ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРОКУРАТУРА КРАСНОДАРСКОГО КРАЯ

УПРАВЛЕНИЕ ПРАВОВОЙ СТАТИСТИКИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

«ВИДЫ ХАКЕРСКИХ АТАК И СПОСОБЫ ИХ ПРЕДУПРЕЖДЕНИЯ»

г. Краснодар
2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

С развитием цифровых технологий и переходом большинства сфер жизни в онлайн-пространство значительно увеличилось количество хакерских атак. Под ударом оказываются не только крупные компании и государственные учреждения, а также обычные пользователи интернета. Именно поэтому данный вопрос сегодня приобретает особую актуальность и требует пристального внимания.

Как правило злоумышленники таким способом стремятся получить материальную выгоду. Причем далеко не всегда приходится что-то взламывать. Сколько бы ни появлялось статей о том, как важно подбирать надежный пароль, культура интернет-безопасности в целом остается низкой. Пользователи интернета выбирают одни и те же кодовые слова для разных сайтов, переходят по подозрительным ссылкам из спама и принципиально отказываются от менеджеров паролей. Обычно злоумышленники пользуются следующими методами:

1. Фишинг – метод взлома аккаунтов, при котором пользователя заманивают на сайт, выдающий себя за настоящий, и предлагают ввести пароль, который попадает к злоумышленникам.

2. Вредоносное программное обеспечение (далее – ПО) – это программы, намеренно разработанные и внедряемые для нанесения ущерба компьютерам и компьютерным системам.

3. Социальная инженерия – в контексте информационной безопасности означает психологическое манипулирование людьми с целью совершения ими определенных действий или разглашения конфиденциальной информации.

4. Подбор пароля – обладая информацией о пользователе, которую легко найти в социальных сетях, можно попробовать угадать пароль. Также возможен автоматизированный метод взлома систем защиты, основанный на систематической проверке всех возможных или вероятных вариантов паролей, ключей шифрования или других секретных данных.

Чаще всего взломщикам не нужно подбирать пароль – они действуют другими методами. У крупных сайтов почти всегда работает эффективная защита от перебора, которую можно обойти, лишь имея очень крупную сеть подконтрольных компьютеров (ботов) и растягивая атаку на многие месяцы, но никак не вручную.

1. ОСНОВНЫЕ МЕТОДЫ ВЗЛОМА ИНФОРМАЦИОННЫХ СИСТЕМ

Злоумышленники постоянно адаптируют и улучшают свои методы цифрового нападения, нередко комбинируя несколько видов вмешательства одновременно.

Фишинг осуществляется через электронную почту, социальные сети, мессенджеры или веб-сайты, которые выглядят так, будто они принадлежат легитимным организациям. Примеры фишинговых атак включают в себя отправку поддельных электронных писем, в которых пользователя просят ввести свои учетные данные на поддельной веб-странице, или использование маскированных

веб-сайтов для сбора личной информации. Специфика фишинга заключается в том, что жертва мошенничества предоставляет свои конфиденциальные данные добровольно.

Существует несколько видов фишинга:

Почтовый фишинг – злоумышленник отправляет письмо, внутри которого находится компьютерный вирус или фишинговая ссылка, по которой нужно перейти. Сообщение замаскировано под настоящее и может прийти якобы от коллеги. Адрес отправителя может быть очень похож на подлинный, а текст содержать информацию, которая известна узкому кругу лиц, поэтому письмо кажется настоящим;

СМС-фишинг – в СМС могут предложить перейти по ссылке или подтвердить данные. Тогда мошенники получат доступ к учетной записи работника и всей открытой для него информации. Сообщения вызывают доверие, потому что их отправляют от имени уже знакомых контактов и используют личную информацию в тексте СМС;

Голосовой фишинг (вишинг) – злоумышленники пытаются обмануть по телефону. Номер телефона при этом может быть известен, так как мошенники используют переадресации, или он просто будет скрыт;

Веб-фишинг – мошенники создают фишинговый сайт-копию, который сложно отличить от настоящего. Они могут скопировать визуальные элементы дизайна и фирменный стиль, использовать похожее сочетание букв в URL-адресе, что незначительно отличит его от оригинала.

Вредоносное ПО оказывается на компьютере пользователя разными способами. Если злоумышленники не занимаются целевой атакой на конкретного человека, а стремятся заразить наибольшее число компьютеров (а это более распространенная тактика среди компьютерных преступников), то они предпочитают получить доступ к популярным сайтам и внедрить в них вредоносный код. Посещение такого сайта с компьютера, где не установлены последние обновления безопасности, антивирус или браузер, который умеет предупреждать о зараженных сайтах, может привести к его заражению и попаданию под полный контроль атакующих. Вредоносное ПО реализовано так, чтобы незаметно проникать в систему и воровать данные, блокировать файлы или превращать устройство в инструмент для новых атак.

Когда речь идет о направленных атаках – таких, где жертва является публичным лицом или имеет доступ к важной информации, – может использоваться механизм, при котором жертву заманивают на знакомый ей сайт, но иными методами. Допустим, он может подключиться к публичной сети Wi-Fi, которую контролирует злоумышленник. В ней пользователя автоматически направляют на фишинговый сайт, похожий на привычную социальную сеть, или просто сайт со зловредным кодом, который, например, может быть размещен на приветственной странице входа в сеть Wi-Fi.

Неопытные пользователи довольно часто используют один и тот же пароль на нескольких сайтах или нескольких программах. В этом случае, взломав одну базу данных с паролями или украв пароль от одного сайта, атакующий получает доступ и к другому, возможно, более ценному ресурсу. Помимо самого взлома

аккаунта, возможны ситуации, когда пароль не скомпрометирован, но злоумышленники все равно имеют возможность действовать от лица пользователя. Например, многие сталкивались с возможностью «войти на сайт», используя мессенджер «ВКонтакте». Нажимая на такую кнопку, пользователь оказывается на странице социальной сети, где у него спрашивают, доверяет ли он этому стороннему сайту. Иногда среди действий, которые просит разрешить сторонний сайт, оказывается и публикация новых сообщений от имени пользователя. В результате злоумышленникам необязательно взламывать, например, мессенджер «ВКонтакте», чтобы публиковать сообщения.

В современном мире логин от социальной сети может быть важнее почтового. Почтовые системы накопили большой опыт борьбы со злоумышленниками, а пользователи проводят в интерфейсе социальной сети больше времени, чем в почте.

2. ДЕЙСТВИЯ ПРИ ВЗЛОМЕ АККАУНТА

Как только заметили признаки взлома, действовать нужно сразу. Первые минуты решают, удастся ли ограничить доступ мошенников к вашим данным:

- Если доступ к аккаунту есть на другом устройстве, завершите сессии и смените пароль;
- Вспомните, были ли к учетной записи привязаны банковские карты, если да, лучшим вариантом будет их заблокировать до возвращения доступа;
- Предупредите близких и друзей о том, что аккаунт взломали, объясните, что вы не попали в беду и вам не требуется помощь, важно действовать быстро – пока люди не перевели мошенникам деньги;
- Если доступ к профилю закрыт, попробуйте восстановить пароль через телефон или почту;
- Оформите жалобу в службу поддержки, подтвердите, что вы настоящий владелец – в социальной сети «ВКонтакте», например, для этого нужно сделать фото с листком, где написан код из письма;
- Попросите друзей пожаловаться на вашу взломанную страницу. Чем больше жалоб, тем быстрее мошенника заблокируют;
- Не поддавайтесь на угрозы и шантаж, не платите выкуп – нет никакой гарантии, что взломщик получит деньги и вернет аккаунт в сохранности или не выложит ваши персональные данные в общий доступ.

3. КАК ЗАЩИТИТЬ СВОЙ АККАУНТ

Универсального средства, способного защитить от всех видов киберпреступлений, не существует. Однако есть базовые, но крайне важные меры, которые стоит регулярно применять, чтобы минимизировать риск хакерских атак и сохранять цифровую осознанность.

Чтобы защитить свой аккаунт от взлома или кражи необходимо:

- Внимательно читайте сообщения – если вы не просили вам что-то прислать, не переходите по ссылкам и не скачивайте файлы;

- Используйте надежный пароль, регулярно его меняйте, используя сложную комбинацию из букв разного регистра, символов и цифр;

- Включите двухэтапную аутентификацию в разделе «Конфиденциальность и безопасность»;

- Проверяйте активные сеансы в настройках и завершайте неизвестные;

- Установите разблокировку кодом-паролем, на случай если устройство украдут;

- Отключите автозагрузку файлов.

4 ТРЕБОВАНИЯ К ПАРОЛЯМ

Из-за слабого пароля злоумышленникам даже не приходится прибегать к фишингу. Чтобы не забыть пароль, пользователи используют простые комбинации типа «12345», «qwerty», «password» и другие – которые легко подбирают взломщики.

Надежный пароль нельзя угадать методом перебора, он должен:

- Состоять из букв разного регистра, символов и цифр;

- Содержать не менее 12 символов, а лучше больше;

- Быть уникальным для каждой платформы, где пользователь регистрируется;

- Меняться с частотой раз в 2–3 месяца;

- Быть абстрактным – не означать ничего, что связано с личной жизнью.

Чтобы взломать такой пароль, хакеру понадобится слишком много времени.

Специалисты подсчитали, сколько уйдет на подбор пароля в зависимости от его сложности. Комбинацию только из цифр взломают моментально, а 11-значный пароль из цифр и букв разного регистра – за 3 года.

Чтобы не запоминать сложную комбинацию самому, можно сохранить ее в менеджере паролей – стандартные есть в «Google-аккаунте» и на «MacOS». Существуют программы еще и с функцией генерации надежных паролей: «KeePass», «LastPass» или «1Password». Их можно установить на компьютер или в браузер.

5. ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

Многие социальные сети и мессенджеры предлагают пользователям двухфакторную или двухэтапную аутентификацию. Она нужна, чтобы подтвердить, что в аккаунт входит именно владелец, а не кто-то другой. После ввода пароля сервис запрашивает подтверждение с помощью смс-кода, кода внутри приложения, QR-кода и других вариантов.

Включить двухфакторную аутентификацию можно в настройках. В разделе «Безопасность» выберите пункт «Двухфакторная аутентификация» и способ, которым потом будет подтверждаться вход.

Кроме двухэтапной аутентификации, можно установить код-пароль – с его помощью можно заблокировать приложение, и злоумышленник не сможет войти в него, если получит доступ к телефону или компьютеру.

Хранить личные данные в переписке с собой или в избранном – еще одна угроза безопасности. Если аккаунт взломают, важная информация окажется в руках злоумышленников, и тогда пользователь потеряет не только доступ к этой учетной записи, но и к остальным. Для хранения паролей лучше использовать вышеуказанные менеджеры.

6. НЕ ПЕРЕХОДИТЕ ПО ПОДОЗРИТЕЛЬНЫМ ССЫЛКАМ

Кроме того, важно внимательно следить за тем, какие ссылки и файлы вам присылают, особенно если вы о них не просили. Аккаунт друга уже могли взломать злоумышленники и теперь нацелились на ваш.

Часто домен в ссылке отличается от знакомого всего одной буквой, не заметить легко. Стоит взять за правило вовсе не переходить на сайты из подозрительных сообщений и тем более не вводить на них свои данные. Скачивать файлы, которые прикреплены к таким сообщениям, так же опасно. Рекомендуем запретить в настройках автоскачивание, если такая опция есть, и установить антивирусное ПО – оно поможет определить угрозу.

7. РЕГУЛЯРНО ОБНОВЛЯЙТЕ ПРИЛОЖЕНИЕ

В каждом приложении есть уязвимости – лазейки, через которые хакер может получить доступ к данным. Чтобы обезопасить пользователей, разработчики находят уязвимости, устраняют их и выпускают новую версию приложения.

8. НЕ ПРИВЯЗЫВАЙТЕ БАНКОВСКИЕ КАРТЫ К ПРОФИЛЮ

Во многих социальных сетях есть возможность привязать к аккаунту банковскую карту для внутренних платежей. Достаточно ввести данные и подтвердить их один раз, а потом автоматически оплачивать подписку и другое. Но так платежные данные подвергаются дополнительной опасности – злоумышленник получит к ним доступ, как только взломает аккаунт.

Рекомендуем для платежей в социальных сетях завести отдельную карту, можно виртуальную, и каждый месяц переводить на нее нужные суммы.

9. НЕ АВТОРИЗУЙТЕСЬ ЧЕРЕЗ СОЦИАЛЬНЫЕ СЕТИ НА СОМНИТЕЛЬНЫХ САЙТАХ

Многие сайты предлагают упрощенную процедуру регистрации – через социальные сети. На самом деле это упрощает и работу взломщиков. Информация о доступе появляется на стороннем сайте, а если его взломают, то украсть аккаунты не составит большого труда.

Особенно опасно авторизовываться через социальные сети, к которым привязана банковская карта. В случае взлома стороннего сайта злоумышленнику остается пару шагов до платежных данных.

Несмотря на то, что интернет-мошенники всё активнее используют различные формы цифрового нападения, снизить риски и защитить данные и информацию помогает грамотное соблюдение принципов кибербезопасности, приведенные в указанных методических рекомендациях.