4 Підготовка, перепідготовка та підвищення кваліфікації спеціалістів системи захисту інформації

УДК 681.3.

ЗАДАЧИ И ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Александр Архипов, Валерий Ворожко*

Национальный технический университет Украины "КПИ",

**Национальная академия Службы безопасности Украины*

Анотація: **Аналізуються задачі, які треба розв'язати при побудові комплексних систем захисту інформації, та можливості кадрового забезпечення цієї сфери.**

Summary: **The problems are analyses, which are necessary for deciding for want of construction of complex protective systems of an information, and possibility of personnel maintenance of this sphere.**

Ключові слова: **Захист інформації, комплексні системи захисту, підготовка кадрів.**

В последние годы, когда процессы информатизации в Украине приняли глобальный характер, весьма актуальной становится проблема безопасности информации, требующая в своем решении комплексного подхода, суть которого – одновременное использование в системе защиты информации взаимосвязанной совокупности правовых, экономических, организационно-технических и программно-математических методов и средств защиты информации. Практическая реализация комплексной системы защиты предполагает удовлетворение ряда принципов, среди которых центральным является принцип системности, требующий учета при построении защиты всех возможных угроз безопасности информации. В полном объеме выполнение этого принципа возможно лишь в том случае, если от традиционного ретроспективного выявления угроз (оборонительная стратегия защиты от уже известных по многолетней практике вариантов угроз) перейти к упреждающей стратегии защиты, предполагающей предсказание принципиально новых путей реализации угроз информации.

Прогностический подход к анализу угроз позволяет реализовать еще один принцип комплексной защиты, называемый принципом разумной достаточности: нельзя создать абсолютно непреодолимую систему защиты, поэтому целесообразно говорить о некотором приемлемом уровне безопасности информации (уровне её защищенности, уязвимости), при котором достигается компромисс между затратами на построение системы защиты и размерами возможного ущерба от потерь защищаемой информации.

Принцип разумной достаточности становится особенно актуальным для сложившейся ныне в Украине экономической ситуации, когда практическое большинство структур, организаций и предприятий вынуждены решать проблему защиты информации в условиях жесткого ограничения финансовых, материально-технических и кадровых ресурсов (последнее утверждение может представляться спорным, ниже ему будет дано более детальное обоснование). Упреждающая стратегия защиты позволяет предсказать возможные направления наиболее вероятных атак и, сконцентрировав на них основные средства защиты, создать эффективную и одновременно экономичную, относительно низкозатратную систему комплексной защиты информации. Однако практическая реализация подобного подхода подразумевает выполнение ряда специфических предпосылок. Главная из них – наличие научно обоснованной методологии построения систем комплексной защиты, в основе которой – системный анализ и прогноз угроз информации, оценка вероятностей их реализации, оценка рисков и общей уязвимости информации, а затем непосредственное рассмотрение задачи синтеза системы защиты как оптимизационной задачи, решение которой определяется из требования разумного баланса затрат на обеспечение определенного уровня эффективности системы защиты (гарантий безопасности информации) и размера проигрыша владельца информации в случае полного или частичного преодоления системы защиты.

Учитывая, что представления о "разумном балансе" могут быть достаточно разнообразны и вариабельны, например, достижение заданного уровня защищенности информации при минимальных затратах на систему защиты либо максимально возможного уровня защищенности при заданных ограничениях на затраты, становится очевидной сложность, многоаспектность и наукоемкость проблем анализа и синтеза систем комплексной защиты информации, результативное решение которых требует привлечение к работе в данной предметной области профессионально подготовленных специалистов весьма высокого класса. Причем

характер деятельности подобного специалиста подразумевает, что он владеет необходимым набором умений и знаний в области проектного менеджмента, достаточным для планирования, организации и координации всего комплекса работ по созданию системы защиты информации, знает особенности инфраструктуры и рыночного поведения в этой сфере. Объем подготовки специалистов такого рода должен быть достаточно массовым, так как число объектов информационной деятельности, на которых необходимо осуществлять защиту информации, уже велико, а в будущем, учитывая нарастающую тенденцию информатизации общества, будет продолжать увеличиваться.

Сложившаяся на сегодняшний день традиционная система подготовки специалистов в области защиты информации при своем создании была ориентирована на аспектный (позадачный) подход к защите информации. Эта система готовит специалистов по отдельным направлениям защиты, достаточно хорошо и глубоко владеющих методами, средствами и технологиями защиты в соответствующих направлениях, однако не имеющих навыков проектного менеджмента, аналитико-синтетической системной обработки информации и принятия решения, достаточной экономико-управленческой и правовой подготовки.

Следует также учесть, что методология построения систем комплексной защиты информации пока еще не сложилась, более того, процесс её становления, по-видимому, далек от завершения. Пока достаточно интенсивно развиваются направления, связанные с формализацией и математизацией основных методов и положений комплексной защиты, постепенно формируя область знаний, которую можно было бы условно определить как математические основы комплексной защиты информации. Однако в практических исследованиях высок вес вербальных описаний, особенно в постановочных разделах задачи синтеза защиты, процедурах переработки информации и принятия решений в вербальной форме (методы вербального анализа и оптимизации). К сожалению, дисциплины, в которых излагаются подобные методы обработки информации, в учебных планах для специалистов по защите информации отсутствуют.

Синтез систем защиты информации является ответственным, но отнюдь не финальным этапом процесса защиты. Еще один принцип комплексной защиты – принцип непрерывности утверждает, что защита – не разовое мероприятие, а непрерывный целенаправленный процесс, продолжающийся в ходе функционирования и эксплуатации уже созданной системы комплексной защиты. В этой ситуации особо значимой становится функция управления защитой, задача которой – обеспечение рационального использования созданных механизмов защиты информации, адаптация системы защиты к изменениям условий функционирования объекта информационной деятельности, изменениям характеристик угроз и состояния информационного противоборства в целом. На первое место выходят вопросы административно-организационного обеспечения защиты информации, менеджмента комплексной системы защиты. Необходимо обязательно учитывать, что этот менеджмент осуществляется в условиях еще не сложившейся нормативно-правовой базы в сфере защиты информации, развитие и становление которой – процесс достаточно продолжительный. Следовательно, полноценному специалисту по комплексной защите информации требуется основательная правовая подготовка.

Из изложенного выше следует, что для разработки и эксплуатационного сопровождения комплексных систем защиты информации необходимо наличие профессионально подготовленных кадров, совмещающих фундаментальную общеобразовательную подготовку, органично увязанную с комплексом специфических знаний инженерно-прикладного характера, с навыками организационно-управленческой работы, опирающейся на глубокое понимание действующего нормативно-правового законодательства в информационной сфере в сочетании с принципами разумной достаточности и экономической адекватности системы защиты.

Рассмотрим некоторые аспекты квалификационной характеристики специалиста в области комплексной защиты информации.

Данные специалисты предназначены для работы в службах и подразделениях защиты информации центральных и местных органов власти, в предприятиях, учреждениях и организациях любой формы собственности, в научно-исследовательских и проектных организациях, учебных, консультативных и других заведениях, являющихся объектами информационной деятельности.

Специалист в области комплексной защиты информации может выполнять следующие виды профессиональной деятельности:

- организационно-управленческую;
- организационно-эксплуатационную;
- экспериментально-исследовательскую;
- организационно-проектную.

При этом он ориентирован на выполнение сложных и ответственных работ на всех стадиях разработки и эксплуатации систем защиты информации. Осуществляет сбор и проводит предварительный анализ материалов об объекте информационной деятельности, участвует в их обследовании, аттестации и

категорировании, определяет и классифицирует информацию, подлежащую защите, определяет возможные технические каналы утечки информации и способы несанкционированного доступа к ней, формирует модель угроз. Участвует в разработке системы защиты информации на этапах её проектирования, реализации, внедрения, аттестации и эксплуатации, организует взаимодействие специалистов различного профиля на этих этапах. Организует и проводит работы по оценке технико-экономического уровня и эффективности проектируемых и реализуемых мер и средств комплексной защиты информации, обеспечивает формирование и принятие организационно-технических решений. Разрабатывает необходимые нормативно-технические и методические материалы, организационно-распорядительные документы, инструкции, регламентирующие управление системой защиты в ходе её проектирования, построения и эксплуатации.

Для решения перечисленных выше задач специалист по комплексной защите информации должен знать совокупность естественнонаучных, экономических, правовых и гуманитарных дисциплин, определяющих его базовую подготовку. В состав базового блока входят нормативные учебные дисциплины, а также дисциплины, номенклатура которых определяется из условия обеспечения последующего успешного усвоения профессионально-ориентированных и специальных дисциплин. Дополнительное требование, которое следует учитывать при формировании блока базовых дисциплин, состоит в том, что защита информации – это обеспечивающая функция относительно информационных процессов в различных сферах человеческой деятельности, поэтому особое внимание должно уделяться информационному блоку дисциплин, включающему, помимо традиционно изучаемых вопросов использования современных средств вычислительной техники и телекоммуникационных систем, рассмотрение принципов и методов организации информационных процессов, управления информационными потоками, различных аспектов информационного обеспечения деятельности предприятий и учреждений, информационных проблем общества в целом.

Кроме того, в базовой подготовке специалиста по комплексной защите информации должен быть представлен блок дисциплин менеджмента, включая менеджмент организаций, административный менеджмент, проектный менеджмент, законы и принципы теории организаций, методы, приемы и инструментарий социальной психологии для прогнозирования поведения личности в различных ситуациях, конфликтология, основы системного анализа.

В структуре профессионально-ориентированных и специальных дисциплин можно выделить три блока:

1) введение в защиту информации;
2) средства и технологии защиты информации;
3) методология и организация комплексной защиты информации.

В последнем блоке в свою очередь можно выделить два раздела:

3.1) теоретические основы комплексной защиты информации;
3.2) организационно-правовые и экономические аспекты комплексной защиты информации.

В блоке 1) рассматривается история, современная структура, организационно-правовые аспекты защиты информации, цели защиты, принципы и критерии классификации защищаемой информации, каналы утечки, методы и средства несанкционированного доступа, анализ и модели угроз информации, методики анализа уязвимости информации.

В блок 2) включаются дисциплины, в которых излагаются математические, физические и организационные основы защиты информации, описаны программные, аппаратные, инженерные средства защиты, технологии логико-математической и организационно-правовой защиты, направление и методы защиты информации в зависимости от её содержания и степени секретности, методики анализа и контроля эффективности применяемых средств и технологий защиты, принципы защиты интеллектуальной собственности.

Блок 3) содержит изложение методологии и основных направлений защиты информации, основы построения комплексных систем защиты информации, технологии управления этими системами, методы организации и управления службами защиты информации, методы анализа и оценки рисков, определения размера ущербов вследствие разглашения информации с ограниченным доступом, методы конкурентной разведки, методологию аналитической обработки информации с целью упреждающего анализа возможных угроз и рисков, ситуационного моделирования и прогноза развития процессов информационного противоборства, методов принятия решения (в том числе и при вербальном описании альтернатив).

Как уже отмечалось выше, традиционная система подготовки специалистов в области защиты информации не ориентирована на подготовку специалистов в области комплексной защиты информации. В какой-то степени восполнить этот пробел может введенная в 1997 г. по инициативе НТУУ “КПИ” по согласованию с Госкомсекретов Украины специальность 7.160104 “Административный менеджмент в сфере защиты информации с ограниченным доступом”. При введении этой специальности, в частности, при выборе её названия существенным оказалось влияние специальности 8.000007 “Административный менеджмент”,

учебный план которой предполагалось взять за базовый для новой специальности, усилив в нем физико-техническую и инженерную компоненту и добавив блок специальных дисциплин, адаптированный к области комплексных систем защиты информации. К сожалению, начавшаяся было разработка пакета нормативных документов к специальности 7.160104 "Административный менеджмент в сфере защиты информации с ограниченным доступом" прервалась с ликвидацией Госкомсекретов Украины. На сегодняшний день подготовка специалистов по этой специальности на основе самостоятельно разработанных учебных планов ведется в Национальном авиационном университете (г. Киев), Национальном горном университете (г. Днепропетровск), Государственном университете информационно-коммуникационных технологий (г. Киев). Во всех трех вузах преимущественный акцент при подготовке специалистов заметно смещен в сторону инженерно-технической компоненты образования, что объясняется традициями и спецификой этих вузов и может рассматриваться как введение технической специализации исходной специальности 7.160104. Вопрос о подготовке специалистов непосредственно в области комплексных систем защиты информации пока остается открытым.

УДК 681.3

МАТЕМАТИЧЕСКИЕ ОСНОВАНИЯ АСИММЕТРИЧНОЙ КРИПТОГРАФИИ

Михаил Савчук
Национальный технический университет Украины "КПИ"

Анотація: **На основі матеріалів публікацій обговорюються математичні ідеї, на яких базується криптографія з відкритим ключем.**
Summary: **Mathematical ideas, on which the public key cryptography is based, are discussed on the grounds of open materials.**
Ключові слова: **Криптографія, криптосистеми з відкритим ключем, автентифікація, цифровий підпис.**

I Введение

После более чем двух тысяч лет развития криптография, благодаря идеям, изложенным Диффи и Хеллманом, а также Ривестом, Шамиром и Адлеманом в их революционных работах [1, 2], соответственно 1976 и 1978 годов, существенно изменила свой облик как с практической стороны, так и в теоретическом отношении. Новая криптография, называемая асимметричной или с открытым ключом, позволила решить такие практические задачи и создать такие криптографические протоколы, которые невозможно было осуществить средствами криптографии с секретными ключами. Две первые практически назревшие с распространением электронных средств обработки и передачи информации проблемы – распространение ключей и цифровая подпись – как раз и решались в работах [1, 2]. С теоретической точки зрения криптография превратилась в математическую дисциплину, которая с одной стороны опирается на фундаментальные математические результаты последних десятилетий (в частности, в теории сложности [3–5]) и сама ставит задачи, решение которых будет означать существенное продвижение в чисто математических областях. С другой стороны современная криптография имеет массу практических приложений в области защиты современных информационных технологий. Бурный рост научных публикаций по криптографии и количество специалистов, ею занимающихся по всему миру, говорит о том, насколько интересна и важна сегодня эта область. В настоящей статье, опираясь на публикации, приведенные, в частности, в списке литературы (прежде всего на работы [6–8]) обсуждаются основные математические идеи, лежащие в основе криптографии с открытым ключом.

II Односторонние функции

Два понятия – односторонней функции и односторонней функции с "потайным ходом", или "лазейкой" – являются центральными для всей криптографии с открытым ключом. Рассмотрим произвольные конечные множества X и Y, а также некоторую функцию $f : X \to Y$. Обозначим через $f[X]$ область значений f. Функция f называется *односторонней,* если ее значение $f(x)$ может быть легко вычислено для каждого аргумента $x \in X$, тогда как почти для всех $y \in f[X]$ нахождение хотя бы одного такого $x \in X$, что $f(x) = y$, является трудновычислимым. В этом неформальном определении нужно уточнить два момента.