О практике внедрения технологии распознавания фотомонтажа в страховой компании корреспонденту портала «Википедия страхования» рассказал исполнительный директор Департамента противодействия мошенничеству САО «ВСК» Владимир Клеев.

– Владимир Анатольевич, после публикации о проверке подлинности цифровых фотографий к нам поступили вопросы по автоматизированной системе для контроля достоверности цифровых фотографий, о которой Вы говорили. Поясните, пожалуйста, более подробно, что это такое.

– Совсем недавно на российском рынке стали предлагаться автоматизированные системы для контроля достоверности цифровых фотографий. Службы безопасности страховых компаний уже достаточно давно проверяют цифровые фотографии на предмет фотомонтажа, кто-то с переменным успехом, кто-то более успешно, так как страховые мошенники постоянно совершенствуют свое мастерство в фальсификации цифровых фотографий. Все эти проверки в ручном режиме происходят выборочно после наступления страхового случая, так как проверить все фотографии, которые поступают в страховую компанию, без автоматизированных систем было нереально. Сейчас такие решения появились, автоматизированная система интегрируется с ERP решением страховой компании и в автоматическом режиме, при загрузке цифровых фотографий проверяет последние на подлинность. То есть появился инструмент выявления страхового мошенничества на входе в страховую компанию договора страхования (хотя это вход условный, так как обычно полис уже выдан страхователю и договор страхования вступил в силу). Хотя по ряду видов страхования фотографии появляются на этапе андеррайтинга, но «заливают» их обычно позже. Все зависит от бизнес-процессов страховой компании, как они настроены менеджментом. В любом случае, при выявлении фотомонтажа появляется время для расторжения договора страхования, если информация подтвердилась, вне зависимости от того, заявлен

страховой случай или нет. Или, на крайний случай, для противодействия страховым «жуликам», которых после срабатывания системы мы уже «знаем в лицо», то есть система работает как индикатор страхового мошенничества. А сейчас очень часто страховая компания выплачивает страховое возмещение, вообще не подозревая о страховом мошенничестве, не имея возможности противодействия страховым «жуликам».

«Европротокол» аналогично подтолкнул страховые компании к внедрению автоматизированных систем для контроля достоверности цифровых фотографий, но успешных внедрений очень немного, отчасти это связано с тем, что случаев оформления по «европротоколу» мало, так как выполнить все требования по фото- и видеофиксации страхователям крайне сложно. Но «европротокол» развивается, и количество оформленных страховых случаев в дальнейшем будет расти, а проверить фотографии и видео, сделанные страхователями, в ручном режиме будет невозможно.

– Что главное при внедрении такой автоматизированной системы?

– Как это ни странно, чем меньше сотрудников страховщика знают о внедрении, тем лучше, так как страховые мошенники быстро «научатся» обходить ваше решение. А название вашей автоматической системы вообще должно быть тайной, в противном случае внешние «жулики» сначала протестируют фотомонтаж на аналогичной системе, а потом уже сдадут вам фотографии на проверку, заранее зная результат.

И конечно, необходимо иметь квалифицированный персонал для расследования выявленных инцидентов, иначе потраченные деньги будут выброшены на ветер.

– Какие основные ошибки допускаются при работе с такой автоматизированной системой?

– Это когда страховая компания вообще экономит на персонале и делает два режима: «зеленый» и «красный». При «зеленом» фотографии попадают в хранилище и о них забывают, при «красном» – автоматически возвращаются назад. Получив назад фотографии, страховые мошенники дорабатывают свои ошибки и спокойно сдают в следующую «заливку». А у добросовестных пользователей и контрагентов, у которых

идут ложные срабатывания, копится раздражение и недовольство работой службы безопасности.

Вторая ошибка – когда обслуживание автоматизированной системы и проведение расследований по выявленным инцидентам поручают кому угодно, но не службе безопасности страховой компании.

Третья ошибка: если в службе расследований по выявленным инцидентам работает некомпетентный персонал, который крайне слабо понимает, чем он занимается, например, не различает ретуширование и клонирование, то успеха в работе системы не будет.

Это основные ошибки, есть еще с десяток менее значимых, но не менее мешающих успешной работе системы.

– С чего надо начинать внедрение автоматизированной системы?

– С разработки регламентирующих документов, которые определяют требования к цифровым фотографиям для анализа, эти сведения вам даст вендор, чье решение вы выберете для внедрения.

Главное в настоящий момент – это исключить «сжатые» фотографии, кроме пакетной обработки, так как основное мошенничество совершается простым и эффективным методом «сильного сжатия», после этого установить подлинность фотографии невозможно. И второе – должно быть достаточно высокое качество фотографии, так как при низком разрешении произвести пиксельный анализ невозможно.

После разработки этих регламентов выяснятся все ваши «узкие места», которые не позволят вам сразу успешно внедрить решение. Обычно в самом начале это отсутствие ресурсов для хранения цифровых фотографий и «большой вес» пересылаемых фотографий по «узким» каналам удаленных филиалов. Позже постепенно приходит понимание о недостаточной квалификации обслуживающего персонала и

«шероховатости» взаимодействия с другими подразделениями компании.

Все эти проблемы решаемы, а экономический эффект увеличения финансового результата очень серьезен.

– В прошлом интервью мы коснулись создания специального софта для предотвращения редактирования цифровых фотографий, насколько это реально?

– Это совершенно реально, как, например, внедрение телематики в автостраховании. Совсем недавно телематика казалась недостижимой мечтой страховщика, а сейчас около десяти страховых компаний ее используют и довольны, так как страховые мошенники уходят в компании, где ее (телематики) нет. Конечно, в США и Европе проникновение телематики идет быстрее, российское страхование более консервативно, но все меняется достаточно серьезными темпами.

Так и со специальным софтом для фотосъемки. Его создание позволит серьезно сократить страховое мошенничество в цифровой фотографии. Сейчас проконтролировать своих сотрудников при фотосъемке сложно, а партнеров вообще малореально. И конечно, применение геометок позволит эффективно противостоять мошенникам, это реализовано и в телематике. Только мастерство страховых мошенников постоянно совершенствуется, они могут как полностью переписать EXIF-файл, а потом убрать следы фоторедактора сжатием, так и изменить геометки. Значит, одновременно с созданием специализированного софта необходимо предусмотреть защищенные от взлома боксы, где будут храниться сделанные специализированным софтом фотографии. А защита специализированных программ для съемки фотоизображений от взлома станет самой актуальной задачей, которая будет стоять перед службой информационной безопасности страховой компании.

Квалифицированным страховым мошенникам могут противостоять только сотрудники с высокими компетенциями, другого не дано.

Источник: Википедия страхования , 19.10.15