УДК 004.056

В. В. Смелов, канд. техн. наук

МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Modern information system is an element global information space, in which she interacts with the other system. The most important state problems costing is a building of the system of the rules of the interaction of the information systems in common information space. The complex of rules and systems providing central to information safety infrastructure is identified in country to national information safety. The article is dedicated to analysis of the infrastructure to national information safety of the Republic Belarus. It is considered legislative and normative base to information safety, principles of management, government regulation and licensing, administrative and criminal responsibility in sphere of protection to information. They are analyzed main standards to information safety of the Republic Belarus and is fixed their relationship with international standard. Infrastructure to national information safety formulates new requirements for information systems and requires new methodology of the building of the modern information systems.

Введение. Глубина и размах технологических и социальных последствий компьютеризации и информатизации различных сфер общественной жизни дали основание говорить об информационной революции. Западная общественно-политическая мысль выдвинула концепцию «информационного общества», основное назначение которой является объяснение явлений, порожденных этим этапом научно-технического прогресса. В условиях информационного общества ***практически любая автоматизированная система (АС) становится элементом глобального информационного пространства***.

Отражением этих общих тенденций является действующая с 2003 г. в Республике Беларусь государственная программа поэтапного перехода к информационному обществу «Электронная Беларусь», которая предполагает создание в нашей стране единой инфраструктуры с широким использованием информационных технологий в государственном управлении, народном хозяйстве, образовании, медицине, торговле и других сторонах жизни общества. В настоящий момент программа состоит из девяти направлений и включает порядка 100 проектов.

Обратной стороной информатизации общества является проблема защиты информации. Утечка, искажение или разрушение информации может негативно отразиться на деятельности государственных органов управления, предприятий и организаций, нарушить права физических лиц и т. п. В условиях информационного общества одной из основных задач, стоящих перед государством, является построение инфраструктуры национальной информационной безопасности.

Инфраструктура национальной информационной безопасности. Инфраструктура национальной информационной безопасности (ИНИБ) представляет собой комплекс взаимосвязанных обслуживающих систем различной природы (организационных, правовых, информационных и т. п.), обеспечивающих основу для решения задачи информационной безопасности (ИБ) в масштабах страны. ИНИБ является составной частью общей системы национальной безопасности государства. На рисунке представлена обобщенная схема ИНИБ, исторически сложившаяся в большинстве развитых стран. Здесь изображены основные элементы ИНИБ (замкнутые фигуры различной геометрии) и подписанные стрелки, указывающие тип взаимоотношений между парами элементов.

Основой любой ИНИБ является законодательная и нормативно-правовая база обеспечения информационной безопасности (ЗБИБ), выражающая государственную политику в этой сфере. Государство исходит из того, что информационные ресурсы являются объектами собственности, участвующими в хозяйственном обороте. Законы и правовые акты ЗБИБ наделяют определенные органы государственной власти полномочиями осуществлять государственное регулирование, контроль (мониторинг) и управление в сфере информационной защиты, а также определяют взаимоотношение субъектов информационной деятельности. Технические нормативные акты представляют собой стандарты и технические регламенты, которые могут (или обязаны) использовать субъекты информационной деятельности. Ответственность субъектов информационной деятельности за нарушение законов в сфере информационной безопасности определяется Уголовным и Административным кодексами.

Условно субъекты в сфере информационной безопасности можно разбить на три группы: государственные учреждения, осуществляющие государственное регулирование в этой сфере (группа Г); разработчики технических средст защиты информации (группа Р) и пользователи (группа П). Очевидно, что все эти группы пересекаются.

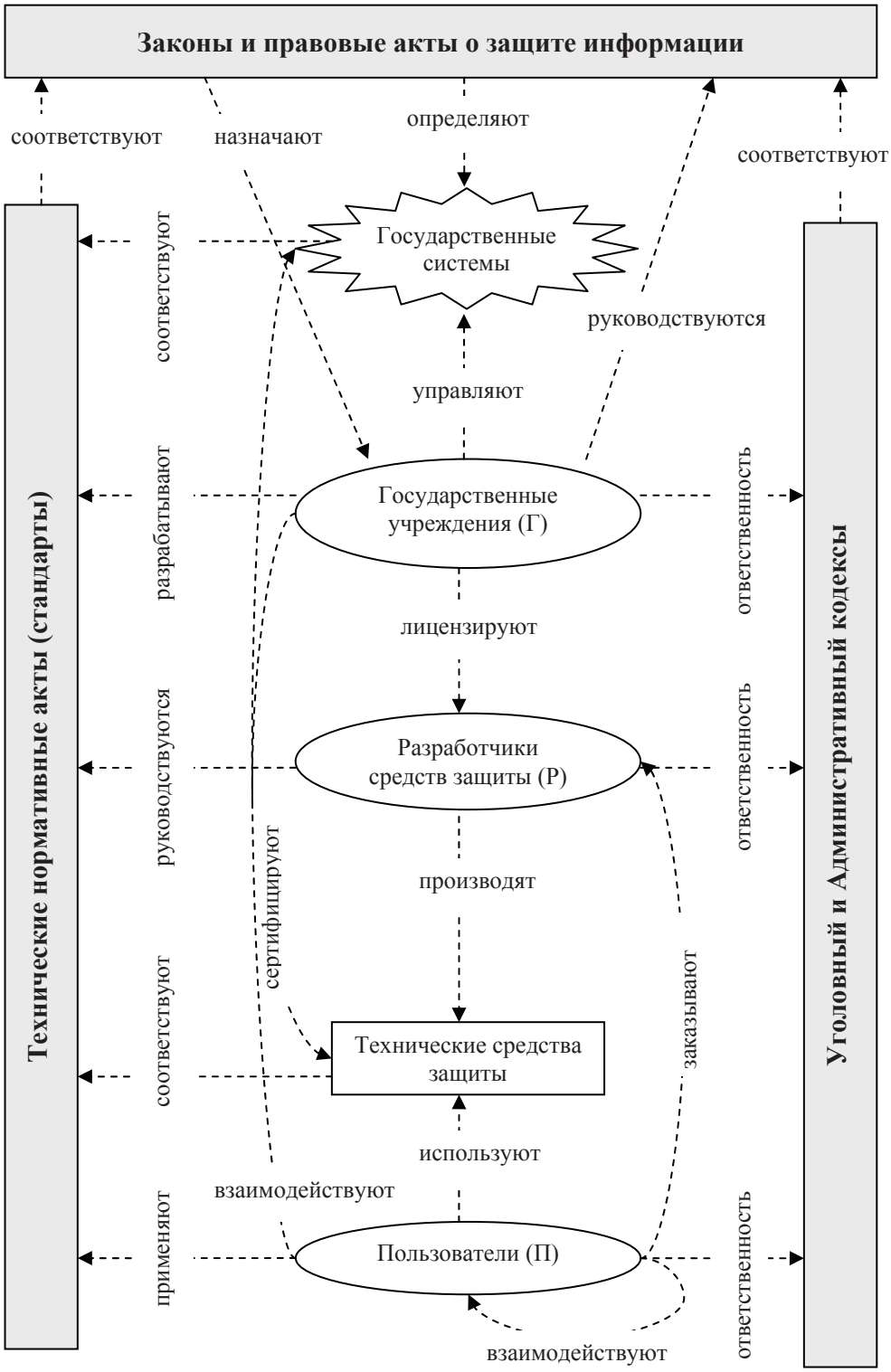

Рисунок. Инфраструктура информационной безопасности

Полномочия и деятельность субъектов группы Г определены законом или специальными положениями. Группа Г координирует и лицензирует всю деятельность по технической защите информации, разрабатывает (или участвует в подготовке) нормативные правовые акты, осуществляет экспертизу (сертификацию) технических средств информационной безопасности. Кроме того, субъекты этой группы управляют государственными информационными системами, связанными с информационной безопасностью (например, удостоверяющие и регистрационные центры).

Основной деятельностью субъектов группы Р является разработка технических средств защиты информации. Свою деятельность они осуществляют на основе лицензии, а все созданные ими средства защиты должны пройти сертификацию, прежде чем они будут применяться пользователями. Сертификация – это

процедура подтверждения соответствия продукции определенным техническим нормативным документам (стандартам).

Пользователи информационных систем (группа П) представляют самую многочисленную группу субъектов в сфере информационной безопасности. Субъекты этой группы применяют средства технической защиты информации для защиты собственных информационных ресурсов и взаимодействуют с системами защиты других субъектов. В своей деятельности они могут использовать государственные автоматизированные системы, обеспечивающие сервисные услуги в области технической защиты информации.

Исторически первой ИНИБ сложилась в США. Первый закон о защите информации датируется 1906 г., а на сегодняшний день ЗБИБ США насчитывает их более 500 [3].

Появление глобальных информационных систем привело к необходимости выработки единого подхода к проблемам информационной безопасности на международном уровне. Первым важным шагом, сделанным в этом направлении, стала разработка международных стандартов по информационной безопасности.

По понятным причинам за основу для международных стандартов по информационной безопасности были взяты стандарты, разработанные стандартизирующими организациями ведущих индустриальных стран (прежде всего США и Великобритании). Нормативная документация национальной ЗБИБ, как правило, является гармонизированными международными стандартами.

Международные стандарты по информационной безопасности. Основой для большинства международных стандартов информационной безопасности (таблица) служат нормативные документы, разработанные национальными стандартизирующими организациями ведущих индустриальных стран, профессиональными техническими организациями, международными консорциумами или ведущими в области информационных технологий компаниями.

Исторически первым (1983 г.) стандартом, сформулировавшим критерии безопасности и получившим широкое распространение, стал стандарт Министерства обороны и Национального комитета компьютерной безопасности США «Критерии оценки доверенных компьютерных систем» (Trusted Computer System Evaluation, TCSEC), чаще всего называемый по цвету обложки «Оранжевой книгой». Стандарт определяет четыре «уровня доверия» к компьютерным системам: D, C, B, A (перечислены в порядке усиления требований). Уровни C и B подразделяются на классы: C1, C2 и B1, B2, B3. Европейской переработкой этого стандарта является документ «Гармонизированные критерии европейских стран» (Information Technology Security Evaluation Criteria, ITSEC), опубликованный в 1991 г. от имени соответствующих органов четырех стран: Франции, Германии, Нидерландов и Великобритании.

Таблица

Основные международные стандарты информационной безопасности

Группы стандартов	ISO/IEC	СТБ
Терминология, общие понятия	2383-8; 10164-7; 10164-8; 10181-1; 10181-2; 10181-3; 10181-4; 10181-5; 10181-6; 10181-7; 10745; 24767-1; 15443-1; 15443-2; 15443-3; 9798-1; 15292; 15816; 18014-1; 18014-2; 18014-3	34.101.27; 34.101.30
Требования безопасности, критерии и методологии оценки, методики испытаний	15408-1; 15408-2; 15408-3; 19791; 15446; 18045; 19790; 18045; 24759; 15446	34.101.1; 34.101.2; 34.101.3; 34.101.8; 34.101.9; 34.101.10; 34.101.12; 34.101.13; 34.101.15
Методы и алгоритмы шифрования, цифровая подпись	9797-1; 9797-2; 10116; 10118-1; 10118-2; 10118-3; 10118-4; 13888-2; 13888-3; 15946-1; 18031; 18032; 18033-1; 18033-2; 18033-3; 18033-4; 9796-2; 9796-3; 9798-2; 9798-3; 9798-4; 9798-5; 14888-1; 14888-2; 14888-3; 15945; 9594-8	П 34.101.27; П 34.101.27.31; П ISO/IEC 10118-3; П ISO/IEC 18033-1; П ISO/IEC 18033-3; 34.101.24; 34.101.25; 34.101.26; 34.101.31; 1176-1; 1176-2; ГОСТ 28147-89
Управление ключами	11770-1; 11770-2; 11770-3; 11770-4	
Защита сетевых технологий	18028-1; 18028-2; 18028-3; 18028-4; 18028-5	
Организация информационной безопасности, управление безопасностью, рисками и защитой информации	13335-1; 27001; 27002; 27005; 27006; 18043; 18044; 21827; 24762; 14516; 15447	П ISO/IEC 27001
Специализированные стандарты	9579(SQL); 14762; 29341-13-10; 29341-13-11(UPnP); 15067-4(HES)	

Часто в литературе упоминается федеральный стандарт США FIPS 140-2 «Требования для безопасности криптографических модулей» (Security requirements for cryptographic modules), который был опубликован в 2001 г. и заменил действовавший с 1994 г. аналогичный стандарт FIPS 140-1.

Для оценки уровня безопасности стандарт использует специальную модель – криптографический модуль, представляющий собой набор программных и (или) аппаратных средств, заключенных в пределах явно определенного и непрерывного периметра.

Наиболее известным международным проектом в области оценки безопасности, результаты которого послужили основой международного стандарта ISO/IEC 15408, является проект «Общие критерии оценки безопасности информационных технологий» (Common Criteria IT Security Evaluation, CC), более известный под коротким наименованием «Общие критерии» [2]. Проект стартовал в 1993 г. по инициативе правительственных организаций шести стран: Канады, США, Великобритании, Германии, Нидерландов и Франции. Первоисточниками для проекта авторы называют документы, перечисленные выше. Стандарт предусматривает семь уровней безопасности. Все требования к информационной безопасности разбиты на два вида: функциональные и требования доверия. Модель требований представляется в виде иерархии: класс – семейство – компонент – элемент. Требования безопасности оформляются в виде специальных документов «Профиль безопасности» (для семейства информационных систем) или «Задание по безопасности» для конкретной системы.

Международный стандарт ISO/IEC 15408:1999 фактически совпадает с версией 2.1 отчета «Общие критерии».

Стандарты менеджмента, аудита и сертификации информационной безопасности излагаются в международных стандартах ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 и ISO/IEC 27006. Все они являются развитием британского национального стандарта BS 7799. Важным считается то, что эти стандарты совместимы с известными стандартами ISO 9000, ISO 9001 и ISO 14001, регламентирующими менеджмент качества на предприятии.

Большое влияние на стандарты безопасности оказывают рекомендации одной из старейших стандартизирующих организаций в области телекоммуникаций и радио – Международного союза электросвязи (International Telecommunication Union, ITU). Рекомендации X.800 («Архитектура безопасности для взаимодействия открытых систем»), серия X.500 («Служба директориев») лежат в основе стандартов безопасности распределенных систем.

Стандарты безопасности Интернет разрабатываются группой IETF (Internet Engineering Task Force) сообщества Интернет (ISOC). Наиболее применяемыми являются следующие спецификации:

– IKE/IPSec (RFC 2401–2412, 2451) для протокола IP версий 4 и 6;

– TLS (RFC 2246) для протокола транспортного уровня;

– GSS-API (RFC 2744) – обобщенный прикладной интерфейс службы безопасности;

– протокол Kerberos (RFC 1510, 1964) для аутентификации в разнородной распределенной среде.

Международные стандарты представляют собой исчерпывающую основу для построения систем информационной безопасности. Национальные стандартизирующие организации в основном идут по пути гармонизации (адаптации) международных стандартов. Процесс гармонизации определяется руководством ISO/IEC 2 и, как правило, сводится к переводу, изменению шифра и (или) формы.

Инфраструктура национальной информационной безопасности Республики Беларусь. Инфраструктура национальной информационной безопасности Республики Беларусь соответствует схеме, приведенной на рисунке, но имеет собственное наполнение.

Законы и правовые акты о защите информации в Республике Беларусь. ЗБИБ Беларуси основывается на двух законах: «Об информатизации» и «Об электронном документе».

Закон «Об информатизации» был принят 6 сентября 1995 г., а 9 октября 2008 г. Палатой представителей Национального собрания Республики Беларусь был утвержден проект закона Республики Беларусь «Об информации, информатизации и защите информации», внесенный Советом Министров Республики Беларусь и предполагающий отмену закона 1995 г. Закон определяет процедуры управления и регулирования в сфере защиты информации.

Закон «Об электронном документе» был принят 10 января 2000 г., а 10 сентября 2008 г. в Совет Министров Республики Беларусь был представлен проект закона «Об электронном документе и электронной цифровой подписи». Этот закон «устанавливает правовые основы применения электронных документов, определяет основные требования, предъявляемые к электронным документам, а также права, обязанности и ответственность участников правоотношений, возникающих в сфере обращения электронных документов». Кроме того, закон определяет понятие электронной подписи как неотъемлемую часть электронного документа.

Государственное регулирование и управление в сфере защиты информации. Согласно

статье 8 нового закона, «государственное регулирование и управление в сфере информации, информатизации и защиты информации осуществляется Президентом Республики Беларусь, Советом Министров Республики Беларусь, Оперативно-аналитическим центром при Президенте Республики Беларусь, Министерством связи и информатизации Республики Беларусь, Национальной академией наук Беларуси и иными государственными органами в соответствии с компетенцией, определенной настоящим Законом и иными актами законодательства Республики Беларусь».

Статьи 9–14 разграничивают полномочия перечисленных государственных органов управления.

Координация и лицензирование деятельности по защите информации, а также организация и проведение работ по технической защите информации в национальном сегменте (BY) возложена на Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ).

В соответствии с Указом Президента от 28.11.2000 г., № 639 головной научно-исследовательской организацией Республики Беларусь в области защиты информации является Научно-производственное республиканское предприятие «Научно-исследовательский институт технической защиты информации» (НИИ ТЗИ) [1]. Эта организация обеспечивает координацию в области научных, исследовательских, методических и практических работ по технической защите информационных систем в интересах министерств, ведомств и организаций Республики Беларусь.

Государственное научное учреждение «Объединенный институт проблем информатики» Национальной академии наук Беларуси привлекается ОАЦ и НИИ ТЗИ для выполнения работ по разработке проектов нормативных актов в сфере защиты информации, а также исследовательских работ в области методологии и оценки эффективности защиты информации.

Лицензирование в сфере технической защиты информации в Республике Беларусь. Порядок лицензирования и виды лицензируемой деятельности в сфере защиты информации определяется «Положением о лицензировании деятельности по технической защите информации, в том числе криптографическим методам, включая применение электронной подписи», утвержденным постановлением Совета Министров Республики Беларусь от 20.10.2003 г. № 1374.

В соответствии с этим Положением выдачу и учет лицензий на осуществление деятельности по технической защите информации осуществляет ОАЦ. Лицензируемой является практически любая деятельность, связанная с проектированием, разработкой, установкой и оказанием услуг в области технической защиты информации.

Административная ответственность в сфере защиты информации в Республике Беларусь. Административный кодекс Республики Беларусь предусматривает ответственность за следующие правонарушения в сфере защиты информации (глава 22 Административного кодекса Республики Беларусь):

1) самовольное использование сетей электросвязи;

2) несанкционированный доступ к компьютерной информации;

3) нарушение правил защиты информации;

4) незаконная деятельность в области защиты информации.

Уголовная ответственность в сфере защиты информации в Республике Беларусь. Уголовный кодекс Республики Беларусь предусматривает уголовную ответственность за следующие преступления против информационной безопасности (раздел XII Уголовного кодекса Республики Беларусь):

– несанкционированный доступ к компьютерной информации;

– модификация компьютерной информации;

– компьютерный саботаж;

– неправомерное завладение компьютерной информацией;

– изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети;

– разработка, использование либо распространение вредоносных программ;

– нарушение правил эксплуатации компьютерной системы или сети.

Анализ определения и сущности понятия «информационная безопасность» с точки зрения уголовного права рассматривается в [5, 6].

Технические нормативные акты в сфере защиты информации в Республике Беларусь. Основные стандарты в сфере защиты информации являются гармонизированными международными стандартами (таблица), и, судя по всему, эта тенденция будет продолжаться. Исключением является ГОСТ 28147-89 «Система обработки информации. Защита криптографическая. Алгоритм криптографический», успешно применяемый с 1989 г.

Заключение. В Республике Беларусь планомерно ведется работа, направленная на создание условий информатизации общественной жизни [4].

Важнейшим этапом на этом пути является создание инфраструктуры национальной информационной безопасности. В основном сформирована законодательная основа, определены органы управления и регулирования, созданы

механизмы контроля. Ясно, что существующая на сегодняшний день инфраструктура совершенна, но предпосылки для ее развития есть.

Значительным тормозом развития информационных технологий является отсутствие национальных стандартов. Но и здесь в последнее время наметился существенный прогресс. Гармонизация международных стандартов в области защиты информации будет способствовать интеграции Республики Беларусь в мировое информационное пространство.

Построение инфраструктуры национальной информационной безопасности формулирует ряд новых требований для автоматизированных систем и, по сути, создает новую среду для их функционирования. Все это потребует переосмысления методологии построения новых автоматизированных систем и реижиниринга уже работающих.

Литература

1. Официальный сайт Научно-производственного республиканского предприятия «Научно-исследовательский институт технической защиты информации» [Электронный ресурс]. – Режим доступа: http://www.niitzi.by. – Дата доступа: 20.03.2009.

2. Официальный сайт проекта Common Criteria [Электронный ресурс]. – Режим доступа: http://www.commoncriteriaportal.org. – Дата доступа: 20.03.2009.

3. Беззубцев, О. А. ФАПСИ: Законодательное регулирование в области защиты информации / О. А. Беззубцев, А. Н. Ковалев // Технология и средства связи. – 1997. – № 1. – С. 94–96.

4. Макаров, О. С. Концепция правового регулирования электронного документооборота / О. С. Макаров, А. В. Орлов, А. А. Тепляков // Управление защитой информации. – 2008. – Т. 12, № 2. – С. 238–240.

5. Савицкая, Н. А. Объект компьютерных преступлений в УК Беларуси / Н. А. Савицкая // Управление защитой информации. – 2008. – Т. 12, № 3. – С. 362–366.

6. Ахраменка, Н. Ф. Уголовно-правовая и криминологическая характеристика преступлений против информационной безопасности (УК Республики Беларусь) / Н. Ф. Ахраменка // Управление защитой информации. – 2008. – Т. 12, № 1. – С. 104–108.