Разрушение устоев: аутентификация без факторов

En **Destruction of Foundations: Authentication without Factors**

S. V. Konyavskaya,
PhD (Philology)
OKB SAPR, Moscow Physics and Technology Institute
cd@okbsapr.ru

The article is devoted to the analysis of the existing classification of authentication data and the proposal for its improvement. It is shown that the classification of data using a list of «authentication factors» does not meet the requirements for classifications, as well as the current state of science and technology. The alternative classification proposed in the article is based on this experience and the requirements for scientific classifications.

Keywords: authentication data, authentication, authentication factor

Статья посвящена анализу существующей классификации аутентификационных данных и предложению ее усовершенствования. Показано, что классификация данных с помощью перечня «факторов аутентификации» не соответствует требованиям к классификациям, а также современному состоянию науки и техники. Предложенная в статье альтернативная классификация строится с учетом этого опыта и требований, предъявляемых к научным классификациям.

Ключевые слова: аутентификационные данные, аутентификация, фактор аутентификации

Светлана Валерьевна Конявская,
кандидат филологических наук
ОКБ САПР, Московский физико-технический институт
cd@okbsapr.ru

О науке и технике (или спор о словах)

Довольно часто приходится слышать о том, что спорить о терминах нельзя, что давать определения понятиям не обязательно, поскольку «и так всем ясно» что это означает, и «зачем говорить о словах, когда можно – о деле». Таким образом, чтобы прослыть дельным человеком, словам следует придавать как можно меньше значения. Это иногда приводит к тому, что теоретические построения в так называемых «тех.» науках получаются заметно более приблизительными, чем в «не тех.». В таких случаях, думается, надо начать с начала – в строгом соответствии с общей прикладной теорией систем [1] и Интернационалом.

В свое время «Факторы» аутентификации сыграли положительную роль в популяризации вопросов аутентификации за счет своей наглядности. Однако в настоящее время они используются как фундамент системы представлений об этом феномене [2], что представляется неприемлемым.

Общим местом является список из трех факторов (знание, владение, биометрия (обладание некоторой биологической особенностью)). Согласно NIST [3], биометрический фактор является дополнительным, способным подтвердить обладание субъекта тем предметом, который для него воплощает фактор «владения» (например, биометрическое подтверждение того, что данная смарт-карта принадлежит определенному человеку): «Биометрия ДОЛЖНА (*выделено в источнике*) использоваться только как часть многофакторной аутентификации с физическим

аутентификатором (*то, что у вас есть*)» [3, раздел 5.2.3][1]. То есть в многофакторной аутентификации этот «фактор» может быть только третьим. Если *заменить* ввод пароля к смарткарте предъявлением отпечатка пальца, то аутентификация перестанет считаться многофакторной, так как допустимо только *добавить* предъявление биометрического признака[2].

Иногда к факторам также относят расположение аутентифицируемого субъекта в определенном месте [4], но, согласно ISO, – это не фактор, а лишь свидетельство, то есть данные, которые могут дополнительно привлекаться для усиления уверенности в положительном результате аутентификации или при первичной идентификации. В то же время, согласно ISO/IEC 29003, факторов все-таки четыре, но четвертый – это не расположение в пространстве, а характерные для субъекта действия (например, какие-то поведенческие паттерны) [5, раздел 3.6].

Использовать инструмент популяризации в целях классификации и кодификации – неверно, однако это происходит [3, 5, 6, 7], порождая коллизии, которые приходится снимать, вводя большое количество разных оговорок относительно того, как и что понимать в каком контексте.

Пришло время признать, что использование системы понятий, сформировавшейся вокруг сленгового идиоматического выражения «факторы аутентификации», на современном этапе развития науки и техники вредно и должно быть прекращено.

Нет ничего практичнее хорошей теории, поэтому для проверки собственной убежденности в том, что от «факторов» необходимо отказаться, прибегнем к научной методологии.

В отношении классификаций в научном исследовании возможна постановка нескольких принципиальных вопросов:

1) является ли рассматриваемое классификацией, или имеет место результат какой-то другой операции над предметом изучения – именно к классификации применимы требования быть исчерпывающей, построенной на одном основании, причем на основании одинаково значимого для всего классифицируемого множества признака, и т. д.;

2) корректна ли классификация, то есть соответствует ли она действительному наблюдаемому положению вещей;

3) целесообразна ли классификация, то есть продуктивна ли она, позволяет ли она решить какие-либо задачи (прогнозирование, объяснение причин и др.), устанавливаются ли соответствие или связи иного рода между нею и другими фрагментами научного описания того же сегмента действительности.

Всегда желательно минимизировать изменения в устоявшейся практике, поэтому если выявлено, что классификация аутентифицирующих данных, в настоящее время в научном обороте представленная перечнем «факторов аутентификации», построена с нарушениями, но при этом целесообразна, то имеет смысл постараться ее сохранить, устранив недостатки, а не создавать новую классификацию на других основаниях.

Означаемое и означающее

Определение «факторов»

Понятие, лежащее в основе классификации, очевидно, должно быть определено, так как этим определением задаются границы класса. Необходимо, чтобы все, что попадает в область определения этого понятия – каждый конкретный случай его проявления – можно было отнести к какой-либо из выделяемых классификацией групп. Без такого определения проверить корректность и полноту классификации нереально.

Определение фактора аутентификации дано в проекте «ГОСТ Р. Идентификация и аутентификация. Общие положения» [6]: «фактор аутентификации: вид (форма) существования аутентификационной информации, предъявляемой субъектом доступа или объектом доступа при аутентификации».

Похожее определение есть в [4] и других работах. Определение из проекта ГОСТа предлагается к рассмотрению потому, что он разработан теми же авторами и является последним по хронологии, то есть аккумулирует результаты развития их взглядов на предмет.

Однако все, что возможно почерпнуть из этого определения, – это то, что понятие фактор *каким-то образом связано* с аутентифицирующими данными (так как «предоставляемые при аутентификации» и «аутентифицирующие» – в общем случае синонимичные выражения). Как именно связано – напрямую установить невозможно, поскольку смысл словосочетания «вид существования информации» (или «форма существования информации») – не ясен.

Надо отметить, что «форма существования» – это формула, естественная для научного дискурса вообще, и к понятию информации она применяется достаточно часто. По системе определений, сформулированной А. А. Стрельцовым [8], информация существует в форме сведений и сообщений, при этом и та, и другая форма существования информации – определены и четко отделены одна от другой. По системе

[1] *В пункте 4.2.1 при этом есть примечание: «Примечание. Если биометрическая аутентификация соответствует требованиям, изложенным в разделе 5.2.3, устройство должно быть аутентифицировано в дополнение к биометрической – биометрия признается как фактор, но сама по себе не распознается как аутентификатор. Поэтому при проведении аутентификации с использованием биометрии нет необходимости использовать два аутентификатора, поскольку связанное устройство служит „чем-то, что у вас есть“, в то время как биометрия служит „тем, чем вы являетесь“».*
Чтобы исключить искажение смысла некорректным переводом, приведем оригинал: «Note: When biometric authentication meets the requirements in Section 5.2.3, the device has to be authenticated in addition to the biometric – a biometric is recognized as a factor, but not recognized as an authenticator by itself. Therefore, when conducting authentication with a biometric, it is unnecessary to use two authenticators because the associated device serves as „something you have“, while the biometric serves as „something you are.“». Судя по всему, этот текст тоже указывает на некоторую несвободу биометрического признака, хотя и не говорит ничего о природе этой несвободы.

[2] *Благодарю А. Г. Сабанова за это уточнение, данное в личной беседе.*

определений В. А. Конявского [9], в цифровой среде следует говорить не об информации как таковой, а о ее отображении (если провести параллель с системой определений Стрельцова, то в ней сведения отображаются в сообщениях). Отображается информация или в статической форме – в форме данных (чисел, представляющих собой упорядоченное множество символов) или в форме процессов – динамической форме. В обеих системах дефиниций понятны и природа определяемых феноменов, и их взаимосвязи, и следствия из них – «форма существования» информации в виде сведений и сообщений позволяет выделить и определить предмет правоотношений, форма существования в виде данных и процессов – построить модель электронного документа и его защиты.

Что позволяет прояснить существование аутентифицирующей информации в форме факторов аутентификации?

Поскольку определение должно анализироваться не изолированно, а в совокупности с введенным в научный оборот закрытым перечнем «факторов аутентификации», можно сделать вывод, что «вид» и «форма» здесь парадоксальным образом характеризуют как раз не форму, а содержание. Целесообразность такого оксюморона в научном определении представляется не очевидной. Речь ведется о разделении всех возможных для применения в процессе аутентификации данных на классы по их содержанию (по тому, какова их диктумная предметность, *чем* в реальном физическом мире является их источник – знанием, характеристикой какого-то предмета, физиологической особенностью, местом, образом действия). «Расположение в пространстве» – это не форма и не вид существования геолокационных данных, это метафорическое высказывание, а метафоры, как и оксюмороны или любые другие тропы, желательно исключить при построении основ системы.

Содержание понятий раскрывает, помимо определений и прямых классификаций, контекст их применения. В другом проекте ГОСТа [7] упоминается еще один процесс (помимо предъявления при аутентификации), в котором участвуют аутентифицирующие данные и факторы аутентификации: «для достоверного установления соответствия необходимо осуществить привязку идентификационных данных к субъекту (объекту) доступа. При этом должны использоваться механизмы привязки с использованием следующих факторов…». Здесь снова, казалось бы, создается некоторый интуитивно понятный образ: данные с помощью чего-то привязываются к субъекту, который будет затем их предъявлять. Но, вообще говоря, совершенно не понятно, что же именно за этим стоит, если пытаться рассмотреть какой-то конкретный пример. Например, отпечаток пальца – идентификационные данные человека. Он *привязывается к субъекту с использованием биометрического фактора*? Что это может означать? Как можно привязать информацию к чему-либо с помощью формы ее же существования?

При обсуждении терминов часто высказывается позиция о том, что обсуждение употребления тех или иных выражений только отвлекает от сути вопроса, заставляя искать и запоминать новые формулировки для того, что и так понятно: ведь все, кто использует слово «доступ» или «фактор», или иное обсуждаемое – прекрасно понимают, о чем идет речь, а давать красивые определения – дело гуманитариев. Разобранные выше примеры показывают, что это «понимание» – мнимое, оно исчезает сразу, как только задаешь себе вопрос «что конкретно?»

Как гуманитарий могу объяснить также то, почему нельзя просто переопределить понятие «фактор» более удачно и оставить общественности привычное словоупотребление. Казалось бы, в случае номинального определения – то есть присвоения некоторому явлению некоторого имени – рассуждать о том, что «на самом деле – это не так», – неуместно. Как условимся – так и будет, речь может идти только о целесообразности или нецелесообразности определения, а не о его истинности или ложности.

Во многом это справедливо, но есть одно ограничение – полностью свободны мы в назначении определения словам, которые до сих пор не значили вообще ничего. Пока слово «слон» свободно от значения – мы можем определить его как мелкого грызуна с рыжей шерстью, но как только у слова «слон» появляется некоторое значение, вошедшее в употребление и закрепленное словарями, эту свободу определения мы утрачиваем, и договориться называть грызуна слоном больше нельзя, даже по взаимному согласию (за исключением, конечно, каких-то игровых контекстов).

Так вот, у слова «фактор» уже есть значение:

«ФАКТОР, -а; м. [от лат. *factor* – делающий, производящий] Книжн. Существенное обстоятельство, способствующее какому-л. процессу, явлению. *Учесть все факторы. Немаловажный ф. Постоянно действующий ф. Неизбежный ф. Ф. времени. Ф. успеха, победы. Ф. внезапности* (*воен.*; неожиданные для противника действия, способствующие его поражению). *Поражающие факторы ядерного взрыва* (совокупность причин, приводящих к разрушениям, смерти). *Человеческий ф.* (роль и значение человека в общественной жизни, в социальных процессах; всё то, что связано в этих процессах с человеком как субъектом деятельности)» [10].

То есть словосочетание «фактор аутентификации» может означать или обстоятельство, влияющее на аутентификацию, или саму аутентификацию как влияющее на что-то явление[3]. Назначить этому выражению смысл «вид (форма) существования информации» нельзя ни на

[3] *К слову, при словарной трактовке слова «фактор» и знание чего-либо, и владение чем-либо, и биологические признаки чего-либо – действительно являются факторами аутентификации – то есть тем существенным обстоятельством, которое оказывает на аутентификацию влияние, способствует ей, должно учитываться. Надо признать, что эта трактовка разрушает всю построенную вокруг «факторов аутентификации» систему терминов, то есть ее принятие, фактически, равносильно отказу от «факторов*

русском, ни на английском языке, где слово *factor* тоже, разумеется, имеет латинское происхождение.

Однако, даже если неприемлемы и сам термин, и его определение, все же имеет смысл рассмотреть саму классификацию. Если она сама по себе жизнеспособна, то, вероятно, замена термина на более удачный позволит оставить ее в целом неизменной.

Классификация «факторов»

Основания считать, что перечень факторов аутентификации позиционируется как классификация, есть. Перечень классов всегда представляется как закрытый, несмотря на то, что факторов от 2 до 4. При этом самих пунктов 5 (знать, владеть, биометрия, расположение, поведение), но все 5 одновременно в одном перечне никогда не встречаются. Более того, в построениях, в которых факторы используются вне перечней, эксперты ISO склонны, напротив, сужать количество факторов «в чистом виде» до 2, а остальные называть «дополнительным», «свидетельством» и т. д.

Однако в классификации должен быть ясно выраженный классификационный признак, все классы должны быть выделены на одном основании и, наконец, классификация должна быть исчерпывающей и желательно постоянной в своем составе (или, по крайней мере, разные представления о составе классификации должны быть соотнесены между собой в какой-то дискуссии, а не просто существовать параллельно).

Классификационный признак

Классификационный признак должен быть связан с целью, для которой проводится классификация, он должен быть объясним. Однако не удается обнаружить явных причин, которые бы объясняли тот факт, что классифицировать аутентифицирующие данные целесообразно именно *по содержанию*. Более того, в случае *использования* «факторов» аутентификации в построении дальнейших рассуждений в дело идут не содержательные характеристики данных, а признаки, характеризующие степень их связанности с субъектом (чаще всего – *насколько необходимо* вступать в *насколько тесный* контакт с субъектом, чтобы завладеть этими данными). Другими словами, разделяются феномены на группы по одному признаку, а далее используются другие признаки, свойственные этим же группам.

Единое основание

О едином основании в перечислении «знать, владеть, биометрия» говорить невозможно. Если отклонить «биометрию» как «дополнительный» фактор, все равно невозможно выделить ясно формулируемое основание, более узкое, чем «признак».

Полнота классификации

I. Охвачены не все типы субъектов.

Первое, что необходимо отметить в связи с полнотой классификации: классификация «знать – владеть – биометрия» оставляет полностью не закрытым один из двух (!) типов субъектов аутентификации.

Неуниверсальность подхода становится очевидной при попытке применения «факторов» для создания общего описания процессов идентификации и аутентификации *любых субъектов:* не только пользователей в смысле людей, но и сущностей цифровой природы. Именно это мы наблюдаем в разрабатываемом ГОСТе [7], в частично уже приведенном фрагменте:

«Для достоверного установления соответствия необходимо осуществить привязку идентификационных данных к субъекту (объекту) доступа. При этом должны использоваться механизмы привязки с использованием трех факторов[4].

1. *Фактор знания.* Привязка устанавливается с использованием информации, которая известна субъекту (объекту) доступа.

2. *Фактор владения.* Привязка устанавливается с использованием идентификационных данных, которые имеет (которыми обладает) субъект (объект) доступа. При этом идентификационные данные свойственны (присущи) субъекту (объекту) доступа или содержатся в его свидетельствах, представляющих собой документальное подтверждение. Субъект (объект) доступа должен правомочно обладать данными свидетельствами.

3. *Фактор биометрический.* Привязка устанавливается по результатам верификации биометрических характеристик, которые свойственны субъекту доступа. При этом принимается, что эталонные характеристики субъекта доступа действительно принадлежат ему.

Примечания

А. Условно считается, что при привязке для субъектов доступа и объектов доступа, которые являются информационными и вычислительными ресурсами (средствами вычислительной техники, автоматизированными (информационными)

аутентификации» как основы всех дальнейших построений (например, если попытаться подставить это значение в «многофакторную аутентификацию», получается очевидный тупик). Важнее, однако, другое – в своем «словарном» значении понятие «фактор аутентификации», скорее всего, не может быть положено в основу классификации, так как исчерпывающий перечень факторов, влияющих на аутентификацию, едва ли возможно сформировать и привести к единому основанию. В этот список, например, необходимо будет включить фактор времени аутентификации (причем, в обоих смыслах – и продолжительность процедуры, и время (год, день недели, время суток), в которое она может завершаться по-разному), фактор дееспособности субъекта (или исправности, если субъект не является человеком), фактор намерения (субъект может иметь целью пройти аутентификацию успешно или наоборот – неуспешно, подтвердить, что он «тот» или подтвердить, что он, напротив, «не тот») и тому подобные явления. Вероятно, можно составить классификацию типов факторов, но сама эта классификация и ее задачи будут далеки от того, как используются «факторы аутентификации» сейчас. Это не говорит о ненужности такой работы (например, она может быть полезной при составлении Модели угроз и при выборе способа и реализации системы аутентификации), но ее целесообразность нуждается в оценке и обосновании.

[4] *Общая характеристика факторов – по ГОСТ Р Идентификация и аутентификация. Общие положения.*

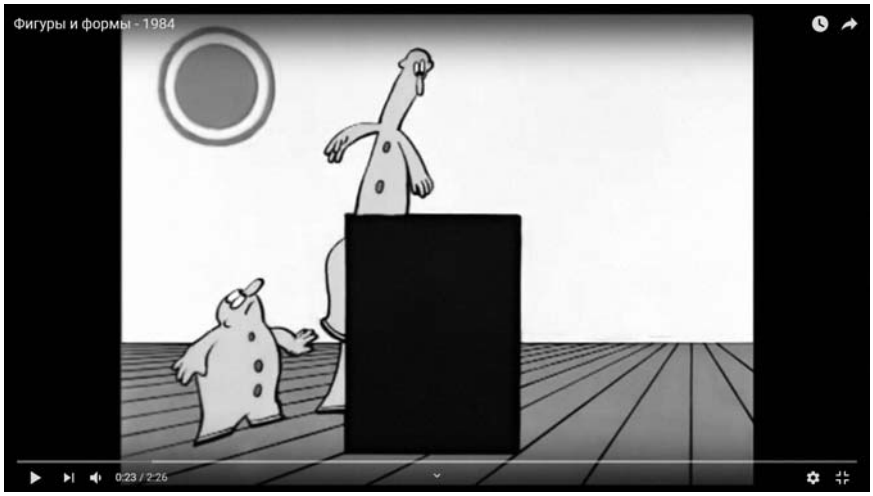

Рис. 1. ***Кадр из начала мультфильма «Фигури и форми»***

системами и т. п.) может использоваться один фактор – фактор владения.

Б. Привязка с использованием биометрического фактора применяется для субъектов доступа, ассоциированных с физическими лицами. Порядок и правила применения фактора биометрического определяются соответствующими действующими нормативными правовыми документами и документами по стандартизации».

Отдельно надо заметить, что примечание *Б* избыточно, так как в примечании *А* уже указано, что применяться может только один фактор, стало быть отдельно оговаривать невозможность применения одного из оставшихся не имеет смысла, однако это лишь проект стандарта, и его редактирование продолжается.

Очевидно, что не просто «не все», а ни один из «факторов» (кроме относительно нового и «не совсем фактора», который коротко назовем «расположение») не может быть *без оговорок* отнесен ни к процессу, ни к техническому или программному средству, ни к информационной системе в целом (ничто из перечисленного не может ни знать, ни владеть, ни иметь биологические особенности).

Представляется, что связанность информационных и вычислительных ресурсов скорее соотносится с биометрическими признаками человека, чем с владением, однако на таком метафорическом уровне разговор о технических параметрах в любом случае не вполне уместен.

Оговорки позволяют некоторым образом снять самые очевидные противоречия, однако терминологическая система, подходящая без оговорок только одной из двух глобальных групп субъектов, очевидно, несовершенна.

II. Охвачены не все фактически применяемые для аутентификации виды данных.

Эмпирически из словоупотребления в стандарте и дискуссиях вокруг него выявляется, что «формы существования» аутентифицирующих данных, которые без оговорок не укладываются в «знать» и «владеть», зачастую называются «свидетельствами». Например, паспорт – это официальное свидетельство. Действительно, в парадигме «знать – владеть – биометрия» классификация паспорта как того, с помощью чего человек аутентифицируется, затруднительна хотя бы потому, что некоторые из паспортов – биометрические, а некоторые – нет. А главное, в отношении паспорта представляется весьма сомнительным установление связи «владение». С другой стороны, кроме этого затруднения, нет никаких причин отказывать паспорту в том, что он является носителем аутентифицирующих данных.

Но свидетельства в парадигме понятий ГОСТов [6, 7] могут применяться только в процессах идентификации, а не аутентификации, а значит, паспорт не может применяться для аутентификации, а только – для идентификации[5]. Хотя наблюдение над практикой аутентификации показывает обратное.

Разумеется, не охвачены классификацией те виды данных, которые предъявляются субъектами цифровой природы – контрольные суммы, серийные номера, *unique identifiers* (UID) и аналогичные им.

Таким образом, наблюдается разрыв между кодифицируемой аксиоматикой и практикой уже на этапе разработки первой, а это значит, что в дальнейшем он будет только увеличиваться.

О влиянии точки зрения на реальность

Любопытно, что между приведенными в качестве примеров серийными номерами и паспортом гораздо больше общего, чем представлялось сначала. В обсуждении представленных в этой статье выкладок от некоторых специалистов-практиков звучали возражения, что серийные номера и UID – это идентификаторы, а отнюдь не аутентификаторы. Легко заметить, что это возражение абсолютно симметрично утверждению А. Г. Сабанова о том, что идентификатором, а не аутентификатором, является паспорт человека.

В 1984 году был снят гениальный болгарский мультфильм «Фигури и форми»[6] (это на болгарском, поэтому название выглядит странно). В нем высокий и низкий человек смотрят на один и тот же объект и спорят о том, круг это или квадрат (рис. 1).

В конце мультфильма объект падает и выясняется, что это цилиндр (рис. 2), однако герои продолжают спорить, так как теперь высокий видит квадрат, а низкий – круг. И только тот, кто, как выяснилось, был

[5] *Этот вывод не является вымыслом автора, он получен от А. Г. Сабанова в личной беседе о том, к какому фактору аутентификации относить паспорт.*

[6] *https://www.youtube.com/watch?v=tMpkcpTSN_s/.*

внутри объекта, сообщает героям, что это – цилиндр.

Разумеется, правы оба героя, так как они ясно определяют то, что видят. Однако видят они то, что видно с их точки зрения.

Что такое нож – кухонная утварь или орудие преступления? Ответ зависит от того, что им в данный момент делают (или уже сделали).

Если я труп и рядом со мной обнаружен мой паспорт, то он (паспорт) – идентификатор. Если я пришла в присутственное место и представилась, а подтвердила свою самопрезентацию демонстрацией паспорта на такие же ФИО, то это аутентификатор. Если мы ищем устройство с серийным номером 1765390, то номер – идентификатор, если мы проверяем серийный номер устройства, чтобы дать или не дать разрешение на его использование – то это аутентификатор.

Признак может быть идентификационным или аутентификационным в зависимости от того, что сейчас происходит – идентификация или аутентификация, в каком смысле признак предъявляется.

Это не означает, что один и тот же признак будет (или должен быть) непременно принят в любом качестве. Однако это совершенно другой вопрос.

Выход рядом

Не будучи официальным оппонентом, критиковать, не предлагая альтернативы, нехорошо. Представляется вполне возможным устранить все приведенные выше недостатки системного описания аутентифицирующих данных таким образом, чтобы его можно было распространить на всю область определения субъектов аутентификации, причем без коренного разрушения привычной понятийной системы и без слова «фактор».

Коренные изменения нецелесообразны, в первую очередь, потому, что сама предметная область характеризуется высокой степенью стабильности: если что-либо начинает использоваться для аутентификации, то остается в таком качестве как минимум надолго, несмотря на

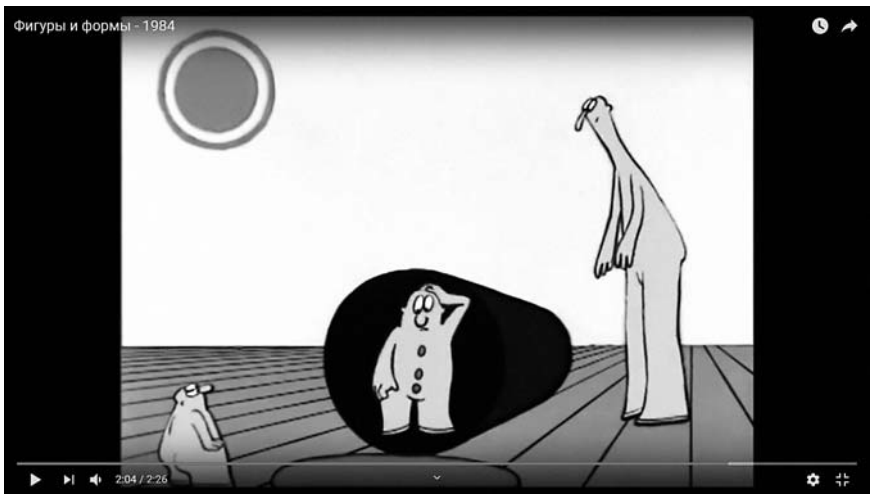

Рис. 2. ***Кадр из окончания мультфильма «Фигури и форми»***

все недостатки способов аутентификации с помощью данных этого типа, как происходит, например, с паролями.

Если достаточно стабилен сам перечень возможных данных и нет оснований считать, что он должен быть радикально изменен, то задача сводится к изменению *описания* сегмента действительности как есть, то есть к фиксации результатов наблюдения над практикой.

Классификация, полученная таким – эмпирическим – способом, может быть принята к рассмотрению, если она будет полной, на едином основании, целесообразной и совместимой с другими объектами этого же семантического поля, например, будет без противоречий накладываться на перечень способов аутентификации, фактически применяемых на практике, а желательно – позволять спрогнозировать возможные, но до сих пор не используемые, способы или механизмы.

Предмет классификации

В первую очередь необходимо зафиксировать, что в информационную систему мы в любом случае представляем только *данные*, а не знания, не собственность или что-то еще из аналогового или духовного мира. Поэтому речь должна идти о данных, характеризуемых какими-либо *признаками* или наборами признаков.

Таким образом, предмет классификации – аутентифицирующие данные.

Способы аутентификации и *аутентифицирующие данные*, безусловно, связаны, хотя и не должны смешиваться. Является общим местом, что значение имеет не только и не столько то, какие данные используются для аутентификации, а то, каким образом реализован механизм аутентификации в системе. Так, реализация парольной защиты может быть признана слабой, если она не включает в себя проверку на слабые пароли или какие-то механизмы блокирования угроз, связанных с возможным применением слабого пароля. Также она может быть признана слабой и в случае, если использование слабых паролей в ней исключено, но сильные пароли хранятся и передаются в открытом виде и в форме, делающей их доступными для нелегального применения. То есть так или иначе, слабость пароля и слабость реализации – это две разные слабости.

Далее речь пойдет не о способах и не о механизмах аутентификации, а именно об аутентифицирующих данных и их признаках. Следствия из полученной классификации, имеющие значение для выводов о механизмах или способах аутентификации, вероятно, станут развитием этого рассуждения.

Классификационные признаки

Значение имеет не только то, какую особенность сегмента действительности взять за основу, но и то, каким признаком ее описать (например, вес и цена золотого слитка).

Особенностей у аутентифицирующих данных можно выделять множество, и значительная часть описывающих эти особенности признаков будет важна с точки зрения защиты информации. Например, данные могут быть:

- инвариантны или вариативны – сравнение может требовать точного совпадения или совпадения в рамках некоторого диапазона (пример первого – пароль, второго – биометрический эталон);
- постоянными/временными/однократными:
  - *постоянные* – статические биометрические данные (никогда не меняются);
  - *временные* – пароль, ключи в токене (могут меняться, и если не меняются, это все равно – *время действия*);
  - *однократные* – одноразовый пароль, динамические биометрические данные (каждый раз разные) и т. д.

Это все важные параметры, и они характеризуют именно те самые *особенности* аутентифицирующих данных, которые определяют их принципиальную применимость и конкретные способы их применения в механизмах аутентификации. Но для классификации нужны такие признаки, которые характеризуют одновременно *все* возможные данные, причем характеризуют информативно, а не формально (так, наличие частоты не дает оснований классифицировать звук и цвет по длине волны в одну сплошную классификацию).

Признаки, по которым данные будут классифицированы, должны позволять строить на основе этой классификации рассуждения о защищенности механизмов аутентификации, использующих эти признаки аутентифицирующих данных. Значит, они должны быть связаны с ключевыми элементами системы аутентификации – аутентифицирующимися сторонами (назовем их субъектом и объектом аутентификации, так как даже при *взаимной* аутентификации все равно целесообразно ассоциировать аутентификацию с доступом, относительно которого так или иначе всегда выделяют *субъект* и *объект*), а также *носителем* аутентифицирующих данных.

Отдельно необходимо оговорить, что *объектом доступа* может быть некоторый целевой ресурс, а не информационная система целиком или даже СВТ. Например, аутентификацию в идентификации/аутентификации банкомата клиент банка проходит для того, чтобы получить доступ к своему счету, а не к банкомату. И *объектом аутентификации* будет банкомат как информационно-вычислительный ресурс, предоставляющий доступ к целевому *объекту доступа*.

Канал передачи данных от субъекта в подсистему аутентификации объекта, с одной стороны, зачастую детерминирован носителем данных (USB-токен не передаст данные через сканер отпечатка пальца и наоборот). С другой стороны, сами данные как раз с каналом их передачи практически не связаны, поэтому отдельно выделять его не представляется целесообразным.

«Связанность» чего-либо может быть разной степени (например, по возрастанию – соотнесенность, зависимость, неотчуждаемость), и связанность аутентифицирующих данных с каналом их передачи, безусловно, вполне реально установить, но это будет не более, чем ***соотнесенность***. Признак связанности такой степени не продуктивен, поэтому не будет браться в расчет.

Однако и ***неотчуждаемость*** также представляется непродуктивным для классификации признаком, так как этот признак может характеризовать только те данные, которые *не могут* передаваться в систему (и подсистему аутентификации в частности) *в непреобразованном виде*. От чего бы неотчуждаемыми ни были эти данные, они неотчуждаемы от того, что находится за *рамками* системы, а значит, в систему они *никогда не попадают*. Таким образом, признак неотчуждаемости от чего бы то ни было, фактически, делит аутентифицирующие данные на два класса – передаваемые и не передаваемые в систему. Никакой другой полезной информации из этого признака извлечь невозможно.

При этом признак ***зависимости*** позволяет описать в том числе и те случаи, когда данные от чего-либо неотчуждаемы. Такие данные в систему не передаются, но что-то другое – передается: иначе не состоится аутентификация. Передаются данные, которые от них тем или иным образом *производны*, то есть *зависимы* от того элемента, от которого первые данные неотчуждаемы.

В связи с этим нужно иметь в виду, что в части случаев аутентифицирующие данные представляют собой *цепочку данных*. Вполне вероятно, для каких-то задач этот факт может оказаться значимым, поскольку, хотя все процессы жизненного цикла «первичных» неотчуждаемых данных протекают вне подсистемы аутентификации, процедура *создания передаваемых в систему данных* из «первичных» неотчуждаемых располагается в границах этой подсистемы.

Однако непосредственно для классификации аутентифицирующих данных это представляется избыточным.

Еще одним дискуссионным вопросом является самостоятельность третьего выделенного элемента – носителя аутентифицирующих данных. В рамках процесса аутентификации он всегда находится на стороне субъекта аутентификации и предъявляется объекту. Видится целесообразным представлять зависимость от носителя видом зависимости от субъекта.

Характеристики по классификационным признакам

Зависимость – это понятие с крайне размытой областью определения, поэтому в качестве характеристики нецелесообразно брать «наличие» и «отсутствие» зависимости. В то же время, вполне реально формализовать *характер* зависимости – как от системы, так и от субъекта. Иначе говоря, данные, используемые для аутентификации, могут характеризоваться по тому, *как* они зависят от субъекта аутентификации и от объекта классификации: например, они могут быть *назначены* субъекту, либо могут быть с ним *ассоциированы*, либо ему *имманентны*.

Совсем не зависеть от объекта аутентифицирующие данные не могут, так как иначе они окажутся не в состоянии сыграть целевую для них роль – доказательства. Объект должен располагать какими-то данными для того, чтобы принять решение о корректности представленного подтверждения. Эти данные могут быть *именно теми*, которые субъект будет предъявлять, или какими-то *косвенными данными*, позволяющими определить корректность данных, не располагая ими «в лоб». Например, так производится проверка закрытого ключа сертификата: закрытым ключом субъекта объект не располагает, но располагает возможностью его проверить.

Возникает сомнение: имеет ли значение – порождаются данные, системой или записываются в нее. На текущем этапе работы над классификацией не обнаружено каких-либо доводов в пользу того, что это разделение может быть для чего-то полезным.

Если проводить параллель между субъектом и объектом (то есть сравнивать порожденные системой и записанные в нее данные с назначенными и ассоциированными с субъектом данными), то разница между назначенными и ассоциированными данными состоит в том, что ассоциированные не тиражируются, то есть носитель одновременно может находиться только у одного пользователя, если считать носитель условно некопируемым (так как мы смотрим в данном случае только на данные, а не на конкретную реализацию). Это значимо с точки зрения защищенности способов аутентификации, которые используют одни или вторые данные, поэтому такую разницу целесообразно учитывать.

А что зависит от того, сам ли объект породил данные для последующей аутентификации субъекта, – не столь очевидно. Возможно, это помогает при определенных реализациях затруднить мошеннические действия пользователя, но эти различия лежат скорее в области характеристики механизмов, чем данных. Аналогично этому от реализации системы аутентификации будет зависеть, постоянными или временными окажутся данные, ассоциированные с субъектом или назначенные ему:

- система может использовать заводской номер идентификатора (он постоянный) или вычисление от каких-либо данных, записанное в память идентификатора, или даже им осуществляемое (и это будут временные данные);
- система может требовать или не требовать смены пароля по регламенту, предъявлять или не предъявлять требования к его сложности и т. д.

Однако разделение этих данных на «аппаратный идентификатор» и «пароль» все равно справедливо находится уровнем выше, а детали реализации будут определять качество (лучше/хуже), а не архитектуру системы.

Субъектно-объектная классификация аутентифицирующих данных

Суммируя все вышеизложенные выкладки, можно сформулировать следующие варианты зависимости аутентифицирующих данных от субъекта и объекта.

1. ***Зависимость от объекта аутентификации*** может быть:

1) ***прямой*** – в системе хранятся (или создаются) сами данные, сравнение с ними производится напрямую (в этом смысле не имеет значения, *что сравнивается* – «пароль с паролем» или «свертка со сверткой», и точное совпадение должно быть или вероятностное – главное, что сравнивается непосредственно то, что получается от субъекта при аутентификации;

2) ***косвенная*** – в системе хранится «стимул», порождающий данные в качестве ответа, который можно *проверить*, или какие-то признаки, на предмет которых *проверяются* предъявленные данные (атрибутный сертификат).

По этому признаку данные можно разделить на *сравниваемые и проверяемые*. Данные, которые объект сравнивает с ранее зарегистрированными, соответственно, будут «сравниваемыми», а данные, которые проверяются на основании каких-то других данных и механизмов, которыми располагает объект, будут «проверяемыми».

2. ***Зависимость от субъекта аутентификации***, при которой данные могут быть:

1) ***назначены*** субъекту – назначение может производиться в том числе и самим субъектом, но при этом важно, что любые данные могут быть назначены любому субъекту; строго говоря, зависимости нет – мой пароль никак от меня не зависит, даже если я сама его выдумала;

2) ***ассоциированы*** с субъектом – зависимы от чего-то (в случае с человеком – от носителя), что не имманентно субъекту;

3) ***имманентны*** субъекту – для человека это преимущественно биометрические данные, а для информационных и вычислительных ресурсов – любые присущие им признаки, такие как серийные и заводские номера, фрагменты кода, контрольные суммы и т. п.).

По этому признаку данные лучше всего разделить на одноименные группы: «назначенные», «ассоциированные», «имманентные».

Классификация

Данные одновременно характеризуются какой-то зависимостью и от субъекта, и от объекта, то есть получается 6 вариантов сочетаний характеристик, которые дают нам 6 классов аутентификационных данных:

1) сравниваемые назначенные;
2) проверяемые назначенные;
3) сравниваемые ассоциированные;
4) проверяемые ассоциированные;
5) сравниваемые имманентные;
6) проверяемые имманентные.

Эти пересечения можно представить в следующем виде (табл. 1).

Необходимо оговориться, что по данным, передаваемым объекту аутентификации как таковым, в отрыве от каких-либо сопутствующих условий или обстоятельств, определить, какого они типа, не представляется возможным. Как принято говорить: «это просто нули и единицы». Различия проступают наглядно тогда, когда мы смотрим на систему

Таблица 1. ***Пересечение признаков аутентификационных данных с точки зрения их связи с субъектом и объектом аутентификации***

Объект / Субъект	Сравниваемые	Проверяемые
Назначенные	***Сравниваемые назначенные*** **Объект** сравнивает предъявленные данные с эталоном. **Субъекту** данные назначаются. Те же данные могут быть предъявлены другим субъектом или множеством других субъектов[7].	***Проверяемые назначенные*** **Объект** проверяет корректность предъявленных данных на основании других данных и проверочных механизмов. **Субъекту** данные назначаются. Те же данные могут быть предъявлены другим субъектом или множеством других субъектов.
Ассоциированные	***Сравниваемые ассоциированные*** **Объект** сравнивает предъявленные данные с эталоном. **Субъекту** ассоциирован носитель данных. Носитель не имманентен субъекту, но условно не тиражируем (то есть может быть предъявлен другим субъектом, но не несколькими одновременно).	***Проверяемые ассоциированные*** **Объект** проверяет корректность предъявленных данных на основании других данных и проверочных механизмов. **Субъекту** ассоциирован носитель данных. Носитель не имманентен субъекту, но условно не тиражируем (может быть предъявлен другим субъектом, но не несколькими одновременно).
Имманентные	***Сравниваемые имманентные*** **Объект** сравнивает предъявленные данные с эталоном. **Субъекту** имманентны данные, то есть они являются его неотъемлемой принадлежностью и не могут быть предъявлены другим субъектом.	***Проверяемые имманентные*** **Объект** проверяет корректность предъявленных данных на основании других данных и проверочных механизмов. **Субъекту** имманентны данные (являются его неотъемлемой принадлежностью и не могут быть предъявлены другим субъектом).

на уровне «аутентификаторов»[8] или сценариев использования данных. Поэтому выделенные ниже типы аутентификационных данных иллюстрируются именно через эти два проявления. Такое сведение друг к другу разных понятий становится возможным вследствие их детерминированности. Одному типу данных может соответствовать (и, как правило, соответствует) несколько типов аутентификаторов и сценариев аутентификации, но не наоборот.

1. ***Сравниваемые назначенные*** – прямая зависимость от объекта, назначается субъекту: пароль, в том числе одноразовый (с точки зрения *данных*, а не механизма, отличий нет), контрольные вопросы, талончики в очереди[9]. Важная особенность этого случая заключается в том, что с помощью таких аутентифицирующих данных субъект может подтвердить только одно – «бронирование» права на взаимодействие с системой.

2. ***Проверяемые назначенные*** – косвенная зависимость от объекта, назначается субъекту. Случай довольно экзотический, однако в жизни встречается: например, такими аутентифицирующими данными являются многие билеты[10], с которых считывается штрих-код, подтверждая их подлинность. Собственно, именно с этим связаны не искорененные до сих пор проблемы с подделкой билетов – назначенные данные не связаны с субъектом, а значит, бесконтрольно тиражируемы (а тут уж кто первый встал, того и тапки).

3. ***Сравниваемые ассоциированные*** – прямая зависимость от объекта, ассоциированность с субъектом (зависит от носителя). Аппаратный идентификатор (ничего кроме того, что это обладатель идентификатора (возможно, случайный), мы о субъекте не знаем)[11]: предельные

[7] *Здесь и далее в таблице речь ведется о действиях в аналоговой среде, без применения информационных технологий и кибератак (отсюда определение «условно» у некопируемости носителя). Возможность «подслушивания» и повторной передачи сохраненных данных в данном случае не учитывается, так как она характеризует не данные, а реализации механизмов аутентификации. Выше мы условились называть данными то, что передается в систему, то есть данные цифровой природы, а возможность копирования цифровых данных зависит не от особенностей данных, а от особенностей реализации системы, в которой они хранятся и обрабатываются.*

[8] *«Аутентификатор» – понятие в русскоязычной практике терминологически не оформленное, и здесь хотелось бы воздержаться от его определения, ограничившись ссылкой [11]. Нестрого «аутентификатор» можно определить как инструмент аутентификации.*

[9] *Очевидно, что система не хранит список номеров талончиков и выдает их по одному, а формирует номера по порядку с учетом каких-то дополнительных входных данных. Также очевидно, что талончик не связан с субъектом, а назначается ему. О зависимости от носителя тут тоже говорить некорректно, так как напечатанное на талончике от носителя не зависит, а полностью формируется системой. Можно возразить, что такой же номерок, но напечатанный на чем-то другом, не будет принят как подтверждение очереди, однако тут опять налицо связь с системой, а не с носителем, ибо талончики именно в таком как есть виде целиком являются ее продуктом. При этом доступ дается на основании сравнения данных талончика с номером, который высветился над соответствующим окошком. Суммируя все сказанное, можно утверждать, что это ни что иное, как вариант реализации одноразового пароля.*

[10] *Необходимо иметь в виду один нюанс: билеты могут включать в себя какие-либо идентифицирующие данные, которые поддаются проверке. Это будет другой, отдельный процесс аутентификации человека как легального владельца билета (проверяется законность его владения билетом, а не его эксклюзивное право посмотреть спектакль). Отличаются случаи, когда аутентифицирующими данными являются собственно данные субъекта, а билет представляет собой только способ учета: так, при авиаперевозках несмотря на существование билетов регистрация на рейс осуществляется не по ним, а по паспорту (случай № 3 – сравниваемые ассоциированные).*

[11] *Аппаратный идентификатор с одноразовым паролем, а также, например, аппаратный идентификатор, в котором пользователь аутентифицируется по биометрии, а тот отправляет объекту аутентификации некоторую производную информацию, относятся к этой же категории, меняется только реализация механизма. Но при одном условии – если переданные данные объект аутентификации сравнивает с эталоном. Отличаются эти случаи тем, что в них будет два отдельные процесса аутентификации: сначала субъект «пользователь» относительно объекта «идентификатор», а затем, в зависимости от реализации, субъект «пользователь» относительно основного объекта (допустим, ПК) или субъект – «идентификатор» относительно того же объекта.*

случаи – разовые гостевые пропуска – карты СКУД или социальная карта в качестве подтверждения статуса пенсионера для получения льготы, положенной не лично тому или иному лицу, а любому пенсионеру.

4. ***Проверяемые ассоциированные*** – косвенная зависимость от объекта, ассоциированность с субъектом. Сертификат закрытого ключа[12], «рукопожатие» СВТ с аппаратным идентификатором, какое-то вычисление, например, контрольной суммы (объект передает данные, на основании которых вычисление производится устройством, ассоциированным с субъектом, или самим субъектом аутентификации (если это программа или система)).

5. ***Сравниваемые имманентные*** – прямая зависимость от объекта, имманентность субъекту. Это биометрические данные, сравниваемые с шаблоном (данные имманентны субъекту и зарегистрированы в объекте), или неотчуждаемые характеристики, например, характеристики СВТ, сравниваемые с зарегистрированными в служебном носителе «Секрет».

6. ***Проверяемые имманентные*** – косвенная зависимость от объекта, имманентность субъекту. Интерактивная биометрия, стимул-реакция, клавиатурный почерк при наборе фразы по запросу.

Чтобы убедиться в детерминированности связей между типами аутентифицирующих данных, аутентификаторами и сценариями аутентификации, сведем их в таблицу (табл. 2).

Таблица 2. ***Аутентификаторы и сценарии для аутентификационных данных разных типов***

Примеры / Тип	Примеры аутентификаторов		Примеры сценариев аутентификации	
	Субъект-пользователь	*Субъект – вычислительный ресурс*	*Субъект-пользователь*	*Субъект – вычислительный ресурс*
Сравниваемые назначенные	Пароль Одноразовый пароль Контрольные вопросы Талончики на очередь	Имя (файла, процесса, СВТ)	Объект дает доступ субъекту, если предъявленный пароль совпадает с эталонным	Объект дает доступ субъекту-процессу, если тот называется Word, или рабочей станции с именем Mikhail
Проверяемые назначенные	Билеты, например, в кино	«Маска»	Объект дает доступ субъекту, если предъявленные им данные соответствуют некоторым требованиям: с билета считывается штрих-код, билет легальный	Объект проверяет субъект-ресурс, претендующий на доступ, на соответствие «маске» – некоторому набору параметров, например, расположению в каталоге и т. п.[13]
Сравниваемые ассоциированные	Аппаратный идентификатор, предающий какие-либо данные (свой номер или свертку от каких-то данных – не имеет значения)	Доменное имя СВТ, сетевой адрес	Объект дает доступ субъекту, если данные, переданные его аппаратным идентификатором, совпадают с теми, что зарегистрированы для этого субъекта в базе данных объекта	Доступ предоставляется только субъектам-вычислительным ресурсам с указанными параметрами. Отличие от сравниваемых назначенных в том, что штатным образом назначить это же значение параметра другому субъекту нельзя
Проверяемые ассоциированные	Аппаратный идентификатор, осуществляющий «рукопожатие» с СВТ. Сертификат закрытого ключа на каком-либо носителе (отчуждаемом или стационарном)	«Рукопожатие» двух устройств. Результат некоторого вычисления, например, контрольной суммы	Объект передает данные, на основании которых производится какое-либо вычисление в устройстве, ассоциированном с субъектом, а его результат передается объекту для проверки	Объект передает данные, на основании которых субъектом производится какое-либо вычисление, а его результат передается объекту для проверки
Сравниваемые имманентные	Биометрические данные (папиллярный узор пальцев рук, сосудистое русло ладоней и т. д.), сравниваемые с эталоном	Неотчуждаемые характеристики СВТ, такие как номер материнской платы	Объект дает доступ субъекту, если вероятность совпадения предъявленных данных с эталоном не ниже установленной	Объект доступа сравнивает номер материнской платы компьютера, к которому его подключили, с тем, который указан в списке зарегистрированных в нем разрешенных компьютеров
Проверяемые имманентные	Реакция на стимул (движение глаз вслед за точкой на экране, чтение текста, клавиатурный почерк при наборе фразы по запросу)	«Маска» по неотчуждаемому параметру ресурса, например, по типу устройства	Объект генерирует случайный стимул, фиксирует данные о движении глаз и определяет, соответствуют ли эти данные особенностям рефлекторной дуги этого субъекта. Если да – доступ предоставляется	Объект, например, личный кабинет в какой-либо системе, предоставляет доступ с разными правами в зависимости от того, с клиентского устройства какого типа приходит запрос

[12] *Разумеется, сертификат не обязательно предъявляется с какого-то отчуждаемого носителя (токена или смарт-карты), хотя именно так дело обстоит в большинстве случаев. Вполне возможно следующее построение системы: сертификат установлен на определенный компьютер, с которого субъект аутентифицируется на каком-либо удаленном ресурсе. В этом случае «носителем» сертификата, который не имманентен субъекту, но ассоциирован с ним, будет этот ПК. Тот же пользователь с другого ПК аутентифицироваться успешно не сможет. Именно такая ситуация лучше всего описывает доступ в доверенном сеансе связи [12, 13], где средство обеспечения доверенного сеанса связи [14–17] является и компьютером и носителем.*

[13] *Для отнесения к данному типу принципиально, чтобы этим параметрам могли быть установлены разные значения – разместить в нужном каталоге, назвать на букву т и т. д. Если маска включает в себя неизменные параметры, то это тип «проверяемые имманентные».*

Что нам это дает

Получается, что любое из пересечений значений признаков дает описание реально применяющихся в жизни аутентифицирующих данных, причем охвачены даже такие виды данных, *способы* аутентификации на основе которых в настоящее время еще не реализованы, а только разработаны на уровне концепций (рефлекторная биометрия «стимул – реакция» [18, 19]), а также те, которые не очевидно ассоциируются именно с аутентификацией (талончики на очередь).

Примера данных, который не подпадал бы ни под одну из шести получившихся категорий, пока не обнаружено. Это, безусловно, не говорит само по себе о том, что классификация верна, однако усиливает ее правдоподобность.

Классы данных расположены по возрастанию сложности нелегального получения в распоряжение данных этих классов:

- прямо сравниваемые данные можно перехватить при аутентификации легального субъекта и затем «подложить», а косвенная зависимость требует более сложной атаки;
- несвязанные с субъектом данные могут быть переданы неограниченно большому кругу лиц, растиражированы (они не могут быть по каким-либо причинам нетиражируемыми);
- устройство теоретически может быть нетиражируемым (в любом случае, его тиражирование сложнее);
- неотчуждаемые характеристики теоретически воспроизводимы, но сделать это еще сложнее, причем заметно, и т. д.

В то же время нельзя не заметить, что также возрастает и сложность реализации подсистемы идентификации/аутентификации, использующей данные разных типов. Однако это в некоторой степени компенсируется тем, что снижаются требования к обеспечению доверия тем или иным компонентам системы, которые могут в разных случаях быть легче или сложнее доступны для контроля. Иногда проще сделать доверенным клиентское устройство, иногда – использовать намного более сложную систему аутентификации, а клиентские устройства не контролировать совсем. Эти параметры (контроль какого компонента необходимо усилить, а какого – допустимо ослабить) тоже можно получить как следствие из предложенной классификации.

Обеспечение доверенной среды на СВТ и идентификация/аутентификация, особенно при доступе к удаленным ресурсам, как правило реализуется разными подсистемами. Это часто приводит к проблемам на тех этапах жизненного цикла системы, для которых наиболее ярко выражена зависимость от человеческого фактора. На этапе проектирования они возникают потому, что требования к разным подсистемам зачастую предъявляются независимо одни от других, а затем так же они и реализуются. На этапе эксплуатации зависимость от человеческого фактора еще выше: сменился человек, у нового свои представления о том, что в наибольшей степени отвечает современным вызовам, и одна из подсистем модернизируется без учета взаимовлияния с другой. Установление же таких взаимосвязей позволит существенно снизить влияние субъективных факторов на принятие проектных решений на всем жизненном цикле.

Это означает, что классификация обладает определенной продуктивностью, то есть целесообразна. Верна ли она – покажет анализ со стороны широкого круга специалистов. ■

ЛИТЕРАТУРА

1. Ван Гиг Дж. Прикладная общая теория систем. В двух книгах. Книга 1. – М.: Мир. – 1981. – 336 с.

2. Аутентификация // Википедия – свободная энциклопедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Аутентификация#Факторы_аутентификации (дата обращения: 29.04.2019).

3. NIST Специальная публикация 800-63B. Руководство по цифровой идентификации. Аутентификация и управление жизненным циклом. 2017 [Электронный ресурс]. – Режим доступа: https://pages.nist.gov/800-63-3/sp800-63b.html (дата обращения: 30.04.2019).

4. Комаров А. Современные методы аутентификации: токен и это все о нем..! // T-Comm. – 2008. – № 6. – С. 13–16.

5. ISO/IEC 2nd WD 29003 – Information technology – Security techniques – Identity proofing. 2013 [Электронный ресурс]. – Режим доступа: https://cabforum.org/pipermail/public/attachments/20130814/f2f4a333/attachment.pdf (дата обращения: 30.04.2019).

6. ГОСТ Р «Идентификация и аутентификация. Общие положения». Проект, окончательная редакция.

7. ГОСТ Р «Защита информации. Идентификация и аутентификация. Уровни доверия к результатам идентификации». Проект, первая редакция.

8. Стрельцов А. А. Обеспечение ИБ России. Теоретические и методологические основы. – М.: МЦНМО. – 2002. – 296 с.

9. Конявский В. А., Гадасин В. А. Основы понимания феномена электронного обмена информацией. – Минск, 2004. – 327 с. (Серия «Библиотека журнала "УЗИ"»).

10. Большой толковый словарь русского языка / Сост. и гл. ред. С. А. Кузнецов. – СПб.: Норинт. – 1998. – 1536 с.

11. Authenticator // Wikipedia – The Free Encyclopedia [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Authenticator (дата обращения: 22.06.2019).

12. Конявский В. А. Серебряная пуля для хакера // Защита информации. Инсайд. – 2013. – № 4. – С. 54–56.

13. Конявский В. А. Серебряная пуля для хакера (Окончание) // Защита информации. Инсайд. – 2013. – № 5. – С. 69–73.

14. Конявский В. А., Чугринов А. В. Съемный носитель информации // Патент на полезную модель № 102139. 2011. Бюл. № 4.

15. Конявский В. А. Съемный носитель информации с безопасным управлением доступом // Патент на полезную модель № 123571. 2012. Бюл. № 36.

16. Конявский В. А. Съемный носитель информации на основе энергонезависимой памяти с расширенным набором функций информационной безопасности // Патент на полезную модель № 130441. 2013. Бюл. № 20.

17. Конявский В. А. Модем для безопасных коммуникаций в компьютерных сетях // Патент на полезную модель № 128055. 2013. Бюл. № 13.

18. Конявский В. А. Новая биометрия. Можно ли в новой экономике применять старые методы? // Information Security/Информационная безопасность. – 2018. – № 4. – С. 34–36.

19. Конявский В. А. Интерактивный способ биометрической аутентификации пользователя // Патент на изобретение № 2670648. 2018. Бюл. № 30.