УДК004.89

В.Г. Шерстюк, Н.А. Козуб

СЦЕНАРНО-ПРЕЦЕДЕНТНОЕ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОГО ОБЪЕКТА

Введение. Системы безопасности и охраны важных объектов военного, энергетического и промышленного назначения создаются с целью предупреждения широкого спектра угроз, начиная от банальных краж имущества и вплоть до террористических актов [1].

Значительную проблему составляет построение системы безопасности территориально распределенного объекта (ТРО), имеющего рассредоточенные на значительные расстояния площадки, конструкции и строения, содержащие разнородное защищаемое имущество. Отличительной особенностью ТРО является протяженный трудно контролируемый периметр, усложняющий использование эффективных инженерных и технических средств, поскольку при значительных контролируемых расстояниях стоимость системы безопасности может превысить стоимость самого объекта. Кроме того, протяженный периметр исключает возможность защиты объекта патрулированием и стационарными постами охраны из-за значительных расходов на содержание подразделений службы охраны.

На сегодняшний день эффективное обеспечение безопасности ТРО предусматривает организацию интегрированных систем, обеспечивающих физическую, объектовую и территориальную безопасность с целью выявления и предупреждения угроз на ранней стадии формирования [2]. Как правило, такие интегрированные системы включают специальные инженерные и технические средства, а также используют дежурные силы стационарной и подвижной охраны [3, 4].

Современные инженерные и технические средства, эффективно решая задачи наблюдения, обнаружения, мониторинга, идентификации угроз, являются, тем не менее, лишь составной частью сложных полиэргатических охранных комплексов, в которые обычно входят также стационарные посты, подвижные патрули, группы реагирования, центры управления и т.д. [5, 6].

Для обеспечения гарантированного уровня безопасности ТРО требуются модели и методы оптимального управления безопасностью [7, 8], позволяющие минимизировать расходы на создание и содержание необходимых сил охраны при обеспечении максимального уровня безопасности объекта.

Таким образом, разработка научно обоснованных моделей управления безопасностью территориально распределенных объектов представляет собой *актуальную* научную проблему, рассмотрение одного из способов решения которой является *задачей* данной работы.

Целью работы является выработка и обоснование подходов к построению систем управления безопасностью (СУБ) территориально распределенных объектов.

Организация системы управления безопасности объекта

На рис. 1 представлена упрощенная схема обеспечения безопасности ТРО.

Конфигурация периметра ТРО диктуется как непосредственным расположением охраняемых объектов $\{O_1...O_6\}$, так и производственными, топографическими, климатическими и иными обстоятельствами.

В систему обеспечения безопасности входят зона охраны внешнего периметра и зона охраны внутреннего периметра, каждая из которых имеет свою область ответственности. Реальные ТРО могут иметь значительно более эшелонированную систему защиты, в том числе с трехмерным построением областей безопасности (например, для защиты ТРО от угроз из воздушного пространства).

В систему обеспечения безопасности включены технические средства охраны внешнего $\{C_1...C_6\}$ и внутреннего $\{E_1...E_4\}$ периметра, наряд дежурных сил в составе стационарных постов охраны $\{B_1...B_4\}$ (в районах подъездных путей и проходов), мобильных патрулей охраны внутреннего $\{D_1...D_3\}$ и внешнего $\{A_1...A_7\}$ периметра ТРО, мобильных групп быстрого реагирования $\{F_1, F_2\}$. Элементы множества дежурных сил будем называть далее субъектами обеспечения безопасности (СОБ).

В реальных ТРО могут использоваться оборудование и технические средства различных классов и типов, кроме того, для управления охраной создаются центры мониторинга, управления и связи.

Широкий спектр различных угроз ТРО разбивается на определенные классы. Решение задачи обеспечения безопасности предполагает составление одного или нескольких планов действий для штатных ситуаций и планов реагирования на нештатные ситуации (возникновение внешних угроз) соответственно идентифицированному классу угрозы.

В общем случае возникновение и идентификация определенной угрозы безопасности ТРО приводит

в действие один из планов противодействия ей, в котором задействуется некоторая часть СОБ из дежурного наряда сил охраны (остальные СОБ продолжают нести охрану в штатном режиме).

Выполнение плана противодействия угрозе предполагает постановку конкретных задач каждому из участников и координацию их совместных действий по выполнению плана. При исчезновении угрозы СУБ переходит в штатный режим.

Исходя из анализа представленной обобщенной схемы организации безопасности, для современных СУБ характерно:

- целенаправленное планирование мероприятий по устранению угроз безопасности, что позволяет в большинстве случаев свести задачу обеспечения безопасности к задаче планирования и выполнения планов [9];

Рис. 1. Система обеспечения безопасности ТРО

- действия злоумышленников, как правило, являются целеустремленными, и зачастую представляют собой хорошо спланированную многоходовую атаку на СУБ ТРО (в т.ч. разнесенную по времени и в пространстве), что требует своевременной идентификации целей злоумышленников и планируемых способов их достижения;
- сообразно ходу процесса противодействия угрозе, цели плана мероприятий СУБ могут динамически изменяться (корректироваться), т.е. выполнение планов в СУБ должно осуществляться адаптивно к изменению состава и характера угроз;
- действия всех СОБ, задействованных при выполнении плана противодействия угрозе, подчинены определенным сценариям, составляемым заранее и подвергаемым корректировке в процессе выполнения адаптивного плана СУБ;
- действия всех СОБ для достижения поставленной (и динамически изменяющейся) цели противодействия должны быть скоординированы на уровне звена управления СУБ;
- наличие человека в контуре противодействия угрозам (в составе всех элементов дежурного наряда сил, в том числе в звеньях управления) ставит выполнение задачи противодействия в зависимость от воздействий т. наз. «человеческого фактора»;
- возникающие в реальных СУБ ТРО уязвимости в большей части обусловлены не огрехами планирования противодействия угрозам, а психофизиологическими и личностными свойствами (усталость, невнимательность, нерешительность, нерациональность, неуверенность и т.д.) конкретных исполнителей планов [10, 11].

В реальных СУБ ТРО особенно существенны два последних фактора. Обеспечение гарантированной безопасности ТРО требует распараллеливания, дублирования и резервирования контуров защиты СУБ, в которых задействован человек-исполнитель.

В то же время, одним из главных критериев выбора СУБ на сегодняшний день является ее экономическая эффективность и ценовая доступность. В современных условиях требования к безопасности и функциональности СУБ ТРО растут, а бюджеты остаются ограниченными. Вышесказанное не позволяет держать на объекте значительный наряд сил безопасности и охраны ТРО по экономическим соображениям.

Современные методы управления [12] позволяют переложить часть функций СУБ с человека на интеллектуальную систему. Так, интеллектуальная система управления безопасностью (ИСУБ) ТРО могла бы решать задачи адаптивного планирования и координации взаимодействия технических средств и дежурного наряда сил охраны (мобильных групп, постов и патрулей) с целью предотвращения различных угроз, в том числе в случае множественных нарушений режима объекта.

Использование методов интеллектуального управления и поддержки принятия решений по обеспечению комплексной безопасности ТРО ввиду представленных выше особенностей должно опираться на концепцию обеспечения безопасности, в основе которой находится ИСУБ [13].

Концепция обеспечения безопасности объекта

Концепция обеспечения безопасности ТРО может рассматриваться (рис. 2) на:

- *стратегическом уровне*, где определяется план совместной активности инженерно-технических средств и наряда дежурных сил охраны;
- *тактическом уровне*, где определяются основные элементы операции по предупреждению и противодействию в соответствии с обнаруженными потенциальными угрозами и ставятся соответствующие цели СОБ;
- *уровне координации*, где сосредоточены адаптивные механизмы, позволяющие сопоставить цель и задачи операции с целями и сценариями действий ее участников;
- *уровне сценариев* отдельных СОБ, где каждым участником с некоторой долей автономности реализуются предопределенные сценарии выполнения элементов предупреждения и противодействия.

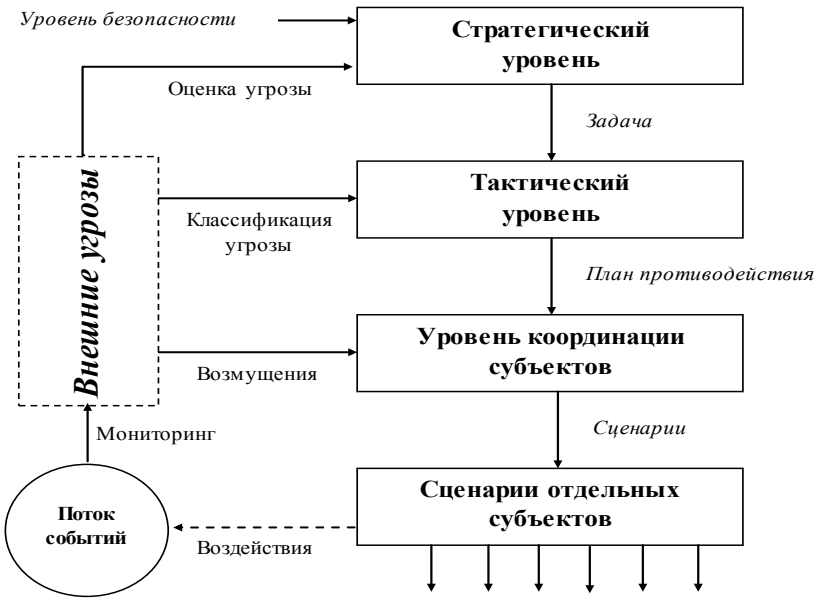

Рисунок 2 – Концепция системы управления безопасностью ТРО

На стратегическом уровне целью управления безопасностью является обеспечение заданного уровня безопасности объекта, соответственно, ИСУБ решает задачи идентификации угрозы и оценки ее влияния на безопасность ТРО. Возникновение потенциальной угрозы ставит задачу ее предупреждения или (если потенциальная угроза становится реальной) противодействия на тактическом уровне.

На тактическом уровне угроза классифицируется, и согласно классу угрозы производится выбор конкретной операции предупреждения или противодействия (блокирование, перехват, задержание, отклонение и т.д.). Для выбранной операции подбирается план необходимых мероприятий, в котором задействуется некоторое подмножество СОБ дежурного наряда сил. Каждому из задействованных СОБ

план доводится в виде цели и предполагаемого сценария действий.

На уровне сценариев цель каждого СОБ состоит в достижении определенной (заданной по сценарию) позиции в требуемый момент времени в охраняемом пространстве, а сценарий предполагает выполнение определенного действия при достижении каждой из заданных позиций.

На уровне координации реализуется адаптация сценариев задействованных СОБ и планов операции в целом к изменению цели и внешним возмущениям. Необходимо отметить, что злоумышленник, обнаружив противодействие, будет изменять свою цель (например, уходить от СОБ) и/или план атаки. Кроме того, возможно влияние третьих лиц, изменяющее условия проведения операции (например, присутствие посторонних лиц ограничивает возможность применения табельного оружия).

Соответственно, цель проведения операции может динамически корректироваться по ходу ее выполнения. Сценарии каждого из участвующих в операции СОБ и план операции также могут корректироваться в широких пределах, вплоть до динамической замены одних исполнителей другими (в т.ч. по критерию близости к нарушителю).

В ситуациях множественных угроз безопасности, когда злоумышленниками реализуются сценарии рассредоточенных по времени и в пространстве атак, роль уровня координации значительно возрастает, поскольку именно на этом уровне необходимо перераспределить задачи и цели СОБ между рядом последовательных или параллельных операций противодействия, планируемых на тактическом уровне.

Исходя из представленной выше концепции СУБ, для интеллектуальной поддержки принятия решений по обеспечению безопасности ТРО могут быть использованы сценарно-прецедентный подход [14] и позиционно-целевой метод управления [15].

Формализация описания ситуаций в ИСУБ

В основу СУБ ТРО могут быть положены следующие понятия: позиция, время, действие, сценарий, план, прецедент, проблемная ситуация.

Позиция описывает местонахождение объекта (субъекта) в заданной двух(трех)-мерной системе координат, и представляется в форме пары (тройки) вида $p=(\xi,\chi)$, где ξ, χ – координаты по соответствующим осям.

Время задается отсчетами t относительно начального значения t_0 на заданной временной шкале T T, упорядоченной по $<_T$.

Пусть заданы множество угроз Ψ, множество СОБ $Z=\{A,B,D,F\}$ и множество допустимых действий СОБ U. Каждый из СОБ $z\in Z$ в момент времени t выполняет некоторое действие $a_{z_t}\in U$.

Триадой назовем кортеж вида $\langle p,t,a_{z_t}\rangle$.

Триада является элементарным фрагментом планов и сценариев противодействия угрозам, триадой также может быть задана цель сценария (цель может состоять в достижении позиции p к моменту t, тогда a_{z_t} может быть нулевым).

Активность СОБ $z\in Z$ представлена его выполняемым сценарием Σ_z.

Сценарий Σ_z СОБ z представляет собой кортеж вида

$$\Sigma_z=\langle t_s,t_r,[...,\langle t_i,p_i,a_i\rangle,...],g\rangle, \quad (1)$$

где $[...,\langle t_i,p_i,a_i\rangle,...]$ – упорядоченная последовательность триад, такая что $t_i <_T t_{i+1}$;

t_s – момент запуска выполнения сценария;

t_r – планируемый момент запуска;

$g=\langle t_e,p_e,a_e\rangle$ – конечная цель выполнения сценария,

t_e – конечный момент времени;

p_e – конечная позиция;

a_e – действие, выполняемое по достижению конечной позиции $\langle t_e,p_e\rangle$.

Соответственно, для каждого СОБ $z\in Z$ в любой момент времени $t\in T$ можно получить его местоположение p_{z_t}, выполняемый им сценарий Σ_z и, зная t_s, конкретное выполняемое действие a_{z_t}.

Представленный способ формализации позволяет корректировать назначенную любому из СОБ

$z \in Z$ цель g_z и/или выполняемый сценарий Σ_z «на лету», без перезапуска цикла функционирования ИСУБ.

Угроза $\psi \in \Psi$ может быть представлена классом K_ψ и множеством нарушителей L, для каждого из которых $l \in L$ в любой момент времени $t \in T$ известно его местоположение p_{l_t}

$$\psi_t = \left\langle K_\psi, \left\{ \left(l, p_{l_t} \right), ... \right\} \right\rangle \ \forall l \in L . \tag{2}$$

Позиционный контекст угрозы ψ_p описывается перечислением множества текущих позиций нарушителей $\psi_p = \left\{ \left(l, p_l \right), ... \right\} \ \forall l \in L$.

Каждой тактической операции Ω, выполняемой в ответ на угрозу $\psi \in \Psi$, соответствует множество участвующих в ней СОБ $Z_\Omega \subseteq Z$ и *план* мероприятий Π_Ω, представляющий собой кортеж вида

$$\Pi_\Omega = \left\langle \psi, Z_\Omega, \left\{ ..., \left(z_k, \Sigma_{z_k} \right), ... \right\} \right\rangle, \tag{3}$$

где $\left\{ ..., \left(z_k, \Sigma_{z_k} \right), ... \right\}$ – множество выполняемых сценариев Σ_{z_k} для каждого из СОБ $z_k \in Z_\Omega$.

Позиционный контекст ситуации s_p содержит занимаемые СОБ $z \in Z$ позиции:

$$s_p = \left\{ ..., \left(z_i, p_{z_i} \right), ... \right\} \ \forall z_i \in Z . \tag{4}$$

Операционный контекст ситуации s_Ω содержит множество выполняемых операций $\left\{ \Omega_j \right\}$, планов выполняемых операций $\left\{ \Pi_{\Omega_j} \right\}$, множество участвующих СОБ $z_{k_j} \in Z_{\Omega_j}$ и соответствующих сценариев Σ_{kj} для каждого из них:

$$s_\Omega = \left\langle \left\{ \Omega_j \right\}, \left\{ \Pi_{\Omega_j} \right\}, \left\{ Z_{\Omega_j} \right\}, \left\{ \Sigma_{kj} \right\} \right\rangle \ \forall z_{kj} \in Z_{\Omega_j} . \tag{5}$$

Ограничением является то, что каждый из СОБ $z_k \in Z$ в любой момент времени t может выполнять один и только один сценарий Σ_{kj}, соответствующий плану Π_{Ω_j} операции $\Omega_j \in \Omega$, такой что $z_{k_j} \in Z_{\Omega_j}$. В случае, если в момент времени t СОБ $z_m \in Z$ не участвует ни в одной из операций $\Omega_j \in \Omega$, т.е. $\forall j \, z_{m_j} \notin Z_{\Omega_j}$, считаем, что z_m выполняет заданный штатный сценарий $\Sigma_{z_{m0}}$.

Текущая *ситуация* s_t описывается конфигурацией угроз, текущими позиционным и операционным контекстами:

$$s_t = \left\langle s_{p_t}, s_{\Omega_t}, \left\{ \psi_{m_t} \right\} \right\rangle \ \forall \psi_m \in \Psi . \tag{6}$$

Представленный формализм описания ситуаций учитывает возможность возникновения множественных угроз, т.к. конфигурация угроз и операционный контекст описывают множества угроз и, соответственно, выполняемых операций противодействия.

В момент возникновения угрозы для ИСУБ складывается *проблемная ситуация*, требующая своего разрешения путем выполнения операций предупреждения или противодействия.

Управление безопасностью ТРО в проблемной ситуации возлагается на сценарно-прецедентную интеллектуальную систему.

Модель сценарно-прецедентной ИСУБ

Сценарно-прецедентные интеллектуальные системы основаны на принципах: а) повторяемости ситуаций; б) возможности использования ранее принятых решений в случае возникновения сходных проблемных ситуаций; в) представления решений в форме планов и сценариев [16].

Пусть S – пространство возможных ситуаций, R – пространство возможных решений.

Выберем для описания ситуаций $s \in S$ некоторый язык представления знаний Λ.

Прецедент e есть пара $\langle s, r \rangle \in \mathrm{E} = S \times R$, состоящая из дескриптора ситуации $s \in S$ и связанного с ней решения $r \in R$.

Всякой ситуации s могут соответствовать несколько решений, таким образом, в ИСУБ допустимы прецеденты вида $\langle s, r\rangle$ и $\langle s, r'\rangle$, которые различны в случае, если $r \neq r'$.

Данные в ИСУБ представлены множеством (*хранилищем*) прецедентов E:

$$\mathrm{E} = \{\langle s_1, r_1\rangle, \langle s_2, r_2\rangle, ..., \langle s_n, r_n\rangle\}. \tag{7}$$

Каждый прецедент e_i в ИСУБ рассматривается как условная импликация вида

$$s_i \Rightarrow r_i, \tag{8}$$

т. обр., если задана некоторая ситуация $s \approx s_j$ и существует прецедент $e_j = \langle s_j, r_j\rangle$, можно утверждать, что r_j является приближенным (или правдоподобным) решением для ситуации s. Более того, чем ближе ситуация s к ситуации s_j, тем правдоподобнее, что r_j является решением для s [17].

Поскольку решением $r \in R$ прецедента $e \in \mathrm{E}$ является план Π мероприятий по противодействию угрозе, включающий в себя сценарии действий Σ_k для всех участвующих в мероприятиях СОБ $z_k \in Z_\Omega$, сценарно-прецедентная интеллектуальная система хорошо вписывается в предложенную концепцию ИСУБ и соответствует формальному аппарату описания ситуаций.

Множество уместных планов $\{\Pi_m\}$, соответствующее конфигурации угроз $\{..., \psi_m\}$ в проблемной ситуации s_t, есть множество решений r_i множества прецедентов e_i, выбранных из хранилища прецедентов E по степени близости ситуации s_t к s_i.

Для нахождения степени близости ситуации s_t к ситуации s_j и, соответственно, оценки близости решения r_j к искомому используется функция подобия ζ, на ее основе строится отношение подобия между прецедентами и выводится мера подобия SIM.

Сценарно-прецедентная система представляет собой структуру

$$PS = \langle \mathrm{E},\ SIM, K\rangle, \tag{9}$$

где $\Im$ – хранилище прецедентов, SIM – мера подобия, K – множество высказываний на языке Λ.

Множество формул K составляет базу знаний о предметной области, которая является структурным элементом ИСУБ.

Для каждого прецедента e_i можно с помощью оценки подобия вычислить степень уместности решения r_i в ситуации, близкой к s_i. В случае, если для этого можно также использовать имеющиеся знания о предметной области, можно утверждать, что $K \to \left(s_t \to \Diamond_{SIM} s_i\right) \vDash \top$ для класса ситуаций $C \mid s_t \in C$.

Таким образом, на стратегическом уровне ИСУБ поиск в хранилище E ситуаций $\{s_i\}$, подобных текущей проблемной ситуации s_t, дает возможность выбора для некоторой угрозы ψ (инициирующей проблемную ситуацию s_t) уместной операции противодействия Ω и плана ее выполнения Π_Ω, представляющего собой решение $e_i.r$.

На тактическом уровне производится выбор множества участников Z_Ω и назначение им сценариев действий Σ_k на основании прототипа, содержащегося в плане $\Pi_\Omega \in e_i.r$.

Отличительной особенностью сценариев в данной трактовке является их многовариантность, т.е. допустимость рассмотрения нескольких альтернативных вариантов развития ситуации, а соответственно, и нескольких целей.

Поскольку между проблемной ситуацией s_t и неким эталоном s_i, хранящимся в виде прецедента e_i, существует отношение подобия ζ (но не эквивалентности!), проблемная s_t и эталонная s_i ситуации принадлежат некоторому классу ситуаций (прототипу) C, такому что $s_t \in C \wedge s_i \in C$. Различные экземпляры класса ситуаций C имеют как схожие (например, позиционный контекст) свойства, так и различающиеся

(например, параметры действий СОБ).

Поскольку контекст проблемной ситуации s_t, как правило, отличается от контекста уместного прецедента $e.s_i$, необходимо производить *адаптацию* плана $\Pi_\Omega \in e_i.r$, осуществляя привязку параметров множества сценариев $\{\Sigma_k\} \in \Pi_\Omega$ к условиям контекста s_t.

Адаптация сценариев действий СОБ $\{z_k\} \in Z_\Omega$ в процессе их совместной активности по выполнению плана Π_Ω к динамически изменяемому контексту (как позиционному, так и операционному) ситуации s_t составляет задачу ИСУБ на уровне координации.

На уровне сценариев ИСУБ работает с *адаптированными сценариями,* полученными из уместного прецедента e_i привязкой его решения r_i к контексту текущей проблемной ситуации e_t, $r_i|s_i \to r_t|s_t$.

Функционирование сценарно-прецедентной ИСУБ

Принцип функционирования сценарно-прецедентной ИСУБ представлен на рис. 3.

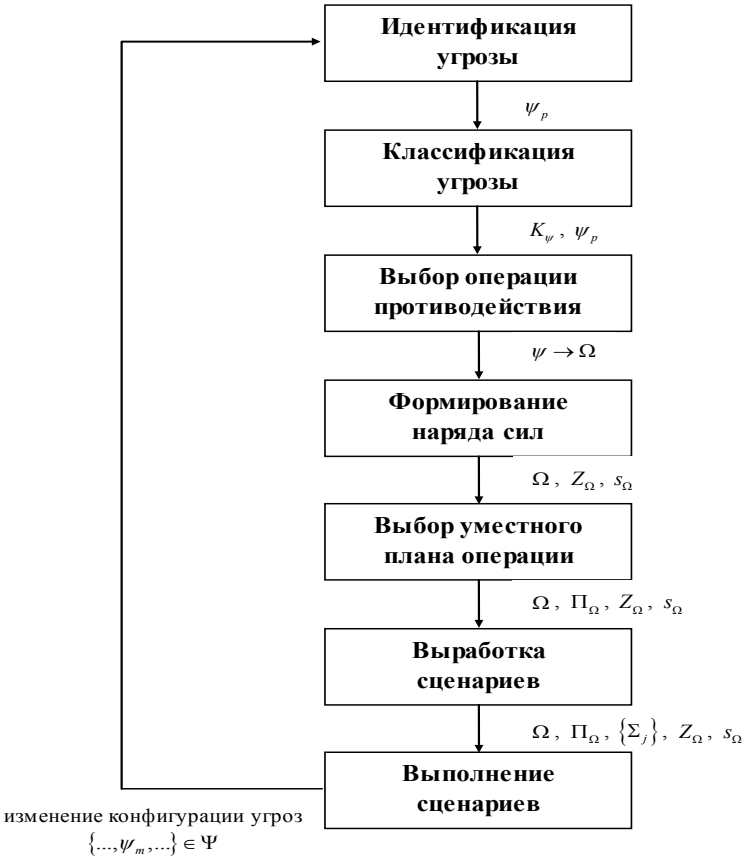

Рисунок 3 – Этапы функционирования ИСУБ

Цикл функционирования ИСУБ состоит из семи этапов.

Этап 1. Идентификация угрозы.

На данном этапе ИСУБ, контролируя с помощью технических средств наблюдения и мониторинга окружающую обстановку, получает позиционный контекст потенциальных угроз ψ_p и оценивает степень угрозы безопасности ТРО. Если угроза безопасности имеется, запускает следующий этап.

Этап 2. Классификация угрозы.

Классификация угроз может производиться как по прецедентам, так и иными известными методами. В результате классификации каждой обнаруженной угрозе $\psi \in \Psi$ сопоставляется класс K_ψ.

Этап 3. Выбор операции противодействия.

Производится по имеющимся прецедентам в соответствии с известными на текущий момент времени исходными данными (возможно, неполными и неточными), $\psi \to \Omega$. ИСУБ может также предоставлять ЛПР право выбирать операцию противодействия «вручную».

Этап 4. Формирование наряда сил противодействия.

Формирование наряда сил противодействия для каждой обнаруженной угрозы $\psi \in \Psi$ производится исходя из имеющегося позиционного контекста s_p на основе формально заданного критерия близости (например, $\min J(p_z, p_l)$). В результате для выбранной операции создается операционный контекст s_Ω, в котором формируется множество участвующих в операции СОБ Z_Ω.

Этап 5. Выбор уместного плана операции.

План Π_Ω выбранной операции Ω получают на основе отношения подобия $SIM(s_t, \mathrm{E}.e.s)$ между текущим описанием проблемной ситуации s_t и дескрипторами ситуаций прецедентов e, накопленных в хранилище E ИСУБ. Из наиболее близких (подобных) прецедентов сценарно-прецедентный механизм отбирает наиболее уместное решение $e.r$, содержащее план Π, которым и дополняют операционный контекст ситуации s_Ω.

Этап 6. Выработка сценария для каждого из участников операции.

Производится на основании операционного контекста ситуации s_Ω. Поскольку отобранное на предыдущем этапе уместное решение прецедента $e.r$ содержит план, элементами которого являются сценарии Σ_j, задача данного этапа состоит в сопоставлении каждому участвующему в операции Ω СОБ $z_k \in Z_\Omega$ соответствующего его позиции и задаче сценария $\Sigma_j \in \Pi$ ($p_{z_k} : z_k \to \Sigma_j$).

Этап 7. Выполнение плана противодействия.

На данном этапе каждый из участников операции z_k выполняет свой сценарий Σ_k. ИСУБ осуществляет координацию плана, наблюдая за развертыванием ситуации, при этом могут изменяться цели (задачи) и/или сценарии отдельных участников.

Появление событий, изменяющих конфигурацию угроз $\{..., \psi_m, ...\} \in \Psi$, принуждает ИСУБ, не прекращая выполнение операции Ω, вернуться к этапу 1 (идентификации угроз) и запустить цикл функционирования заново. Поскольку на этапах 4-6 план противодействия и сценарии участников зависят от операционного контекста ситуации, на этапах 2,3 выполняется проверка класса угроз, и если при этом не требуется изменение вида (характера) операции противодействия, план и сценарии участников сохраняются далее.

В противном случае выбирается новый план и соответствующие ему сценарии участников.

Основой ИСУБ может являться динамическая сценарно-прецедентная интеллектуальная система [18], которая, основываясь на информации от технических систем наблюдения и обнаружения, классифицирует возможных нарушителей и возникающие от них угрозы, на основе сохраненных в хранилище шаблонов активности предлагает план совместной активности мобильных групп и патрулей для предупреждения потенциальных и реальных угроз.

Результаты наблюдения и классификации ИСУБ, как и хранилище прецедентов, могут быть расположены в специальной структуре данных – правдоподобной древовидной сети событий [19], позволяющей получать вывод в реальном времени при получении каждого очередного события или сигнала.

Основные результаты и выводы

В результате проведенного исследования на основе анализа особенностей процесса управления безопасностью ТРО предложена концепция интеллектуальной системы управления безопасностью на основе сценарно-прецедентного подхода, выполнена ее формализация, показан механизм и основные этапы ее функционирования.

Предложенный подход к решению задачи управления безопасностью ТРО позволяет реализовать на практике ИСУБ ТРО на основе сценарно-прецедентного механизма, рассматривая выбор возможных операций противодействия как задачу поиска решения по прецедентам, и адаптируя к контексту проблемной ситуации хранящийся в прецеденте план операции, состоящий из множества сценариев участвующих в выбранной операции СОБ.

Использование сценарно-прецедентного подхода к интеллектуальному управлению системой безопасности территориально распределенных объектов позволяет минимизировать время реагирования на формируемые угрозы, достигнуть требуемой эффективности и координированности действий дежурного наряда сил по обеспечению безопасности объекта.

ЛИТЕРАТУРА

1. Куделькин, В. Методы и инструментальные средства мониторинга состояния комплексной безопасности стратегических объектов и территорий / В.А. Куделькин, В.Ф. Денисов // Мониторинг. Наука и безопасность. – 2012. – №2(6). – С.16-24.
2. Павлов, А. Будущее безопасности: комплексные мониторинговые центры / А.К. Павлов // Системы безопасности. – 2011. – №1. – С.142-143.
3. Кондратьев, С. Комплексная безопасность опасного производственного объекта: построение и управление / С.Ю. Кондратьев // Системы безопасности. – 2009. – № 1. – С.102-104.
4. Коварцев, А. Распределенная информационная система контроля безопасности / А.Н. Коварцев, Э.И. Коломиец // Сб. трудов V Межд. научно-практ. конф. Современные информационные технологии и ИТ-образование. – М., 2010. – С. 361-363.
5. Евдокимов, Д. Классификация интегрированных систем безопасности / Д.Е. Евдокимов // Системы безопасности. – 2007. – № 6. – С.94-97.
6. Зуйков, В. Защита объектов силами и средствами вневедомственной охраны / В.Н. Зуйков // Защита и безопасность. – 2011. – №3(58). – С.16-18.
7. Бурков, В. Модели и механизмы управления безопасностью / В.Н. Бурков, Е.В. Грацианский и др. – М.: СИНТЕГ, 2001. – 160 с.
8. Леус, А. Оптимизация структуры интегрированной системы безопасности / А.В. Леус, Г.Ф. Шанаев // Системы безопасности. – 2011. – №1. – С.124-127.
9. Панин, О. Анализ эффективности интегрированных систем безопасности: принципы, критерии, методы / О.А. Панин // Системы безопасности. – 2006. – №2. – С.101-105.
10. Воробьев, Ю. Теория риска и технологии обеспечения безопасности. Подход с позиций нелинейной динамики / Ю.Л. Воробьев, Г.Г. Малинецкий, Н.А. Махутов // Проблемы безопасности при ЧС. – 1998. – Вып. 11. – С.26-40.
11. Багринцева, О. Управление качеством принимаемых решений при моделировании системы охраны объектов в условиях преднамеренных помех / О.В. БАГРИНЦЕВА, С.В. БЕЛОКУРОВ // Вестник Воронежского института МВД России. – 2012. – №2. – С.60-64.
12. Интеллектуальные системы управления организационно-техническими системами / Под ред. А.А. Большакова. – М.: Горячая линия – Телеком, 2006. – 160 с.
13. Крахмалев, А. О концепции комплексной безопасности / А.К.Крахмалев // Системы безопасности. – 2008. – № 1. – С.112-114.
14. Шерстюк, В. Сценарно-прецедентный подход к управлению динамическими объектами в стесненных навигационных условиях / В. Г. Шерстюк // Искусственный интеллект. – 2011. – №1. – С.113-123.
15. Шерстюк, В. Позиционно-целевое управление подвижными объектами в полиэргатических системах / В. Г. Шерстюк // Вестник Херсонского национального технического университета. – 2012. – №1(44). – С.18-26.
16. Шерстюк, В. Сценарно-прецедентный подход к формированию управляющих воздействий в системе управления морского подвижного объекта / В.Г. Шерстюк // Проблемы информационных технологий. – 2009. – №2(6). – С.69-77.
17. Dubois, D. Fuzzy modeling of case-based reasoning and decision / D. Dubois, F. Esteva, P. Garcia, L. Godo, R.L. de Mántaras, H. Prade // Case-Based Reasoning Research and Development: Lecture Notes in Computer Science. – 1997. – Vol. 1266. – Pp. 599-610.
18. Шерстюк, В. Динамическая сценарно-прецедентная интеллектуальная система для управления подвижными объектами / В. Г. Шерстюк // Искусственный интеллект. – 2011. – №4. – С.362-373.
19. Шерстюк В.Г. Использование деревьев событий для представления знаний в динамических прецедентных интеллектуальных системах / В.Г. Шерстюк // Вестник Херсонского национального технического университета. – 2011. – №2(41). – С.306-317.

ШЕРСТЮК Владимир Григорьевич – к.т.н., доцент кафедры информационных технологий Херсонского национального технического университета.

Научные интересы: интеллектуальные системы принятия решений реального времени, принятие решений на основе прецедентов, мультиагентные системы, комбинированные логические системы представления знаний.

КОЗУБ Наталья Александровна – к.т.н., доцент кафедры информационных технологий Херсонского национального технического университета.

Научные интересы: интеллектуальные системы принятия решений.