К.А. Афанасьев

ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ ИНТЕГРИРОВАННЫХ СИСТЕМАХ БЕЗОПАСНОСТИ И ЖИЗНЕОБЕСПЕЧЕНИЯ ОБЪЕКТОВ

В настоящее время существует настоятельная необходимость разработки и совершенствования современных систем безопасности потенциально опасных объектов (ПОО).

Реализация принципа обеспечения интегральной безопасности позволяет обеспечить создание хорошо контролируемых и управляемых многоуровневых иерархических систем безопасности, сочетающих высокую связанность различных подсистем, возможность принятия научно обоснованных оптимальных решений в чрезвычайных ситуациях, оперативное информирование городских спецслужб и вышестоящих организаций об опасных отклонениях в поведении систем и нарушениях их функционирования. Такие возможности достигаются за счет применения современного аппаратного и программного обеспечения, позволяющего реализовать прием и обработку информации, анализ и прогнозирование развития различных экстремальных ситуаций на основе использования новых информационных, коммуникационных и организационных технологий [1].

Однако недостаточная исследованность процессов защиты информации в автоматизированных системах безопасности и жизнеобеспечения (АИСБЖО) ПОО не позволяла создавать высокоэффективные АИСБЖО ряда важнейших объектов.

Автором выполнена работа, в которой проанализированы состояние, проблемы и тенденции защиты информации в АИСБЖО, приведена классификация средств защиты. Рассмотрено содержание и проблемы формирования научно-методической базы защиты информации в автоматизированных системах безопасности и жизнеобеспечения потенциально опасных объектов.

Сформулированы основные положения проблемы обеспечения безопасности информационных систем в АИСБЖО. Приведена структура и общее содержание целей обеспечения информационной безопасности, а также классификация конфиденциальной информации и структуризация средств ее защиты – организационно-правовая, техническая (инженерно-техническая), программно-аппаратная и криптографическая защита с учетом психологических, морально-этических видов защиты и ее концептуальной комплексности.

Сформулированы и проанализированы основные закономерности возникновения и классификации угроз информационной безопасности в АИСБЖО. Построены теоретико-множественные модели установления со-

ответствия и композиции подсистем АИСБЖО. Приведен ряд характерных признаков, особенностей и уязвимостей информационных технологий в АИСБЖО. Приведены виды угроз безопасности информации, условия их проявления и их классификация в АИСБЖО, а также основные пути реализации угроз и факторы, обуславливающие информационные потери и различные виды ущерба.

Определены основные пути и каналы утечки и несанкционированного доступа к информации в АИСБЖО. Построена обобщенная информационная модель канала утечки конфиденциальной информации, представленная множеством элементов физического пути от источника информации к злоумышленнику:

$$\mathrm{E_{oc}} = \{I, C, Z, S, N, R\},$$

где I – множество источников конфиденциальной информации или опасных сигналов; C – множество объектов системы обработки информации; $Z = \{Z_a, Z_n, Z_{от}\}$ – множество механизмов защиты атмосферного, промышленного и организационно–технического типа, препятствующих попаданию конфиденциального сигнала в среду распространения; $S = \{o, a, e, m\}$ – среда распространения сигналов, включающая оптическую, акустическую, электромагнитную и материально–вещественную составляющие; N – источник помех; R – приемник перехвата.

В этой модели конфиденциальная информация I как некоторый знаковый алфавит преобразуется объектами системы обработки информации различной природы (человеческого, человеко-машинного и технического типов) в сигналы и сообщения $\{C_т, C_{от}, C_ч\}$. Эти сигналы и сообщения поступают в систему защиты, где подвергаются определенному ослаблению или блокированию $\{C_т', C_{от}', C_ч'\}$. Далее при распространении в определенной среде S сигналы подвергаются ослаблению, а также воздействию шумов искусственного и естественного происхождения N. В результате на вход приемника перехвата R поступают такие сигналы $\{C_т'', C_{от}'', C_ч''\}$, которые, после обработки в приемнике, на его выходе будут иметь значение $E_{ос,}$ исключающее получение нарушителем содержания передаваемой информации.

В работе показано, что с позиций защиты информации технический канал утечки информации в АИСБЖО должен характеризоваться показателем, учитывающим ее основные свойства и, в первую очередь, количество защищаемой информации, независимо от ее вида и структуры. Таковым может быть показатель, аналогичный пропускной способности канала связи, но характеризующий минимальную пропускную способность этого канала:

$$C_{\min} = v_{\mathrm{x}} \min \{I(E_{\mathrm{oc}}, \Delta)\},$$

где v_x – скорость передачи опасного сигнала $E_{ос}$, зависящая от свойств

канала, в том числе средств защиты информации, среды распространения, приемника перехвата источника сигнала, характеризующегося средней продолжительностью символов передаваемого сигнала, $v_x=1/t_x$; Δ – значение принятого сигнала на выходе приемника перехвата; $I(E_{ос}, \Delta)=H(E_{ос}) - H(E_{ос}|\Delta)$ – количество информации, передаваемое по техническому каналу утечки информации (средняя взаимная информация между передаваемым $E_{ос}$ и принимаемым Δ сигналами), не зависящее от вида применяемого источника сигнала; $H(E_{ос})$ – энтропия источника опасного сигнала, характеризующая среднюю неопределенность передаваемого сигнала до приема; $H(E_{ос}|\Delta)$ – средняя условная энтропия ансамбля источника опасных сигналов при известных принятых сигналах Δ, характеризующая остаточную среднюю неопределенность передаваемых сигналов при известных принимаемых.

Тогда условием максимальной (абсолютной) защищенности информации в рассматриваемом канале будет равенство $H(E_{ос}|\Delta) = H(E_{ос})$, при котором $I(E_{ос},\Delta) = 0$. В случае $H(E_{ос}|\Delta) = 0$ незаконный пользователь (технический работник, нарушитель, противник) получает полную информацию об $E_{ос}$, т.е. $I(E_{ос},\Delta) = H(E_{ос})$, в таком случае защита отсутствует.

В работе приведена классификация каналов утечки информации в АИ СБЖО.

Литература

1. Топольский Н.Г. Концепция создания интегрированных систем безопасности и жизнеобеспечения // Матер. 3-й НТК "Информатизация систем безопасности – ИСБ-1994". -М.: ВИПТШ МВД России, 1994.