ВЕРБАЛЬНОЕ ОПИСАНИЕ МОДЕЛИ МОНИТОРИНГА И УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ ПОДСИСТЕМОЙ БЕЗОПАСНОСТИ СИСТЕМЫ АНТИТЕРРОРИСТИЧЕСКОЙ И ПРОТИВОКРИМИНАЛЬНОЙ ЗАЩИТЫ ОБЪЕКТОВ

А. В. Алексеев (Санкт-Петербург)

Рост преступности, хищение оружия и боеприпасов, совершение диверсионно-террористических акций на гражданских объектах и объектах государственной власти представляют собой наибольшую угрозу безопасности государства. Наносимый при этом ущерб по числу жертв, моральному воздействию на общество, перебоям в функционировании предприятий и загрязнению окружающей среды в большинстве случаев превосходит ущерб даже от катастроф и аварий техногенного характера.

В этих условиях всё большую актуальность приобретают системные вопросы оптимального построения и интегрирования средств, организации и эффективного использования систем комплексной безопасности (СКБ) объектов.

Особое внимание заслуживают сегодня вопросы повышения качества подсистем управления и, в первую очередь, информационной подсистемы. Именно непрерывное наблюдение за состоянием объекта, полномасштабный контроль и прогнозирование ситуационного развития в интересах принятия своевременных и эффективных управленческих решений по использованию технических комплексов и систем безопасности объектов, снижению их уязвимости при антитеррористической и противокриминальной защите (АТПКЗ) обеспечивает реальную возможность эффективного управления.

Проблема уязвимости ТСБ крупных компаний, в том числе устойчивости их информационных подсистем в составе систем АТПКЗ встаёт уже при первых попытках анализа системных аспектов мониторинга СКБ, поиска конструктивных путей информационного противодействия силам и средствам, которые могут быть применены для снижения эффективности использования СКБ.

Именно стремление установить функциональную связь влияния факторов информационного воздействия на СКБ с их предназначением лежит в основе анализа их информационной устойчивости (ИУ), под которой понимают любую характеристику информационной подсистемы СКБ, использование которой нарушителем может привести к реализации информационной угрозы. Под уязвимостью СКБ понимают комплекс их свойств и характеристик, использование которых может привести к реализации угроз глобального характера (невосстанавливаемый отказ).

Теория и практика реализации политики обеспечения информационной безопасности компаний, ИУ используемых ТСБ указывает, прежде всего, на необходимость: своевременного анализа угроз безопасности компании (мониторинга угроз); формули-

рования концепции и политики её обеспечения при АТПКЗ; согласованных с нею политик обеспечения ИУ ТСБ. При этом значительное внимание должно уделяться правовым аспектам информационной безопасности, лицензированию деятельности в области защиты информации, технологическому обеспечению ИУ ТСБ в условиях АТКПЗ. Для крупных компаний принято считать одним из первостепенных вопросов информационную устойчивость систем телекоммуникаций (СТК), автоматизированных информационных систем (АИС), поставку и освоение современных средств и комплексных систем защиты информации (КСЗИ), подготовку и переподготовку кадров в области обеспечения информационной безопасности.

Проблема ИУ КСБ акционерных обществ при АТПКЗ рассматривается во взаимосвязи с такими традиционными информационными аспектами, как чувствительность к входной информации систем обеспечения и принятия решений, систем мониторинга и управления, меры защищённости СКБ при АТПКЗ.

Структура мер обеспечения устойчивости функционирования ТСБ крупных компаний

Основными вопросами исследования ИУ являются: классификация основных факторов ИУ ТСБ, выявление корреляционных связей между ними и систематизация этих факторов по их значимости и влиянию на результаты деятельности: по информационным признакам; по степени влияния на наиболее значимые функциональные свойства и показатели ТСБ и КСБ; исследование прикладных аспектов анализа ИУ при решение задач в нетиповых (динамических, экстремальных, деградационных) условиях, характерных для АТПКЗ; изыскание устойчивых связей и закономерностей в модельном описании поведения и функционирования КСБ в интересах прогнозирования их поведения с учётом факторов естественного и искусственного происхождения при АТПКЗ.

При этом различают и отображают при мониторинге такие показатели КСБ, как уязвимость, информационная безопасность, устойчивость, защищённость, надёжность, адаптивность. Комплексной характеристикой потенциальных и фактических результатов использования системы мониторинга с учётом степени соответствия этих результатов целям, стоящим перед СКБ при АТПКЗ, является, как известно, понятие «эффективности системы», под которым подразумевается, в общем случае, критерий степени соответствия СКБ своему предназначению (см. рисунок), т.е. СКБ при решении характерных задач АТПКЗ.

При этом должны учитываться следующие факторы, влияющие на функциональную эффективность СКБ:

Структура и показатели оценки функциональной устойчивости СКБ

оперативность функционирования СКБ [время устаревания информации, её точность по месту, время развёртывания (подготовки) сил к действиям, их работное время, параметры движения нарушителя режима (НР) и др.]; достоверность используемой для управления СКБ информации (соотношение потоков ценных и ложных сообщений, избыточность сообщений, ценность сведений о НР, дальность действия средств СКБ и др.); устойчивость функционирования СКБ (надёжность, помехозащищённость, живучесть средств, вероятность доведения сигналов до сил и др.); скрытность функционирования СКБ (скрытность развёртывания и применения средств, сил реагирования, скрытность доведения сигналов управления, результативность отвлекающих и демаскирующих действий и др.); непрерывность функционирования СКБ (непрерывность по времени, пространству, объёму и информативности используемых данных, непрерывность информационного и физического воздействия на НР и др). Все названные факторы и показатели эффективности СКБ как системные показатели качества должны отображаться при АТПКЗ в форме, удобной для восприятия лицами, обеспечивающими (ЛОР) и принимающими (ЛПР) ответственные решения в системе управления.

При отсутствии оперативных действий в подобных системах мониторинга и управления информационной подсистемой системы АТКПЗ объекта особое внимание, естественно, уделяется таким характеристикам СКБ (см. рисунок), как их надёжность и живучесть, информационная устойчивость в условиях информационных разведывательных действий и информационных вторжений, т.е. обеспечению информационной защиты объекта в рамках АТПКЗ.

При ведении оперативных действий подобные системы мониторинга непосредственно используются для управления силами и средствами АТПКЗ.

Отличительными особенностями представленного подхода к построению и применению системы мониторинга и управления информационной подсистемой безопасности системы АТПКЗ в сравнении с традиционными подходами к построению и применению пунктов управления силами и средствами следует считать: комплексное объединение решения главной (управления силами и средствами) и обеспечивающей (управление информационной подсистемой) задач с целью минимизации функциональной нагрузки на операторов пункта управления (ЛОР и ЛПР) благодаря максимальной автоматизации процессов управления СКБ и минимизации тем самым времени их межличностного взаимодействия; комплексное (одновременное) использование информационных потоков в системе АТПКЗ и её отображение на экранах коллективного пользования пункта управления (два–три оператора, одновременно решающих весь комплекс задач для ЛОР и ЛПР) с целью повышения доверия к представляемым данным и их аналитической обработки за счёт эффекта «эмерджентной свёртки» и мажоритарности совместных решений в группе ЛПР и т.п.

При таком системно-техническом решении задачи информационного обеспечения АТПКЗ объектов в процессе мониторинга и управления СКЗ должны дополнительно учитываться следующие факторы: ценность и достоверность добываемой и анализируемой информации; групповая ценность операторов; возможность многокритериального оценивания; анализ и контроль ценности добываемой и используемой информации; оптимальность структур и алгоритмов функционирования сложных критических информационных подсистем СКБ; снижение влияния субъективных факторов на принятие управленческих решений в группе (активизация ресурса межличностного взаимодействия); новые возможности интегрированной системы управления-связи-мониторинга; циркулярность доведения, систематизации и обработки управленческой информации; возможность сложных саморегулирующихся систем управления при принятии групповых управляющих решений.

Подобное нетрадиционное решение построения и использования мониторинга и управления информационной подсистемой безопасности должно, с учётом специфики решения задач по АТПКЗ объектов: сократить время реагирования и адекватного принятия решений в динамичных ситуационных условиях развития обстановки; уменьшить штатный состав пунктов управления АТПКЗ объектов и соответствующие затраты; повысить устойчивость функционирования СКБ благодаря сокращению времени реагирования системы управления на дестабилизирующие факторы технического характера; сократить номенклатуру (специализации) операторов пунктов управления СКБ при АТПКЗ при одновременном повышении требований к их специальной и оперативной подготовке, затрат на их обеспечение.

В докладе на основе приведенной вербальной (концептуальной) модели мониторинга и управления АТПКЗ предлагается состав и структура имитационной системы, с помощью которой предполагается исследовать рассматриваемые системы комплексной безопасности объектов

Литература

1. **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.
2. **Ивченко Б. П., Мартыщенко Л. А., Монастырский М. Л.** Теоретические основы информационно-статистического анализа сложных систем. – СПб.: Лань, 1997. – 320 с.
3. **Алексеев А.В.** Информационные аспекты качества создания и использования морских информационных систем. – СПб. Конверсионные технологии гидроакустики, ГА-6,1996.– С.64.
4. **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.
5. **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.