Посвящается 80-летию профессора В. А. Герасименко

А. А. Малюк

К ВОПРОСУ ОБ ИНТЕНСИФИКАЦИИ ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ

В различного рода энциклопедических изданиях понятие «интенсивный» определяется как ‘напряженный, усиленный, имеющий высокую производительность’. В соответствии с этим интенсификацию можно определить как ‘усиление, увеличение напряженности, производительности, действенности’. В 70–80-е годы прошлого века данный термин активно применялся в СССР по отношению к индустриальному производству. В этом случае интенсификация конкретизируется как развитие производства на основе применения все более эффективных средств и технологических процессов, использования передовых методов организации труда, достижений научно-технического прогресса. Альтернативным интенсивному способу является способ экстенсивный, при котором рост объема производства достигается за счет количественного увеличения вовлекаемых в производство ресурсов без качественных изменений производственных процессов.

Приведенные выше общие положения довольно характерны и для процессов, происходящих в последнее время в области защиты информации. При этом преобладавший до недавнего времени подход к защите информации, который условно может быть назван экстенсивным, в его чистом виде означает независимую организацию защиты на каждом объекте информатизации. Интенсивный же подход, являющийся предметом нашего рассмотрения, предполагает организацию защиты информации в соответствии с некоторой единой, научно обоснованной концепцией в масштабах региона и государства в целом.

Короче говоря, в развернутом виде переход к интенсивным способам защиты означает целенаправленную реализацию всех достижений теории и практики, которые в концентрированном виде отражены в унифицированной концепции защиты информации (УКЗИ). Данная концепция достаточно подробно изложена в работах профессора В. А. Герасименко (например: [1]) и развита автором данной статьи в ряде работ [2, 3 и др.], выполненных в 2000–2005 г. С сегодняшних позиций можно выделить ряд основных положений УКЗИ, практическая реализация которых и будет означать переход к интенсивным способам защиты информации. Рассмотрим их более подробно.

1. Структурированное описание среды защиты. Такое описание представляет структуру защищаемого объекта или системы и применяемую технологию обработки информации в виде направленного графа, вершины которого отображают структурные компоненты объекта (системы), а дуги — направления циркуляции информации в процессе их функционирования. При этом удобно

в целях унификации методов такого представления структуры объекта или системы ввести понятия типового структурного компонента и его типового состояния.

2. Количественный анализ (хотя бы приближенный, оценочный, рамочный) степени уязвимости информации. Такой анализ требуется прежде всего для возможно более объективной оценки реальных угроз информации и необходимых усилий и расходов на ее защиту. Представляется, что при нынешних масштабах работ по защите информации суммарный эффект от оптимизации расходов на защиту будет огромным. В основах теории защиты информации (см., например: [4—11]) разработана довольно развитая методология оценки уязвимости информации, состоящая из трех элементов: системы показателей уязвимости, системы угроз информации и системы моделей определения текущих и прогнозирования ожидаемых значений показателей уязвимости. Эта методология создает объективные предпосылки для научно обоснованного решения данной задачи. Однако практическая реализация разработанной методологии сопряжена с преодолением значительных трудностей, связанных с формированием баз исходных данных, необходимых для моделей оценки уязвимости. Подходы к преодолению этих трудностей мы попытаемся осветить ниже.

3. Научно обоснованное определение (причем желательно в количественном выражении) требуемого уровня защиты. Трудности решения этой задачи связаны с тем, что на уровень защиты информации на конкретных объектах в конкретных условиях их функционирования оказывает влияние большое количество разноплановых факторов. В силу этого в настоящее время требуемый уровень защиты оценивается только качественно. В [4] рассмотрен подход к более объективному определению требуемого уровня защиты, основанный на структуризации влияющих на него факторов и их количественных оценках, которые определяются экспертным путем. Можно предположить, что опора на эту методику позволит повысить уровень обоснованности требований, предъявляемых к системе защиты информации.

Таким образом, интенсификация процессов защиты информации на основе единой унифицированной методологии должна, в конечном счете, обеспечить построение оптимальных систем защиты с количественными оценками получаемых решений. При этом оптимизация систем защиты понимается нами в одной из следующих постановок: первая — при имеющихся ресурсах, выделенных на защиту, обеспечить максимально возможный уровень защиты информации; вторая — обеспечить требуемый уровень защиты информации при минимальном расходовании ресурсов. Для достижения указанных целей в упоминавшейся выше УКЗИ предложен кортеж концептуальных решений, представляющий собой следующую последовательность: функции защиты — задачи защиты — средства защиты — система защиты.

Приведем определения этих элементов кортежа.

Функция защиты — совокупность однородных в функциональном отношении мероприятий, регулярно осуществляемых в автоматизированной системе различными способами и методами, с целью создания, поддержания и обеспечения условий, объективно необходимых для надежной защиты информации.

Задача защиты — организованные возможности средств, методов и мероприятий, осуществляемых в автоматизированной системе с целью полной или частичной реализации одной или нескольких функций защиты.

Система защиты — организованная совокупность всех средств, методов и мероприятий, выделяемых (предусмотренных) в автоматизированной системе для решения в ней выбранных задач защиты.

Кортеж концептуальных решений создает основу для синтеза оптимальных систем защиты информации с количественными оценками достигаемого уровня защиты. Детальное рассмотрение взаимодействия компонентов кортежа было проведено в упоминавшейся выше книге [4]. В конспективном виде оно сводится к следующему.

1. По требуемому уровню защиты информации определяется требуемый уровень надежного осуществления каждой из полного множества функций защиты.

2. Из всех потенциально возможных наборов задач защиты выбираются те, которые обеспечивают требуемый уровень надежного осуществления каждой из функций наименьшим числом решаемых задач.

3. Из всех потенциально возможных наборов средств защиты выбираются те, которые обеспечивают решение всех выбранных на предыдущем этапе задач защиты при минимальном расходовании ресурсов.

4. Все выбранные средства защиты информации объединяются в единую систему защиты по всем канонам построения систем организационно-технологического типа.

Рассмотрим теперь более подробно проблемы, связанные с преодолением трудностей, возникающих при практической реализации приведенного кортежа концептуальных решений по защите информации.

Наиболее серьезной проблемой здесь является формирование баз исходных данных, необходимых для реализации моделей систем и процессов защиты информации, используемых в УКЗИ. Задача эта весьма трудоемкая, к тому же она не может быть решена на основе формальных методов.

О трудоемкости задачи можно судить хотя бы по количеству данных, которые надо определять. Так, для реализации самых простых моделей оценки уязвимости информации необходимо знать вероятность доступа нарушителей различных категорий в различные зоны объекта защиты, вероятность проявления в этих зонах различных каналов несанкционированного получения информации (КНПИ) в различных структурных компонентах защищаемого объекта, вероятность доступа нарушителей различных категорий, находящихся в зоне, к проявившимся там КНПИ, вероятность наличия в проявившемся КНПИ защищаемой информации в момент доступа к нему нарушителя. Если учесть, например, что, по расчетам профессора В. А. Герасименко, приведенным в [4], число категорий потенциальных нарушителей может быть ограничено 10, число зон злоумышленных действий при использовании пятирубежной модели защиты составляет соответственно 5, число типовых структурных компонентов в большинстве случаев не превышает 25, а КНПИ — 100, то общее число необходимых исходных данных составит $N = 10 \times 5 + 100 \times 25 + 100 \times 10 + 100 \times 25 = 6050$.

Определение требуемого уровня защиты информации должно также учитывать показатели важности каждого влияющего на него фактора. В [4] было выделено 67 таких факторов, объединенных в 5 групп по характеру их происхождения, характеру обрабатываемой информации, технологии ее обработки, архитектуре объекта защиты, условиям организации работы.

Трудности формирования указанных баз исходных данных помимо большого их объема усугубляются еще и весьма высоким уровнем неопределенности, связанной с непредсказуемостью поведения злоумышленников. Исследования данного аспекта проблемы в процессе формирования теории защиты информации на сегодняшний день привели нас к выводу, что единственным возможным решением задачи формирования исходных данных является применение методов экспертных оценок, «мозгового штурма» и психоинтеллектуальной генерации. Таким образом, мы приходим к безальтернативному выводу о том, что интенсификация процессов защиты информации предполагает широкое использование неформально-эвристических методов.

Однако эффективность указанных методов существенно зависит от представительности выборок, на которых они осуществляются. Кроме того, непрерывное изменение условий защиты, постоянный рост возможностей злоумышленного доступа к защищаемой информации, а также совершенствование методов ее защиты требуют того, чтобы экспертные оценки были не просто перманентными, а практически непрерывными. Этого можно достичь лишь при наличии стройной и целенаправленной организации системы сопровождения работ по защите информации. Наиболее полным и наиболее адекватным решением этой проблемы было бы создание сети специализированных центров защиты информации (ЦЗИ), аккумулирующих все новейшие достижения в области защиты

и специализирующихся на формировании научно-методологического и инструментального базиса решения соответствующих задач на интенсивной основе (включая и базы необходимых исходных данных). Концепция создания и организации работы ЦЗИ к настоящему времени разработана нами достаточно полно, наиболее детально она изложена в [12, 13]. В соответствии с этой концепцией сегодня в системе высшей школы уже созданы 29 региональных учебно-научных центров.

Как ясно из вышесказанного, одной из весьма важных функций ЦЗИ должна стать непрерывно проводимая экспертиза в целях формирования баз исходных данных для моделирования процессов защиты информации. Формами экспертизы могут быть:

- обследование конкретных объектов, являющихся абонентами соответствующего ЦЗИ;
- непрерывное наблюдение за процессами функционирования действующих систем защиты информации;
- традиционные экспертные оценки;
- организация сеансов «мозгового штурма»;
- организация сеансов психоинтеллектуальной генерации.

В качестве экспертов могут выступать сотрудники ЦЗИ (которые по определению должны быть высококвалифицированными специалистами), компетентные специалисты служб защиты информации на объектах, сотрудники организаций, занимающиеся вопросами защиты, профессорско-преподавательский состав, научные сотрудники и аспиранты вузов, готовящих соответствующих специалистов.

Нетрудно увидеть, что при достаточно развитой сети ЦЗИ (а создание именно развитой сети центров является на сегодня, по нашему мнению, объективной необходимостью) будет решена (и весьма эффективно) задача массовой экспертизы, в чем и заключается центральная идея данного мероприятия.

Один из дискуссионных вопросов, поднимаемых в процессе обсуждения проблемы организации массовой экспертизы, заключается в чрезвычайно большом разнообразии условий защиты информации на современных объектах информатизации. При этом практически невозможно выразить единым значением ту или иную характеристику, общую для всех объектов. Ведь, например, при прочих равных условиях вероятность доступа злоумышленника к некоторым КНПИ существенно зависит даже от этажа, на котором расположены средства обработки защищаемых данных. Игнорировать это обстоятельство при решении конкретных практических задач никоим образом нельзя. В этих условиях необходимо четко определить подход к проведению экспертизы. В принципе здесь возможны два метода — метод синтеза и метод анализа.

Экспертиза по методу синтеза заключается в формировании соответствующих данных каждым ЦЗИ для конкретных объектов — абонентов центра. Полученные данные в дальнейшем могут подвергаться всесторонней аналитико-синтетической обработке в целях выработки оценок любого уровня обобщения.

Экспертиза по методу анализа осуществляется в два этапа. Сначала формируется наиболее полный перечень факторов, влияющих на защиту информации, выбираются возможные значения каждого из факторов и экспертно определяются относительные веса групп факторов и различных факторов в пределах группы. Затем выбираются возможные значения каждого фактора в их общей совокупности.

На втором этапе по этим данным формируется поле потенциально возможных условий защиты (как сочетаний значений всех выбранных факторов) и определяется вес каждого из условий этого поля. Затем методами кластерного анализа поле потенциально возможных условий может быть разделено на некоторое число классов, каждый из которых будет объединять однородные (сходные) в некотором смысле условия. После этого необходимые данные могут определяться отдельно для каждого класса.

Подведем некоторые итоги нашего рассмотрения особенностей проблемы защиты информации в современных условиях формирования информационного общества.

Ретроспективный анализ развития подходов к решению проблем защиты информации показывает, что их история может быть довольно четко разделена на ряд периодов, в течение

которых прослеживается постепенный переход от выбора средств защиты на базе опыта к разработке в настоящее время основ теории защиты информации, постановке задачи многоаспектной комплексной защиты и формированию унифицированной концепции защиты. Изменялись и применяемые средства защиты от функционально ориентированных механизмов до системы комплексной защиты и создания изначально защищенных информационных технологий.

Современный взгляд на защиту информации как на комплексную проблему неминуемо приводит к пониманию роста значимости системных вопросов, связанных с процессом защиты. Среди них: формирование и обоснование общей политики защиты, оптимизация процессов проектирования и функционирования комплексных систем защиты, подбор, обучение и расстановка соответствующих кадров специалистов, сбор и аналитико-синтетическая обработка данных о функционировании реальных систем защиты информации.

Таким образом, возникают необходимые объективные предпосылки для перехода к новому этапу в решении задач защиты — этапу, который может быть назван интенсификацией процессов защиты информации.

Переход от экстенсивных к интенсивным способам защиты информации означает целенаправленную реализацию всех достижений теории и практики защиты, которые в концентрированном виде отражены в унифицированной концепции защиты информации, а именно: структурированное описание среды защиты, всесторонний количественный анализ степени уязвимости информации на объекте (или в системе), научно обоснованное определение требуемого уровня защиты в конкретных условиях функционирования объектов (систем), построение оптимальных систем защиты на основе единой унифицированной методологии.

Заметим в заключение, что реализация всех этих требований возможна лишь при наличии стройной и целенаправленной организации системы сопровождения работ по защите информации. Наиболее полным и адекватным решением этой проблемы является, на наш взгляд, создание сети специализированных центров информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. *Герасименко В. А.* Защита информации в автоматизированных системах обработки данных. Кн. 1 и 2. М.: Энергоатомиздат, 1994.
2. *Малюк А. А.* Современные проблемы теории и практики защиты информации // Безопасность информационных технологий. 2002. № 3, 4.
3. *Малюк А. А.* Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие. М.: Горячая линия — Телеком, 2004.
4. *Герасименко В. А., Малюк А. А.* Основы защиты информации: Учебник. М.: МИФИ, 1997.
5. *Герасименко В. А.* Информация, информатизация и информационная безопасность // Безопасность информационных технологий. 1996. № 4.
6. *Поздняков А. И.* Информационная безопасность: концептуальные основы, современные проблемы, перспективы // Безопасность информационных технологий. 1996. № 4.
7. *Герасименко В. А., Малюк А. А.* Системный подход к защите информации на современном объекте // Безопасность информационных технологий. 1999. № 2.
8. *Шумский А. А., Шелупанов А. А.* Системный анализ в защите информации: Учебное пособие. М.: Гелиос АРВ, 2005.
9. *Малюк А. А.* Защита информации: Конспект лекций. М.: МИФИ, 2002.
10. *Герасименко В. А., Малюк А. А.* Кортеж концептуальных решений по защите информации // Безопасность информационных технологий. 1997. № 3.
11. *Малюк А. А., Пазизин С. В., Погожин Н. С.* Введение в защиту информации в автоматизированных системах: Учебное пособие. М.: Горячая линия — Телеком, 2004.
12. Проблемы создания и организации работы центров защиты информации / Под ред. А. А. Малюка // Безопасность информационных технологий. 1997. № 4.
13. *Малюк А. А., Поляков А. А.* Региональные учебно-научные центры по проблемам информационной безопасности — организационная основа реализации положений Доктрины информационной безопасности Российской Федерации в системе высшей школы // Материалы VIII Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы». М., 2001.