АНАЛИЗ СИСТЕМ ЗАЩИТЫ ОТ КОНТРАФАКТА И ФАЛЬСИФИКАТА

I. ВСТУПЛЕНИЕ.

Любое мошенничество связано с манипуляцией информацией.

Поэтому возможность проверить аутентичность предъявленной информации (ее подлинность, целостность, неизменность, актуальность и авторство)– является насущной проблемой для предотвращения различных злоупотреблений и мошенничеств.

В сфере электронной информации задача обеспечения аутентичности информации решена достаточно успешно – через использование технологии электронной подписи, проверка валидности (подлинности и действительности) которой позволяет получить информацию о подлинности, неизменности, целостности, неотказуемости от авторства, а также о времени подписания информации. И это ставит существенный барьер для различного рода мошенничеств.

Но сфера вещественных носителей информации еще долго будет присутствовать в нашей жизни. И когда простой человек имеет дело с вещественным носителем (бумажным документом, ценной бумагой, упаковкой, этикеткой, купюрой и т.п.) – он ВСЕГДА находится в зоне риска. Потому что в большинстве случаем может оценить надежность представленной ему информации сугубо **субъективно** – исходя из внешнего вида носителя информации и самой информации. Но ведь, как правило, у простого человека нет достоверных образцов бланка, печати, подписи, он не знает особенностей применяемой защиты, у него нет навыков сравнения имеющихся на вещественном носителе атрибутов (подписи, печати, элементов защиты и т.п.) с эталонным образцом. И только узкий круг подготовленных специалистов может эффективно пользоваться знаниями нюансов таких систем защиты. Но такие специалисты, как правило, привлекаются уже на стадии расследования совершенных мошенничеств. А было бы правильнее и логичнее иметь возможность любому человеку максимально просто и надежно убедиться в аутентичности представленной ему информации при ее первичном предоставлении – для того чтобы избежать мошенничества и обмана. Ведь мы сталкиваемся с обманом и фальсификацией информации намного чаще, чем нам кажется.

Но даже если мы имеем дело с подлинным документом (или товаром), то мы не можем оценить его **актуальность** на момент ознакомления с ним, так как подлинное служебное удостоверение может быть аннулировано, а подлинная доверенность отозвана.

Наиболее свежим примером может служить скандал с поддельными страховыми полисами ОСАГО, количество которых никто не может оценить достоверно, но счет идет на сотни тысяч.

Вполне логично, что для целей возможности отличить подделку от оригинала применяются различные системы защиты: от полиграфических (защитные бланки строгой отчетности; голограммы; стикеры и т.п.); до высокотехнологичных (чипы, RFID-метки, химические и т.п.).

Технический прогресс с одной стороны, дает возможность обеспечить защитой продукцию и документы, но с другой стороны – дает возможность и производителю подделок и контрафакта обходить или клонировать те средства защиты, которые используются для защиты оригинала.

В мире существует более сотни фирм, которые специализируются на создании различных систем защиты, которые призваны защитить оригинальный товар или документы. И это – помимо того, что и сами производители ищут свои собственные решения. *Например, Hewlett Packard в 2014 г. потратил на защиту своей продукции более $200 млн.*

Не ставя задачи заниматься рекламой или антирекламой этих фирм, производящих средства защиты, целью настоящего исследования является анализ существующих систем защиты с точки зрения их эффективности, надежности, стоимости и других параметров для простых потребителей, которых можно рассматривать как целую армию неподкупных контролеров, которые должны иметь возможность защититься от мошенничества сами и тем самым поставить самый надежный барьер для мошенничеств, в том числе и для сбыта поддельной или контрафактной продукции.

II. АНАЛИЗ СИСТЕМ ЗАЩИТЫ ОТ ПОДДЕЛОК.

При тщательном изучении существующих систем защиты, можно условно разделить их на несколько групп:

1. **Защита «Light».** Это использование особых пробок, упаковок, голограмм и других видов полиграфической или упаковочной промышленности, а также других чисто внешних атрибутов (водяные знаки, бумага, специальные волокна и нити, химическая защита, способы печати и т.п.). Основное направление развития

таких систем – **усложнение клонирования защитных знаков**. Для изготовления используется достаточно высокотехнологическое оборудование, как правило, полиграфической направленности. Основной способ проверки – визуальный, весьма субъективный, т.к. в момент проверки, как правило, под рукой нет эталонного образца, с которым можно сравнить предлагаемый образец защиты. В первую очередь это относится к значимым документам – удостоверениям, ценным бумагам, доверенностям и т.п.

К этой же группе относятся и различные сертификаты, которые **прикладываются** к товару и предъявляются потребителям или контролирующим лицам. Но, к сожалению, в большинстве случаем нет никакой **жесткой и надежной связи** между бумажным сертификатом (качества, подлинности, безопасности, санитарного и т.д.) и конкретной единицей товара. Кроме того, и сам сертификат может быть поддельным.

Такая защита легко обходится путем использования в упаковке товаров и оформлении документов таких же (или внешне похожих!) внешних атрибутов, а сложность их производства легко компенсируется сверхприбылью от сбыта.

РЕЗЮМЕ группы:

Преимущества:

1. **Доступность для потребителя**. *Присутствует на поверхности объекта защиты.*
2. **Упреждаемость.** *Можно воспользоваться ДО приобретения.*
3. **Дешевизна в реализации для производителя**. *В зависимости от применяемых средств защиты цена колеблется в достаточно большом диапазоне – до десятков рублей.*

Недостатки:

1. **Чисто субъективное восприятие**. *При отсутствии под рукой у потребителя эталонного образца защиты, для введения в заблуждения нет необходимости полного копирования, достаточно добиться «похожести».*
2. **Защита от копирования отсутствует.** *Даже при необходимости получить точную копию – сложность обусловлена только величиной затрат. Но в большинстве случаев, ввиду слабой осведомленности потребителей – достаточно добиться «похожести».*

* * *

2. Защита «ReadCode». Это системы защиты, основанные на кодировании в защитных метках информации о товаре**,** но реализуются на стыке полиграфии и инфотехнологий. Это может быть BAR-код, более современный QR-код или любая другая разновидность либо стандартного машиночитаемого кода, либо специально разработанного алгоритма преобразования информации в код. Для считывания используются специальные устройства, которые по заложенному алгоритму раскодируют информацию из кода и выводят результат. Как пример – акцизные алкогольные марки.

В последнее время появились и системы, при которых считать и раскодировать защитную метку и камерой мобильного телефона с использованием стандартных приложений.

РЕЗЮМЕ группы:

Преимущества:

1. **Дешевизна в реализации для производителя**. *Затраты производителя на обеспечение своего оригинального товара этими защитными метками незначительны.*
2. **Упреждаемость.** *Можно воспользоваться ДО приобретения.*

Недостатки:

1. **Отсутствует имитостойкость.** *Так в данной группе используется система КОДИРОВАНИЯ (кодирование – это замена читаемого символа на другой по «жесткой» связи, как пример – азбука Морзе) то понять какой алгоритм используется для преобразования исходной информации в ЗАКОДИРОВАННУЮ не представляет проблемы. Следовательно, злоумышленник, вычислив алгоритм преобразования, сможет по этому же алгоритму свою поддельную защитную метку на своем поддельном товаре или документе обеспечить той самой информацией, которая сможет ввести в заблуждение.*
2. **Доступность.** *Для использования зачастую необходимо специальное оборудование (акцизные марки).*

* * *

3. Защита «ReadAndBackConnect». Эти системы защиты основаны на принципе «обратной связи». По сути – это тоже продукты полиграфии, только с некоторым усложнением: на них имеются определенные уникальные идентификаторы (как правило – скрытые защитным слоем). После удаления этого слоя необходимо отправить идентификатор по определенному адресу, указанному на защитной метке. Как правило, используется в качестве канала связи SMS (услуга платная

для потребителя!). Как бесплатная альтернатива – можно ввести этот идентификатор на соответствующем интернет-портале. В ответ должна прийти информация о товаре, но может быть и более краткое «Товар подлинный». Этот вывод делается на основе наличия или отсутствия в запрашиваемой базе данных этого идентификатора.

РЕЗЮМЕ группы:

Преимущества:

1. **Дешевизна в реализации для производителя**. *При достаточно большом тираже затраты несущественные. На рынке есть предложения от 1 до 5 рублей за единицу.*

Недостатки:

1. **НЕупреждаемость.** *При наличии защитного слоя проверкой можно воспользоваться только ПОСЛЕ приобретения. В противном случае, удаление защитного слоя будет считаться повреждением упаковки в магазине.*
2. **Одноразовость.** *Не позволяет использовать для целей проверки многократно, т.к. в базе данных обычно фиксируется факт выбытия из оборота (на основании снятия защитного слоя, которое возможно только после покупки).*
3. **Относительная сложность.** *Как правило, идентификаторы представляют собой многозначное число (до 16 знаков), которое надо отправить в виде SMS на 11-значный номер. При этом услуга обычно платная.*
4. **Отсутствует имитостойкость.** *Достаточно сделать похожие метки с одним единственным идентификатором, но заменить номер для отправки SMS или адрес сайта для проверки. В этом случае при проверке поддельной метки на поддельном товаре или документе всегда будет приходить положительный ответ.*

* * *

4. Защита «ReadCodeAndBackConnect». По сути это гибрид двух предыдущих групп защиты. Только процесс проверки автоматизирован за счет использования машиночитаемых кодов. Для проверки могут использоваться как специальные устройства (как в планируемой к внедрению системы ЕГАИС), или смартфоны со специальным приложением. В некоторых случаях к запросу может добавляться дополнительная информация (например, координаты проверки). Вывод о подлинности осуществляется на основании ответа с центрального сервера, на основании наличия или отсутствия информации о данной защитной метке.

РЕЗЮМЕ группы:

Преимущества:

1. **Надежность**. *Более надежна по сравнению с предыдущими.*
2. **Доступность.** *Доступна для потребителя (за исключением системы ЕГАИС). Процесс проверки достаточно прост и как правило – бесплатный.*
3. **Упреждаемость.** *Можно проверить подлинность до приобретения.*
4. **Дешевизна в реализации для производителя**. *При достаточно большом тираже затраты несущественные. На рынке есть предложения от 1 до 5 рублей за единицу.*

Недостатки:

1. **Отсутствует имитостойкость.** *Достаточно сделать похожие метки, но заменить адрес обращения с запросом. В этом случае при проверке поддельной метки на поддельном товаре или документе всегда будет приходить положительный ответ.*
2. **Достоверность.** *Как правило, при проверках не учитывается роль проверяющего лица.*

* * *

5. Защита «Hi-Tech». Технологически продвинутые системы защиты, базирующиеся на специальных защитных метках, изготовляемых на достаточно дорогом оборудовании. Это различного рода высокотехнологические произведения, например: оптические или магнитные метки, особые добавки.

Эти метки могут нести в себе информацию о товаре, и довольно сложны для клонирования. Но для считывания этой информации необходимо дополнительное оборудование, которое обычно недоступно рядовому пользователю. Основа таких систем защиты, как правило – в сохранении в строжайшей тайне отличительных признаков этих систем защиты. Одна из бизнес-моделей работы таких систем: «Если хотите убедиться в подлинности приобретаемого товара, но вызовите нашего эксперта и он подтвердит или опровергнет утверждение о подлинности». Обойти такую защиту сложнее, чем системы группы «Light». Хотя понятие «сложнее» - это чисто **количественное** понятие, и если сложность может быть компенсирована сверхдоходами – клонирование перестает быть проблемой.

РЕЗЮМЕ группы:

Преимущества:

1. **Упреждаемость.** *Можно воспользоваться ДО приобретения.*
2. **Повышенная устойчивость к копированию.** *Создает более серьезные препятствия (а, следовательно, и большие расходы) для клонирования.*

Недостатки:

1. **Недоступность и сложность в использовании для потребителя.** *Необходимость иметь специальное оборудование, на сегодняшний день недоступное для рядового пользователя.*
2. **Дороговизна в реализации для производителя**. *Затраты оправданы только при достаточно большом тираже и высокой стоимости защищаемого товара.*

* * *

6. Защита чипами. Данная система становится все популярнее. Основана на обеспечении объекта RFID-меткой, представляющим из себя тонкую этикетку с нанесенными на нее антенной и чипом, обеспечивающая дистанционное чтение и запись информации. При этом перезапись защищается от несанкционированных действий.

РЕЗЮМЕ группы:

Преимущества:

1. **Упреждаемость.** *Можно воспользоваться ДО приобретения.*

Недостатки:

2. **Дороговизна для производителя.** *Экономически оправдана только для при достаточно большой цене защищаемого объекта.*
3. **Ограниченная доступность** *Необходимость иметь специальное оборудование, на сегодняшний день доступное для рядового пользователя только в ограниченных моделях смартфонов.*
4. **Отсутствует имитостойкость.** *При всей сложности чипа и его защищенности, остается возможность скопировать выдаваемый им сигнал и записать его на другую RFID-метку, которой обеспечить подделку.*
5. **Уязвимость.** *Вполне реальной угрозой является возможность дистанционного вывода RFID-меток из строя путем применения мощного электромагнитного импульса. В Интернете уже представлены инструкции как самостоятельно изготовить такие устройства на базе электрошокеров или фотовспышек. Таким образом, возникает угроза создания коллапса – например, вывод из строя чипов на больших партий защищенных изделий, которые после этого будут признаны нелегитимными.*

* * *

7. Защита «INFO». Это максимально широкое информирование потребителей об отличительных особенностях оригинальной продукции, в том числе и о защите, примененной к оригиналу.

К сожалению, это направление вряд ли можно считать эффективным и надежным. Потому что, во-первых, невозможно запомнить или иметь под рукой информацию об особенностях всей предпочитаемой оригинальной продукции. Во-вторых, эта информация в первую очередь интересует производителей фальсификата, т.к. благодаря ей он может достаточно быстро устранить отличия между его подделкой и оригиналом.

Если такое информирование предназначено не широкому кругу потребителей, а только тем лицам, которые в силу своих служебных обязанностей осуществляют контроль подлинности продукции, то, во-первых, эти контролирующие лица могут охватить контролем только небольшие группы товаров, а во-вторых, те сверхдоходы, которые получает рынок контрафакта, могут склонить проверяющего на реакцию, отличную от его служебных обязанностей, тем более о факте выявления контрафакта знают только проверяющий и проверяемый.

РЕЗЮМЕ группы:

Преимущества:

1. **Доступность для потребителя**. *Эту информацию можно получить из СМИ или общедоступных информационных ресурсов в Интернете.*
2. **Упреждаемость.** *Можно воспользоваться ДО приобретения.*
3. **Дешевизна в реализации для производителя**. *Затраты только на размещение этой информации.*

Недостатки:

1. **Доступность для потребителя**. *Необходимо запоминать или иметь под рукой большой объем информации, что практически невозможно.*
2. **Фактически является разглашением коммерческой тайны.** *Такое информирование существенно упрощает для производителя фальсификата достижение максимального сходства поддельной продукции с оригиналом.*
3. **Является временной мерой.** *После устранения отличий между подделкой и оригиналом эта информация теряет свою актуальность.*

* * *

III. РЕКОМЕНДАЦИИ ПО «ИДЕАЛЬНОЙ СИСТЕМЕ ЗАЩИТЫ»

Обобщив все достоинства и недостатки, присущие каждой из рассмотренных групп систем защиты, можно сформулировать **принципиальное решение** для надежной защиты оригинального товара или документа от подделки:

Надо создать такие условия, когда оригинальный объект (товар или документ) при выпуске в обращение должен быть обеспечен такой защитой, на основании которой любое заинтересованное лицо (в первую очередь – рядовой потребитель) сможет без особых усилий отличить оригинал от подделки с учетом его роли.

При этом и факт проверки, и результаты этой проверки должны быть зафиксированы, и предоставлены в юридически значимом виде.

Необходимо отметить, ничего нового в этой идее нет. Уже давным-давно эта идея воплощается в жизнь различными способами и в отношении разных вещей: от простых товаров до денежных знаков. Но, тем не менее – подделки существуют и среди товаров, и среди денег.

Значит, проблема не в идее, а в ее реализации.

Исходя из всего вышеизложенного, можно сформулировать

ТРЕБОВАНИЯ ДЛЯ ИДЕАЛЬНОЙ СИСТЕМЫ ЗАЩИТЫ:

1. **Система должна быть достаточно дешевой для производителя или лица, гарантирующего подлинность.** *То есть не должна существенно влиять на ценообразование оригинальной продукции.*
2. **В части проверки Система должна быть доступной для любого заинтересованного лица - конечного потребителя, посредника в перемещении и сбыте, контролирующего органа.** *Пользование ею не должно создавать сложностей и не быть затратным.*
3. **Система должна быть «упреждающей».** *То есть у конечного потребителя должна быть возможность осуществить проверку **ДО** приобретения товара, и **БЕЗ** повреждения упаковки (того же защитного слоя на метке защиты).*
4. **Система должна быть устойчивой к копированию защитных меток.** *Но не через усложнение их полиграфическими изысками, а через **внутреннее содержание** этих меток. То есть, копирование одной защитной метки и размеще-*

ние клонов на партии подделок не должно давать возможность получения положительного результата о подлинности проверяемого фальсификата.

5. **Система должна быть надежной.** *Попытки вывода из строй элементов системы должны быть исключены.*
6. **Система должна работать на принципе «обратной связи».** *То есть на технологии «запрос-ответ». При этом ответ должен быть достоверным и из надежного источника. Ответ должен содержать и информацию об актуальности проверяемой информации на момент проверки.*
7. **Система должна быть имитоустойчивой.** *То есть исключить (или максимально усложнить!) возможность подмены информации, содержащейся в запросе, подмены информационного ресурса, куда идет обращение и откуда приходит ответ на запрос. Результат ответа и источник не должны иметь возможность подменяться в интересах злоумышленника.*
8. **Система должна быть универсальной.** *То есть должна быть возможность защищать ею любые группы товаров и документов и давать возможность проверить подлинность любому заинтересованному лицу с учетом его роли.*
9. **Система должна быть гибкой.** *То есть должна быть возможность «тонкой настройки» на различные сценарии ее использования и реакции с учетом роли проверяющего лица.*
10. **Система должна быть «фиксирующей».** *То есть все запросы и ответы должны фиксироваться.*

* * *

IV. ЗАКЛЮЧЕНИЕ

При создании системы, обладающей такими свойствами, появляется возможность реализовать примерно следующий сценарий, который даст достаточно положительный эффект для защиты и производителей, и потребителей от рынка контрафактной и поддельной продукции:

1. Добросовестный производитель обеспечивает свою оригинальную продукцию защитными метками, таким образом, чтобы их отделение от товара было невозможно в принципе (например, печатает их на первичной упаковке), или же это отделение было невозможно без видимых повреждений.
2. Конечный потребитель, желая приобрести предлагаемый товар, имеет возможность проверить его подлинность с использованием защитных меток и доступных средств (например, мобильное устройство со специальным приложением). При желании представители контролирующих органов смогут проверять подлинность товаров.

3. Проверив подлинность товара, конечный потребитель получает **гарантированно** достоверный ответ из **надежного** источника, с исключением возможности подмены ответа или источника. Ответ должен быть представлен в юридически значимом виде.

4. В случае отрицательного ответа или предупреждения о риске того, что проверяемый товар является подделкой (например, в случае многократной проверки одной и той же товарной единицы, или в случае если она уже продана), конечный потребитель воздержится от приобретения этой товарной единицы и, либо будет проверять другую товарную единицу, либо вообще откажется от приобретения товара в данном магазине.

5. Все результаты проверки должны фиксироваться для анализа и принятия мер для пресечения сбыта – независимо от желания проверяющего лица.

6. Отсутствие возможности сбыть подделку через магазин должно подвигнуть владельца магазина на более тщательную проверку поставляемого товара (путем аналогичной проверки подлинности товара) или отказаться от сомнительного, который будет невозможно или затруднительно продать.

А невозможность сбыта поддельного товара сделает экономически невыгодным его производство.