****

**Управление Росреестра по Республике Адыгея**

**Вопрос-ответ: как защищены данные собственников в реестре недвижимости?**

*В рамках рубрики «Вопрос – ответ» Росреестр еженедельно публикует материалы, посвященные разъяснению актуальных вопросов в сфере земли и недвижимости.*

**Цифровизация позволила сделать нашу жизнь значительно комфортнее. Теперь с помощью онлайн-сервисов можно оплачивать коммунальные услуги, записываться на прием к врачу и даже управлять собственной недвижимостью. При этом вместе с технологиями развиваются и схемы обмана пользователей. Эксперты Росреестра пояснили, какие технологии используются в ведомстве для обеспечения сохранности информации и как собственники могут самостоятельно защитить сведения о своих объектах недвижимости.**

**Какими способами в Росреестре обеспечивается защита данных о праве собственности?**

Современные технологии информационной безопасности позволяют оперативно выявить и пресечь постороннее вмешательство в электронные ресурсы Росреестра. Так, Федеральная государственная информационная система ведения Единого государственного реестра недвижимости (ФГИС ЕГРН) размещена в территориально распределенных центрах обработки данных. Во ФГИС ЕГРН предусмотрено резервное копирование информации на всех уровнях, благодаря чему устраняются риски потери, искажения или недоступности информации.

Доступ к системе сотрудников ведомства строго регламентирован: во всех субъектах РФ есть определенное количество государственных регистраторов, доступ каждого из которых персонифицирован, в том числе с применением усиленной квалифицированной электронной подписи, что позволяет контролировать процесс работы в системе на каждом из этапов и допускать только легитимных пользователей.

Вместе с тем данные об имуществе, хранящиеся в электронной системе Росреестра, имеют многоуровневую систему защиты как от киберугроз, так и от потери и искажения данных. В частности:

* проводится шифрование сетевого трафика в сети Росреестра с использованием средств криптографической защиты информации на основе отечественных решений и российских алгоритмов шифрования;
* на регулярной основе проводится аудит системы на наличие ошибок и сбоев;
* на регулярной основе проводится анализ защищенности и выявления возможных векторов кибератак на информационные ресурсы Росреестра;
* проводится автоматизированное архивирование базы данных на современный комплекс системы хранения данных;
* налажена система ежедневного резервирования данных, которая гарантирует целостность и сохранность ЕГРН.

Специалистам по информационной безопасности известно, где и в каком виде хранятся данные, кто может получать к ним доступ и какие ресурсы используются системой в любой момент времени. Средства идентификации и контроля доступа в сочетании с непрерывным мониторингом данных гарантируют безопасность.

Кроме того, в Росреестре организована системная работа по повышению информационной безопасности среди сотрудников ведомства. В рамках недели информационной безопасности в декабре 2021 года более 800 работников Росреестра прошли обучение на курсе «Основы информационной безопасности».

**Как защищены данные, получаемые с помощью электронных сервисов Росреестра?**

Официальный сайт Росреестра работает по протоколу безопасного соединения HТТPS, используя SSL-сертификат. SSL-сертификат содержит данные об организации, её владельце и подтверждает их существование.

Использование сертификата безопасности для сайта гарантирует:

* целостность передаваемой информации. При транспортировке от сервера к браузеру данные не изменятся и не потеряются;
* Конфиденциальность. Применяемый уровень шифрования исключает доступ злоумышленников к информации.

**Как собственники могут защитить свои данные и имущество?**

Для защиты собственности специалисты рекомендуют **внести информацию об адресе электронной почты в ЕГРН**. В этом случае правообладатель может оперативно получать из Росреестра информацию о любых действиях с его недвижимостью.

Указать адрес электронной почты можно при подаче заявления на осуществление учетно-регистрационных действий. Для этого адрес электронной почты нужно указать в нужной графе заявления.

Если права уже зарегистрированы, но в ЕГРН отсутствует адрес электронной почты, подать заявление о внесении данных сведений можно в любом офисе МФЦ, в [личном кабинете на сайте Росреестра](https://rosreestr.gov.ru/), а также по почте – в таком случае подпись на заявлении должна быть нотариально удостоверена.

Еще один способ защиты своей недвижимости – подача **заявления о невозможности государственной регистрации перехода, ограничения (обременения), прекращения права на принадлежащие объекты недвижимости без вашего личного участия**. В ЕГРН будет внесена соответствующая запись, и документы, поданные без личного участия собственника (например, по доверенности), рассматриваться не будут.
Их возвратят обратно заявителю.

Исключением являются случаи, когда основанием для учетно-регистрационных действий является вступившее в силу решение суда или требование судебного пристава-исполнителя. В этом случае обозначенная выше запись в ЕГРН не учитывается.

Такое заявление можно подать в отделениях МФЦ, в [личном кабинете на сайте Росреестра](https://rosreestr.gov.ru/) (в этом случае нужно иметь сертификат усиленной квалифицированной электронной подписи), а также в офисах Федеральной кадастровой палаты (если заявление подается экстерриториально). Это можно сделать и по почте – тогда подпись на заявлении должна быть нотариально удостоверена.

Не стоит забывать о **базовых правилах информационной безопасности:**

* храните пароли и конфиденциальные данные в автономном режиме;
* проверяйте безопасность подключения к сайтам и используйте только защищенное соединение (в адресной строке браузера перед адресом сайта должен стоять зеленый замок и должно быть прописано HTTPS);
* оставляйте личные данные только на сайтах с защищённым соединением;
* защитите свои учетные записи с помощью надежных паролей и двухфакторной аутентификации, не используйте одинаковый пароль для разных ресурсов;
* ни в коем случае никому не сообщайте свои пароли и другие личные данные;
* не нажимайте на подозрительные ссылки и не заходите на подозрительные сайты;
* не открывайте вложения от неизвестных отправителей, авсе вызывающие недоверие письма отправляйте в папку «спам»;
* своевременно обновляйте свое устройство и приложения;
* выбирайте сети с защищенным подключением и не используйте общественные сети Wi-Fi для передачи конфиденциальной информации;
* дважды проверяйте достоверность информации онлайн.

 **-------------------------------------**

Контакты для СМИ:

 (8772)56-02-48

01\_upr@rosreestr.ru

www.rosreestr.gov.ru

385000, Майкоп, ул. Краснооктябрьская, д. 44