



*О распространенных заблуждениях и реальном положении дел в сфере выявления страхового мошенничества с помощью проверки подлинности предоставляемых страхователями цифровых фотографий корреспонденту портала «Википедия страхования» рассказал исполнительный директор Департамента противодействия мошенничеству САО «ВСК» Владимир Клеев.*

– Владимир Анатольевич, в чем состоят мифы и какова реальность в проверке подлинности цифровых фотографий автоматической системой?

– Главный миф состоит в том, что с помощью автоматической системы проверки подлинности цифровых фотографий можно полностью искоренить мошенничество. Нет, это невозможно, но серьезно сократить объем фальшивых фотографий реально.

– А какие фальшивые фотографии выявляются с помощью этих программ?

– Прежде всего – имеющие «пиксельные» нарушения (обработка в фоторедакторах, клонирование, «рисование», ретуширование и т.д.), но если фотографии не «сжимались» и имеют достаточно высокое разрешение. Далеко не все фотографии с «пиксельными» нарушениями определяются такими программами, для начала необходимо ввести первоначальные требования к качеству проверяемой фотографии, разработать регламентирующие документы.

Второе – это фотографии, имеющие нарушения в EXIF-файлах (фотографии из разных фотосетов, сделанные различными камерами, с отредактированными EXIF-файлами и т.д.).

Третье – это фотографии, не отвечающие другим требованиям бизнес-процессов, установленных в страховой компании (например, не имеют геометок, не совпадает адрес акта осмотра и места, где проводилась съемка, и т.д.).

Главная задача автоматизированных систем проверки цифровых фотографий – закрыть доступ в страховую компанию фотографий, имеющих нарушения, и вовремя начать профилактику страхового мошенничества. Именно профилактика дает самый высокий результат по снижению расходов на ведение дела, а не борьба со страховыми «жуликами» постфактум.

– Есть ли еще «подводные камни» при проверке автоматической системой цифровых фотографий?

– Есть, и самый главный «камень» – это необходимость держать в штате сотрудников для проведения служебных расследований по выявленным инцидентам. Компетенции этих сотрудников должны быть достаточно высокими, соответственно, и заработная плата низкой быть не может. Если экономить на персонале в этом случае, можно получить проблемы в качественном принятии решений по выявленным фактам страхового мошенничества. Деньги, потраченные на приобретение и внедрение дорогостоящей программы, будут потрачены впустую.

И необходимо четко понимать, сколько стоит проверка одной цифровой фотографии, необходимо сделать аллокацию расходов и заложить это в расходы на ведение дела.

– То есть ручная проверка цифровых фотографий надежнее?

– Нет, вручную проверить все входящие в страховую компанию фотографии невозможно, это можно сделать только автоматической программой.

– А какие фотографии необходимо проверять в страховании?

– Прежде всего, это фотографии предстрахового осмотра по видам страхования.

Второе – это фотографии по «европротоколу» ОСАГО, так как страхователь делает эти снимки самостоятельно.

Третье – это фотографии при страховом случае, когда страхователь обращается для урегулирования к страховщику. В большинстве случаев их никто не проверяет, безоговорочно «доверяя» штатным сотрудникам и аутсорсерам, и совершенно зря. Доверяй, но проверяй.

И четвертое – фотографии со СТОА по скрытым повреждениям, там большое количество мошенничества со стороны партнеров в сговоре с сотрудниками страховщика.

– Какие главные проблемы при работе с цифровой фотографией?

– Если «пиксельный» анализ отечественные разработчики софта совершенствуют, и процент невыявленных фальсифицированных фотографий постоянно уменьшается, то со второй группой все плохо – EXIF-файл никак не защищен, и на законодательном уровне ничего для устранения проблемы не делается. Эта проблема во всем мире давно стоит достаточно остро, и, например, во многих фотобанках споры об авторском праве не утихают годами, и главная причина – отсутствие защиты EXIF-файла, который является, по сути, паспортом фотографии.

– Тогда расскажите, какие фотографии подделывают страховые мошенники.

– В сегменте недорогих транспортных средств в основном пытаются с помощью «пиксельного» рисования, клонирования, ретуширования застраховать автомобили с повреждениями, полученными до начала действия договора страхования. Но есть и фотографии аналогичных «двойников» с изменением EXIF-файлов, но это редко.

А вот при тотале и поджоге дорогих транспортных средств почти всегда идет «аналогичный» двойник и редактирование EXIF-файлов.

В фотографиях со СТОА при согласовании скрытых повреждений обычно применяется фоторедактор, намного реже меняют EXIF-файл.

Каждый раз страховое мошенничество с фотографиями индивидуально, и стандартов здесь не бывает, важно иметь профессиональный персонал, который умеет выявлять и расследовать факты страхового мошенничества в этом направлении, так как страховые мошенники с каждым годом «шлифуют» свое мастерство.

– Какие решения позволят эффективно бороться со страховым мошенничеством в фотографии?

– В настоящий момент, на мой взгляд, только создание специального софта, который не позволит мошенникам редактировать фотографию ни при каких условиях, и применение геометок. То есть непосредственно у себя страховщик использует специальный софт на смартфоне или фотоаппарате, которым производится съемка, а страхователь по «европротоколу» фотографирует повреждения транспортного средства смартфоном с авторизованным софтом, скачанным со специализированного ресурса.

Сейчас есть все возможности и условия создать и использовать такой софт и такие технологии, надо иметь только желание. Это позволит уменьшить количество случаев фальсификации цифровых фотографий в страховании, соответственно, и убыточность по страховым случаям значительно пойдет вниз.

До создания такого софта единственная возможность борьбы с мошенничеством – это

разработка требований к фотографиям внутренними регламентами и автоматическая проверка с расследованием выявленных инцидентов. А это тема отдельного разговора, если читателям будет интересно.

Источник: [Википедия страхования](#) , 14.09.15