд, пока выбираете куда сохранить файл, обратите внимание на его название и расширение, это добавит минимальной уверенности в том, что вы делаете, или наоборот заставит задуматься „а нужно ли мне это вообще?“», — поделился советами Иван Никрошкин.

Самый последний, четвёртый совет от нашего эксперта, для многих может прозвучать не приятно, но всё же — привыкайте потреблять лицензионный контент. Производитель несёт ответственность за то, что публикует и передаёт — тут ваши права защищены, а риски минимальны, потому что репутация дороже.

Ранее мы писали о том, что новосибирца подозревают во взломе 70 веб-камер российских компаний.

Анастасия Аксёнова