А. А. Малюк

К ВОПРОСУ О ТИПИЗАЦИИ И СТАНДАРТИЗАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

В самом общем виде и на чисто прагматическом уровне требования к защите информации могут быть определены как предотвращение угроз информации, по крайней мере тех из них, проявление которых может привести к существенно значимым последствиям. Но поскольку защита информации есть случайный процесс (показатели уязвимости носят вероятностный характер), то и требования к защите должны выражаться терминами и понятиями теории вероятностей.

По аналогии с требованиями к надежности технических систем, обоснованными в классической теории систем, требования к защите могут быть сформулированы в виде условия:

$$P \geq \overline{P},$$

где $P_з$ — оценка реальной вероятности защищенности информации, а $\overline{P}$ — требуемый уровень защищенности.

С требованиями, выраженными в таком виде, можно оперировать с использованием методов классической теории систем. Однако на практике решение проблем защиты информации сопряжено с исследованиями и разработкой таких систем и процессов, в которых и конкретные методы, и общая идеология классической теории систем могут быть применены лишь с большими оговорками. Для повышения степени адекватности применяемых моделей реальным процессам необходим **переход от концепции создания инструментальных средств получения необходимых решений на инженерной основе к концепции создания методологического базиса и инструментальных средств для динамического оптимального управления соответствующими процессами** (иными словами, необходим переход от экстенсивных к интенсивным способам решения проблем защиты информации).

Проблема определения требований к защите информации имеет комплексный характер и может рассматриваться как в организационном, так и в техническом аспектах. Причем в условиях автоматизированной обработки информации существует большое количество каналов несанкционированного ее получения, которые не могут быть перекрыты без применения специфических технических и программно-аппаратных средств. Это серьезно повышает удельный вес технических аспектов и приводит к необходимости определения требований к системам защиты, содержащим указанные средства.

Наиболее подходящим здесь оказывается подход, основанный на выделении некоторого количества типовых систем защиты, рекомендуемых для использования в тех или иных конкретных условиях и содержащих определенные механизмы защиты, т. е. подход, базирующийся на создании системы стандартов в области защиты информации.

Основу такой системы, действующей в настоящее время в Российской Федерации, составляют руководящие документы Гостехкомиссии России, разработанные в начале 1990-х годов и дополненные впоследствии рядом нормативных актов Федеральной службы по техническому и экспортному контролю. Эти документы были созданы в результате исследований и практической деятельности в данной области (с учетом «Критериев оценки доверенных компьютерных систем» Министерства обороны США, которые достаточно широко известны под названием «Оранжевая книга» и которые вместе с Европейскими и Канадскими критериями легли в последнее время в основу «Общих критериев» — стандарта ISO 15408—99 «Критерии оценки безопасности информационных технологий»).

Одновременно Россия использует ряд международных стандартов, принятых в качестве прямого заимствования и ориентированных на обеспечение информационной безопасности при взаимодействии открытых систем.

Кроме того, имеются стандарты, касающиеся защиты информации от ее утечки через побочные электромагнитные излучения и наводки (ПЭМИН).

Если не рассматривать вопросов криптографии и защиты информации от утечки через ПЭМИН, которые решаются во всех странах на национальном уровне, общие вопросы обеспечения безопасности информационных технологий развиваются во всех странах параллельно, а в последние годы совместно. Основу обеспечения безопасности информационных технологий составляет решение трех задач: обеспечение секретности (конфиденциальности), обеспечение целостности и обеспечение доступности. Эта основа заложена в стандартах, касающихся обеспечения безопасности информационных технологий, практически всех стран.

Аналогичный подход реализован и в упоминавшихся выше «Общих критериях». Анализ этого международного стандарта, проведенный российскими специалистами, свидетельствует о том, что он полностью соответствует по сути сложившейся в России методологии защиты информации от несанкционированного доступа. Однако по уровню систематизации, полноте и степени детализации требований, универсальности и гибкости «Общие критерии» несколько превосходят российские стандарты.

Наличие представленных методик определения требований по защите информации и закрепление их в официальных документах создают достаточно надежную базу для решения практических проблем защиты. Однако очевидно, что с точки зрения современной постановки задачи защиты информации все они являются недостаточными по ряду причин, а именно:

1) методики ориентированы на защиту информации только в средствах вычислительной техники и практически не затрагивают объектовый, а тем более региональный уровень обеспечения информационной безопасности;

2) в используемых подходах учитываются далеко не все факторы, оказывающие существенное влияние на уязвимость информации;

3) в научном плане методики обоснованы недостаточно (за исключением требований к защите информации от утечки по техническим каналам).

Рассмотрим возможные подходы к преодолению указанных недостатков.

Определим систему защиты информации (СЗИ) как совокупность средств, методов и мероприятий, предусматриваемых в составе автоматизированной системы (АС) для решения выбранных задач защиты. Введением понятия СЗИ постулируется, что все ресурсы, выделяемые для защиты информации, должны объединяться в единую, целостную функционально самостоятельную систему.

Концептуально важнейшим требованием, предъявляемым к СЗИ, является требование адаптируемости, которое обуславливается, с одной стороны, тем, что многочисленные факторы, влияющие на требуемый уровень защиты, могут существенно изменяться, а с другой — тем, что сами процессы защиты информации относятся к слабоструктурированным. Управление такого рода процессами эффективно только при условии адаптируемости системы.

Помимо этого, к СЗИ предъявляются также различные требования функционального, эргономического, экономического, технического и организационного характера.

Еще в работе [1] были сформулированы общеметодологические принципы построения и функционирования СЗИ. В настоящее время в условиях системно-концептуального подхода к защите эти принципы несколько видоизменяются и включают в себя: концептуальное единство системы, адекватность предъявляемым требованиям, адаптируемость, функциональную самостоятельность, удобство использования, минимизацию предоставляемых прав, полноту контроля, активность реагирования, экономичность.

Очевидно, что архитектура СЗИ должна быть аналогичной архитектуре защищаемой системы и может рассматриваться в функциональном, организационном и структурном аспектах.

Функционально СЗИ представляет собой совокупность реализуемых ею функций защиты. Организационно она состоит из механизмов обеспечения защиты информации, механизмов управления ими и механизмов общей организации работы системы. В понятие организационного построения СЗИ входит также распределение ее элементов по организационно-структурным компонентам защищаемой системы. Исходя из этого в организационном построении СЗИ должны быть предусмотрены подсистемы защиты в каждом из структурных компонентов и некое управляющее звено, которое справедливо назвать ядром СЗИ.

Определим ядро системы защиты как специальный компонент, предназначенный для объединения всех подсистем СЗИ в единую целостную систему для организации, обеспечения и контроля ее функционирования [1]. С учетом этого функциями ядра СЗИ должны быть: организация и обеспечение блокирования бесконтрольного доступа к базам защищаемых данных; включение компонентов СЗИ в работу при поступлении запросов на обработку защищаемых данных; управление работой СЗИ в процессе обработки защищаемых данных; организация и обеспечение проверок правильности функционирования СЗИ; организация и ведение массивов эталонных данных СЗИ; обеспечение реагирования на сигналы о несанкционированных действиях; ведение протоколов СЗИ.

Структурно СЗИ строится по аналогии со структурным построением защищаемой системы. Таким образом, ее структурная схема может быть представлена так, как показано на рис. 1.

Большое значение для обеспечения надежности и экономичности защиты имеют типизация и стандартизация систем защиты информации. Типизация в этом случае понимается как разработка типовых аппаратных, программных или организационных решений, а также технологических процессов защиты, а стандартизация — как процесс установления и применения стандартов (исходных для сопоставления с ними образцов, эталонов, моделей).

Анализ концептуальных подходов к защите информации показывает, что в интересах создания наилучших предпосылок для оптимизации защиты целесообразно выделить три уровня типизации и стандартизации: высший — уровень системы защиты в целом; средний — уровень составляющих компонентов; низший — уровень проектных решений по средствам и механизмам защиты.

Рис. 1. Общая структурная схема системы защиты информации

Типизация и стандартизация на высшем и среднем уровнях предполагают классификацию СЗИ, при которой все системы делились бы на группы, при этом каждая из них была бы адекватна некоторым вполне определенным требованиям к защите информации, а вся совокупность таких групп охватывала бы все потенциально возможные условия защиты.

В работе [2] был рассмотрен теоретико-эмпирический подход к решению такого рода задачи. Основу этого подхода составляют формирование полного множества всех потенциально возможных вариантов условий защиты, определение количественных характеристик каждого из вариантов и кластеризация всего поля вариантов по критерию непревышения заданного числа классов или меры различия количественных характеристик вариантов в пределах каждого из классов. Применив эмпирическую часть данного подхода к типизации СЗИ, мы можем получить их классификацию по уровню защиты, обеспечиваемому соответствующей системой, и активности реагирования на несанкционированные действия.

Исходя из практического опыта все СЗИ по уровню обеспечиваемой защиты целесообразно разделить на следующие четыре категории:

1) системы слабой защиты — рассчитанные на такие случаи, когда обрабатывается информация, имеющая низкий уровень конфиденциальности;

2) системы сильной защиты — рассчитанные на случаи обработки информации, подлежащей защите от несанкционированного доступа, однако объемы этой информации не очень велики, и обрабатывается она эпизодически;

3) системы очень сильной защиты — рассчитанные на случаи регулярной обработки больших объемов конфиденциальной информации;

4) системы особой защиты — в случаях регулярной обработки информации повышенной секретности.

По активности реагирования на несанкционированные действия все системы защиты можно разделить на следующие три типа:

1) пассивные СЗИ, в которых не предусматриваются ни сигнализация о несанкционированных действиях, ни воздействие системы защиты на нарушителя;

2) полуактивные СЗИ, в которых предусматривается сигнализация о несанкционированных действиях, но не предусматривается воздействие системы на нарушителя;

3) активные СЗИ, в которых предусматриваются как сигнализация о несанкционированных действиях, так и воздействие системы на нарушителя.

В общем случае можно предположить, что СЗИ каждой категории по уровню защиты могут относиться к разным типам активности реагирования. Однако исходя из здравого смысла вряд ли целесообразно строить активные системы слабой защиты. В то же время системы особой защиты обязательно должны быть активными. Таким образом, при классификации можно говорить об обязательных (О), целесообразных (Ц), нецелесообразных (НЦ), допустимых (Д) и недопустимых (НД) СЗИ. В итоге получается вариант, приведенный на рис. 2.

Тип СЗИ / Категория СЗИ	Пассивные	Полуактивные	Активные
Слабой защиты	Д / Ц (1)	Д / Ц*	Д / НЦ
Сильной защиты	НД	Д / Ц (2)	Д / Ц*(2а)
Очень сильной защиты	НД	Д*/ Ц*(3а)	Д / Ц / О*(3)
Особой защиты	НД	НД	О (4)

Рис. 2. Допустимые и целесообразные типы СЗИ для различных категорий (— в отдельных случаях)*

Далее для учета типа информационно-вычислительной системы воспользуемся классификацией, предложенной В. А. Герасименко [3]. Будем различать персональную ЭВМ, используемую локально (ПЭВМ), групповую ЭВМ, используемую локально (ГЭВМ), вычислительный центр предприятия или организации (ВЦП), вычислительный центр коллективного пользования (ВЦКП), локальную вычислительную сеть (ЛВС), слабо распределенную (в пределах населенного пункта, небольшой территории) вычислительную сеть (СВС), сильно распределенную, региональную вычислительную сеть (РВС), глобальную вычислительную сеть (ГВС).

Для всех перечисленных типов может быть предложен типовой проект СЗИ каждого из шести классов, показанных на рис. 2. Однако, как и в предыдущем случае, очевидно, что нецелесообразно использовать активные СЗИ особой защиты для защиты информации в ПЭВМ. С другой стороны, явно недостаточно использовать пассивные СЗИ слабой защиты для защиты информации в РВС и ГВС. Поэтому, как и в предыдущей классификации, в полном множестве СЗИ необходимо предусмотреть выделение целесообразных, допустимых и обязательных систем, что в итоге приведет нас к классификации, показанной на рис. 3.

Вариант СЗИ / Тип АС	1 Слабой защиты Пассивные	2 Сильной защиты Полуактивные	2а Сильной защиты Активные	3 Очень сильной защиты Активные	3а Очень сильной защиты	4 Особой защиты Активные
ПЭВМ	Ц (1)	Д/Ц* (1а)				
ГЭВМ	Ц* (2а)	Ц (2)	Д/Ц*			
ВЦП	Д* (3а)	Ц (3)	Д/Ц*	Д* (3в)		
ВЦКП			Ц (4)	Ц* (4а)	Ц* (4б)	Д* (4в)
ЛВС		Ц* (5а)	Ц (5)	Д* (5б)		
СВС		Ц* (6а)	Ц* (6б)	Ц (6)	Ц* (6в)	Д* (6г)
РВС			Ц* (7а)	Ц (7)	Д* (7б)	Ц* (7в)
ГВС				Ц (8)		Ц* (8а)

Рис. 3. Итоговая классификация СЗИ
*(Ц — целесообразно, Д — допустимо, * — в отдельных случаях)*

Что касается типизации и стандартизации на среднем уровне, то она предусматривает разработку типовых проектов структурно или функционально ориентированных компонентов СЗИ. В качестве первых логично выбрать компоненты СЗИ, ориентированные на защиту информации в конкретных типовых структурных компонентах защищаемой системы. В качестве же функционально ориентированных можно выбрать такие компоненты, как регулирование доступа на территорию, в помещения, к техническим средствам, программам и массивам данных, подавление излучений и наводок, предупреждение наблюдения и подслушивания, маскировка информации и, наконец, управление системой защиты.

Одним из перспективных, на наш взгляд, вариантов покомпонентной типизации и стандартизации СЗИ является метод, основанный на так называемой семирубежной модели. Достаточно подробно он изложен в работе [1]. Под рубежом защиты здесь понимается соответствующим образом организованная совокупность всех средств, методов и мероприятий,

используемых на рассматриваемом элементе системы или объекта для защиты информации. Очевидно, что тем или иным сочетанием перечисленных рубежей может быть представлена СЗИ практически любой системы (объекта). Каждый из рубежей защиты при этом может быть реализован с помощью типовых проектных решений.

Последней из рассматриваемых нами является типизация и стандартизация на низшем уровне, которая предполагает разработку типовых проектных решений по реализации различных средств защиты информации. Основными здесь являются технические, программные, организационные и криптографические средства.

Таким образом, можно констатировать, что у нас имеются весьма широкие возможности для типизации и стандартизации средств, механизмов и компонентов СЗИ и даже целых СЗИ. Дальнейшее развитие данного вопроса идет в направлении синтеза подходов, изложенных в данной статье.

СПИСОК ЛИТЕРАТУРЫ:

1. *Герасименко В. А., Малюк А. А.* Основы защиты информации: Учебник. М.: МИФИ, 1997.
2. *Малюк А. А.* Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие. М.: Горячая линия — Телеком, 2004.
3. *Герасименко В. А.* Защита информации в автоматизированных системах обработки данных. Кн. 1 и 2. М.: Энергоатомиздат, 1994.