01 Базовые принципы

Образ мышления, основанный на базовых принципах, предполагает, что все ваши действия опираются на основополагающие убеждения, или базовые принципы.

Рид Хастингс,
генеральный директор Netflix

...Чтобы изучить процесс приобретения [знаний], мы должны начать с исследования тех основных причин, которые называются принципами.

Рене Декарт, философ

Я считаю, что при рассуждении важно руководствоваться базовыми принципами, а не аналогиями... [При их использовании] вы сводите все к фундаментальным истинам... и затем рассуждаете, опираясь на них.

Илон Маск,
основатель компании SpaceX

Обзор главы

Эта глава предназначена для тех читателей, кто не знаком с такой общепринятой передовой научной практикой, как концепция базовых принципов. Это не просто мем, о котором можно услышать в Twitter. Ученые издавна используют ее, чтобы открывать тайны природы и общества. Данная книга представляет собой мое исследование этой концепции применительно

к кибербезопасности. Разумеется, основы кибербезопасности широко обсуждались, но, как будет показано далее, уже в начале 1970–1980-х годов исследователи считали, что основным принципом обеспечения кибербезопасности является создание полностью защищенного компьютера. К началу 2020-х годов большинство практиков отказались от этой идеи, сочтя ее непрактичной. При этом сообщество специалистов по ИБ не заменило ее ничем существенным, если не считать концепции триады «конфиденциальность, целостность и доступность» (КЦД). Однако даже сторонники этой триады не возводят ее в ранг базового принципа и говорят о ней просто как об одной из лучших практик. В этой главе я объясняю, почему триада КЦД, равно как и другие общепринятые лучшие практики: соблюдение правил кибергигиены (исправление ошибок), предотвращение заражения вредоносным ПО, реагирование на инциденты, следование контрольным спискам ИБ-фреймворков и соблюдение требований международного законодательства — не могут считаться абсолютным базовым принципом. В конце главы я предлагаю свое видение того, каким должен быть настоящий атомарный первичный принцип кибербезопасности.

Что такое базовые принципы

Идея базовых принципов была предложена великим философом Аристотелем (384–322 годы до н. э.) в его труде «Физика» [12] (опубликован примерно в 340 году до н. э.), где он изложил свои представления о натурфилософии — способе изучения природы (physis). Однако прежде, чем приступить к изложению своего основного тезиса, он указал на то, что невозможно полностью понять какую-либо концепцию до тех пор, пока не разберешься в ее сущности: «Ибо мы не считаем вещь познанной до тех пор, пока не познакомимся с ее первичными причинами, или первичными принципами, и не проанализируем ее простейшие элементы». Далее Аристотель описал свой метод нахождения этих причин: для этого мы берем то, что нам известно из наблюдений, и доходим до самой сути. Он сказал: «Естественный способ это сделать — двигаться от вещей, которые более понятны и очевидны для нас, к тем, которые являются более явными и понятными по природе» [12]. При этом он уточнил, что эти известные природе атомарные идеи являются уникальными строительными блоками, с которых начинается любое исследование: «Ибо первичные принципы не должны выводиться ни друг из друга, ни из чего-либо другого, тогда как все должно выводиться из них» [12]. После нахождения этих важнейших понятий они становятся

«большим взрывом» для всей гипотезы. «Первичные принципы вечны и не имеют скрытых причин» [13, 14, 122, 126].

Евклид, знаменитый греческий математик и учитель, ни разу не упомянул о первичных принципах в своей основополагающей книге «Начала» (около 300 года до н. э.), однако его краткое изложение 23 определений, пяти постулатов, или аксиом, и пяти общих понятий на протяжении более чем 23 веков являлось основой геометрии и других математических дисциплин [75]. Не существует более убедительного доказательства того, что образ мышления, основанный на базовых принципах, способен привести нас к пониманию истинной природы окружающего мира [6, 301, 311].

В 1644 году величайший философ и скептик всех времен, отец современной философии Рене Декарт опубликовал свой труд «Начала философии» [66, 67]. В нем он начинает «с самых общих вопросов, например с того, что слово “философия” обозначает занятие мудростью, под которой понимается не только благоразумие в делах, но и совершенное знание всего, что может познать человек; это же знание направляет нашу жизнь, служит сохранению здоровья, а также открытиям во всех искусствах». Это весьма масштабная цель, не правда ли? Как же ее можно достичь? По словам Декарта, для получения этого понимания мы должны вывести его из первичных источников: «А чтобы оно стало таковым, оно обязательно должно быть выведено из первичных причин так, чтобы тот, кто старается овладеть им (а это и значит, собственно, философствовать), начинал с исследования этих первичных причин, именуемых началами». Далее он говорит о том, что эти начала должны отвечать двум требованиям: «Во-первых, они должны быть столь ясны и самоочевидны, чтобы при внимательном рассмотрении человеческий ум не мог усомниться в их истинности; во-вторых, познание всего остального должно зависеть от них, тогда как сами эти принципы должны быть познаваемы помимо познания прочих вещей». Под этим он подразумевает то, что все знание о предмете исходит из этих первичных принципов: «Затем надо попытаться вывести знание о вещах из тех начал, от которых они зависят, таким образом, чтобы во всем ряду выводов не встречалось ничего, что не было бы совершенно очевидным».

Следует отметить, что нахождение базовых принципов любого предмета — очень сложная задача. Своей книгой Декарт полностью перевернул сложившийся на тот момент философский образ мышления, заявив, что Аристотель и его современники (Платон и Сократ) так и не смогли найти первичный

принцип философии. Подход Декарта, предполагающий сомнение во всем, установил абсолютный первичный принцип философии: «Я мыслю, следовательно, существую» (Cogito, ergo sum) [312].

В 1910 году два британских математика, Альфред Уайтхед и Бертран Рассел, опубликовали книгу *Principia Mathematica*, в которой попытались с нуля перестроить язык математики на основе небольшого набора базовых принципов [314]. Они обнаружили некоторые несоответствия в существующем на тот момент наборе правил, используемых математическим сообществом. С помощью одних и тех же правил можно было получить два разных и абсолютно правильных результата. Это открытие получило название парадокса Рассела [120]. Для мира точной инженерии это означало потенциальную катастрофу. Поэтому они вернулись к чертежной доске и начали с нуля. Их математическое доказательство того, что 1 + 1 = 2, заняло 80 страниц. В одной из сносок Уайтхед и Рассел написали: «Приведенное ранее утверждение иногда бывает полезным». А вы думали, что математики не умеют шутить.

Отвечая на вопрос о том, как он подошел к созданию концепции экономичных космических полетов, Илон Маск не сказал, что он опирался на то, что агентство НАСА и компания Boeing делали в 1960-х годах в рамках программ «Аполлон» и «Спейс шаттл». Он отбросил все эти наработки и начал с чистого листа. Это, безусловно, очень смелый шаг, и, возможно, именно поэтому он является мультимиллионером, а я — нет [56, 186, 308].

Аристотель, Евклид, Декарт, Уайтхед, Рассел и Маск говорят о том, что для решения любой сложной проблемы практик должен свести ее к первичной сущности.

Базовые принципы той или иной проблемной области настолько фундаментальны, что являются самоочевидными, настолько элементарны, что ни один специалист в данной области не может их оспорить, настолько важны для того, чтобы мы хорошо ее поняли, что без них инфраструктура, на которой держится наша передовая практика, рассыпалась бы как песчаный замок во время прилива. Они атомарны. Эксперты используют их как строительные блоки для получения всего остального, что известно в выбранной проблемной области. Все новые знания, полученные в ней, зависят от ранее сформулированных базовых принципов.

Если это правда, а я считаю, что так и есть, то отсюда следует логичный вопрос: каковы первичные принципы кибербезопасности?

Предыдущие исследования базовых принципов кибербезопасности

Компьютерная эра началась тогда, когда мейнфреймы стали использоваться правительством, университетами и коммерческими организациями (примерно в 1960–1981 годах). Прошло около десяти лет, прежде чем пользователи мейнфреймов осознали вероятность возникновения проблемы компьютерной безопасности, и первыми это поняли американские военные. Начало этому процессу положила работа Уиллиса Уэра *Security Controls For Computer Systems* [309], которую он опубликовал в 1970 году, будучи сотрудником корпорации Rand. Эта работа представляла собой не столько определение понятия кибербезопасности, сколько перечисление и описание всех проблем, которые могут возникнуть в будущем, когда компьютеры будут объединены в сеть и начнут совместно использовать ресурсы. Я бы отнес этот документ к категории «первый шаг в решении любой проблемы — это признание ее наличия». Он намекает на то, что сообщество специалистов по безопасности должно найти способ построения защищенной системы. Эта идея находилась в центре внимания исследователей на протяжении 1990-х годов. В опубликованной в 2021 году книге *A Vulnerable System: The History of Information Security in the Computer Age* [296], попавшей в Зал славы Cybersecurity Canon, ее автор Эндрю Стюарт сетует на то, что с самого начала цифровой эры никто так и не смог построить защищенную систему. От этого отказались практически все.

В статье *Computer Security Technology Planning Study* [8], написанной Джеймсом Андерсоном в 1972 году, были развиты идеи, изложенные в работе Уиллиса Уэра. Вероятно, в ней была впервые высказана мысль о том, что о безопасности нужно думать не после создания системы, о чем специалисты говорят и сегодня, когда обсуждают концепцию сдвига влево или принцип конструктивной безопасности. Она подразумевает, что создание безопасной системы является конечной целью, но при этом предполагает, что любая безопасная система нуждается в способе ее мониторинга на предмет наличия дефектов и вторжений.

Годом позже Дэвид Белл и Лен Лападула, на тот момент работавшие в организации MITRE, опубликовали работу *Secure Computer Systems: Mathematical Foundations* [26], в которой привели арифметическое доказательство, гарантирующее безопасность компьютерной системы. При этом они сразу признали, что даже при возможности построения системы, соответствующей этому доказательству, ее создатели не могли бы гарантировать правильность

ее реализации. Теоретически это возможно, но как можно поручиться за правильность практически? И эта проблема остается актуальной для такого рода исследований на протяжении 30 лет.

В 1975 году Джером Зальтцер и Майкл Шредер опубликовали труд под названием *The Protection of Information in Computer Systems* в журнале *Proceedings of the IEEE* [192]. В нем они изложили первые зачатки триады КЦД, хотя и не использовали эту терминологию. Они также впервые доказали, что комбинация «имя пользователя — пароль» — это слабая форма защиты и однажды возникнет потребность в двухфакторной аутентификации. Кроме того, они одними из первых выступили за снижение сложности во всем, что связано с разработкой системы безопасности, и за то, чтобы ее разработка не скрывалась от посторонних глаз. Другими словами, это, вероятно, первые исследователи, публично высказавшиеся против применения принципа «безопасность через неясность». Наконец, они продвигали идею использования *безопасных умолчаний* (fail-safe defaults), которая предполагает изначальный запрет всего с последующим разрешением в виде исключения. Эта идея, вероятно, является первым зародышем концепции защиты периметра, то есть создания внешнего барьера, позволяющего контролировать доступ к сети. Она была высказана примерно за десять лет до появления соответствующих технологий (межсетевых экранов).

В 1991 и 1992 годах доктор Фред Коэн опубликовал первые работы, в которых для описания общей модели обеспечения кибербезопасности в сообществе сетевых защитников использовалась концепция эшелонированной защиты [51–53]. Не он придумал этот термин, но, скорее всего, именно он первым описал соответствующую концепцию в своей работе. Эшелонированная защита предполагает возведение электронного барьера между Сетью и цифровыми активами организации. Чтобы преодолеть этот барьер со стороны Интернета, необходимо было пройти через контрольный пункт, которым обычно служил межсетевой экран, а в первые годы иногда еще и маршрутизатор. Начиная с 1990-х годов и по сей день общепринятой практикой является добавление дополнительных средств контроля позади межсетевого экрана для обеспечения более гибких функций. В первые годы это были системы обнаружения вторжений и антивирусные системы. Все вместе эти средства образовывали так называемый *стек безопасности*, принцип работы которого заключается в том, что если один из инструментов стека не сможет предотвратить доступ злоумышленника, то это сделает следующий. Если и он не справится с задачей, его место займет следующий. В этом и заключается суть концепции эшелонированной защиты.

В 1998 году Донн Паркер опубликовал книгу *Fighting Computer Crime: A New Framework for Protecting Information*, в которой резко осудил элементы триады КЦД, назвав их неадекватными [172]. При этом словосочетание «триада КЦД» не упоминалось. Он предложил добавить еще три элемента — владение или контроль, аутентичность и полезность, результатом чего стала модель под названием «гексада Паркера». Но она не получила широкого распространения по причинам, которые, вероятно, может объяснить лишь маркетолог.

В этот период большинство специалистов по ИБ в той или иной форме занимались совершенствованием стека безопасности. Однако с появлением облачных окружений, возникших примерно в 2006 году, количество нуждающихся в защите цифровых сред многократно увеличилось. Организации начали хранить и обрабатывать данные в различных местах, которые я называю *островами данных* (к ним относятся традиционные центры обработки данных, мобильные устройства, облачные среды и SaaS-приложения). Идея стека безопасности стала более абстрактной. Речь шла уже не об одном наборе инструментов, физически развернутом за межсетевым экраном, — это была целая серия стеков безопасности, развернутых для каждого отдельного острова данных. Стек безопасности превратился в набор всех развернутых инструментов, укрепляющих оборонительную позицию организации вне зависимости от места их расположения, иными словами, концепция эшелонированной защиты стала применяться абстрактно ко всем средам. Большая часть проводимых в этот период исследований была направлена на улучшение возможностей триады КЦД путем создания более совершенных инструментов для стека безопасности, таких как межсетевые экраны уровня приложений, системы управления идентификацией и доступом, средства для расширенного обнаружения и реагирования (XDR) и т. д., и более совершенных моделей для противодействия противнику (работа Киндервага о стратегии нулевого доверия *No More Chewy Centers*, 2010 [133]; модель убийственной цепочки Lockheed Martin, 2010 [115]; модель Diamond Министерства обороны США, 2011 [39]; база знаний компании Mitre ATT&CK Framework, 2013 [299]).

Точно не помню, когда услышал о работе Уайтхеда и Рассела, но размышлять и писать о базовых принципах кибербезопасности я начал еще в 2016 году. Тогда мои мысли еще не были полностью сформулированы, но я уже понимал, что сообщество специалистов по информационной безопасности движется в неправильном направлении. Почему-то все мы полагали, что защита отдельных систем с помощью триады КЦД — верное решение. Тем не менее количество сообщений о взломах продолжало расти. Уже тогда

я понимал, что триада КЦД недостаточно элементарна. Нам не нужно было защищать отдельные компьютерные системы. Следовало предотвращать причинение существенного ущерба нашим организациям. Тогда я осознал необходимость возвращения к базовым принципам.

Примерно в это же время научное сообщество впервые задумалось о способах применения идеи базовых принципов к области кибербезопасности. Сотрудники Университета Буффало Чарльз Арбутина и Сарбани Банерджи связали то, что они называют *основополагающими утверждениями*, с контрольным списком Агентства национальной безопасности США (АНБ), содержащим критерии, которым должны соответствовать защищенные системы [195]. Однако в этой работе предполагается, что создание защищенной системы является абсолютным базовым принципом кибербезопасности, не подлежащим обсуждению. Идея следовать первичным принципам кибербезопасности правильная, но недостаточно атомарная: она не позволяет понять, что же на самом деле является базовым принципом. Некоторые из предложенных задач, в том числе разделение доменов, изоляция процессов и сокрытие информации, могут и должны использоваться в качестве тактик, однако в своей работе авторы не иллюстрируют того, что именно они пытаются сделать. Они не доходят до сути проблемы.

В 2017 году доктор Мэтью Хейл, доктор Робин Ганди и доктор Бриана Моррисон в своей работе *Introduction to Cybersecurity First Principles*, предназначенной для учащихся начальной школы, предложили аналогичный подход с использованием контрольного списка АНБ [95]. А в 2021 году доктор Джон Сэндс, Сьюзан Сэндс и Джейми Махони из Общественного колледжа Брукдейла осветили эту тему более подробно, но опять же не привели никаких аргументов в пользу того, почему указанные ими принципы являются первичными [193].

В 2020 году на 7-м семинаре ACM по защите движущихся целей Шоухуай Сюй опубликовал свою работу *The Cybersecurity Dynamics Way of Thinking and Landscape* [319]. В ней он представил трехмерную ось, включающую такие базовые принципы, как анализ методом моделирования, основанный на предположениях, анализ данных, основанный на экспериментах, и метрики, зависящие от применения и семантики. Однако он также не привел аргументов в пользу элементарности предложенных принципов.

В 2021 году в Университете Айдахо Николас Сили опубликовал магистерскую диссертацию *Finding the Beginning to Discover the End: Power System Protection as a Means to Find the First Principles of Cybersecurity* [199]. Из всех упомянутых здесь работ эта наиболее полная с точки зрения осмыс-

ления первичных принципов. Сили также проанализировал большинство из них, прежде чем сделать выводы, и утверждает, что основные идеи, вытекающие из этих работ, вращаются вокруг проблемы доверия. Затем он задается вопросом о том, является ли концепция доверия достаточно фундаментальной для того, чтобы быть базовым принципом. Он цитирует Джеймса Коулмана — автора книги *The Foundations of Social Theory*, в которой говорится о том, что «ситуации, предполагающие проявление доверия, относятся к подмножеству ситуаций, связанных с риском». Или, как говорит Сили, «при отсутствии риска в доверии нет необходимости». Сили утверждает, что риск — это функция вероятности, мера неопределенности. Он считает неопределенность более фундаментальной концепцией по сравнению с триадой КЦД и любыми другими контрольными списками, предложенными вышеупомянутыми авторами. Интересно то, что в своей книге *The Foundations of Decision Analysis Revisited* отец теории анализа решений доктор Рон Ховард утверждает то же самое.

Из книги Лумана, Кинга и Моргнера *Trust and Power* Сили заимствует идею о том, что доверие позволяет нам уменьшить сложность своей жизни [144]. Затем, подобно Евклиду, он предлагает набор допущений (постулатов или аксиом) в качестве базовых принципов кибербезопасности.

- Полное знание о системе недостижимо, поэтому в нашем понимании этой системы всегда будет некоторая доля неопределенности.
- Принципал системы вынужден доверять одному или нескольким агентам.
- Известные риски могут быть уменьшены посредством их контроля, передачи и избегания, в противном случае они должны быть приняты.
- Неизвестные риски проявляются через сложность.

Затем он останавливается на определении абсолютного первичного принципа кибербезопасности и использует свои аксиомы для разработки лучшего, чем у Белла и Лападулы, доказательства того, что один дизайн системы более безопасен по сравнению с другим, анализируя собственные значения соответствующих графов. Другими словами, он возвращается к традиционному способу проектирования безопасных систем.

Концепция образа мышления, основанного на представлении о базовых принципах, существует практически с момента зарождения просвещенной научной мысли. Однако ее применение к сфере кибербезопасности — относительно новая идея.

Хотя отцы-основатели кибербезопасности (Уэр, Андерсон, Белл и Лападула, Зальтцер и Шредер, Кларк и Уилсон) никогда не упоминали о первичных принципах, они сформулировали две основные концепции, которые, по сути, и были положены в основу этой дисциплины. Первая заключается в том, что мы все пытаемся формализовать безопасность систем. Исследовательское сообщество в конце концов отказалось от этой идеи в 1990-х годах, сочтя ее нерабочей. Мы обнаружили, что чем более защищенными становятся машины, тем менее полезными они оказываются для решения распространенных задач. Защищенные системы могут применяться в специфических случаях, например связанных с государственной тайной, но рядовому пользователю Интернета они не очень полезны. Второй была концепция триады КЦД. Несмотря на жалобы критиков на ее неадекватность и попытки улучшения, ее общий смысл оставался неизменным с момента публикации работы Зальтцера и Шредера. Учитывая то, что в 2020 году ее признавали даже такие организации, как Национальный институт стандартов и технологий (NIST), триада КЦД фактически является первым принципом кибербезопасности.

В следующем разделе я постараюсь доказать, что она не подходит на эту роль, и предложу более надежный базовый принцип.

Атомарный базовый принцип кибербезопасности

В предыдущем разделе я говорил о том, что сообщество специалистов по ИБ обеспечило постепенный прогресс в плане цифровой защиты наших организаций. Очевидно, что мы прошли долгий путь. Однако, ознакомившись с работой Уайтхеда и Рассела, я подумал о том, что мы столкнулись с парадоксом, аналогичным описанному в ней. Мы продолжаем добавлять к уже сделанному множество разных вещей, не задумываясь о правильности выдвинутых ранее предположений. Наши защитные системы были значительно усовершенствованы, но складывается впечатление, будто это никак не повысило эффективность предотвращения кибератак. Более того, учитывая количество успешных атак, ежедневно попадающих в заголовки прессы, можно сделать вывод о том, что защита ухудшилась. Это относится не ко всем. Некоторые справляются с задачей довольно успешно. Я говорю о сообществе ИБ-специалистов в целом. Как и в случае с Уайтхедом и Расселом, разные группы, входящие в это сообщество, используя одни и те же передовые методы, получают разные результаты.

Я пришел к следующему выводу: все, что мы делаем как сообщество в плане защитной триады «люди — процессы — технологии», с помощью которой пытаемся обеспечить безопасность своих организаций, вероятно, не является настолько фундаментальным, чтобы оказывать существенное влияние. Разумеется, все это дает определенный эффект. Но проблема в том, что даже полноценная реализация этой триады оказывается недостаточной либо слишком сложной или дорогостоящей и поэтому не приводит к успеху.

И я не согласен с мнением, что обеспечение кибербезопасности чем-то отличается от остальных мировых проблем и является настолько уникальной проблемой, что ее невозможно решить. В конце концов, мы высадили людей на Луну, приручили атомную энергию и изобрели Интернет. Я считаю, что обеспечение кибербезопасности представляет собой гораздо менее масштабную задачу по сравнению с этими и многими другими. Проблема, как мне кажется, заключается в том, что у нас нет единого понимания термина «обеспечение кибербезопасности». Если вы попросите трех специалистов в сфере защиты сети описать, что именно они пытаются сделать с помощью своей программы по обеспечению ИБ, то получите три принципиально разных ответа.

Если сообщество не может договориться о том, что именно мы пытаемся сделать, значит, пора вернуться к первичным принципам. Более того, пришло время определить абсолютный принцип, способный послужить базовым определением кибербезопасности. До сих пор сообщество использовало набор терминов и фраз для обозначения кибербезопасности или ее компонентов. Некоторые его представители говорят:

- о реализации триады КЦД;
- создании надежной программы исправления ошибок;
- защите от вредоносных программ;
- быстром обнаружении и эффективном устранении угроз (реагировании на инциденты);
- развертывании NIST Cybersecurity Framework или другого фреймворка;
- поддержании работы программы обеспечения соответствия нормативным требованиям.

Существует и множество других направлений, некоторые весьма хороши. Но ни одно из них не кажется достаточно фундаментальным. Ни одно не дотягивает до статуса того основополагающего элемента, на базе которого мы могли бы строить свои программы. Как же вышло, что за 30 лет работы в со-

обществе так и не сформировалось единого мнения о том, к чему именно мы все стремимся? Это и является основным тезисом данной книги.

Как я уже говорил в начале главы, создание набора первичных принципов кибербезопасности предполагает сведение концепции защиты сети к ее основной сути. Перечисленные ранее идеи могут присутствовать в нашем списке в качестве потенциальных тактик, но они недостаточно атомарны. Мы не можем использовать их как строительные блоки для выведения всего, что известно в данной проблемной области, уподобившись Уайтхеду и Расселу, которым потребовалось 80 страниц для доказательства простой математической концепции.

Итак, первым делом я объясню, почему перечисленные идеи не являются главными принципами кибербезопасности.

Является ли триада КЦД абсолютным первичным принципом?

С момента своего возникновения в 1970-е годы и до начала 2020-х годов триада КЦД оставалась основополагающей философией обеспечения информационной безопасности. В документе *NIST Special Publication 1800-25: Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, опубликованном в 2020 году Национальным институтом стандартов и технологий США (NIST), говорилось о том, что «триада КЦД описывает три столпа информационной безопасности». Другими словами, именно она лежит в основе стратегии защиты государственных систем [43].

В августе 2022 года в ходе беседы со мной Дженнифер Рид, специалист в области безопасности и технологий с 20-летним стажем, привела доводы в пользу того, что статья Зальтцера и Шредера является первым публичным упоминанием о триаде КЦД — концепции того, что для обеспечения безопасности системы архитекторам необходимо позаботиться о конфиденциальности, целостности и доступности. По ее словам, несмотря на то что Зальтцер и Шредер не использовали словосочетание «триада КЦД» и не упоминали такие термины, как «конфиденциальность», «целостность» и «доступность», они «с точки зрения специалистов по безопасности говорили о трех типах вторжений, известных как: а) несанкционированный доступ к информации (конфиденциальность); б) несанкционированная модификация информации (целостность); в) несанкционированный отказ в использовании (доступность)».