КОНЦЕПЦИЯ И МОДЕЛЬ ЭФФЕКТИВНОГО УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ КРУПНЫХ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

А. А. Фролов, А. В. Алексеев (Санкт-Петербург)

Подсистема обеспечения информационной безопасности является неотъемлемой частью любой корпоративной информационной системы. Чем больше роль и значимость автоматизированных информационных систем (АИС) в деятельности компании, тем более жёсткие требования должны предъявляться к подсистемам обеспечения их информационной безопасности (ПИБ).

Вместе с тем верхний уровень иерархии в любой АИС всегда занимает человек–оператор АИС, играющий главную роль в обеспечении информационной безопасности (ИБ). Это означает, что в основе организованной системы обеспечения ИБ должна лежать не только нормативно-распорядительная документация (рис. 1), как это часто бывает, но, прежде всего, адекватность в действиях требованиям этой документации главного распорядителя – Администратора информационной безопасности АИС (АБ).

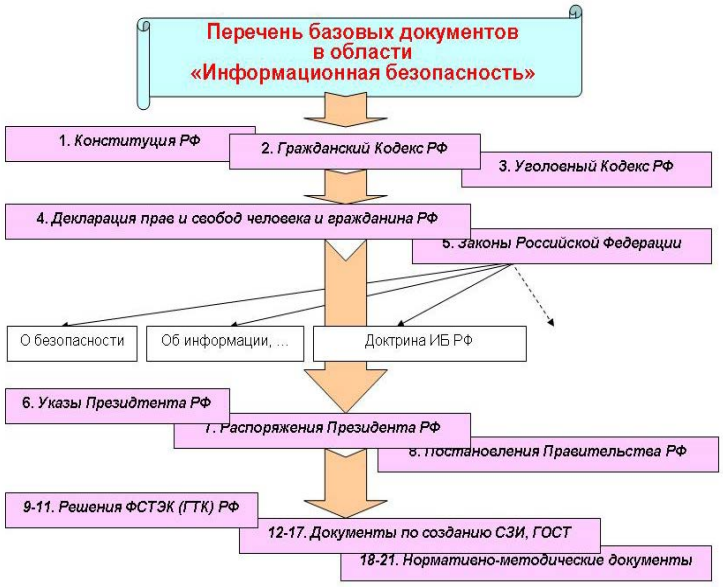

Рис. 1. Базовые документы в области ИБ

Технические средства защиты информации в совокупности с деятельностью персонала, прежде всего АБ АИС, всего лишь реализуют требования обеспечения ИБ, декларируемые в федеральных законах «О безопасности», «О техническом регулировании», «Доктрине информационной безопасности Российской Федерации», международном стандарте «Общие критерии» (ИСО/МЭК 15408-99) и других указах, постановлениях, решениях, ГОСТах, документах по ИБ предприятий и компаний.

Как показывает практика, реализация требований и фактический уровень ИБ компаний и АИС различного ранга определяются отнюдь не дорогостоящими и многофункциональными комплексными системами защиты информации (КСЗИ) АИС, а качеством их функционирования и эксплуатации, зависящим всецело от качества функционирования развёрнутой в компании комплексной системы организационно-нормативного обеспечения ИБ АИС (КСОНО) и её центрального звена – системы анализа и прогнозирования обстановки (сканирования информационных вторжений, мониторинга ИБ АИС) в составе автоматизированной подсистемы управления (АСУ) АИС во главе с её Администратором безопасности АИС (рис. 2).

Именно поэтому в состав используемых общих критериев оценки эффективности функционирования КСЗИ, а тем более критериев оценки эффективности АИС, в которую в качестве структурного элемента входит ПИБ АИС, могут и непременно должны включаться критерии типа:

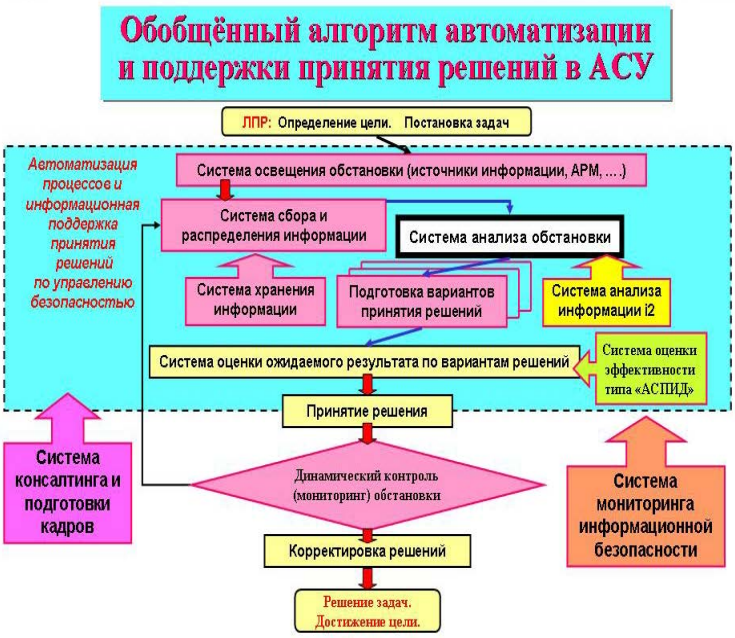

Рис. 2. Обобщённый алгоритм автоматизации управления

- адекватность принятых АБ АИС решений при управлении ИБ по показателю, например, индекса доли правильно принятых решений к их общему числу;
- техническая готовность АИС по показателю, например, индекса доли исправных элементов (подсистем АИС) к их общему числу;
- готовность АИС по показателю, например, индекса доли времени работоспособного состояния АИС к требуемому (заданному) времени готовности;
- информационная готовность АИС по показателю, например, аналогичному для критерия готовности АИС, но с учётом времени нахождения АИС в состоянии отказа по причине устранения «информационных проблем» (ликвидации последствий информационных вторжений различного характера) и т.п.

Автоматизация процесса контроля (мониторинга) подобных событий, как можно полагать, является весьма несложной, а достигаемая при этом «прозрачность» в вопросе обеспечения ИБ АИС вполне соответствует второму из четырёх основных принципов государственной политики (открытость в реализации функций обеспечения ИБ), лежащих в основе «Доктрины информационной безопасности Российской Федерации» (статья 8).

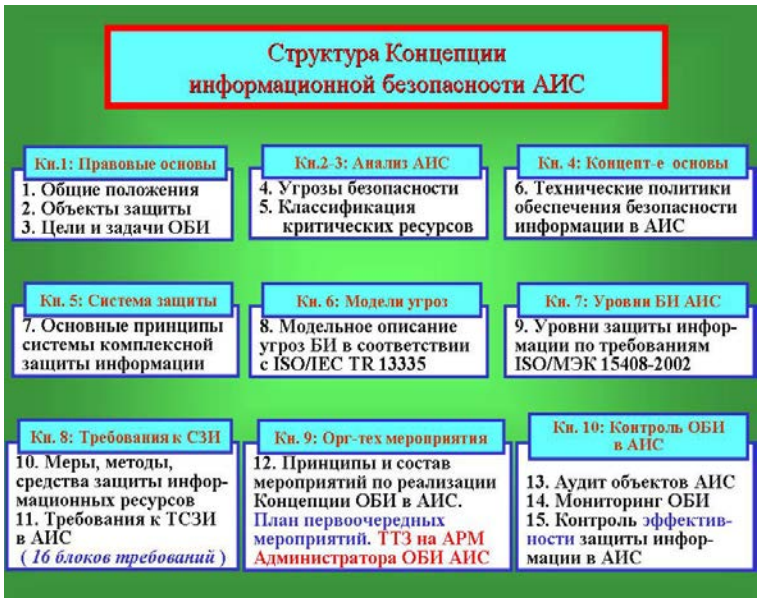

Рис. 3. Вариант структуры концепции ИБ АИС

Данное принципиальное положение, как правило, не встречается в нормативно-распорядительных документах – концепциях (вариант структуры приведён на рис. 3), политиках, положениях, инструкциях АБ и пользователям и даже в регистрационных журналах и отчётах. Можно отметить, что и в обобщённом алгоритме автоматизации и поддержки принятия решений в автоматизированных системах управления (АСУ), как правило (вариант схемы приведён на рис. 2), эта процедура также не находит своего достойного места.

Между тем именно в структурах разрабатываемых и реализуемых концепций ИБ АИС этот важнейший принцип для автоматизированных комплексов и систем может и должен быть закреплён юридически.

Введение данного принципа, соответствующих аспектов и концептуальных положений может иметь место, например, в разделе 12 (см. рис. 3), в том числе в виде дополнительного блока требований к действиям АБ АИС, а также требований к процедурам мониторинга при управлении ИБ АИС и др.

Теория и практика реализации политики обеспечения ИБ в крупных информационных системах, как правило, указывают на необходимость своевременного анализа угроз безопасности компании, формулирования концептуальных положений по её обеспечению. Значительное внимание уделяется правовым аспектам информационной безопасности, лицензированию деятельности в области защиты информации, технологическому обеспечению ИБ. При этом, как следует из анализа тенденций развития ИБ АИС, далеко не в полной мере учитывается пресловутый «человеческий фактор», хотя многие специалисты и отмечают его большую значимость для АИС. Особое значение данный фактор приобретает для крупных (сложных) АИС регионального и федерального масштабов. Именно для них ущерб от реализации данной угрозы информационной безопасности является и наиболее «естественным», и наиболее ощутимым.

Поэтому для эффективного функционирования АИС в защищённом исполнении необходимо обеспечить гармоничное сочетание при реализации следующих принципов:

- известного, но концептуально важного для эффективного управления сложной информационной системой принципа непрерывного анализа (мониторинга) эффективности функционирования АИС в целом (в том числе, например, по приведённым выше несложным в реализации критериям), а также её подсистемы обеспечения ИБ;
- принципа использования «равнопрочных» по устойчивости (надёжности) элементов при их объединении в сложную систему (на этапе концептуального и технического проектирования КСЗИ АИС), а именно – использования в сложной человеко-машинной системе «равнопрочных» по информационной устойчивости элементов (КСЗИ и Администратора ИБ АИС).

Реализация изложенного подхода, как можно полагать, приведёт к развитию технологий и управления информационной безопасностью АИС (в первую очередь, крупномасштабных), сместив акценты в сторону «человеческого фактора», позволит наряду с «информационной прозрачностью» сократить информационную и техническую избыточность. Это, в свою очередь, сделает саму систему управления безопасностью более динамичной и результативной благодаря концентрации соответствующих ресурсов на главных направлениях. В докладе представлены предложения по организации комплексного (аналитико-имитационного) моделирования рассматриваемой АИС.

Литература

1. **Воробьёв В. И., Заболотский В. П., Иванов В. П.** Средства обеспечения безопасности при информационном противоборстве//Информационная безопасность региона: Сб. тез. докл. и сообщ. СПб НПС, 13–16 мая 1997 г. – СПб., 1997. –С. 7–9.
2. **Иржавский А. А., Лебедь С. В.** Организационно-нормативная база системы обеспечения информационной безопасности комплекса информационных систем предприятия//Information Security/Информационная безопасность. – 2004. –№ 6. –С. 28–31.
3. **Сердюк В. В.** Уязвимость информационных сетей, функционирующих на базе стеков протоколов TCP/IP, и методы их защиты//Системы безопасности, связи и коммуникаций.– 2000.– № 33.– С. 77–81.

4. **Ивченко Б. П., Мартыщенко Л. А., Монастырский М. Л.** Теоретические основы информационно-статистического анализа сложных систем. – СПб.: Лань, 1997. – 320 с.
5. **Алексеев А. В.** Информационная устойчивость морских радиоэлектронных систем в условиях широкомасштабной информационной войны//Наука и техника: Вопросы истории и теории. Тез. 18-й конф. СпбО Национал.комитета по истории и философии науки и техники. Вып. XIII.– СПб.: СПбФ ИИЕТ РАН, 1997. – С. 13–14.
6. **Алексеев А. В.** Информационные аспекты качества создания и использования морских информационных систем//Конверсионные технологии гидроакустики. ГА-6. – СПб., –1996.– С. 64.
7. **Алексеев А. В., Кириллов Н. П.** Информационные аспекты качества обеспечения информационной безопасности//Информационная безопасность региона: Сб. тез. докл. и сообщ. СПб НПС, 13–16 мая 1997 г. – СПб, 1997. С. 14–15.