А. А. Малюк

ПРИНЦИПЫ ФОРМИРОВАНИЯ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

С философской точки зрения наиболее полное и адекватное представление о любом объективном процессе или явлении может быть получено на основе некоторой теории, являющейся совокупностью основных идей и дающей целостную картину закономерностей и существенных связей действительности. Если представить защиту информации как некоторый фрагмент объективного мира, то, естественно, сказанное в полной мере относится и к ней. Поэтому задача разработки целостной теории защиты информации была сформулирована в качестве одного из главных направлений работ по формированию научно-методологического базиса обеспечения информационной безопасности.

Можно констатировать, что в процессе исследований по этому направлению на сегодняшний день удалось сформулировать основы такой теории защиты. Достаточно подробное изложение их содержится в учебном пособии [1]. Первоначальный вариант основ теории защиты носил сугубо вербальный характер, в последующем частично удалось сформировать ее структуру в аксиоматическом представлении.

На содержание теории существенное влияние оказывает то обстоятельство, что процессы защиты информации носят ярко выраженный стохастический и в значительной мере непредсказуемый характер. В силу этого методология и методы классической теории систем оказались не вполне адекватными для описания и моделирования процессов защиты информации. Возникла необходимость широкого привлечения методов, основанных на использовании эвристических способностей человека.

Дадим определение и сформулируем основные понятия теории защиты информации.

Теория защиты информации определяется нами как система основных идей, дающая целостное представление о сущности проблемы защиты, закономерностях ее развития и существенных связях с другими отраслями знания, формирующаяся и развивающаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

Из приведенного определения довольно четко могут быть выведены основные задачи теории защиты, которые в развернутом виде формулируются следующим образом. Теория защиты информации должна:

- предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты;
- полно и адекватно отображать структуру и содержание взаимосвязей с родственными и смежными областями знаний;

- аккумулировать опыт предшествующих исследований, разработок и практического решения задач защиты информации;
- ориентировать в направлении наиболее эффективного решения основных задач защиты и предоставлять необходимые для этого научно-методологические и инструментальные средства;
- формировать научно обоснованные перспективные направления развития теории и практики защиты информации.

Сформулированные таким образом основные задачи определяют состав и общее содержание теории защиты информации. Составными частями ее, очевидно, должны быть:
- полные и систематизированные сведения о происхождении, сущности и содержании проблемы защиты;
- систематизированные результаты ретроспективного анализа развития теоретических исследований и разработок, а также опыта практического решения задач защиты, полно и адекватно отображающие наиболее устойчивые тенденции в этом развитии;
- научно обоснованная постановка задачи защиты информации, полно и адекватно учитывающая текущие и перспективные концепции построения информационных технологий, потребности в защите информации и объективные предпосылки их удовлетворения;
- общие стратегические установки на организацию защиты информации, учитывающие все многообразие потенциально возможных условий защиты;
- методы, необходимые для наиболее эффективного решения всех задач защиты и содержащие как общеметодологические подходы к решению, так и конкретные приложения;
- методологическая и инструментальная база, содержащая необходимые методы и инструментальные средства решения любой совокупности задач защиты в рамках любой выбранной стратегической установки;
- научно обоснованные предложения по организации и обеспечению работ по защите информации;
- научно обоснованный прогноз перспективных направлений развития теории и практики защиты информации.

Приведенный перечень даже при таком очень общем представлении содержания задач свидетельствует о многоаспектности теории защиты, что, естественно, порождает значительные трудности ее формирования. Положение усугубляется еще и тем, что по мере развития исследований, разработок и практической их реализации появляются новые аспекты, защита информации представляется все более комплексной и все более масштабной проблемой. Существенное влияние оказывает также неординарность этой проблемы, связанная с повышенным влиянием на процессы защиты случайных трудно предсказуемых событий. Таким образом, изначально предопределяется настоятельная необходимость выбора и обоснования методологических принципов формирования самой теории защиты.

Анализ истории развития науки и техники показывает, что всю совокупность общеметодологических принципов формирования нового научного направления удобно разделить на две группы: общетеоретические и теоретико-прикладные принципы.

Основные принципы общетеоретического характера могут быть сформулированы следующим образом.

1. Четкая целевая направленность исследований и разработок, причем цели должны быть сформулированы настолько конкретно, чтобы на любом этапе работ можно было предметно оценить степень их достижения. Применительно к теории защиты информации целевой установкой может являться приведенный выше перечень ее составных частей.

2. Неукоснительное следование главной задаче науки, которая заключается в том, чтобы видимое, лишь выступающее в явлении движение свести к действительному внутреннему

движению, которое, как правило, скрыто. Данный принцип ориентирует на поиск научно обоснованных решений изучаемой проблемы, которые в общем случае существенно эффективнее эмпирических. Для рассматриваемых нами проблем защиты информации данное обстоятельство особенно важно, поскольку сейчас по-прежнему превалируют эмпирические подходы к их решению.

3. Упреждающая разработка общих концепций, на базе которых могли бы решаться все частные вопросы. Достаточно очевидно, что данный принцип является дальнейшим развитием предыдущего. Его требования заключаются в том, чтобы все получаемые научно обоснованные решения образовывали единую систему. Применительно к защите информации речь в данном случае должна идти о формировании некоторой унифицированной концепции защиты, справедливой для широкого спектра требований и условий организации соответствующих процессов.

4. Формирование концепций на основе реальных фактов, а не абстрактных умозаключений. Сущность этого принципа очевидна и не требует дополнительных пояснений. Следуя ему, в работе [2], например, были приведены результаты ретроспективного анализа фактографических данных о развитии подходов к защите информации.

5. Учет всех существенно значимых связей, относящихся к изучаемой проблеме. Практическая очевидность данного принципа в дополнительной аргументации не нуждается и дает достаточно оснований рассматривать его в качестве одного из основных принципов общетеоретического характера.

6. Строгий учет диалектики взаимосвязей количественных и качественных изменений. Для рассматриваемых нами проблем защиты информации данный принцип имеет прямое действие, конкретное содержание которого изложено ниже при обосновании следующего принципа.

7. Своевременное видоизменение постановки изучаемой проблемы или решаемой задачи. Сущность этого принципа заключается в том, что назревшие качественные изменения, подготовленные изменениями количественными в процессе предшествующего развития изучаемого явления, должны быть актуализированы путем видоизменения самой постановки решаемой задачи. Если говорить о развитии способов и методов защиты информации, то сегодня мы должны опираться на принципиально новый подход к формулированию соответствующей задачи, рассмотрению которого целиком посвящена статья [2].

Таким образом, с учетом современного этапа развития теории и практики защиты информации приведенные общетеоретические принципы могут быть интерпретированы так, как представлено в табл. 1.

Таблица 1. Интерпретация общеметодологических принципов развития науки применительно к современным проблемам защиты информации

№№п/п	Формулировки принципов	Интерпретация
1.	Строгая целевая направленность.	Главная цель — формирование научно-технических предпосылок, необходимых для перехода от экстенсивных способов решения проблем защиты информации к интенсивным, т. е. 1) дальнейшее развитие основ теории защиты; 2) формирование регулярных методологии анализа степени уязвимости информации и обоснования целесообразного уровня защиты; создание методологии синтеза систем защиты, оптимальных по всей совокупности существенно значимых критериев, и оптимального управления ими в процессе их функционирования.

2.	Неукоснительное следование главной задаче науки — за внешними проявлениями вскрыть внутренние движения.	Необходимо: 1) провести тщательную аналитико-синтетическую обработку всей совокупности доступных статистических данных, относящихся к обеспечению защиты информации; 2) выявить устойчивые тенденции в эволюционном развитии теории и практики защиты информации; 3) осуществить прогноз наиболее вероятных направлений развития выявленных тенденций.
3.	Упреждающая разработка общих концепций.	1. Уточнение и строгое научное обоснование концепции защиты информации. 2. Формирование на базе кортежа концептуальных решений по защите информации единой методологии создания, организации и обеспечения функционирования систем защиты информации, соответствующих заданным требованиям к защите.
4.	Формирование концепций на основе реальных фактов.	1. Формирование структуры и содержания информационного кадастра по проблеме защиты информации. 2. Организация систематического и целенаправленного сбора и накопления всех данных, относящихся к обеспечению защиты информации. 3. Регулярная обработка всех накопленных данных в целях обновления и пополнения информационного кадастра по защите информации. 4. Периодический анализ данных информационного кадастра в целях выявления новых фактов относительно различных аспектов защиты информации.
5.	Учет всех существенно значимых факторов, влияющих на изучаемую проблему.	1. Рассмотрение защиты информации как комплексной проблемы в целевом, инструментальном и организационном аспектах. 2. Рассмотрение проблемы комплексной защиты как составной части более общей проблемы управления информацией. 3. Рассмотрение проблемы управления информацией как составной части глобальной проблемы информатизации современного общества.
6.	Строгий учет диалектики взаимосвязей количественных и качественных изменений в развитии изучаемых явлений.	Необходимо предметно обосновать, что к настоящему времени в развитии проблем защиты информации произошли (накоплены) такие количественные изменения (масштабы работ, объемы расходуемых ресурсов, арсеналы используемых средств), на основе которых вполне созрела необходимость качественных изменений в подходах к организации и обеспечению защиты в общегосударственном масштабе.
7.	Своевременное видоизменение постановки задачи.	Интерпретация требований данного принципа заключается в разработке и обосновании необходимости, сущности и содержания перехода от экстенсивных к интенсивным способам решения всех проблем защиты информации.

Что касается теоретико-прикладных принципов, то их содержание представляет собой требования и рекомендации по организации самого процесса изучения сложных проблем. Представляется, что в их число должны быть включены следующие четыре принципа.

1. Построение адекватных моделей изучаемых систем и процессов. В постановочном плане данный принцип понятен и общепризнан. Однако следует иметь в виду, что решение задачи построения моделей, адекватных моделируемым системам и процессам, не вызывает особых трудностей только для технических (т. е. строго формальных) систем. Для систем же организационно-технологического типа, к числу которых относятся и системы защиты информации, подверженных серьезному влиянию случайных и даже трудно предсказуемых факторов, построение адекватных моделей наталкивается на сложности принципиального характера. В этом случае методы классической теории систем оказываются недостаточно приспособленными для систем этого класса. Попытки построения моделей указанных систем с использованием традиционных методов чаще всего приводят к серьезной трансформации постановки задачи, уменьшающей, а то и полностью исключающей влияние случайных факторов. В итоге создаваемые модели оказываются неадекватными моделируемым системам. Таким образом, методы моделирования, ориентированные на формальные системы, нуждаются в существенном расширении и дополнении.

2. Унификация разрабатываемых решений. Содержание данного принципа очевидно. Фактически он детализирует в известной мере один из аспектов общеметодологического принципа упреждающей разработки общих концепций, поскольку любое унифицированное решение есть своего рода концепция.

3. Максимальная структуризация изучаемых систем и вырабатываемых решений. Под структуризацией здесь понимается процесс формирования архитектуры разрабатываемых систем и технологических схем их функционирования, наилучшим образом удовлетворяющих всей совокупности условий эксплуатации и дальнейшего совершенствования. В более общей постановке структуризация может рассматриваться как одно из направлений расширения научно-методологического базиса классической теории систем.

4. Радикальная эволюция в реализации разработанных концепций. Результатом изучения сложных проблем, как правило, являются предложения и решения (концепции) по более или менее кардинальному совершенствованию архитектуры соответствующих систем или процессов организации и обеспечения функционирования. Естественно, при этом возникает вопрос о способах практического претворения в жизнь разработанных концепций. Крайними вариантами будут: 1) выбросить (убрать, демонтировать) прежние решения и заново построить систему в строгом соответствии с новыми концепциями, 2) отказаться от новых концепций во имя сохранения прежних решений. В реальной жизни эти крайние варианты если и будут разумными, то лишь в каких-то неординарных ситуациях, в подавляющем же большинстве ситуаций рациональным будет какой-то промежуточный вариант. Для ориентации в подобных ситуациях В. М. Глушков еще в 70-х годах XX в. сформулировал принцип так называемой радикальной эволюции, суть которого, как следует из самого названия, сводится к тому, что надо стремиться к радикальным совершенствованиям, но реализовывать их эволюционным путем.

СПИСОК ЛИТЕРАТУРЫ:

1. *Малюк А. А.* Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие. М.: Горячая линия — Телеком, 2004.

2. *Малюк А. А.* К вопросу о периодизации подходов к защите информации // Проблемы информационной безопасности. Компьютерные системы. 2010. № 2. С. 24–30.