с задачами поддержания международного мира, безопасности и стабильности.

В качестве основных угроз в области обеспечения международной информационной и коммуникационной безопасности в российско-бразильском Соглашении названы следующие:

использование информационных и коммуникационных средств и технологий в международных конфликтах во враждебных целях как в гражданской, так и в военной сферах, включая выведение из строя критически важных инфраструктур;

использование информационных и коммуникационных средств и технологий для осуществления террористической деятельности и в террористических целях;

использование информационных и коммуникационных средств и технологий для осуществления преступной деятельности и в преступных целях;

использование доминирующего положения в сфере информационных и коммуникационных средств и технологий в ущерб интересам и безопасности других государств;

стихийные бедствия и технологические аварии, влияющие на безопасное и стабильное функционирование глобальных и национальных информационных и коммуникационных инфраструктур.

Как видно из сравнения приведенных выше двух определений понятий и двух перечней угроз, в данной трактовке само понятие «информационная и коммуникационная безопасность» и относящийся к нему перечень угроз уже. При этом они не охватывают становящиеся все более актуальными в настоящее время угрозы, затрагивающие различные чувствительные сферы жизнедеятельности общества, в частности, угрозы связанные с возможным деструктивным использованием интернет-технологий в целях осуществления негативных форм социального взаимодействия, представляющих общественную опасность.

В то же время следует отметить, что упомянутое выше понятие «информационная и коммуникационная безопасность» шире предложенного Комиссией Евросоюза (2001 г.) англоязычного понятия «сетевая и информационная безопасность» (Network and Information Security), которое определено как «способность сети или информационной системы противостоять при заданном уровне надежности случайным угрозам или умышленным вредоносным действиям, которые подвергают риску доступность, подлинность, целостность и конфиденциальность хранимых или передаваемых данных и связанных с ними служб, доступ к которым осуществляется с помощью таких сетей или систем».

В свете вышесказанного проработка вопросов понятийного аппарата и содержательного наполнения терминологического глоссария для сферы информационной безопасности представляется все более актуальной.

УДК 34.03:004.056.5

М.В. Губич, Д.С. Якжик

ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Информация является одним из основных объектов деятельности органов внутренних дел (далее – ОВД) и с каждым годом приобретает все большую ценность. Информация в ОВД существует в различных формах: на бумаге, в электронном виде, пересылается по почте или посредством электронных средств связи, визуализируется при помощи средств мультимедиа или циркулирует в виде звуковых волн. Вне зависимости от формы представления, средств распространения либо хранения информация ОВД должна всегда быть защищена должным образом.

В соответствии с указом Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» информационная безопасность (далее – ИБ) является составной частью национальной безопасности, следовательно, ИБ ОВД также является элементом национальной безопасности. При этом следует отметить, что практически вся информация ОВД относится к информационным ресурсам, подлежащим защите, среди которых можно выделить сведения, составляющие государственные секреты; информацию ограниченного распространения; персональные данные; банковскую тайну; коммерческую тайну, тайну переписки и иные охраняемые законом категории сведений. При этом и несекретная служебная информация в силу специфики деятельности ОВД также является охраняемым информационным ресурсом.

В настоящее время в Республике Беларусь обеспечение безопасности вышеуказанных видов информации регламентируется многочисленными республиканскими и ведомственными нормативными правовыми актами, что негативно сказывается на практической реализации мероприятий по обеспечению ИБ. Так, только в сфере защиты государственных секретов принято более 80 республиканских нормативных правовых актов.

По нашему мнению, с учетом того, что для достижения ИБ необходимо проведение согласованных мероприятий в различных сферах деятельности ОВД, следует принять единый нормативный правовой акт, устанавливающий требования к обеспечению ИБ, дифференцированные в зависимости от категории информационных ресурсов, подлежащих защите.

Опыт унифицированной регламентации мероприятий по обеспечению ИБ сложился в США и странах Западной Европы. Так, вопросы обеспечения ИБ на протяжении последних трех десятилетий являются объектом регулирования многих международных и национальных нормативных правовых актов зарубежных государств.

С 1983 по 1988 гг. Министерство обороны США и Национальный комитет компьютерной безопасности разработали систему стандартов в области компьютерной безопасности, которая включает более десяти документов. Этот список возглавляют «Критерии оценки безопасности компьютерных систем» (по цвету обложки чаще называют «Оранжевой книгой» США). В соответствии с системой стандартов США надежность компьютерных систем оценивается по двум основным критериям: политика безопасности и гарантированность.

Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. Чем надежнее система, тем строже и многообразнее должна быть политика безопасности.

Гарантированность – мера доверия, которая может быть оказана архитектуре и реализации системы. Гарантированность можно определить тестированием системы в целом и ее компонентов. Гарантированность показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности.

Необходимо указать, что «Критерии оценки безопасности компьютерных систем» открыли путь к ранжированию информационных систем по степени надежности. В «Оранжевой книге» определяются четыре уровня надежности (безопасности) – D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к надежности систем предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием надежности. Таким образом, всего имеется шесть классов безопасности – C1, C2, B1, B2, B3, A1. Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее политика безопасности и гарантированность должны удовлетворять соответствующим требованиям.

Итогом работы британских специалистов в сфере ИБ стал стандарт BS 7799 Part 1 // Code of Practice for Information Security Management (Практические правила управления информационной безопасностью). Данный документ описывает механизмы контроля, необходимые для построения системы управления информационной безопасностью (СУИБ) организации, определенные на основе лучших примеров мирового опыта в данной области.

В 2000 г. BS 7799 Part 1 утвержден в качестве международного стандарта ISO/IEC 17799:2000 (BS 7799-1:2000), на основе которого в настоящее время разрабатываются национальные стандарты в области ИБ. Так, например, приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 447-ст утвержден Национальный стандарт Российской Федерации «Информационная технология. Практические правила управления информационной безопасностью» ГОСТ Р ИСО/МЭК 17799-2005, который полностью идентичен международному стандарту ИСО/МЭК 17799:2000.

Стандарт не является техническим документом, а определяет общую организацию, классификацию данных, системы доступа, направления планирования, ответственность сотрудников, использование оценки риска в контексте информационной безопасности.

Этот стандарт является инструментом, позволяющим управлять конфиденциальностью, целостностью и сохранностью важной информации, и может с одинаковым успехом применяться как индивидуальными предпринимателями, так и предприятиями с численностью сотрудников в десятки тысяч человек.

Таким образом, по нашему мнению, необходимо, опираясь на мировой опыт в сфере ИБ, разработать нормативный правовой акт, определяющий мероприятия по обеспечению ИБ ОВД, дифференцированные в зависимости от категории информационных ресурсов ОВД, подлежащих защите.

УДК 681.324.067

В.В. Иванов

О ПУТЯХ СОВЕРШЕНСТВОВАНИЯ ОРГАНИЗАЦИОННО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Проблема обеспечения информационной безопасности является в настоящее время одной из самых острых в развитых странах мира. Опыт эксплуатации информационных систем и ресурсов в различных сферах жизнедеятельности показывает, что существуют различные и весьма реальные угрозы потери информации, приводящие к материальным и иным ущербам. Развитие информационных технологий создает качественно новые угрозы, способные приводить порой к катастрофическим по своим масштабам последствиям. Но противостоять этим угрозам можно и нужно, объединив усилия всех заинтересованных сторон.

Организационно-правовое обеспечение информационной безопасности представляет собой совокупность нормативных правовых актов и других документов, регламентирующих общую организацию работ по обеспечению информационной безопасности, требований, нормативов, руководств и практических действий по созданию и обеспечению функционирования систем защиты информации на конкретных объектах.

Разработка и совершенствование законодательной базы информационной безопасности является необходимой мерой, удовлетворяющей первейшую потребность в защите информации при развитии социально-экономических, политических, военных направлений деятельности каждого государства.