ОСНОВЫ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

В.Д. Фомичев (НТЦ ЯРБ)

1. Постановка вопроса

Настоящая статья носит обзорный характер и рассчитана в первую очередь на специалистов, которым по роду своей служебной и научной деятельности приходится решать вопросы защиты информации, в том числе и на специалистов в области государственного регулирования безопасности при использовании атомной энергии, занимающихся обеспечением в пределах своей компетенции защиты сведений, составляющих государственную тайну [1, 2].

Удовлетворение все возрастающих потребностей современного общества при неуклонном увеличении народонаселения земного шара требует резкого повышения эффективности всех сфер общественной деятельности. Важнейшим и непременным условием такого повышения выступает адекватное повышение эффективности применения информационных технологий (информатизации). Технологиями называют элементы экономического потенциала, которыми располагает общество и которые при необходимости могут быть использованы для достижения конкретных целей хозяйственной или иной деятельности. Для современного общества проблема информационного обеспечения всех сфер деятельности по своей значимости и актуальности превосходит проблему дальнейшей индустриализации производства, до недавнего времени считавшейся одной из центральных. Давно стали привычными и общеупотребительными такие категории, как материальные, финансовые, трудовые, природные ресурсы, вовлекаемые в хозяйственный оборот, их назначение понятно каждому. Но в последние годы появились понятия ”информация”, “информационная безопасность,” “информационные технологии”, и, хотя они узаконены, но осознаны пока еще недостаточно. Информационные технологии являются собственностью, находятся в ведении соответствующих органов и организаций, подлежат учету и защите, так как информацию можно не только использовать для производства товаров и услуг, но и превратить ее в наличность, продав кому-либо [3, 4].

Собственная информация для производителя представляет значительную ценность, поскольку нередко получение (создание) такой информации весьма трудоемкий и дорогостоящий процесс. Ценность информации (реальная или потенциальная) определяется в первую очередь приносимыми доходами.

В этих условиях основным выступает правило: кто владеет информацией, тот владеет миром.

Одна из наиболее острых проблем – проблема надежной защиты информации, т. е. обеспечение ее от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и т. п. Особую остроту проблема защиты информации приобретает в связи с повсеместной и массовой компьютеризацией информационных процессов, с широким внедрением информационно-вычислительных сетей, с доступом к их ресурсам большого количества пользователей [4, 5]. Сравнительно недавно основное внимание уделялось прежде всего защите информации пользователей и в значительно меньшей мере регламентировалась защита от преднамеренного воздействия так называемой технологической информации, т.е. информации, от которой зависит устойчивое функционирование самой системы или ее прикладного про-

граммного обеспечения. В настоящее время и технологической информации уделяется должное внимание, особенно в так называемых информационно-телекоммуникационных сетях, т. е. технологических системах, предназначенных для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. К таким системам относятся системы управления экологически потенциально опасными объектами использования атомной энергии (ОИАЭ), а в отношении обеспечения их безопасности – это системы физической защиты объектов использования атомной энергии (СФЗ ОИАЭ) и системы учета и контроля ядерных материалов (СУиК ЯМ). Поскольку всякое управление есть информационный процесс, то информация приобретает статус главного ресурса общества со всеми вытекающими из этого требованиями, предъявляемыми к обращению с ним. В данном случае актуально решение проблемы обеспечения безопасности информации, циркулирующей в СФЗ ОИАЭ и СУиК ЯМ, в интересах решения триединой задачи: обеспечения целостности, доступности и конфиденциальности информации. Нарушения конфиденциальности, целостности и доступности информации возникают в результате реализации угроз безопасности информации. Здесь и далее под угрозой будем понимать совокупность условий и факторов, которые в случае их реализации могут привести к утечке информации или нарушению ее целостности или доступности [3, 5].

2. Основы защиты информации

Информация – очень сложная для понимания категория, поскольку ее роль, место и сущность формировались человечеством на протяжении многих тысячелетий и в большинстве случаев интуитивно, без научной поддержки. Обеспечивая существо человеческой жизни, информация является глобальной категорией, так как совместно с веществом и энергией составляет основу мира.

Во взаимодействии с веществом и энергией информация используется разумным субъектом для удлинения дистанции энергоматериального взаимодействия путем подачи команд на подключение дополнительных источников, т.е. для управления материально-энергетическими процессами. Кроме того, она используется для общения разумных субъектов. Это тоже можно толковать как управление, осуществляемое в итоге по двум трактам: по интеллектуальному и техническому (физическому).

Однако, в отличие от вещества и энергии, информация нематериальна. Она продукт нашего разума. Из-за этого информация внутри разума многократно "переиспользуется", образуя хитроумные сочетания (картину мира), не подчиняющуюся законам сохранения или даже простым балансовым соотношениям. Вне разума информация неограниченно тиражируется на многочисленные носители и незаметно распространяется, т.е. становится известной другим субъектам.

Перечисленные свойства многообразия и неосязаемости имеют кардинальное значение для защиты информации, особенно основанной на ее выборе по какому-то качеству. Не имея предметной основы для выбора, дифференцированная защита становится нереальной, чисто словесным желанием. Вот почему для движения вперед в настоящее время принципиально необходима разработка теоретических основ защиты информации как методологического фундамента технологии ее реализации [6].

По взглядам И. В. Кузнецова, в прошлом директора Института истории естествознания и техники АН СССР, развитая физическая теория включает три элемента - основание, ядро и воспроизведение конкретного в понятиях. Основа-

нием теории служит совокупность эмпирических фактов, фундаментальных понятий и идеализированных объектов. Ядро теории составляют выраженные математически законы. Воспроизведение конкретного в понятиях складывается из объяснений известных фактов, представления новых явлений и интерпретации основного содержания теории [7].

Взяв данное положение за основу, раскроем содержание указанных элементов применительно к разрабатываемой теории защиты информации. Это позволит разложить на составляющие очень сложные и запутанные положения новой информационной технологии, каковой является дифференцированная защита информации, т.е. защита обоснованно выбранной наиболее ценной информации.

2.1. Основание теории защиты информации определяется фактом, что неценное людьми не защищается. Тогда в основании теории защиты информации должен лежать процесс создания и использования информации как материальной ценности. При этом величина ценности должна определяться предметным содержанием и объемом (количеством) информации.

Существующая теория информации К. Шеннона не может ответить на вопрос о ценности информации, ибо ее назначение состоит в установлении закономерностей взаимосвязи только тех характеристик информации, которые соответствуют характеристикам каналов ее передачи. В основе этой теории молчаливо полагается, что информация – это то, что передается. К. Шеннон писал: "Сообщение имеет содержание. Оно, однако, совершенно несущественно в проблеме ПЕРЕДАЧИ информации" [8].

Эта коммуникативная сторона информации правильна только частично, поскольку прежде чем передаться (переместиться), она должна быть создана. То есть присвоенное в теории Шеннона название "информация" было шире рассматриваемого в ней явления – передачи сообщения. Поэтому для конструктивного рассмотрения основных направлений дифференцированной защиты информации как материальной ценности нам необходимо выяснить сущность и строение информации более полно. Для этого возьмем за основу определения информации, данные учеными, занимавшимися более широкими областями науки, чем существующая теория информации.

Отец кибернетики Н. Винер определил информацию так: "Информация – это обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему..." Дж. фон Нейман полагал, что для "описания (содержания!) и измерения количества информации необходимы два подхода: информация – это совокупность сведений; информация – это устраненная неопределенность" [9]. Эта двойственность очень хорошо объясняется, если вспомнить Г. Лейбница, который полагал: "При помощи разума человек обязан получить представление о реальности и получить определенность в направлении к наилучшему" [10]. Причем полнота "представления о реальности" – это совокупность сведений, т.е. содержание информации, а "определенность в направлении к наилучшему" – это снятая неопределенность, определяющая количество информации. Поскольку объединение указанных двух сторон информации осуществляется только при помощи разума человека, механизм функционирования которого нам неизвестен, его очень трудно отразить формальной теорией.

Чтобы обойти возникшее затруднение, люди для решения насущных задач передачи информации поступали проще. Они (Хартли, Шеннон) сформулировали "снизу", от физики, энтропийную меру неопределенности ситуации и связали ее с количеством информации, опустив определение содержания информации. Этого оказалось достаточно для определения емких и конструктивных характеристик

каналов передачи информации. В теории информации наступила эра энтропийной эйфории, принесшая не только положительные результаты. К. Шеннон написал: "Значение теории информации было преувеличено и раздуто… Здание нашего несколько искусственно созданного благополучия слишком легко может рухнуть..."

Причина столь бурного успеха использования энтропийной характеристики неопределенности как количественной меры информации объясняется большой потребностью людей в такой характеристике и отсутствием полной ясности в содержании интеллектуального (!) понятия "неопределенность". Поэтому, получив конкретную возможность решать практически нужные задачи передачи информации, люди стали меньше думать об основах этой возможности, а стремились ее как можно шире использовать. И не только для передачи информации. А основы оказались не всеобъемлющими.

Формально энтропийная мера выражает частную неопределенность - неопределенность выбора конкретного события из заданной полной группы событий. Тем самым теория информации К. Шеннона служит ветвью теории вероятности [11]. Однако люди чаще всего сталкиваются не с вероятностной неопределенностью выбора. Основная неопределенность заключается в том, что люди не знают, из чего и что выбирать, т.е. не могут сформулировать полную группу событий. Это объясняется тем, что полнота представления свидетельствует о полноте знания, а ее никогда не бывает.

Есть еще и алгоритмическое затруднение, заключающееся в сложности представления неопределенной ситуации набором одноуровневых дискретных событий, составляющих полную группу. Истинная информация как совокупность сведений, знаний является не дискретной, а многоуровневой (многослойной) непрерывной характеристикой представления материальных вещей. Вот тут лежит еще более мощный барьер на пути использования энтропийной меры информации в более широкой области. Будучи физической величиной и дискретной в основе, энтропия по глубине не “дотягивала" до интеллектуальной категории непрерывного представления содержания информации. Поэтому содержательная сторона информации, как излишняя для энтропийного подхода к информации, теорией информации не развивалась. Из-за этого разрыв между двумя сторонами информации был "заморожен". Он продолжался до тех пор, пока не возникла потребность практики – необходимость выборочной защиты информации в соответствии с ее ценностью, определяемой содержанием и количеством информации. Нам необходимо уточнить сущность информации как средства отражения реальности.

Это можно сделать, если соответствующим образом раскрыть содержание процессов возникновения и представления информации. Для этого необходимо раскрыть приведенное выше определение информации, данное Н. Винером, как "обозначение содержания, полученного субъектом из внешнего мира".

Эпикур сказал: "Каждый предмет получает благодаря впервые ему присвоенному названию свою ясность, очевидность, отчетливость". Оставив на время в стороне нераскрытым содержание понятия "название", отмечаем, что предметы реального мира получают нематериального заместителя, удобного для оперирования механизмом разума субъекта, ибо понятия "отчетливость", "ясность" имеют умственную природу.

Сущность информационного отражения реальности – формирование механизмом разума субъекта для элементов реального мира их обозначающих заместителей, удобных для абстрактного оперирования. Такой заместитель элемента реальности называется знаком [12]. То есть строение информации опре-

деляют знаки различного типа и содержания (семиотического наполнения). Источниками же знаков служат объекты реального мира с их свойствами. Поэтому сущность информации – представление реальности совокупностью знаков, сформированных разумом субъекта и размещенных в накопленной интеллектуальной среде.

Удобство использования знака, как заместителя реальности, определяется двумя его свойствами: свойствами, присущими знаку как представителю и выразителю реальности, и свойствами знака как представителя знаковой системы.

Первое свойство определяет способность знака адекватно и полно отражать (замещать) реальность, а второе определяет гибкость (удобство) его использования. Поскольку эти свойства находятся в строгом противоречии (первое определяется теснотой связи с реальностью, а второе, наоборот, – отдаленностью), то для удовлетворения всех потребностей субъекта в информационном отображении реальности и в их информационном взаимодействии человечеством за свою историю отработана мощная система знаков постепенно усложняющегося содержания.

Основная причина последовательного усложнения содержания знаков заключается в стремлении обойтись их минимальным количеством при сохранении возможности адекватного отображения многомерной реальности. Это повлекло увеличение выразительной "нагрузки" на каждый знак, т.е. увеличение неоднозначности (контекстуальной мощи) знака. "Понимание" реальности, выраженной знаком, обеспечивается при этом усложнением правил использования и трактования знака. Тем самым дискретный по сути знак за счет его многозначности и многоместности использования расплывается в множество его значений, формируя в совокупности непрерывность содержания информации, выражаемой накладкой содержаний множества знаков различных типов.

Таким образом, естественное желание людей обеспечить гибкое информационное отображение реальности и общение индивидуумов с использованием минимального числа типов знаков объективно породило неоднозначность или неопределенность значения знаков. Эта неопределенность легко преодолевается разумом субъекта путем "использования" знака в сформированной картине мира, но является исключительно (непреодолимо!) сложной для формализованного представления их содержания в виде отделимых дискретных значений.

На основе изложенного можно составить представление о модели строения информации как многоуровневой совокупности знаков различной контекстуальной мощности. Контекстуальность, т.е. подразумеваемость по ситуации значения знака и их многослойная накладка обеспечивает непрерывность строения информации, что уже не соответствует теории К.Шеннона.

А. Соломоник [12], обобщив труды по семиотике начиная с древности, сформулировал пять типов знаков постепенно увеличиваемой общности и абстрактности: признак, образ, слово, буква, символ. При этом только первый знак - признак является частью реальности (имеется связь по общему свойству отображаемого объекта и знака), а остальные знаки принадлежат только знаковой системе, являясь метками реальности. То есть прямой связи по основным свойствам отображаемых объектов они уже не имеют. Это полностью абстрактные знаки последовательно увеличиваемой степени, обеспечивающие связь с реальностью только через систему правил их использования.

Отсюда следует важный для нас вывод о том, что имеется информация двух четко различающихся сортов: информация, идущая от источника через его признаки (далее – информация от источника), и информация, представляемая знаковым носителем (далее – информация от носителя), воспроизводящим запи-

си абстрактных знаков. Получение информации от источника осуществляется измерением признаков источника и последующей обработкой результатов измерений, а получение информации от носителя – ее копированием на одноименные носители или переносом на носители другой природы. Хотя носитель тоже материален, но его свойства намного проще свойств источника. Многообразия свойств носителя должно хватать только для отображения многообразия знаков.

Следовательно, основные действия по защите информации должны быть направлены против измерения признаков и против копирования носителей.

Отметим, что если размножение информации от источника возможно только путем размножения объектов материального мира, то размножение информации от носителей в материально-энергетическом плане несоизмеримо проще, легче и дешевле. Это очень удобно для передачи информации и обмена ею, однако порождает иллюзию ее неценности. Основной способ борьбы с этой иллюзией – рассматривать информацию в целом, начиная от признака и кончая записью.

Существование информации от источника в виде совокупности признаков позволяет решить вопрос о содержательной единице информации. В качестве таковой следует принять типовой (по значению) признак (факт). Он должен быть сформулирован таким образом, чтобы имелась возможность установить связь с коммуникативной (технической) единицей информации в один бит и информацией более общего содержания (информацией от носителя).

Усложнение сущности каждого из перечисленных выше знаков приводит к увеличению числа отношений, выражаемых знаком. Чтобы это усложнение сделать более простым и осязаемым, используют иерархический принцип. Он выражается в том, что вокруг каждого типа знака формируется своя частная знаковая система. То есть признак образует естественно-знаковую систему, образ – образную знаковую систему, слово – языковую знаковую систему, буква – алфавитную знаковую систему, символ – кодовую систему.

Формирование этих систем осуществляется расширением значимости знака, формированием контекстуальных значений, разработкой алфавитов и введением знака знаков. Все это в совокупности приводит к более гибкой реализации трех основных информационных функций человека. К ним относятся:

- формирование картины мира;
- языково-письменный обмен;
- символьная коммуникация по физическим и техническим каналам.

Рассмотрим каждую функцию подробнее, поскольку все они имеют принципиальное значение для защиты информации, причем первые две относятся к разумным субъектам, а последняя – к создаваемым ими техническим системам.

Формирование картины мира. Сформированная в уме субъекта картина мира служит основой для знакового обмена, при котором субъекты понимают друг друга. Тем самым допускается "иносказательность" знака, т.е. его замещение не всех свойств объекта, а только его минимальной представительной части. Если бы знак замещал все свойства объекта однозначно 1:1, то это было бы неприемлемо по двум причинам:

- исчезла бы энергоматериальная выгода информационного удлинения (замыкания) дистанции взаимодействия вещества и энергии;
- человеческий мозг не справился бы с отображением многомерного мира, ибо каждый знак дает сжатие представления и тем выше, чем знак сложнее (т.е. абстрактнее) (например, слово обеспечивает сжатие 10^5 ... 10^7 , а символ – еще выше). Следует подчеркнуть, что "иносказательность" знака понимается субъектом только благодаря нали-

чию картины мира, т.е. накопленного представления об обстановке, в которую знак "по месту" вписывается, заполняя "пустые" по значению (знака) места.

Картину мира субъект формирует всю жизнь, в силу чего он становится способным понимать дискреты все более иносказательной информации, переносимой знаком. Отсюда для защиты информации следует очень жесткий вывод: решение о значимости для субъекта поступающей информации можно принять только с учетом содержания его картины мира, которая другому субъекту недоступна из-за неизвестности внутреннего механизма функционирования разума субъекта. Существующая внутрисистемная оценка значимости информации, именуемая смыслом, из-за невыводимости ее во вне не является операционной. Она недоступна некачественному и неколичественному представлению. Поэтому внутрисистемную оценку ценности информации получить нельзя.

Но это относится только к внутриинформационному (внутриумственному) представлению ситуации. Чтобы представление сделать осязаемым, необходимо вывести его результаты на более высокий (надсистемный) уровень, а именно – посмотреть, как на основе полученной информации субъект действует. То есть объем и содержание выполняемых субъектом действий и являются мерой ценности информации. Это составляет основной вывод, позволяющий конструктивно решить задачу о ценности информации, а следовательно, и об ущербе от ее утечки (утраты).

Однако нужно рассматривать действия не вообще, а только в срезе содержания поступившей информации.

Как отделить эти действия в общем случае – очень сложная задача, опирающаяся на механизм одинакового понимания ситуации субъектами. Применительно к защите информации, когда действуют два субъекта с четко связанной (противоположной) мотивацией, это можно сделать упрощенно и асимметрично: смотреть, что делает соперник в той предметной области, которую владелец информации считает важной. Это обеспечивается привязкой к одному и тому же объекту, как источнику информации. Содержание свойств этого объекта и определяет содержание информации, интересной при защите обоим субъектам.

Содержание механизма понимания важно и для определения другой характеристики – количества информации. Под количеством содержательной информации следует понимать количественную меру множества поступающих знаков, исчисляемых на уровне признаков, достаточных для понимания конкретной предметной ситуации.

Чтобы определить эту меру, необходимо хотя бы приближенно оценить механизм понимания формально. Его можно представить как механизм объединения пирамид (в двумерном случае – треугольников), гирлянд с зафиксированным расстоянием между вершинами. Под этим расстоянием понимается содержательная дистанция между фактами, объединяемыми при понимании.

Поскольку эта дистанция до начала понимания велика, то семантической силы поступающих знаков недостаточно для ее перекрытия. Для уменьшения дистанции поступающие знаки сначала наращивают детализацию объединяемыми фактами в глубину, что приводит к глубинному расширению наращиваемых деталями областей. Тем самым формируются пирамиды (треугольники), гирлянды с зафиксированными исходными вершинами. Естественно, расстояния между крайними точками их глубинных оснований сближаются. По мере наращивания детализации основания сближаются настолько, что семантический промежуток между ними замыкается очередным пришедшим знаком. Происходит объединение наращиваемых структур (гирлянд) в общую, т.е. осуществляется понимание

ситуации обоими субъектами. Тогда количество информации определяется взвешенной суммой фактов (признаков), с помощью которых достигнуто понимание ситуации.

За уровни значимости фактов (признаков) применительно к объекту можно взять следующие уровни детализации описания объекта: объект, качество объекта, свойство качества, характеристика свойства, измеряемые и вычисляемые характеристики, измеренное значение характеристики, допуск (зазор) между соседними значениями. Строя детализирующую гирлянду по этим уровням, мы получаем пирамидальную (треугольную) структуру, сближаемую в глубине детализации с другой (понимаемой) структурой при зафиксированной дистанции между двумя фактами (объектами). Таким образом, за единицу содержательной информации следует взять средневзвешенный факт (признак).

Языково-письменный обмен. Поскольку он осуществляется словами, то здесь необходимо рассмотреть связь между содержанием слова и количеством содержащихся в слове признаков. Это позволит установить количество единиц информации, содержащихся в рассматриваемом слове.

Формально данную связь можно установить с помощью фрейм-сценария [13] путем формирования последовательности вопросов типа "что", "где", "когда", "зачем" и "если – то". Ответы на эти вопросы формулируются по привлекаемым источникам информации. Множество ответов на эти вопросы и определят количество признаков, т.е. единиц информации, содержащихся в слове. Однако таким образом можно раскрыть пока не все слова.

Кроме того, содержание информации в форме записей необходимо анализировать и с точки зрения доступности к ней. При этом следует различать бумажные и безбумажные (электронные) носители записей.

Символьная коммуникация по физическим и техническим каналам является содержанием теории информации К. Шеннона. В основе этой теории лежат самые абстрактные знаки – символы, которые генерируются абстрактным источником сообщений. У источника сообщений интересуются только теми параметрами, которыми описываются каналы связи. Таких параметров два: пространственные и временные. К пространственным параметрам относится полоса пропускаемых частот, к временным – время задействования канала. Сообщения переносятся своим канальным носителем – сигналом. Они доступны и средствам перехвата соперника.

Информация, переносимая сигналами, воспринимается техническими средствами и используется разумными субъектами для пополнения картины мира. В этом факте заложена объективная связь между содержательной и технической (битовой) единицей информации.

Для решения первоочередных задач защиты информации достаточно достижения ограниченной цели, а именно установления способа определения ценности информации. Это можно сделать, исключив из рассмотрения неизвестный механизм функционирования мозга субъекта путем решения надсистемной задачи по принципу "черного ящика". На вход "черного ящика" поступает информация, а на выходе определяется содержание действий, выполняемых человеком на ее основе. При этом на основе ценности (эффективности) реализованных действий определяется ценность информации. Однако и тут есть сложности. Рассмотрим их.

Информация в уме человека рассматривается "клубком", используется многократно. Чтобы избежать многократного учета одних и тех же ценностей, необходимо четко отделять вновь создаваемую информацию от ранее поступившей и накопленной. То есть мы должны рассмотреть способы получения новой ин-

формации. Их несколько. Следует различать физические действия по добыванию информации, например эксперимент; информационные действия по добыванию информации – моделирование, абстрактное мышление и комбинированные – проектирование (функционирование) нового изделия. Но мы рассмотрим один – проектирование (функционирование) ОИАЭ (СФЗ ОИАЭ, СУиК ЯМ).

Для нас важно лишь то, что информация о свойствах (деятельности) ОИАЭ интересна (нужна) второму субъекту, имеющему недружественные интересы к первому субъекту – проектировщику (руководителю) ОИАЭ, т.е. владельцу (руководителю) новой информации. Тем самым мы фиксируем предметное содержание информации.

Для определения ценности информации, создаваемой при проектировании (функционировании) ОИАЭ, необходимо установить связь количества информации со свойствами ОИАЭ, ценность которых можно определить. При этом возможны варианты. Во-первых, в качестве ценностных свойств ОИАЭ можно взять его потребительские свойства, что соответствует надсистемной оценке ценности. Эти свойства ОИАЭ характеризуются потенциалом, выражающим способность ОИАЭ (СФЗ ОИАЭ, СУиК ЯМ) к выполнению цели (функции), которую можно достигнуть совместно с другими системами.

Потенциал является универсальной характеристикой "мощи" ОИАЭ, независимой от их природы и достаточной для сопоставления (соизмерения) “мощи” различных ОИАЭ. Вследствие этого он служит удобной характеристикой для сопоставления способов достижения сложных (комплексных) результатов средствами различной природы, функциональное соизмерение результативности которых путем раскрытия закономерностей их функционирования требует сложных математических моделей [6].

Возможность его использования определяется и тем, что разработанный Т. Саати [14] метод анализа иерархий позволяет достаточно просто определять значения потенциалов ОИАЭ количественно. Его универсальность для ОИАЭ различной деятельности простирается до тех пор, пока сохраняется возможность сформулировать общую цель использования оцениваемых ОИАЭ с присущим им "весом", т.е. потенциалом.

Значение потенциала определяется вектором характеристик двух видов – характеристиками качества ОИАЭ и характеристиками силы сопротивления соперника, препятствующей реализации потенциала. Величина этой силы зависит от степени знания соперником характеристик, определяющих его слабые (уязвимые) свойства. Эти знания соперник получает по каналам утечки информации о свойствах ОИАЭ.

Отсюда следует, что идеальный объект теории защиты информации составляет замкнутый контур действий двух разумных субъектов по генерированию новой информации путем проектирования (функционирования) ОИАЭ первым субъектом; по перехвату этой информации вторым субъектом (называемым соперником) и по реализации соперником на основе перехваченной информации комплекса действий по снижению потенциала проектируемого (функционируемого) ОИАЭ при его применении, учитываемого проектировщиком изделия.

То есть предметом теории защиты информации является конфликт двух разумных субъектов, обусловливаемый их специфическим информационным взаимодействием в конкретной (заданной) предметной области.

С одной стороны, эта область определяется сущностью проектируемого (функционируемого) ОИАЭ, а с другой – мероприятиями соперника по снижению результативности (эффективности) ОИАЭ. Это составляет предмет теории защи-

ты информации в микропостановке, предназначенной для установления закономерностей вычисления ценности утерянной информации в рамках одного ОИАЭ.

Ценность информации в денежном выражении можно определить изложенным методом только в том случае, если известна стоимость единицы потенциала. Для традиционных ядерно-опасных ОИАЭ, используемых длительно, это имеет место. Однако для уникальных, совершенно новых ОИАЭ такие данные отсутствуют. В этом случае ценность информации вычисляется другим способом – через кривую безразличия микроэкономики.

Ее сущность состоит в наличии возможности эластичной замены объема материальных действий по созданию ОИАЭ с потенциалом П на эквивалентный объем информации, определяющий содержание этих действий. Эта замена возможна в определенных пределах – в области эластичности, в которой и существует кривая (закономерность) безразличия. Влияние же утечки информации, приводящей к снижению потенциала П, формально проявляется в сдвиге кривой безразличия по биссектрисе ее координатного угла. То есть кривая безразличия идет “дальше” потенциального подхода к определению ценности информации.

Ситуация, определяемая кривой безразличия, – это конструктивная единица анализа комплексной и глобальной проблемы защиты информации, объединением которой строятся агрегаты, определяющие макроситуации. Она увязывает три закономерности:

- объем материальных действий по созданию ОИАЭ – источника информации;
- объем информации как мер снятой неопределенности, реализуемой при создании ОИАЭ, измеряемой количеством учтенных состояний, определяемых ответами на вопросы “ что”, “где”, “когда”, “зачем”, “если – то” и количеством вскрытых при этом признаков ядерно-опасных ОИАЭ;
- потенциал ОИАЭ – источника информации.

Указанные закономерности определяются действиями первого субъекта – владельца источника информации. Для определения ущерба от утечки информации необходимо учитывать действия и другого субъекта. Его действия, выполняемые на основе перехваченной при утечке информации, формализуются сдвигом кривой безразличия, являющимся четвертым параметром модели [6].

2.2. Ядро теории защиты информации составляют законы, выраженные математически. Установленные зависимости ценности информации об ОИАЭ от его свойств позволяют определить величину ущерба от утечки информации.

2.3. Воспроизведение конкретного в понятиях относится в первую очередь к закономерностям управления ущербом от утечки информации реализацией мер по ее защите, В конкретном случае это соответствует синтезу системы защиты информации, облик которой диктуется обстановкой.

На основании изложенного в таблице приведены основные характеристики информации, важные с точки зрения ее защиты.

Основные характеристики информации

Характеристика	Содержание характеристики	Роль и значимость	Предметное ограничение
Определение информации	Представление реальности совокупностью знаков, сформулированных разумным субъектом для представления в интеллектуальной среде	"Рабочее тело" функционирования интеллектуальной сферы разумных субъектов	Информация разделяется: создаваемая вновь; защита в автоматизирован-ных системах управления; распространяе-мая средствами массовой информации; хранимая в накопителях; информация о личности
Статус по объективности	Создается разумом субъекта, но длительно проверяется и корректируется на соответствие объективному	Отражение с замещением объективной реальности идеальными (знаковыми) заместителями	Знаки бывают: признаки, образы, слова, буквы, символы
Назначение (функция)	Удлинение дистанции вещественно энергетического взаимодействия и обеспечение обмена представлениями о реальности разумных субъектов	Увеличивается степень охвата вещественно-энергетической сферы жизни разумными действиями субъектов	Достигнутые возможности воздействия субъектов на окружающую среду
Сущность функции	Управление вещественно-энергетическими процессами по двум трактам: интеллектуальному и физическому (техническому)	Увеличивается рациональность использования вещественно-энергетических ресурсов	Управление реализуется квантами, соответствующими содержанию целей управления

Характеристика	**Содержание характеристики**	**Роль и значимость**	**Предметное ограничение**
Структура информационного представления	Многоуровневая совокупность знаков различной контекстуальной мощности (значимости). Более мощные (абстрактные, общие) знаки в меньшем количестве располагаются вверху, менее мощные, но более конкретные знаки в большем количестве располагаются внизу	Обеспечивает адекватное представление интересующего (рассматриваемо-го, обозначенного) фрагмента реальности минимальной совокупностью знаков. Их количество и тип диктуется адекватностью и подробностью представления реальности	Ограничивается выразительной способностью совокупности знаков
Формальный аналог структурного представления информационного фрагмента. Основа определения ценности информационного фрагмента	Фрейм, т.е. граф-гирлянда фрагментов (терминалов) постепенно повышаемой детальности. Связь "информация –действие, выполняемое субъектом на ее основе"	Формальное представление многоуровневого многомерного предметного фрагмента определенной структуры. Обеспечивает вывод внутри информационного содержания из нераскрываемой интеллектуальной сферы на более высокую прагматическую ступень измеряемой ценности	—

Характеристика	Содержание характеристики	Роль и значимость	Предметное ограничение
Содержание меры ценности информации	Зависимость потребительской ценности изделия от количества содержащейся в нем информации; зависимость ценности, произведенной при создании изделия от количества произведенной информации	Позволяет учитывать производимую информацию как материальную ценность	Первая оценка ценности является надсистемной, вторая – внутрисистемной относительно изделия

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информатизация – организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных технологий.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная безопасность – состояние защищенности ее национальных интересов в информационной сфере от внутренних и внешних угроз.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Литература

1. Положение о Федеральной службе по экологическому, технологическому и атомному надзору. Утверждено постановлением Правительства Российской Федерации от 30 июля 2004 г. № 401.
2. Федеральный закон “Об информации, информационных технологиях и о защите информации” от 14 июля 2006 г. № 149-ФЗ.
3. Герасименко В.А., Малюк А.А. Основы защиты информации. Учебник. М.: МИФИ, 1997.

4. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2004.
5. Язов. Ю.К. Основы технологии проектирования систем защиты информации в телекоммуникационных системах. Учебное пособие. Воронеж, ГОУВПО “Воронежский государственный технический университет”, 2005.
6. Бугров Ю.Г., Щербаков Б.В. Системные основы оценивания и защиты информации. Учебное пособие. Воронеж, ГОУВПО “Воронежский государственный технический университет”, 2005.
7. Проблемы истории и методологии научного познания / Под ред.Б. М. Кедрова и Н. Ф. Овчинникова. М.: Наука, 1974.
8. Шеннон. К. Работы по теории информации и кибернетики / Пер. с англ. М.: ИЛ,1963.
9. Левин Б. Р., Шварц В. Вероятностные модели и методы в системах связи и управления. М.: Радио и связь, 1985.
10. Ленин В.И. Философские тетради. М.: Политиздат, 1990.
11. Реньи А. Трилогия о математике / Пер. с англ. М.: Мир, 1980.
12. Соломоник А. Семиотика и лингвистика. М.: Молодая гвардия, 1995.
13. Минский М. Фреймы для представления знаний. М.: Энергия, 1979.
14. Саати Т., Керне К. Аналитическое планирование. Организация систем/ Пер. с англ. М.: Радио и связь, 1992.