Б. И. Скородумов (к. т. н., доцент)
Московский инженерно-физический институт (государственный университет)

О ПОНЯТИЙНО-ТЕРМИНОЛОГИЧЕСКОМ АППАРАТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мир находится на пороге глобальных изменений: новое информационное общество приходит на смену обществу индустриальному, в связи с чем новые информационные технологии все более и более проникают во все области деятельности человека, особенно в промышленность и общественную жизнь, ускоряя процессы глобализации и интеграции мировой экономики и мирового сообщества [8]. Становление информационного общества в России стремительно развивается. Например, в одном из своих докладов 2007 года министр информационных технологий и связи Российской Федерации Л. Д. Рейман обратил внимание аудитории на опережающее развитие российской отрасли ИТ, которая ежегодно прирастает на 30%.

Процесс информатизации общества привел к тому, что компьютерная информация превратилась в основной товар, обладающий значительной ценностью, в своеобразный стратегический ресурс.

Генеральная Ассамблея ООН приняла 27 марта 2006 г. Резолюцию под номером A/RES/60/252, которая провозглашает 17 мая Международным днем информационного общества. В рамках всемирной встречи на высшем уровне по вопросам информационного общества, которая прошла в два этапа: в Женеве в 2003 г. и в Тунисе в 2005 г., была принята «Тунисская программа для развития информационного общества» и Обращение к Генеральной Ассамблее ООН с призывом объявить 17 мая Всемирным днем информационного общества (http://www.cnews.ru).

Генеральный секретарь ООН Кофи Аннан в своем заявлении по поводу провозглашения 17 мая Международным днем информационного общества отметил важность повышения доверия пользователей к ИКТ. Он подчеркнул, что в современном мире, окутанном одной общей Сетью, у общества появилось много угроз, включая предумышленные атаки на важные информационные объекты, что ведет к ослаблению экономики и общества в целом. Для того чтобы повысить доверие к электронной торговле, к электронным банковским системам, к телемедицине, к электронному правительству, необходима общая сплоченность в вопросах информационной безопасности на международном уровне. И поскольку это зависит от политики безопасности каждой страны, бизнеса и каждого гражданина, необходимо *развить культуру инфобезопасности* на международном уровне.

Кофи Аннан призвал все страны — члены ООН и заинтересованные стороны способствовать *росту глобального уровня знаний в сфере информационной безопасности* и развитию международных инициатив и общих мер для *противодействия рискам* в этой сфере.

Наша страна вносит свой вклад в дело решения обозначенных проблем развития культуры инфобезопасности, противодействия рискам в этой сфере и росту глобального уровня знаний в сфере информационной безопасности. Например, четвертая Международная конференция по вопросам обучения информационной безопасности (4th World Conference on Information Security Education) прошла в Москве. Следует добавить, что в нашей стране массово издается специализированная литература по защите информации. Высшая школа регулярно выпускает специалистов по информационной безопасности в соответствии с требованиями семи образовательных стандартов.

Конференция была организована рабочей группой 11.8 IFIP (IT Security Education) совместно с Министерством образования и науки РФ и Московским инженерно-физическим институтом (государственным университетом) с целью ознакомления специалистов с передовым международным опытом подготовки кадров по информационной безопасности, осуществляемой в учебных заведениях. В конференции приняли участие 70 специалистов, представляющих 12 государств, среди которых: Австралия, Великобритания, Германия, Россия, США, Швеция, ЮАР. 39 докладчиков ознакомили присутствующих

с новыми разработками, методиками обучения и учебными программами в области информационной безопасности. В программе конференции были рассмотрены основные проблемы: международные стандарты в области обучения информационной безопасности, обучения расследованию компьютерных преступлений и т. д. Общение на конференции проходило в атмосфере взаимопонимания коллег, несмотря на то, что доклады делались на различных языках. На подобных отечественных мероприятиях часто бывают случаи разногласий по, казалось бы, давно решенным вопросам. Анализ противоречий позволяет сделать вывод о том, что одной из наиболее значимых проблем являются вопросы терминологии.

Отсутствие устоявшейся терминологической базы по проблемам информационной безопасности является одной из актуальных проблем, что влечет за собой неразбериху в учебном процессе по защите информации. Первопричиной такой ситуации является отсутствие в стране юридически значимого базового определения информационной безопасности. В российских законах нет подобной дефиниции. Государственные организации практически не выполнили плановые задания правительства по выпуску технических регламентов по защите информации, в которых должны были быть раскрыты вопросы понятийно-терминологического аппарата информационной безопасности.

Доктрина информационной безопасности Российской Федерации определяет главные термины и понятия защиты государственной информации [2]. В частности, под информационной безопасностью Российской Федерации в доктрине понимается: «Состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства». Данное определение, сформулированное для госсектора, получило широкое распространение (в том числе в учебной литературе) применительно к другим сферам деятельности без учета их особенностей, что противоречит положениям доктрины. Большинство авторов учебной литературы берут за основу положения, разработанные в прошлом веке только для защиты государственной тайны, забывая, что страна перешла на специфические рыночные отношения, о чем свидетельствует появление законов «О техническом регулировании», «О коммерческой тайне» и «О персональных данных».

В Доктрине отмечено, что: «В каждой сфере жизнедеятельности общества и государства наряду с общими методами обеспечения информационной безопасности Российской Федерации могут использоваться частные методы и формы, обусловленные спецификой факторов, влияющих на состояние информационной безопасности».

Общеизвестно, что главные цели и задачи функционирования любого бизнеса обычно не совпадают с государственной идеологией. Об этом же свидетельствуют и материалы российско-американского семинара, секции «Кибернетический терроризм» [7]. Из выступления руководителя американской делегации Уильяма А. Вульфа, Президента Национальной инженерной академии США, следует, что *«свое понятие безопасности должно быть выработано для каждой существующей реалии...»*.

Решая задачи обеспечения информационной безопасности бизнеса, необходимо помнить, что главной целью любого предпринимателя является прибыль, для получения которой он должен снижать издержки производства и реализации продукта. Весь бизнес-процесс сопровождается расчетами, построенными на базе измерений и учета. Слабым местом всего процесса расчетов является почти полное отсутствие количественных метрик информационной безопасности. «Настоящая наука начинается там, где начинаются измерения», говорил Дмитрий Иванович Менделеев. Решению обозначенной проблемы способствует Закон «О техническом регулировании» [1].

В статье 2 закона «О техническом регулировании» вводятся новые понятия, главные и характерные для любого бизнеса. Например, «риск — вероятность причинения вреда...» и «безопасность — состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда...». Применяя данные определения для термина «информационная безопасность» можно получить следующую, ориентированную на бизнес, дефиницию: «информационная безопасность — состояние информации при допустимом риске ее уничтожения, изменения или раскрытия, связанном с причинением вреда владельцу или пользователю информации» [9, 10].

Достоинства нового определения:

• Гармонизация положений новых стандартов (ГОСТ Р ИСО/МЭК 15408-1-2002, 27001, 17799) и прежнего научно-технического задела.

• Получение через риск количественных метрик информационной безопасности.

Это хорошо подкрепляется десятилетней практикой применения обобщенного критерия защищенности информации, используемого в методике французской банковской комиссии, построенной на базе управления рисками.

Следует отметить, что в отечественных нормативно-методических документах по информационной безопасности до 2002 года отсутствовало понятие риск, которое впервые появилось в стандарте ГОСТ Р ИСО/МЭК 15408-1-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». В настоящее время количество стандартов с этой дефиницией резко возросло. Стандарты [3—6], приведенные в библиографическом списке, являются основными по направлению рискориентированная информационная безопасность. По данной проблеме наиболее значимый интерес представляет работа: Петренко С. А. «Управление информационными рисками. Экономически оправданная безопасность» [11].

Квинтэссенцией рискориентированного подхода к обеспечению информационной безопасности кредитных организаций стал комплекс документов на базе стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2006. Целесообразно отметить, что пока в комплексе документов на базе данного стандарте используются только качественные метрики риска.

Заключение

1. Необходимо использовать дифференцированный подход в учебном процессе к определению информационной безопасности, в зависимости от формы собственности АС и обрабатываемой информации.

2. Получение количественных метрик информационной безопасности, например, через риск — актуальная задача бизнеса, которую следует учитывать в учебных программах.

3. Наступило время создания отечественных учебных курсов, учитывающих специфику обеспечения информационной безопасности коммерческих АС с учетом информационных рисков.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон от 27.12.2002 № 184-ФЗ (в ред. от 1 декабря 2007 г.) «О техническом регулировании».
2. Доктрина информационной безопасности Российской Федерации (9 сентября 2000 г.).
3. ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы безопасности. Система управления безопасностью информации. Требования».
4. ГОСТ Р ИСО/МЭК 17799 «Информационная технология. Методы безопасности. Руководство по управлению безопасностью информации».
5. ГОСТ Р ИСО/МЭК 15408-1-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
6. ГОСТ Р 51897-2002 Государственный стандарт Российской федерации. Менеджмент риска. Термины и определения.
7. *Уильям А. Вульф (Президент Национальной инженерной академии США)*. Взгляд на исследования в области кибернетической безопасности в Соединенных Штатах // Терроризм. Снижения уровня уязвимости и повышение эффективности ответных мер. Материалы российско-американского семинара. М., 2003.
8. *Кастельс М.* Информационная эпоха: экономика, общество и культура / Пер. с англ. под научн. ред. О. И. Шкаратана. М., 2000.
9. *Круглов А. А., Скородумов Б. И.* Информационная безопасность: от угроз к рискам // Материалы VII Международной научно-практической конференции «Техническое регулирование информационной безопасности». Таганрог, 2005.
10. *Круглов А. А., Скородумов Б. И.* Об информационной безопасности // Вестник Российского нового университета. 2007. № 2.
11. *Петренко С. А., Симонов С. В.* Управление информационными рисками. Экономически оправданная безопасность. М., 2004.