

Риск-ориентированный подход к проектированию системы антитеррористической защищенности образовательных учреждений

В.М. Колодкин¹, Д.М. Варламова¹✉, А.Д. Шакиров¹

¹ Удмуртский государственный университет, г. Ижевск, 426034, Россия

Ссылка для цитирования

Колодкин В.М., Варламова Д.М., Шакиров А.Д. Риск-ориентированный подход к проектированию системы антитеррористической защищенности образовательных учреждений // Программные продукты и системы. 2024. Т. 37. № 1. С. 105–112. doi: 10.15827/0236-235X.142.105-112

Информация о статье

Группа специальностей ВАК: 2.3.1

Поступила в редакцию: 12.07.2023

После доработки: 24.08.2023

Принята к публикации: 04.09.2023

Аннотация. В работе представлен авторский проблемно-ориентированный программный комплекс для компьютерного прогнозирования последствий террористических атак на образовательные учреждения. Одним из основных инструментов прогнозирования является математическое моделирование. В рамках комплекса моделируется динамика развития антагонистического конфликта между нарушителем (террористом) и реципиентами риска в здании образовательного учреждения. При построении программного комплекса использована новая концепция противодействия террористической атаке. Ее особенностью является противодействие террористической атаке со стороны реципиентов риска, которое выражается в движении людских потоков в зоны безопасности по безопасным траекториям в здании. В рамках программного комплекса поддерживается интеграция данных пространственно-информационной модели здания, характеристик модели нарушителя и управляемого движения людских потоков в условиях чрезвычайных ситуаций. Пространственно-информационная модель здания создается в отечественной BIM-системе Renga. Топологический граф, отвечающий топологической модели здания, строится специализированным плагином, созданным средствами Renga. Преимуществом авторского программного комплекса является автоматический режим проектирования реакции реципиентов риска на действия нарушителя. Режим обеспечивает минимизацию ущерба. При проектировании учитываются характеристики инженерно-технической системы защиты учреждения. Оригинальность программного комплекса заключается в обеспечении процесса проектирования безопасных путей движения людских масс в режиме реального времени развития чрезвычайной ситуации. Поддержка режима реального времени предоставляет принципиальную возможность построения на базе проблемно-ориентированного программного комплекса системы поддержки принятия решений. Практическая значимость комплекса обусловлена также возможностью его использования в качестве тренажера для подготовки лиц, отвечающих за комплексную безопасность образовательных учреждений в условиях чрезвычайных ситуаций. В работе показано применение программного комплекса для целей ранжирования образовательных учреждений по уровню антитеррористической защищенности.

Ключевые слова: программный комплекс, численное моделирование, антитеррористическая защищенность, риск-ориентированный подход, образовательные учреждения

Введение. Обострение экономических, политических, социальных противоречий в мире привело к росту террористической опасности [1]. В России реакция на это, в первую очередь, была обусловлена защитой объектов критически важной инфраструктуры, для которых разрабатывались системы обеспечения безопасности, включающие и системы физической защиты [2]. Для проектирования и оценки эффективности систем физической защиты объектов использовались специально разработанные методы, например, вероятностно-временного анализа [3], синтеза рисков [4], методы на основе концептуальной имитационной модели [5] и др. Определяющей в защите объектов критически важной инфраструктуры является концепция прерывания террористической атаки специальными силами (например, силами охраны объекта). Однако в общем случае кон-

цепция защиты критически важных объектов от террористической угрозы неприменима для образовательных учреждений (ОУ), поскольку у них иные условия функционирования и возможности защиты, что делает невозможным распространение алгоритмов и ПО на условия обеспечения безопасности.

Современная система обеспечения комплексной безопасности ОУ должна предусматривать и защиту от террористической угрозы, проявления которой могут быть весьма разнообразными [6]. С появлением новых угроз для ОУ требуется непрерывная модернизация средств защиты, которая при проектировании должна учитывать существующие и прогнозируемые реалии. Поскольку в современных условиях вид и направление террористической атаки предсказать затруднительно, модернизация системы защиты должна в той или иной степени

касаться очень многих ОУ [7, 8]. В связи с этим ограничиться модернизацией систем защиты отдельных ОУ в общем случае не представляется возможным.

Существенным фактором при проектировании и модернизации системы антитеррористической защищенности ОУ являются финансовые ограничения. Каждое ОУ располагает определенными средствами защиты на случай возникновения чрезвычайных ситуаций, которые отвечают его возможностям. Однако не всегда уровень развития средств защиты соответствует уровню угроз. Таким образом, повышение антитеррористической защищенности ОУ предполагает их ранжирование по количественным оценкам уровней угроз, которым подвержены реципиенты риска в учреждениях, и уровней защищенности, по степени соответствия уровней угроз уровням защищенности, а также выделение совокупности ОУ, системы безопасности которых подлежат модернизации в соответствии с финансовыми возможностями.

Система антитеррористической защищенности ОУ ориентирована на сохранение людей (реципиентов риска) в условиях террористической атаки.

Таким образом, повышение антитеррористической защищенности ОУ (модернизация систем комплексной безопасности) предполагает предварительное исследование террористической опасности и реакции на нее со стороны реципиентов риска. Исследование основано на результатах математического моделирования развития антагонистического конфликта между нарушителем и реципиентами риска в рамках проблемно-ориентированного программного комплекса. Математическое моделирование антагонистического конфликта, возможно, является наиболее перспективным методом, позволяющим разрабатывать системы безопасности и постоянно адаптировать их к новым угрозам [9]. Учитывая ограниченность финансовых возможностей ОУ, модернизации системы безопасности должно предшествовать ранжирование ОУ по количественным оценкам уровней защищенности.

Моделирование террористической угрозы

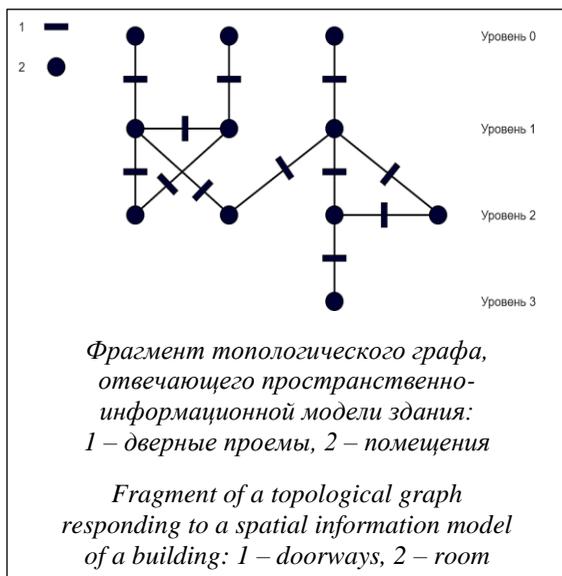
Конкретизируем временной горизонт террористической атаки на уровне порядка 10 минут. Пространственный горизонт системы антитеррористической защищенности ограничим территорией с охватом внешнего контура ОУ.

В условиях высокой неопределенности вида и характеристик террористической атаки будем полагать, что спасение людей при террористической атаке возможно путем целенаправленного движения реципиентов риска в зоны безопасности. В частном случае это может быть экстренная эвакуация людей из здания по безопасным путям, проектируемым в режиме реального времени с учетом текущей ситуации. Этой цели подчинены физические средства, которые обеспечивают предупреждение, обнаружение, реагирование на угрозы и т.п. Синтез инженерно-технических средств защиты направлен на увеличение величины предотвращенного риска в ОУ в условиях чрезвычайной ситуации [4].

Направление модернизации системы антитеррористической защищенности ОУ основано на результатах моделирования террористической атаки и реакции на атаку в рамках электронного полигона – программного комплекса, предназначенного для моделирования террористической атаки и реакции на атаку в модельном пространстве [10, 11]. Модельное пространство представляется координатной плоскостью с охватом внешнего контура ограждения территории и пространственно-информационной моделью каждого здания ОУ, которая создается в отечественной BIM-системе Renga. Для декларируемых целей пространственно-информационная модель здания представляется двудольным графом, включающим вершины двух типов: первый – это зоны здания на этажах и переходах между этажами, второй – элементы соединения между зонами (например, дверные проемы) [12, 13]. Топологическая модель здания, используемая при моделировании конфликта (движение нарушителя, перемещение реципиентов риска), строится с применением специализированного плагина, созданного средствами Renga. Топологической модели здания отвечает топологический граф.

Для конкретизации рассмотрим схему террористической атаки, когда нарушитель передвигается от внешнего контура ограждения до здания, а затем в пределах здания. Другие схемы атаки будем рассматривать как частные случаи общей схемы. Для моделирования террористической атаки в здании используется топологический граф (см. рисунок).

Вершины топологического графа, отвечающие помещениям, характеризуют распределение реципиентов риска и положение нарушителя (источника опасности) в данный момент времени.



Общая схема прогнозирования последствий террористической атаки

Такое прогнозирование базируется на вероятностно-временном анализе двух взаимосвязанных процессов:

- нанесение ущерба при террористической атаке, обусловленного действием нарушителя;
- увеличение предотвращенного ущерба $\Delta U(t)$, обусловленного управляемой активностью реципиентов риска.

Первый процесс порождается нарушителем, действия которого подчинены определенным целям и ограничены реакцией (активной и пассивной) системы обеспечения безопасности. Цели и возможности нарушителя формализуются в виде модели нарушителя. Его стратегия подчинена цели нанесения максимального ущерба для людей в здании ОУ. Нарушители классифицированы по уровню порождаемой опасности – А, В, С. Частота проявления m -модели нарушителя – v_m . Из условия нормировки имеем $\sum_{m=1}^{m^*} v_m = 1$, где $m^* = 3$ – количество конкретизаций модели нарушителя.

Для каждой конкретизации модели нарушителя методом экспертного оценивания с учетом литературных данных определены:

- скорость перемещения нарушителя на территории ОУ и в элементах здания, V ;
- время преодоления нарушителем закрытых проемов ограждения территории, Δt_g ;
- время преодоления нарушителем закрытых дверных проемов в здании, Δt_b ;
- характерный размер области воздействия нарушителя на территории и в здании ОУ, A .

При движении нарушителя области здания, попадающие в зону воздействия нарушителя, становятся недоступными для нахождения в них реципиентов риска.

Второй процесс порождается реакцией реципиентов риска на атаку. Для условий ОУ наиболее важным является направленное движение людских потоков в зоны безопасности (в частном случае – экстренная эвакуация). Этот процесс увеличивает величину предотвращенного ущерба $U(t)$. При движении реципиентов риска в зоны безопасности изменяется распределение людей в помещениях здания. Процесс поддерживается подсистемами обеспечения безопасности: связи и оповещения, световыми указателями управляемого движения людских потоков и др.

Весь процесс террористической атаки при моделировании разбивается на последовательность элементарных временных интервалов $\Delta t^{(k)}$ (временной интервал преодоления нарушителем k -й зоны, протяженность которой $L^{(k)}$). Если ввести в рассмотрение плотность реципиентов риска в здании D [чел./м²] и так называемую топологическую сложность здания Ω , то для временного интервала освобождения здания T_e [с] в условиях управляемой экстренной эвакуации имеем экспериментально установленную регрессионную зависимость [14]:

$$T_e = 115,45 + 725,76 * D + 103,38 * \Omega. \quad (1)$$

Реакция на террористическую атаку проявляется в изменении распределения реципиентов риска по помещениям здания при экстренной эвакуации. Результаты вычислительных экспериментов по управляемой эвакуации [15] позволяют построить оценку зависимости предотвращенного ущерба $U = (N_0 - N(\Delta t))$ от продолжительности террористической атаки Δt в виде

$$\frac{N(\Delta t)}{N_0} = \exp\left(-\chi * \frac{\Delta t}{T_e}\right), \chi = 2,043, \quad (2)$$

где $N(\Delta t)$ – оценка количества реципиентов риска в здании через время Δt с начала террористической атаки; N_0 – количество реципиентов риска в здании до момента атаки. Предполагается, что перемещение реципиентов риска во время террористической атаки отвечает закономерностям теории людских потоков в условиях чрезвычайных ситуаций, разработанной научной школой В.В. Холщевникова.

Соотношения (1) и (2) представляют верхнюю оценку предотвращенного ущерба. Уточненная оценка следует из результатов непосредственного моделирования управляемого движения людских потоков.

Прогнозирование последствий террористической атаки на территории ОУ

Главная задача, решаемая в рамках программного комплекса при моделировании действий нарушителя на территории ОУ вне здания, – определить интервал времени, в течение которого нарушитель достигнет внутренних помещений здания ОУ, где могут находиться реципиенты риска. Этот интервал времени используется реципиентами риска для частичной экстренной эвакуации через выходы из здания, лежащие вне поля видимости нарушителя.

Нарушитель проникает на территорию через узел g внешнего контура ограждения территории ОУ. Множество узлов внешнего контура ограждения территории $G = \{g_i \mid i = 1, g^*\}$, где g_i – узел внешнего контура ограждения (в дальнейшем индекс i опустим); g^* – количество узлов внешнего контура ограждения.

Частота проникновения нарушителя через ограждение внешнего контура $v_g = \alpha_g v_g^*$, где v_g^* – постоянная составляющая, определяемая условием нормировки, α_g – весовой коэффициент. Весовой коэффициент зависит от состояния внешнего контура ограждения и взаимного расположения контура ограждения и здания. Положим, что весовой коэффициент $\alpha_g = 3$ для открытых проемов ограждения, $\alpha_g = 1$ для закрытых проемов. Нарушитель выбирает узел g , если в область видимости из узла g попадает хотя бы один вход в здание, то есть если в область видимости из узла g не попадает ни один из входов в здание, весовой коэффициент $\alpha_g = 0$.

Условие нормировки частот проникновения для совокупности узлов ограждения $\sum_{g=1}^{g^*} \alpha_g v_g^* = 1$. Для постоянной составляющей имеем

$$v_g^* = 1 / \sum_{g=1}^{g^*} \alpha_g.$$

Множество входных дверей здания ОУ, падающих в зону видимости из узла g , представим как

$$B_g = \{(b_g)_i \mid i = 1, b_g^*\},$$

где $(b_g)_i$ – входная дверь здания, попадающая в зону видимости из узла g (в дальнейшем индекс i опустим); b_g^* – количество входных дверей в здание, отвечающих зоне видимости из узла g .

Входные двери, не попадающие в зону видимости из узла g , пометим \bar{b}_g , их количество – \bar{b}_g^* . Из совокупности входных дверей в здание, по-

падающих в зону видимости из узла g , нарушитель будет отдавать предпочтение открытым дверям в соответствии с моделью нарушителя.

Для частоты выбора пути нарушителя $v_{gb} = \alpha_{gb} v_{gb}^*$, где v_{gb}^* – постоянная составляющая, определяемая условием нормировки, α_{gb} – весовой коэффициент. Весовой коэффициент зависит от состояния входных дверей в здание. Положим, что весовой коэффициент $\alpha_{gb} = 3$ для открытых дверей, $\alpha_{gb} = 1$ для закрытых дверей.

Условие нормировки частот выбора пути нарушителем из узла g до входа в здание, находящегося в поле видимости из узла g , следующее:

$$\sum_{b_g=1}^{b_g^*} \alpha_{gb} v_{gb}^* = 1.$$

Для постоянной составляющей имеем

$$v_{gb}^* = 1 / \sum_{b_g=1}^{b_g^*} \alpha_{gb}.$$

Если b – узел, соответствующий входной двери здания ОУ, находящийся в зоне видимости из узла g , то оценка расстояния, которое необходимо преодолеть нарушителю, – $L_{gb}^{(0)}$.

Интервал времени достижения нарушителем первого помещения здания

$$\Delta t_{gb}^{(0)} = t_g(m) + \Delta t(m, g, b) + \Delta t_b(m),$$

где $\Delta t(m, g, b) = L_{gb}^{(0)} / V(m)$; m – модель нарушителя; $t_g(m)$ – временной интервал преодоления нарушителем внешнего контура ограждения в узле g (определен моделью нарушителя); $\Delta t_b(m)$ – временной интервал преодоления нарушителем дверных проемов в здании ОУ в узле b (определен моделью нарушителя); $V(m)$ – скорость нарушителя на территории ОУ, определяемая моделью нарушителя.

Если принять, что в момент начала террористической атаки на здание ОУ все реципиенты риска находились в здании, то ущерб, нанесенный нарушителем за временной интервал $\Delta t_{gb}^{(0)}$, равен $U_v^{(0)}(\Delta t_{gb}^{(0)}) = 0$.

За время $\Delta t_{gb}^{(0)}$ максимальная оценка количества реципиентов риска, покинувших здание в условиях управляемого движения людских потоков (предотвращенный ущерб), будет $U_v^{(0)}(\Delta t_{gb}^{(0)})$. Оценка предотвращенного ущерба при управляемом движении людских потоков определяется соотношениями (1) и (2). Управляемая эвакуация осуществляется через выходы из здания, не попадающие в зону видимости нарушителя. Предполагается идеальная подготовка реципиентов риска и лиц, ответственных за принятие решений в условиях ЧС. Учет реального

уровня подготовки осуществляется на этапе количественной оценки уровня антитеррористической защищенности. На оценку предотвращенного ущерба (при указанных выше предположениях) влияют исключительно имманентные свойства системы физической защиты.

Вероятность подачи сигнала управляемой экстренной эвакуации P_{gb}^{evac} можно оценить по соотношению

$$P_{gb}^{evac} = P_{gb}^{det} * P^{con},$$

где P_{gb}^{det} – вероятность обнаружения нарушителя при перемещении между точками g и b , $P_{gb}^{det} = 1 - \exp(-\gamma * n)$, n – количество приборов контроля, например, видеокамер, характеристики которых позволяют обнаружить нарушителя, γ – коэффициент, определяемый типом приборов контроля в здании ($\gamma \in [1, 2]$). Вероятность $P^{con} = P^{con-f} * P^{con-r}$ характеризует подсистему связи, где P^{con-f} – вероятность доведения актуальной информации об обнаружении нарушителя до ЛПР; P^{con-r} – вероятность устойчивой связи между ЛПР и реципиентами риска в условиях управляемого движения людских потоков. Для оценки P^{con} имеем $P^{con} = S_c / S$, где S_c – площадь здания учреждения с устойчивой связью; S – общая площадь здания ОУ. То есть предполагается, что при наличии в помещении устойчивой связи реципиенты риска получают команду от ЛПР в условиях чрезвычайной ситуации либо от программного комплекса, работающего в автоматическом режиме [14, 15].

Для оценки предотвращенного риска за время преодоления нарушителем территории ОУ имеем

$$R^{(0)} = \sum_{m=1}^{m^*} \sum_{g=1}^{g^*} \sum_{b_g=1}^{b_g^*} v_m v_g v_{gb} * P_{gb}^{det} * P^{con} * U^{(0)}(\Delta t_{gb}^{(0)}),$$

где $U^{(0)}$ – предотвращенный ущерб (количество реципиентов риска, которые покинули здание за время перемещения нарушителя $\Delta t_{gb}^{(0)}$). В соответствии с (2)

$$U^{(0)}(\Delta t_{gb}^{(0)}) = N_0 * \left[1 - \exp\left(-\chi * \frac{\Delta t_{gb}^{(0)}}{T_e}\right) \right].$$

Прогнозирование последствий террористической атаки в здании ОУ

В рамках электронного полигона топологическая модель здания представляется топологическим графом. Характеристики вершин графа соответствуют пространственно-инфор-

мационной модели здания. Из проема, помеченного точкой b , нарушитель попадает в помещение $B^{(1)}$. Путь нарушителя по зданию определяется моделью нарушителя и топологическим графом. В частности, полагается, что траектория движения нарушителя по зданию (переход из k -го помещения n -го уровня топологического графа в $k + 1$ помещение) отвечает следующим приоритетам выбора:

- предпочтение отдается помещениям, где нарушитель еще не был;
- предпочтение отдается переходу в помещение $n + 1$ уровня топологического графа;
- предпочтение нарушителя при переходе в $k + 1$ помещение отдается помещениям с большим количеством реципиентов риска (для нарушителя это принцип нанесения максимального ущерба);
- предпочтение отдается дверным проемам, переход по которым для нарушителя не сопряжен с потерей времени (открытые двери между k -м и $k + 1$ помещениями здания).

Террористическая атака считается законченной, если нарушитель достиг конца топологического графа (обход графа в глубину). Фактически анализируются все пути топологического графа, исходящие из вершины, связанной с выходом из здания. Из полной совокупности траекторий движения нарушителя выбирается траектория, связанная с максимальным количеством жертв среди реципиентов риска.

Интервал времени преодоления нарушителем k -го помещения здания

$$\Delta t^{(k)} = \Delta t(m, d, k) + \Delta t_b^{(k)}(m),$$

где $\Delta t(m, d, k) = L^{(k)} / V(m, d)$, $L^{(k)}$ – характерный размер k -го помещения в здании; m – модель нарушителя; d – характеристика k -го помещения (лестница вверх, лестница вниз, горизонтальное помещение); $V(m, d)$ – скорость перемещения нарушителя на участке помещения с характеристикой d ; $\Delta t_b^{(k)}(m)$ – временной интервал преодоления нарушителем дверных проемов в здании учреждения (определен моделью нарушителя).

Вероятность передачи сигнала управляемого перемещения людских потоков P^{evac} в условиях террористической атаки можно оценить как

$$P^{evac} = P^{det} * P^{con},$$

где P^{det} – вероятность обнаружения нарушителя в помещении здания. Если помещений в здании H , количество приборов контроля, характеристики которых позволяют идентифицировать нарушителя в здании h , то для оценки

вероятности обнаружения нарушителя в помещении здания имеем $P^{det} = h/H$.

Для оценки предотвращенного риска R при террористической атаке на ОУ имеем:

$$R = \sum_{m=1}^{m^*} \sum_{g=1}^{g^*} \sum_{b_g=1}^{b_g^*} v_m v_g v_{gb} P^{con} \left[P_{gb}^{det} U^{(0)}(\Delta t_{gb}^{(0)}) + P^{det} \sum_{k=1}^{n_{gb}} U^{(k)}(\Delta t^{(k)}) \right],$$

где $U^{(k)}(\Delta t^{(k)})$ – предотвращенный ущерб (количество реципиентов риска, которые покинули здание за время $\Delta t^{(k)}$; n_{gb} – количество помещений на пути нарушителя).

Принимая во внимание, что в первом приближении

$$\sum_{k=1}^{n_{gb}} U^{(k)}(\Delta t^{(k)}) \approx U\left(\sum_{k=1}^{n_{gb}} \Delta t^{(k)}\right),$$

и учитывая выражение (2) для оценки количества реципиентов риска U , покинувших здание за время террористической атаки Δt , для оценки предотвращенного ущерба при террористической атаке имеем соотношение

$$R = \sum_{m=1}^{m^*} \sum_{g=1}^{g^*} \sum_{b_g=1}^{b_g^*} v_m v_g v_{gb} P^{con} N_0 \left\{ P_{gb}^{det} \left[1 - \exp \left(-\chi \frac{\Delta t_{gb}^{(0)}}{T_e} \right) \right] + P^{det} \left[1 - \exp \left(-\chi \frac{\Delta t}{T_e} \right) \right] \right\}. \quad (3)$$

Соотношение (3) позволяет оценить величину предотвращенного риска в условиях террористической атаки на ОУ. Причем, как следует из вывода данного соотношения, это оценка сверху.

Для иллюстрации рассмотрим случай террористической атаки на реципиентов риска в корпусах университета, воспользовавшись данными, представленными в работе [14]. Отметим, что внешний контур ограждения отсутствует, поэтому первое слагаемое в фигурных скобках выражения (3) обращается в нуль. Результаты моделирования активности нарушителя и реакции реципиентов риска на террористическую атаку представлены в таблице. Результаты отвечают террористической атаке на реципиентов риска в корпусах университета: № – номер корпуса; D – плотность распределения реципиентов риска в помещениях здания по пути перемещения нарушителя; Ω – топологическая сложность здания; Δt – продолжительность террористической атаки по результатам моделирования; R/N_0 – удельная величина предотвращенного риска.

| № | D , чел./м ² | Ω | Δt , с | R/N_0 |
|---|---------------------------|----------|----------------|---------|
| 1 | 0,079 | 1,36 | 147,14 | 0,617 |
| 2 | 0,102 | 0,84 | 135,48 | 0,633 |
| 3 | 0,071 | 0,32 | 46,84 | 0,380 |
| 4 | 0,126 | 1,84 | 302,73 | 0,789 |
| 5 | 0,03 | 0,95 | 161,01 | 0,753 |
| 7 | 0,046 | 0,81 | 117,97 | 0,645 |

Из анализа данных, представленных в таблице, следует, что с точки зрения количественной оценки одного из определяющих факторов уровня защищенности наименее защищены корпус № 3, наиболее – корпус № 4.

Следующий этап работы связан с выделением корпусов, для которых количественный уровень угроз превышает количественный уровень защищенности. Для выделенных корпусов в рамках электронного полигона проектируются варианты модернизации системы безопасности с учетом существующих финансовых и временных ограничений. Аналогичная процедура должна охватывать ОУ города (региона).

Заключение

В данной работе предложен риск-ориентированный подход к оценке одного из определяющих факторов антитеррористической защищенности ОУ. Подход базируется на прогнозировании предотвращенного риска в условиях террористической атаки. Совокупность ОУ, система антитеррористической защищенности которых требует модернизации, определяется по результатам сопоставления уровней угроз и уровней защищенности с учетом финансовых и инженерно-технических ограничений.

Проектирование системы комплексной безопасности ОУ с учетом существующих реалий поддерживается специализированным ПО.

Отметим, что сложившаяся с антитеррористической защищенностью ОУ ситуация требует принятия срочных мер, направленных на модернизацию систем безопасности. Наряду с появлением новых средств физической защиты объектов появляются новые угрозы, например, связанные с применением беспилотных летательных аппаратов для совершения террористических атак. Модернизация систем обеспечения безопасности ОУ, осуществляемая на изложенных в данной работе положениях, является требованием времени.

Список литературы

1. Тихомиров Н.П., Новиков А.В. Риски террористических актов и особенности их оценки // Вестн. РЭУ. 2019. № 2. С. 198–210. doi: 10.21686/2413-2829-2019-2-198-210.

2. Шрейдер М.Ю., Боровский А.С. Применение многоагентного подхода к построению систем физической защиты объектов // Интеллект. Инновации. Инвестиции. 2017. № 10. С. 66–71.
3. Боровский А.С., Тарасов А.Д., Шрейдер М.Ю. Автоматизированное проектирование и оценка систем физической защиты потенциально опасных объектов. Оренбург: изд-во ОГУ, 2022. 186 с.
4. Бочков А.В. О методе синтеза рисков в управлении безопасностью структурно-сложных систем // Надежность. 2020. Т. 20. № 1. С. 57–67. doi: 10.21683/1729-2646-2020-20-1-57-67.
5. Kostin V., Borovsky A. Definition of basic violators for critically important objects using the information probability method and cluster analysis. CEUR Workshop Proc. Proc. ITNT, 2020, vol. 2667, pp. 343–347.
6. Yu H., Li X., Song W., Zhang J. et al. Pedestrian emergency evacuation model based on risk field under attack event. Physica A: Statistical Mechanics and its Applications, 2022, vol. 606, art. 128111. doi: 10.1016/j.physa.2022.128111.
7. Павлов В.Н., Какадий И.И. Угрозы безопасности образовательного учреждения // Бюлл. науки и практики. 2020. Т. 6. № 6. С. 305–311. doi: 10.33619/2414-2948/55/40.
8. Золотухин М.А. Концепция безопасности образовательного пространства // Техничко-технологические проблемы сервиса. 2018. № 1. С. 117–120.
9. Четверушкин Б.Н., Осипов В.П., Балута В.И., Яковенко О.Ю. Суперкомпьютерное моделирование в задачах обеспечения антитеррористической безопасности объектов // СРТ2019: тр. Междунар. конф. 2019. С. 40–49.
10. Осипов В.П., Четверушкин Б.Н., Балута В.И., Нечаев Ю.И. Формальный аппарат моделирования и интерпретации антагонистических конфликтов на базе электронного полигона // Препринты ИПМ им. М.В. Келдыша. 2018. № 181. С. 1–28. doi: 10.20948/prepr-2018-181.
11. Нечаев Ю.И., Осипов В.П., Четверушкин Б.Н., Балута В.И. Онтологический синтез управленческих решений в условиях антагонистических конфликтов // Препринты ИПМ им. М.В. Келдыша. 2018. № 179. С. 1–22. doi: 10.20948/prepr-2018-179.
12. Галиуллин М.Э. Создание и использование пространственно-информационной модели здания (ПИМ) для расчета величины риска при составлении декларации пожарной безопасности // Безопасность в техносфере: сб. ст. 2015. № 9. С. 59–80.
13. Колодкин В.М., Болтачев И.И. Информационная модель здания образовательного учреждения для системы поддержки принятия решений // Безопасность в техносфере: сб. ст. 2022. № 15. С. 75–79.
14. Колодкин В.М., Чирков Б.В. Валидация модели адаптивного управления движением людских потоков в динамической среде ограниченного пространства // Вестн. Удмуртского университета. Математика. Механика. Компьютерные науки. 2020. Т. 30. № 3. С. 480–496. doi: 10.35634/vm200309.
15. Колодкин В.М., Чирков Б.В. Компьютерное исследование процесса эвакуации людей из здания при пожаре // Современные наукоемкие технологии. 2016. № 12-3. С. 496–500.

Software & Systems

doi: 10.15827/0236-235X.142.105-112

2024, 37(1), pp. 105–112

Risk-oriented approach to designing an anti-terrorist protection system of educational institutions

Vladimir M. Kolodkin ¹, Dina M. Varlamova ¹✉, Artem D. Shakirov ¹¹Udmurt State University, Izhevsk, 426034, Russian Federation

For citation

Kolodkin, V.M., Varlamova, D.M., Shakirov, A.D. (2024) 'Risk-oriented approach to designing an anti-terrorist protection system of educational institutions', *Software & Systems*, 37(1), pp. 105–112 (in Russ.). doi: 10.15827/0236-235X.142.105-112

Article info

Received: 12.07.2023

After revision: 24.08.2023

Accepted: 04.09.2023

Abstract. The paper presents a problem-oriented software package for computer forecasting of the consequences of terrorist attacks on educational institutions. One of the main forecasting tools is mathematical modeling. The complex simulates the development dynamics of an antagonistic conflict between a violator (terrorist) and risk recipients in a educational institution. When building a software package, the authors used a new concept of countering a terrorist attack. The concept feature is countering a terrorist attack by risk recipients expressed in moving human flows into security zones along safe trajectories in a building. The software package supports data integration of the spatial information model of a building, the intruder model characteristics, the characteristics of the controlled movement of human flows in emergency situations. The spatial information model of a building is created in a domestic BIM system Renga. The topological graph corresponding to the building topological model is constructed by a specialized plugin created by Renga. The advantage of the author's software package is the automatic mode of designing the reaction of risk recipients to violator's actions. The mode provides damage minimization. Designing takes into account the characteristics of an institution engineering and technical protection system. The software package originality is to ensure the process of designing safe ways for moving human masses in a real-time emergency situation development. Real-time mode support provides a fundamental opportunity to build a decision support system based on a problem-oriented software package. The practical significance of the complex is also due to the possibility of using it as a simulator for training persons responsible for the integrated safety of educational institu-

tions in emergency situations. The paper shows the application of the software package for ranking educational institutions by the anti-terrorist security level.

Keywords: software package, numerical modeling, anti-terrorist security, risk-oriented approach, educational institutions

References

1. Tikhomirov, N.P., Novikov, A.V. (2019) 'Risks of acts of terrorism and specific features of their estimation', *Vestn. of the Plekhanov RUE*, (2), pp. 198–210 (in Russ.). doi: 10.21686/2413-2829-2019-2-198-210.
2. Shreyder, M.Yu., Borovskiy, A.S. (2017) 'Application of a multi-agent approach to the construction of physical protection systems for objects', *Intellect. Innovations. Investments*, (10), pp. 66–71 (in Russ.).
3. Borovskiy, A.S., Tarasov, A.D., Shreyder, M.Yu. (2022) *Automated design and assessment of physical protection systems for potentially hazardous objects*. Orenburg, 186 p. (in Russ.).
4. Bochkov, A.V. (2020) 'On the method of risk synthesis in the safety management of structurally complex systems', *Dependability*, 20(1), pp. 57–67 (in Russ.). doi: 10.21683/1729-2646-2020-20-1-57-67.
5. Kostin, V., Borovsky, A. (2020) 'Definition of basic violators for critically important objects using the information probability method and cluster analysis', *CEUR Workshop Proc. Proc. ITNT*, 2667, pp. 343–347.
6. Yu, H., Li, X., Song, W., Zhang, J. et al. (2022) 'Pedestrian emergency evacuation model based on risk field under attack event', *Physica A: Statistical Mechanics and its Applications*, 606, art. 128111. doi: 10.1016/j.physa.2022.128111.
7. Pavlov, V.N., Kakadiy, I.I. (2020) 'Threats to the security of an educational institution', *Bull. of Sci. and Pract.*, 6(6), pp. 305–311 (in Russ.). doi: 10.33619/2414-2948/55/40.
8. Zolotukhin, M.A. (2018) 'Concept of safety of educational space', *Tech. and Technological Problems of the Service*, (1), pp. 117–120 (in Russ.).
9. Chetverushkin, B.N., Osipov, V.P., Baluta, V.I., Yakovenko, O. Yu. (2019) 'Supercomputer modeling in the problems of anti-terrorist security of objects', *Proc. Int. Conf. CPT2019*, pp. 40–49 (in Russ.).
10. Osipov, V.P., Chetverushkin, B.N., Baluta, V.I., Nechayev, Yu.I. (2018) 'The formal apparatus of simulation and interpretation antagonistic conflicts on the base of an electronic polygon', *Keldysh Institute Preprints*, (181), pp. 1–28 (in Russ.). doi: 10.20948/prepr-2018-181.
11. Nechaev, Yu.I., Osipov, V.P., Chetverushkin, B.N., Baluta, V.I. (2018) 'Ontological synthesis of management decisions in conditions of antagonistic conflicts', *Keldysh Institute Preprints*, (179), pp. 1–22 (in Russ.). doi: 10.20948/prepr-2018-179.
12. Galiullin, M.E. (2015) 'Creation and use of a spatial information model of a building (SIM) for calculating the magnitude of risk when compiling a fire safety declaration', *Proc. Safety in Technosphere*, (9), pp. 59–80 (in Russ.).
13. Kolodkin, V.M., Boltachev, I.I. (2022) 'Information model of the building of an educational institution for a decision support system', *Proc. Safety in Technosphere*, (15), pp. 75–79 (in Russ.).
14. Kolodkin, V.M., Chirkov, B.V. (2020) 'Validation of the model of adaptive control of the pedestrian flow movement in a dynamic space-limited environment', *The Bull. of Udmurt University. Math. Mech. Comput. Sci.*, 30(3), pp. 480–496 (in Russ.). doi: 10.35634/vm200309.
15. Kolodkin, V.M., Chirkov, B.V. (2016) 'Computer research of evacuation processes of people from building in case fire', *Tech. Sci.*, (12-3), pp. 496–500 (in Russ.).

Авторы

Колодкин Владимир Михайлович¹, д.т.н., профессор, kolodkin@rintd.ru

Варламова Дина Михайловна¹, старший преподаватель, dina@rintd.ru

Шакиров Артем Дмитриевич¹, магистрант, artdmshakirov@gmail.com

Authors

Vladimir M. Kolodkin¹, Dr.Sc. (Engineering), Professor, kolodkin@rintd.ru

Dina M. Varlamova¹, Senior Lecturer, dina@rintd.ru

Artem D. Shakirov¹, Graduate Student, artdmshakirov@gmail.com

¹ Удмуртский государственный университет, г. Ижевск, 426034, Россия

¹ Udmurt State University, Izhevsk, 426034, Russian Federation



В. М. Колодкин, д-р техн. наук, **Д. М. Варламова**, **А. Д. Шакиров**
(Удмуртский государственный университет, Ижевск, Россия);
e-mail: kolodkin@rintd.ru

РАСПРЕДЕЛЕНИЕ РЕСУРСОВ НА ОБЕСПЕЧЕНИЕ АНТИТЕРРОРИСТИЧЕСКОЙ БЕЗОПАСНОСТИ СОЦИАЛЬНО ЗНАЧИМЫХ ОБЪЕКТОВ

Представлен новый программный комплекс – электронный полигон, – предназначенный для повышения антитеррористической защищенности социально значимых объектов. Комплекс поддерживает математическое моделирование антагонистического конфликта между нарушителем и реципиентами риска в условиях террористической атаки.

В основе комплекса лежит авторская методология повышения защищенности, основанная на противодействии террористической атаке управляемым движением людских потоков (управляемая эвакуация) в зоны безопасности по безопасным траекториям.

Активная защита реципиентов риска в условиях атаки учитывает возможности инженерно-технических средств защиты. Алгоритмы моделирования управляемого движения строятся на минимизации ущерба реципиентов риска в условиях террористической атаки. Активная защита целесообразна при временном горизонте атаки порядка 10 минут.

Важнейшая особенность представленного электронного полигона – проектирование траекторий движения реципиентов риска в автоматическом режиме с учетом динамики развития террористической атаки.

Цифровая модель объекта защиты строится с использованием отечественной BIM-системы (Building Information Modeling) Renga. Для моделирования активности нарушителя и движения людских потоков в режиме реального времени модель здания представляется в виде топологического графа.

Количественная оценка уровня террористической безопасности каждого социально значимого объекта основана на сопоставлении уровней угроз и защищенности. Соответствие уровня защищенности уровню угроз является определяющим для выделения совокупности объектов, система защиты которых требует модернизации.

Программный комплекс ориентирован на решение практических задач, в частности распределения ограниченных ресурсов, выделяемых на повышение антитеррористической безопасности. Практическая направленность электронного полигона продемонстрирована на примере распределения средств на модернизацию системы антитеррористической защищенности корпусов образовательного учреждения.

Ключевые слова: система антитеррористической защищенности; математическое моделирование; антагонистический конфликт; динамическая модель.

V. M. Kolodkin, D. M. Varlamova, A. D. Shakirov
(Udmurt State University, Izhevsk, Russia)

DISTRIBUTION OF RESOURCES TO ENSURE ANTI-TERRORIST SECURITY OF SOCIALLY SIGNIFICANT FACILITIES

A new software package – electronic testing ground – designed to increase the anti-terrorist protection of socially significant objects is presented. The complex supports mathematical modeling of antagonistic conflict between the offender and risk recipients in the context of a terrorist attack.

The complex is based on the author's methodology for increasing security, based on countering a terrorist attack through the controlled movement of human flows (controlled evacuation) to security zones along safe trajectories. Active protection of risk recipients under attack conditions takes into account the capabilities of engineering and technical means of protection. Algorithms for modeling controlled movement are built on the conditions of minimizing damage to risk recipients in conditions of a terrorist attack. Active protection is advisable when the attack time horizon is about 10 minutes. The most important feature of the presented electronic test site is the design of movement trajectories of risk recipients in automatic mode, taking into account the dynamics of the development of a terrorist attack.

A digital model of the protected object is built using the domestic BIM system Renga. To simulate the activity of the intruder and the movement of human flows in real time the building model is represented as a topological graph.

Quantitative assessment of the level of terrorist security of each socially significant object is based on a comparison of the levels of threats and security. Correspondence between the level of security and the level of threats is decisive for identifying a set of objects whose protection system requires modernization.

The software package is focused on solving practical problems. In particular, the distribution of limited resources allocated to improve anti-terrorist security. The practical orientation of the electronic training ground is demonstrated by the example of the distribution of funds for the modernization of the anti-terrorism security system for the buildings of an educational institution.

Keywords: Anti-terrorism security system; Mathematical modeling; Antagonistic conflict; Dynamic model.

Статья поступила в редакцию 26.10.2023 г.

Введение

Происходящие в мире изменения сопровождаются возрастанием террористической угрозы, которая затрагивает и *социально значимые объекты (СЗО)*: объекты образования, здравоохранения, коммунальной инфраструктуры и т.д. На возрастание угроз СЗО реагируют организационными мероприятиями, модернизацией инженерно-технических средств защиты, развитием систем поддержки принятия решений в условиях чрезвычайных ситуаций и т.д. [1, 2]. Возрастание уровня угроз требует соответствующего повышения уровня антитеррористической защищенности.

В отношении критически важных объектов концепция обеспечения террористической безопасности развивалась в многочисленных работах [3, 4]. В основе концепции лежит метод вероятностно-временного анализа. Полагается, что безопасность критически важного объекта обеспечена, если силы реагирования успевают пресечь акцию нарушителя до достижения нарушителем уязвимых зон объекта.

Для социально значимых объектов данная концепция в исходном варианте неприемлема по ряду причин, в первую очередь – экономических. Для СЗО более конструктивен риск-ориентированный подход [5], в соответствии с которым защищенность объекта тем выше, чем больше величина предотвращенного риска при террористической атаке.

Отметим, что в данной работе не рассматриваются сценарии предупреждения террористической атаки. Учитывая, что террористическая атака на СЗО обычно развивается на временном горизонте порядка 10 мин, одним из наиболее значимых факторов в увеличении предотвращенного риска становится целенаправленная активность реципиентов риска, под-

держанная инженерно-техническими средствами обеспечения безопасности объекта (активное противодействие реципиентов риска в условиях атаки).

Модель антагонистического конфликта между нарушителем и реципиентами риска при атаке [6] должна учитывать динамику активности реципиентов риска и нарушителей, характеристики участников конфликта, параметры инженерно-технических средств защиты и т.д.

Отметим, что каждый из объектов располагает той или иной системой обеспечения безопасности в условиях чрезвычайных ситуаций, которые различаются в силу неодинаковых возможностей, в первую очередь финансовых.

Особенность террористической угрозы заключается в значимой неопределенности локализации места и времени проявления. Неопределенность локализации угрозы в отношении СЗО обуславливает требование повышения усредненной по отношению к совокупности объектов антитеррористической защищенности.

С развитием инженерно-технических средств защиты теоретически возможно построение системы обеспечения безопасности, отвечающей самым высоким требованиям. Но высокие затраты на систему защиты допускают построение близкой к идеалу системы лишь для отдельно взятого объекта или для ограниченной совокупности объектов.

Предугадать направление террористической атаки затруднительно [7]. Поэтому модернизация системы антитеррористической защищенности должна касаться той части социально значимых объектов, которые наименее защищены и в наибольшей степени подвержены угрозам. При этом должны быть учтены реалии каждого объекта и существующие ограничения ресурсов, поскольку число объектов велико.

Таким образом, требование повышения антитеррористической защищенности социально значимых объектов актуализирует решение следующих задач.

1. Определение совокупности социально значимых объектов, системы обеспечения террористической безопасности которых требуют первоочередной модернизации, с учетом состояния систем защиты и имеющихся ресурсов.

2. Проектирование улучшающих воздействий при модернизации инженерно-технических средств защиты для каждого из объектов.

Рассмотрим первую задачу. Для ее решения необходимо:

- определиться с факторами, влияющими на уровень террористической угрозы;
- определиться с уровнем антитеррористической защищенности каждого из объектов защиты;
- ранжирование совокупности объектов по количественным оценкам отношений уровней угроз и защищенности. Это позволяет выделить множество СЗО, система обеспечения антитеррористической безопасности которых требует модернизации, и определиться с относительным распределением ресурсов на модернизацию.

Алгоритм моделирования антагонистического конфликта

В модели антагонистического конфликта на социально значимом объекте рассмотрению подлежат два взаимосвязанных процесса, определяющих последствия террористической атаки:

- действия нарушителя;
- действия реципиентов риска, реагирующих на атаку.

Процессы моделируются в рамках электронного полигона [6]. Действия нарушителя при атаке отвечают модели нарушителя. Частота проявления конфликта – террористической атаки – соответствует уровню террористической угрозы.

В условиях временного горизонта террористической атаки порядка 10 мин наиболее значимым механизмом реагирования на террористическую атаку СЗО является управляемое перемещение реципиентов риска в зоны безопасности (экстренная эвакуация реципиентов риска) по безопасным путям [8]. Количественная характеристика реагирования реципиентов риска – предотвращенный ущерб при атаке – совместно с частотой проявления ущерба соответствуют

количественной оценке защищенности (оценке предотвращенного риска).

Распределение ограниченных ресурсов на первоочередную модернизацию систем обеспечения безопасности совокупности социально значимых объектов предполагает:

- количественную оценку уровня террористической угрозы для каждого СЗО;
- количественную оценку уровня защищенности каждого СЗО;
- оценку соответствия уровней угроз и уровней защищенности совокупности объектов;
- ранжирование объектов по оценкам соответствия;
- распределение средств на модернизацию системы безопасности в соответствии со списком ранжированных объектов и с учетом существующих финансовых ограничений.

В дальнейшем распределение ресурсов на повышение защищенности проиллюстрируем на примере совокупности корпусов одного из образовательных учреждений. Программное обеспечение электронного полигона моделирования антагонистического конфликта допускает анализ практически неограниченной совокупности СЗО. Однако для целей иллюстрации ограничимся анализом объектов, входящих в совокупность из шести объектов.

Количественная оценка уровня террористической угрозы

К основным численным характеристикам N_k , влияющим на уровень террористических угроз, можно отнести следующие [2, 9, 10]:

N_1 – число человек в здании, чел.;

N_2 – срок службы здания, лет;

N_3 – плотность людей в здании, чел./м²;

N_4 – численность населения в районе расположения объекта защиты, чел.;

N_5 – общий уровень преступности в районе расположения объекта защиты.

В общем случае для достоверного прогнозирования уровня угрозы (привлекательности объекта защиты для нарушителя) требуется большое количество характеристик объекта. Однако при выборе характеристик, определяющих уровень угрозы, необходимо учитывать, что информация по объекту защиты должна быть такой, чтобы нарушитель не обратил ее против реципиентов риска на объекте.

Террористическая угроза для i -го объекта характеризуется параметрами (критериями) $\{(f_k)_i \mid k = 1, m; i = 1, n\}$, определяющими его привлекательность для нарушителя, где n – число объектов защиты в совокупности; m – число критериев. Количественные значения критериев $(f_k)_i$ определяются через численные значения соответствующих характеристик i -го объекта $(N_k)_i$

$$(f_k)_i = (N_k)_i / \langle N_k \rangle,$$

где $\langle N_k \rangle$ – среднее значение k -й характеристики для рассматриваемой совокупности объектов.

В данном случае для i -го объекта защиты имеем пять количественных характеристик террористической угрозы ($m = 5$). Критерии соотношены к средним значениям характеристик по совокупности объектов. Чем больше значение критерия, тем больше влияние критерия на угрозу по отношению к среднему значению. Значения параметров f_k , где $k = 1, \dots, 5$, образуют фигуру площадью $S(f_1, f_2, f_3, f_4, f_5)$. Фигура с площадью $S_0(f_1 = 1, f_2 = 1, f_3 = 1, f_4 = 1, f_5 = 1)$ соотносится со средними по совокупности объектов защиты характеристиками угроз.

Будем характеризовать уровень угрозы по отношению к i -му объекту совокупности значением y_i :

$$y_i = S(f_1, f_2, f_3, f_4, f_5) / S_0(f_1 = 1, f_2 = 1, f_3 = 1, f_4 = 1, f_5 = 1),$$

где $S(f_1, f_2, f_3, f_4, f_5) = 0,5 \sin(2\pi/m)(f_1 f_2 + f_2 f_3 + f_3 f_4 + f_4 f_5 + f_5 f_1)$.

Множество оценок уровня угроз обозначим $Y = \{y_i \mid i = 1, n\}$, где y_i – количественная оценка уровня террористической угрозы для i -го объекта защиты.

В рассматриваемом случае совокупность объектов защиты состоит из объектов одного типа (корпуса образовательного учреждения), все объекты расположены компактно, следовательно, численные значения характеристик N_4, N_5 и соответствующих критериев $\{(f_4)_i \mid i = 1, n\}, \{(f_5)_i \mid i = 1, n\}$ совпадают для всех объектов совокупности.

Численные значения характеристик и значения соответствующих параметров следующие:

– $N_4 = 128\,405$ чел. (численность населения Индустриального района Ижевска [11], где расположены корпуса образовательного учреждения), $f_4 = 1$;

– $N_5 = 9532$ случая (краткая характеристика состояния преступности на территории Ижевска [12]), $f_5 = 1$.

В табл. 1 представлены исходные численные значения характеристик (корпуса 1, 2, 3, 4, 5, 7 [8]) и расчетных параметров для совокупности объектов защиты $i = 1, \dots, 6$.

Из анализа данных (см. табл. 1) следует, что наибольший уровень террористической угрозы соотносится с корпусом № 4, наименьший уровень – с корпусом № 3.

Количественная оценка уровня защищенности

Определяющая часть оценки уровня защищенности при террористической атаке на временном горизонте порядка 10 мин связана с величиной предотвращенного риска. Реципиенты риска реагируют на атаку целенаправленным перемещением в зоны безопасности по безопасным путям (управляемая эвакуация), чему призваны способствовать инженерно-технические средства защиты.

К факторам (критериям), определяющим уровень антитеррористической защищенности СЗО при террористической атаке, в первую очередь, относятся:

- уровень подготовленности реципиентов риска к действиям (активная защита) в условиях террористической атаки;
- уровень подготовленности персонала объекта и сотрудников привлекаемых служб к действиям в условиях террористической атаки;
- уровень информационной безопасности объекта защиты;
- уровень инженерно-технической защищенности.

1. Оценка террористической угрозы

| Объект защиты | Исходные данные | | | Расчетные данные | | | |
|---------------|-----------------|-------|-------|------------------|-------|-------|-------|
| | N_1 | N_2 | N_3 | f_1 | f_2 | f_3 | y_i |
| 1 | 1974 | 57 | 0,21 | 1,26 | 0,95 | 1,09 | 1,11 |
| 2 | 1949 | 92 | 0,26 | 1,24 | 1,53 | 1,34 | 1,51 |
| 3 | 158 | 106 | 0,07 | 0,10 | 1,76 | 0,36 | 0,46 |
| 4 | 3177 | 64 | 0,28 | 2,02 | 1,06 | 1,45 | 1,63 |
| 5 | 1105 | 30 | 0,18 | 0,70 | 0,50 | 0,93 | 0,69 |
| 6 | 1072 | 12 | 0,16 | 0,68 | 0,20 | 0,83 | 0,56 |

Так как анализу подлежит совокупность объектов одного типа (корпуса одного образовательного учреждения), то в первом приближении численные значения соответствующих характеристик и критериев совпадают для всех объектов совокупности: $\{(f_1)_i = const \mid i = \overline{1, n}\}$, $\{(f_2)_i = const \mid i = \overline{1, n}\}$, $\{(f_3)_i = const \mid i = \overline{1, n}\}$. Численные значения критериев следующие: $f_1 = 1, f_2 = 1, f_3 = 1$.

Уровень инженерно-технической защищенности СЗО будем характеризовать относительной величиной предотвращенного риска R при террористической атаке на СЗО – $R(T)/N_0$, где N_0 – число реципиентов риска перед началом террористической атаки, T – продолжительность террористической атаки.

Временной интервал освобождения здания реципиентами риска при эвакуации удовлетворительно описывается регрессионной зависимостью [8]

$$T_e = 115,45 + 725,76D + 103,38\Omega, \quad (1)$$

где D , [чел./м²] – плотность реципиентов риска в здании в момент начала террористической атаки;

Ω – топологическая сложность здания, рассчитывается на основании пространственно-информационной модели здания, представленной в виде графа.

По результатам вычислительных экспериментов эвакуации людей из зданий [13], имеем верхнюю оценку

$$\frac{N(T)}{N_0} = \exp\left\{-\chi \frac{T}{T_e}\right\}, \quad \chi = 2,043,$$

где $N(T)$ – оценка числа реципиентов риска, оставшихся в здании к концу террористической атаки.

Оценка предотвращенного ущерба $U = (N_0 - N(T))$ при террористической атаке представляется выражением

$$U = N_0 \left(1 - \frac{N(T)}{N_0}\right) = N_0 \left(1 - \exp\left\{-\chi \frac{T}{T_e}\right\}\right). \quad (2)$$

При прогнозировании последствий террористической атаки на СЗО моделируются два процесса:

- движение нарушителя, отвечающее соответствующей модели нарушителя;
- направленное движение реципиентов риска в зоны безопасности по безопасным путям, отвечающее теории людских потоков [14, 15].

Процессы моделируются в рамках специализированного программного комплекса – электронного полигона. Для моделирования используется пространственно-информационная модель (ПИМ) здания. Цифровая модель здания создается в BIM-системе (Building Information Modeling) Renga. ПИМ здания, представляемая Json-файлом [16], создается специализированным плагином. При моделировании атаки в здании используется топологический граф (рис. 1). Вершины топологического графа отвечают помещениям здания, ребра – проемам.

На каждом временном шаге τ моделируется перемещение нарушителя по связанным вершинам топологического графа в направлении уменьшения уровня топологического графа. Для нарушителя выбор пути отвечает модели максимального поражения реципиентов риска. Террористическая атака заканчивается, если нарушитель, двигаясь со скоростью $v = 100$ м/мин, достигает последнего помещения здания, что соответствует последней вершине топологического графа. Отметим, что это одна из возможных моделей поведения нарушителя. Обычно расчет поддерживается несколькими моделями, отвечающими за анализ террористических атак [17].

Вершины графа по пути движения нарушителя не доступны реципиентам риска, т.е. траектории движения реципиентов риска, отвечающие кратчайшему по времени пути, перестраиваются по мере развития террористической атаки. Для определения траекторий перемещения реципиентов риска на каждом интервале моделирования используется волновой алгоритм. Процесс перемещения реципиентов риска поддерживается инженерно-техническими средствами защиты – системами связи, оповещения и т.д.

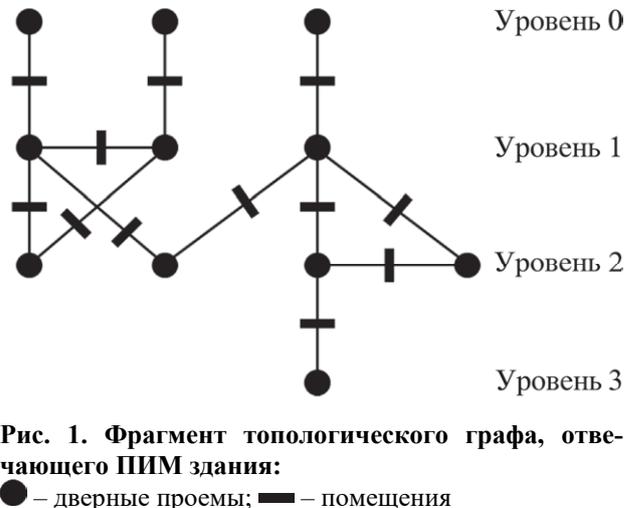


Рис. 1. Фрагмент топологического графа, отвечающего ПИМ здания:
● – дверные проемы; ■ – помещения

Переходя от предотвращенного ущерба (2) к величине предотвращенного риска, в рассматриваемом случае имеем следующее выражение:

$$R = \sum_{m=1}^{m^*} \sum_{b=1}^{b^*} \sum_k v_m v_b P_k^{con} N_0 \times \left\{ P_k^{det} \left[1 - \exp\left(-\chi \frac{\tau^{(k)}}{T_e}\right) \right] \right\},$$

где P_k^{det} – вероятность обнаружения нарушителя в помещениях здания;

P_k^{con} – вероятность корректной работы системы управления людскими потоками в условиях террористической атаки;

v_m – частота проявления m -й модели нарушителя;

m^* – число возможных моделей нарушителя;

v_b – частота атаки нарушителя через b -й вход в здание;

b^* – число возможных сценарий начала атаки в здании;

k – номер шага моделирования.

Если принять в первом приближении

$$\sum_{k=1} U^{(k)}(\tau^{(k)}) \approx U\left(\sum_{k=1} \tau^{(k)}\right),$$

то верхняя оценка предотвращенного риска R при террористической атаке

$$R = N_0 \left(1 - \exp\left(-\chi \frac{T}{T_e}\right) \right).$$

Уровень инженерно-технической защищенности СЗО характеризуется величиной $R(T)/N_0$. Множество оценок уровня антитеррористической защищенности – $Z = \{z_i \mid i = \overline{1, n}\}$, где z_i – количественная оценка уровня антитеррористической защищенности людей i -го социально значимого объекта совокупности:

$$z_i = S(f_1, f_2, f_3, f_4) / S_0(f_1 = 1, f_2 = 1, f_3 = 1, f_4 = 1),$$

где $S(f_1, f_2, f_3, f_4) = 0,5 \sin(2\pi/4)(f_1 f_2 + f_2 f_3 + f_3 f_4 + f_4 f_1)$.

В табл. 2 представлены численные значения характеристик (корпуса 1, 2, 3, 4, 5, 7): D , [чел./м²] – плотность реципиентов риска в здании в момент начала террористической атаки [8]; Ω – топологическая сложность здания [8].

2. Оценка защищенности

| Объект защиты | Исходные данные | | Расчетные данные | |
|---------------|-----------------|----------|------------------|-------|
| | D | Ω | R/N_0 | z_i |
| 1 | 0,079 | 1,36 | 0,617 | 0,99 |
| 2 | 0,102 | 0,84 | 0,633 | 1,00 |
| 3 | 0,071 | 0,32 | 0,380 | 0,84 |
| 4 | 0,126 | 1,84 | 0,789 | 1,09 |
| 5 | 0,030 | 0,95 | 0,753 | 1,07 |
| 6 | 0,046 | 0,81 | 0,645 | 1,01 |

Ранжирование социально значимых объектов

Для i -го социально значимого объекта уровень антитеррористической защищенности характеризуется оценкой соответствия

$$q_i = y_i / z_i.$$

При $q_i > 1$ уровень угрозы превышает уровень защищенности, т.е. требуется усиление системы обеспечения безопасности. При $q_i < 1$ усиление системы безопасности в общем случае нецелесообразно.

Потребность в модернизации системы обеспечения безопасности зависит от соотношения между уровнями угроз и защищенности. Эффективность системы безопасности СЗО будет приемлемой, если уровень угроз будет соответствовать уровню защищенности. Модернизация системы обеспечения безопасности целесообразна в отношении объектов, для которых $\delta_i = q_i - 1 > 0$.

Положим, что I – множество социально значимых объектов, для которых целесообразна модернизация системы обеспечения безопасности:

$$q_i > 1 \quad \forall i \in I.$$

Потребность в модернизации системы безопасности i -го объекта тем выше, чем больше $\delta_i = q_i - 1$ при $\delta_i > 0$. Если i^* – число СЗО, отвечающих условию $q_i > 1$, то уровень антитеррористической защищенности совокупности социально значимых объектов будет тем выше, чем меньше значение целевой функции F :

$$F = \sum_{i=1}^{i^*} (q_i - 1) \rightarrow \min.$$

3. Распределение ресурсов на обеспечение безопасности

| Объект защиты | Расчетные параметры | | | | |
|---------------|---------------------|-------|-------|------------|----------------|
| | y_i | z_i | q_i | δ_i | $\omega_i, \%$ |
| 1 | 1,11 | 0,99 | 1,13 | 0,13 | 11,10 |
| 2 | 1,51 | 1,00 | 1,51 | 0,51 | 45,24 |
| 3 | 0,46 | 0,84 | 0,54 | – | – |
| 4 | 1,63 | 1,09 | 1,49 | 0,49 | 43,66 |
| 5 | 0,69 | 1,07 | 0,64 | – | – |
| 6 | 0,56 | 1,01 | 0,56 | – | – |

Идеальный случай, когда для всех объектов защиты $q_i = 1$, при этом значение целевой функции $F = 0$.

Если ω_i – затраты на модернизацию системы безопасности i -го социально значимого объекта, а W – величина средств, выделяемых на модернизацию систем безопасности совокупности объектов, то

$$W = \sum_{i=1}^i \omega_i \forall i \in I, q_i > 1.$$

Затраты на модернизацию системы обеспечения безопасности i -го социально значимого объекта будут отвечать выражению

$$\omega_i = q_i \frac{W}{F} \forall i \in I, q_i > 1.$$

Табл. 3 иллюстрирует алгоритм распределения средств на модернизацию системы безопасности для рассматриваемой совокупности СЗО (корпуса образовательного учреждения).

Из данных табл. 3 следует, что средства на модернизацию системы антитеррористической защищенности корпусов образовательного учреждения подлежат распределению в отношении $\omega_2:\omega_4:\omega_1 = 45,24:43,66:11,10$. Для объектов с $q_i < 1$ получается $\delta_i < 0$, следовательно, нет необходимости в их модернизации.

Заключение

По ряду причин происходит возрастание террористической опасности для реципиентов риска социально значимых объектов. Возрастание

опасности требует незамедлительного повышения уровня антитеррористической защищенности. Этой цели служит предлагаемая в работе проблемно-ориентированная система, которая также направлена на сопоставление уровней террористических угроз и защищенности. Сопоставление позволяет выделить совокупность социально значимых объектов, системы обеспечения безопасности которых требуют модификации (в рассматриваемом примере это объекты защиты $i = 1, 2, 4$), и обоснованно распределить ограниченные финансовые ресурсы на модернизацию системы антитеррористической безопасности.

Библиографический список

1. Тихомиров Н. П., Новиков А. В. Риски террористических актов и особенности их оценки // Вестник Российского экономического университета имени Г. В. Плеханова. 2019. № 2. С. 198–210. DOI: 10.21686/2413-2829-2019-2-198-210
2. Павлов В. Н., Какадий И. И. Угрозы безопасности образовательного учреждения // Бюллетень науки и практики. 2020. Т. 6, № 6. С. 305–311. DOI: 10.33619/2414-2948/55/40
3. Боровский А. С., Тарасов А. Д. Интегрированный подход к разработке общей модели функционирования систем физической защиты объектов // Труды института системного анализа. 2011. Т. 61. С. 3–14.
4. Костин В. Н. Оценка потенциала опасности критически важных объектов при возникновении чрезвычайных ситуаций на основе информационно вероятностного метода и метода главных компонент // Информационные технологии. 2020. Т. 26, № 5. С. 297–301.
5. Бочков А. В. О методе синтеза рисков в управлении безопасностью структурно-сложных систем // Надежность. 2020. Т. 20, № 1. С. 1–11. DOI: 10.21683/1729-2646-2020-20-1-57-67
6. Формальный аппарат моделирования и интерпретации антагонистических конфликтов на базе электронного полигона / В. П. Осипов и др. // Препринты ИПМ им. М.В. Келдыша. 2018. № 181. 28 с. DOI:10.20948/prepr-2018-181
7. Бецков А. В., Осташкевич В. А., Ранюк М. А. Методологические подходы к выявлению уязвимости социально важных объектов террористическим угрозам // Труды международного симпозиума «Надежность и качество». 2017. Т. 2. С. 307–310.
8. Колодкин В. М., Чирков Б. В. Валидация модели адаптивного управления движением людских потоков в динамической среде ограниченного пространства // Вестник Удмуртского университета. Математика. Механика. Компьютерные науки. 2020. Т. 30(3). С. 480–496. DOI: 10.35634/vm200309

9. **Постановление Правительства РФ** от 02.08.2019 № 1006 (ред. от 05.03.2022) «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)». URL: <http://government.ru/docs/all/123336/> (дата обращения: 19.12.2023).

10. **Постановление Правительства РФ** от 07.11.2019 № 1421 (ред. от 04.04.2023) «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства науки и высшего образования РФ и подведомственных ему организаций, объектов (территорий), относящихся к сфере деятельности Министерства науки и высшего образования РФ, формы паспорта безопасности этих объектов (территорий) и признании утратившими силу некоторых актов Правительства РФ». URL: <http://government.ru/docs/all/124509/> (дата обращения: 19.12.2023).

11. **Демографическая ситуация:** сайт. URL: <https://www.izh.ru/i/info/14842.html> (дата обращения: 05.09.2023).

12. **Краткая характеристика** состояния преступности на территории города Ижевска: сайт. URL: <https://www.izh.ru/i/info/31721.html> (дата обращения: 05.09.2023).

13. **Колодкин В. М., Чирков Б. В.** Компьютерное исследование процесса эвакуации людей из здания при пожаре // *Современные наукоемкие технологии*. 2016. № 12, Ч. 3. С. 496–500.

14. **Холщевников В. В.** Гносеология людских потоков. М.: Академия ГПС МЧС России, 2019. 592 с.

15. **Самошин Д. А.** Состав людских потоков и параметры их движения при эвакуации. М.: Академия ГПС МЧС России, 2016. 210 с.

16. **Колодкин В. М., Болтачев И. И.** Информационная модель здания образовательного учреждения для системы поддержки принятия решений // *Безопасность в техносфере: сб. статей*. 2022. № 15. С. 75–79.

17. **Нападения** на учебные заведения России. URL: https://ru.wikipedia.org/wiki/Нападения_на_учебные_заведения_в_России (дата обращения: 05.09.2023).

References

1. Tihomirov N. P., Novikov A. V. (2019). Risks of terrorist acts and features of their assessment. *Vestnik Rossiyskogo ekonomicheskogo universiteta imeni G. V. Plekhanova*, (2), 198 – 210. [in Russian language] DOI: 10.21686/2413-2829-2019-2-198-210

2. Pavlov V. N., Kakadiy I. I. (2020). Threats to the security of an educational institution. *Byulleten' nauki i*

praktiki, 6(6), 305 – 311. [in Russian language] DOI: 10.33619/2414-2948/55/40

3. Borovskiy A. S., Tarasov A. D. (2011). An integrated approach to the development of a general model for the functioning of physical protection systems for objects. *Trudy instituta sistemnogo analiza*, 61, 3 – 14. [in Russian language]

4. Kostin V. N. (2020). Assessment of the hazard potential of critical objects in the event of emergency situations based on the information probabilistic method and the principal component method. *Informatsionnye tekhnologii*, 26(5), 297 – 301. [in Russian language]

5. Bochkov A. V. (2020). On the method of risk synthesis in safety management of structurally complex systems. *Nadezhnost'*, 20(1), 1 – 11. [in Russian language] DOI: 10.21683/1729-2646-2020-20-1-57-67

6. Osipov V. P. et al. (2018). A formal apparatus for modeling and interpreting antagonistic conflicts based on an electronic test site. *Preprinty IPM im. M.V. Keldysha*, 181. [in Russian language] DOI:10.20948/prepr-2018-181

7. Betskov A. V., Ostashkevich V. A., Ranyuk M. A. (2017). Methodological approaches to identifying the vulnerability of socially important objects to terrorist threats. *Trudy mezhdunarodnogo simpoziuma «Nadezhnost' i kachestvo»*, 2, 307 – 310. [in Russian language]

8. Kolodkin V. M., Chirkov B. V. (2020). Validation of a model for adaptive control of human flows in a dynamic environment of limited space. *Vestnik Udmurtskogo universiteta. Matematika. Mekhanika. Komp'yuternye nauki*, 30(3), 480 – 496. [in Russian language] DOI: 10.35634/vm200309

9. *Decree of the Government of the Russian Federation No. 1006 "On approval of requirements for anti-terrorist protection of objects (territories) of the Ministry of Education of the Russian Federation and objects (territories) related to the sphere of activity of the Ministry of Education of the Russian Federation, and the form of a safety passport for these objects (territories)."* Retrieved from <http://government.ru/docs/all/123336/> (Accessed: 19.12.2023). [in Russian language]

10. *Decree of the Government of the Russian Federation No. 1421 "On approval of requirements for anti-terrorist protection of objects (territories) of the Ministry of Science and Higher Education of the Russian Federation and subordinate organizations, objects (territories) related to the scope of activity of the Ministry of Science and Higher Education of the Russian Federation, forms of safety passports for these objects (territories)) and the recognition of certain acts of the Government of the Russian Federation as invalid."* Retrieved from <http://government.ru/docs/all/124509/> (Accessed: 19.12.2023). [in Russian language]

11. *Demographic situation: website*. Retrieved from <https://www.izh.ru/i/info/14842.html> (Accessed: 05.09.2023). [in Russian language]

12. *Brief description of the state of crime in the city of Izhevsk: website*. Retrieved from <https://www.izh.ru/i/info/14842.html>

izh.ru/i/info/31721.html (Accessed: 05.09.2023). [in Russian language]

13. Kolodkin V. M., Chirkov B. V. (2016). Computer study of the process of evacuating people from a building in case of fire. *Sovremennye naukoemkie tekhnologii*, (12), part 3, 496 – 500. [in Russian language]

14. Holshchevnikov V. V. (2019). *Epistemology of human flows*. Moscow: Akademiya GPS MChS Rossii. [in Russian language]

15. Samoshin D. A. (2016). *Composition of human flows and parameters of their movement during evacua-*

tion. Moscow: Akademiya GPS MChS Rossii. [in Russian language]

16. Kolodkin V. M., Boltachev I. I. (2022). Information model of an educational institution building for a decision support system. *Bezopasnost' v tekhnosfere: sbornik statey*, 15, 75 – 79. [in Russian language]

17. *Attacks on Russian educational institutions*. Retrieved from https://ru.wikipedia.org/wiki/Нападения_на_учебные_заведения_в_России (Accessed: 05.09.2023). [in Russian language]

При цитировании использовать:

Колодкин В. М., Варламова Д. М., Шакиров А. Д. Распределение ресурсов на обеспечение антитеррористической безопасности социально значимых объектов // Вестник компьютерных и информационных технологий. 2024. Т. 21, № 1. С. 46 – 54. DOI: 10.14489/vkit.2024.01.pp.046-054

Kolodkin V. M., Varlamova D. M., Shakirov A. D. (2024). Distribution of Resources to Ensure Anti-Terrorist Security of Socially Significant Facilities. *Vestnik komp'yuternyh i informatsionnyh tekhnologiy*, 21(1), 46 – 54. [in Russian language]. DOI: 10.14489/vkit.2024.01.pp.046-054



Спектр

Издательский дом

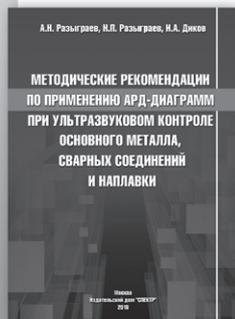
Разыграев А.Н., Разыграев Н.П., Диков И.А.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРИМЕНЕНИЮ АРД-ДИАГРАММ ПРИ УЛЬТРАЗВУКОВОМ КОНТРОЛЕ ОСНОВНОГО МЕТАЛЛА, СВАРНЫХ СОЕДИНЕНИЙ И НАПЛАВКИ

ISBN 978-5-4442-0116-9. Формат - 60x90 1/16, 78 страниц, год издания - 2016.

Настоящие «Методические рекомендации по применению АРД-диаграмм при ультразвуковом контроле основного металла, сварных соединений и наплавки» разработаны в Лаборатории диагностики атомного энергетического оборудования.

Предназначены для операторов, инженерно-технических работников по контролю основного металла, сварных соединений при изготовлении, монтаже и эксплуатации оборудования, трубопроводов и металлоконструкций, а также студентов вузов в качестве учебного пособия.



385 руб.

119048, г. Москва, ул. Усачева, д. 35, стр. 1. 000 «Издательский дом «Спектр»

Телефон отдела реализации: (495) 514-26-34. Дополнительный телефон офиса: (926) 615 17 16.

E-mail: zakaz@idspektr.ru. Http://www.idspektr.ru

www.idspektr.ru

Реклама

Министерство науки и высшего образования
Российской Федерации
ФГБОУ ВО «Удмуртский государственный университет»

МЕЖДУНАРОДНАЯ АССОЦИАЦИЯ СПЕЦИАЛИСТОВ
ПОЖАРНОЙ, ПРОМЫШЛЕННОЙ И ЭКОЛОГИЧЕСКОЙ
БЕЗОПАСНОСТИ

Безопасность в техносфере

16

УДК 004.94

ПРОЕКТИРОВАНИЕ СИМУЛЯТОРА ТЕРРОРИСТИЧЕСКОЙ АТАКИ НА ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

В.М. Колодкин, Н.В. Белкин, А.Д. Шакиров

Удмуртский Государственный Университет, г. Ижевск, Россия

e-mail: kolodkin@rintd.ru, nik.belkin.01@yandex.ru,

artdmshakirov@gmail.com

В работе представлен прототип симулятора, предназначенного для подготовки и переподготовки учащихся и сотрудников образовательных учреждений к действиям в условиях террористической атаки. В основе программного обеспечения симулятора лежит авторская система взглядов на обеспечение террористической безопасности образовательных учреждений. Показано, что программное обеспечение симулятора служит основой системы поддержки принятия решений при террористической атаке.

Ключевые слова: Обучение персонала, система поддержки принятия решений, противодействие терроризму, образовательные учреждения, программное обеспечение.

Основная часть

Современный этап развития общества характеризуется возрастанием уровня и разнообразием угроз (террористических, криминальных, техногенных и т.д.) [1,2]. Это относится и к образовательным учреждениям (ОУ). К разным угрозам образовательные учреждения подготовлены в разной степени. Различный уровень готовности к угрозам имеет объяснение: связанная система взглядов (концепция), направленная, например, на достижение пожарной безопасности, существует очень давно, а в части террористической безопасности только складывается. Появляются новые проявления террористической опасности, например, проявления, связанные с применением беспилотных летательных аппаратов. Общепринятой концепции обеспечения антитеррористической защищенности образовательных учреждений пока не существует. Этим объясняется растерянность, наблюдаемая сегодня среди лиц,

ответственных за безопасность, когда речь идет о повышении уровня террористической безопасности образовательных учреждений. На заседаниях всевозможных комиссий, где процветает «воинствующий дилетантизм», пытаются найти решение проблемы повышения анти-террористической защищенности образовательных учреждений, путем голосования.

Концепция обеспечения террористической безопасности критически-важных объектов развивалась в многочисленных работах, например, - [3, 4]. В основе концепции лежит положение, что силы реагирования успевают пресечь террористическую атаку до того, как нарушитель достигнет критически важной зоны объекта. По ряду причин данная концепция террористической безопасности неприемлема для образовательных учреждений. Значимая террористическая атака, направленная против образовательного учреждения, с высокой вероятностью, не может быть ликвидирована силами учреждения. Но последствия атаки (ущерб) могут быть существенно уменьшены, если реципиенты риска (учащиеся и сотрудники, в том числе и лица, уполномоченные принимать решения в условиях ЧС), оказавшиеся в здании образовательного учреждения во время атаки, будут подготовлены к реагированию на атаку. Целям подготовки и переподготовки сотрудников и обучающихся в части реагирования на террористическую атаку служит симулятор террористической атаки. Программное обеспечение симулятора построено на основе реализации авторской концепции активного противодействия террористической атаке в зданиях образовательных учреждений.

Отметим, что научно-технические достижения теоретически позволяют обеспечить высокий уровень безопасности образовательных учреждений. Но это требует неприемлемых для общества затрат. Образовательные учреждения находятся в разных условиях по отношению к угрозам возникновения чрезвычайных ситуаций; учреждения различаются по уровню готовности к реагированию на атаку. В этой связи, требование времени о повышении антитеррористической защищенности ОУ, требует учета индивидуальных особенностей каждого образовательного учреждения и учета возможностей систем обеспечения безопасности, существующих в той или иной форме в каждом образовательном учреждении.

Уровень террористической угрозы для объекта защиты в определяющей степени определяется его «привлекательностью» для нарушителя [5]. Одна из существенных характеристик защищенности образовательного учреждения - величина предотвращенного риска [6,7] при террористической атаке. Уровень террористической безопасности объекта защиты будет определяться отношением между уровнями угроз и защищенности. Чем выше отношение, тем большее внимание требуется уделять системе обеспечения террористической безопасности.

Если ограничиться рассмотрением временного горизонта террористической атаки на уровне 10 минут, то наиболее значимым механизмом обеспечения безопасности людей является целенаправленное перемещение реципиентов риска в безопасные зоны здания (управляемая эвакуация реципиентов риска). Величина предотвращенного ущерба при атаке, фактически, определяется количеством реципиентов риска, которым удалось достичь зон безопасности в условиях террористической атаки.

Необходимо учесть, что террористическая атака может развиваться по сценарию, который сложно предсказать. Поэтому прогнозирование последствий террористической атаки должно базироваться на вероятностно-временном анализе двух процессов:

- процесса, направленного на нанесение ущерба при террористической атаке, обусловленного действием нарушителя;
- процесса, направленного на увеличение предотвращенного ущерба, обусловленного скоординированными действиями реципиентов риска.

Соответственно и программное обеспечение симулятора террористической атаки должно поддерживать математическое моделирование антагонистического конфликта между нарушителем и реципиентами риска. Симулятор поддерживает математическое моделирование активности нарушителя(ей) [8]. Симулятор обеспечивает проектирование траекторий перемещения реципиентов риска по безопасным путям (траектории перемещения людских потоков не совпадают с элементами траекторий нарушителя). Траектории отвечают условию минимума времени достижения зон безопасности [9].

Предполагается, что существующая система обеспечения безопасности в образовательном учреждении обеспечивает периодический контроль расположения нарушителя(ей) и реципиентов риска в здании. Если контроль на объекте защиты затруднен, то в момент начала террористической атаки предполагается равномерное распределение реципиентов риска по зданию. В дальнейшем распределение реципиентов риска по зданию прогнозируется на основании теории движения людских потоков [10, 11]. В рамках симулятора, траектории движения реципиентов риска в зоны безопасности здания проектируется в автоматическом режиме.

В каждый момент времени для реципиентов риска, находящихся в определённом помещении, выбирается оптимальная траектория к одному из входов в зону безопасности, с учётом анализа вышеупомянутых процессов. Траектории разделяются по типам в зависимости от входа в зону безопасности. Например, если входов в зону безопасности (в частном случае, это могут быть выходы из здания) – десять, то выделяется десять типов траекторий. Группирование траекторий одного типа облегчает визуальное восприятие симуляции и делает эффективным управление людскими потоками средствами систем оповещения.

Таким образом, моделирование сценариев атаки (распространения источников опасности), моделирование скоординированного перемещения людских потоков (реакции реципиентов риска на атаку), позволяют в рамках симулятора наглядно продемонстрировать динамику атаки и траектории движения людских потоков. Разнообразие сценариев террористических атак, обеспечивает всестороннюю подготовку реципиентов риска к действиям в условиях атаки.

Дальнейшая доработка программного обеспечения симулятора с учетом возможностей систем оповещения и управления людскими потоками при террористической атаке, позволит создать систему поддержки принятия решений.

Список литературы

1. Тихомиров Н.П., Новиков А.В. Риски террористических актов и особенности их оценки / Н.П. Тихомиров, А.В. Новиков // Вестник РЭУ. – 2019. - № 2. – С. 198–210.

2. Всероссийская научно-практическая конференция «Комплексная безопасность образовательных организаций: теория и практика»: сборник материалов / редкол.: М.В. Дулясова и др.; под общ. ред. д.э.н., проф. М.В. Дулясовой. — Уфа: Изд-во «Восточная печать», 2017. — 268 с. <https://www.chuvsu.ru/wp-content/uploads/2020/04/2.pdf>.
3. Боровский А.С., Тарасов А.Д. Интегрированный подход к разработке общей модели функционирования систем физической защиты объектов / А.С. Боровский, А.Д. Тарасов // Труды ИСА РАН. – 2011. – Т.61. – С. 3–14.
4. Костин, В. Н. Оценка потенциала опасности критически важных объектов при возникновении чрезвычайных ситуаций на основе информационно вероятностного метода и метода главных компонент / В. Н. Костин // Информационные технологии. – 2020. – Т. 26, № 5. – С. 297–301.
5. Павлов В. Н., Какадий И. И. Угрозы безопасности образовательного учреждения // Бюллетень науки и практики. 2020. Т. 6. №6. С. 305-311. <https://doi.org/10.33619/2414-2948/55/40>.
6. Бочков А.В. О методе синтеза рисков в управлении безопасностью структурно-сложных систем / А.В. Бочков // Надежность. – 2020. – Т. 20, № 1. С. 1–11.
7. Колодкин В.М., Варламова Д.М., Копелев С.М. Риск-ориентированный подход к повышению эффективности инженерных систем антитеррористической защиты // Труды XXVI Всероссийской научно-практической конференции, том 2 «Технические средства предупреждения чрезвычайных ситуаций и противодействия терроризму». Санкт-Петербург, 2023, с. 189-192.
8. Шакиров, А.Д. Моделирование движения нарушителя / А.Д. Шакиров // Безопасность в техносфере: сборник статей / науч. ред. В. М. Колодкин. – Ижевск : Удмуртский университет, 2023. – Вып. 16 – С. 34-40
9. Колодкин В.М., Чирков Б.В. Система адаптивного управления экстренной эвакуацией при пожаре в здании // Безопасность в техносфере, 2017, вып. № 4(67), С. 58-65. DOI: https://doi.org/10.12737/article_5a2907cc4f32d7.65348137.

10. Холщевников В.В. Гносеология людских потоков. Москва: Академия ГПС МЧС России, 2019. 592 с.
11. Самошин Д.А. Состав людских потоков и параметры их движения при эвакуации. М: Академия ГПС МЧС России, 2016. 210 с.

DESIGNING A SIMULATOR OF A TERRORIST ATTACK ON AN EDUCATIONAL INSTITUTION

V.M. Kolodkin, N.V.Belkin, A.D. Shakirov

Udmurt State University, 426034 Russia, Izhevsk, Universitetskaya, 1

e-mail: *kolodkin@rintd.ru, nik.belkin.01@yandex.ru,*

artdmshakirov@gmail.com

The paper presents a prototype of a simulator designed to prepare and retrain students and employees of educational institutions to act in the conditions of a terrorist attack. The simulator software is based on the author's system of views on ensuring the terrorist security of educational institutions. It is shown that the simulator software serves as the basis of a decision support system in a terrorist attack.

Keywords: Personnel training, decision support system, counter-terrorism, educational institutions, software.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
РОССИЙСКАЯ АКАДЕМИЯ РАКЕТНЫХ
И АРТИЛЛЕРИЙСКИХ НАУК



АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ И БЕЗОПАСНОСТИ

ТЕХНИЧЕСКИЕ СРЕДСТВА
ПРЕДУПРЕЖДЕНИЯ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ
И ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ

Труды XXVI Всероссийской
научно-практической конференции

Том 2



Санкт-Петербург
2023

Актуальные проблемы защиты и безопасности: Труды XXVI Всероссийской научно-практической конференции РАРАН (3–6 апреля 2023 г.).

Издание ФГБУ «Российской академии ракетных и артиллерийских наук». Москва – 2023.

Составители и редакторы:

академик РАРАН, д.т.н., профессор В.А. Петров,
член-корреспондент РАН, академик РАРАН, д.т.н., профессор М.В. Сильников,
член-корреспондент РАРАН, к.т.н., доцент А.М. Сазыкин,
академический советник РАРАН, к.т.н. А.С. Алешин.

Санкт-Петербург, 2023.

В шести томах трудов конференции представлен широкий спектр концептуальных вопросов проблем защиты и безопасности: вооружение и военная техника, оружие, в том числе нелетального действия, системы обнаружения, наведения, связи, навигации и управления подразделениями, борьба с терроризмом, обнаружение и обезвреживание взрывчатых веществ и радиоактивных веществ, безопасность особо важных объектов, ядерных центров, проблемы Военно-Морского Флота России, боевая экипировка и средства индивидуальной защиты, современные защитные материалы и конструкции, технологии их производства.

Том 1. «Перспективные направления развития вооружения, военной и специальной техники»

Том 2. «Технические средства предупреждения чрезвычайных ситуаций и противодействия терроризму»

Том 3. «Военно-Морской Флот Российской Федерации: настоящее и будущее»

Том 4. «Направления совершенствования теории и практики боевого применения РВиА»

Том 5. «Проблемы и перспективы развития материально-технического и финансово-экономического обеспечения войск (сил)»

Том 6. «Специальный сборник»

В соответствии с Решением президиума ВАК Минобрнауки России изданиям Российской академии ракетных и артиллерийских наук предоставлено право опубликования научных результатов соискателей ученой степени доктора и кандидата наук.

РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД К ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ ИНЖЕНЕРНЫХ СИСТЕМ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИТЫ

*В.М. Колодкин, Д.М. Варламова, С.М. Копелев
(Удмуртский государственный университет)*

Изменения в политической, социально-экономической ситуации в мире нашли отражение в возрастании террористических угроз, в том числе по отношению к образовательным учреждениям. Если сравнивать с другими объектами, то образовательные учреждения являются наиболее доступными для совершения террористических актов. На возрастание угроз образовательные учреждения реагируют модернизацией инженерно-технических средств защиты.

К причинам террористических атак на образовательные учреждения можно отнести психические расстройства, ненависть, терроризм и т.д. Зачастую нападения совершают бывшие или нынешние ученики [1]. В последнее время набирает популярность криминологическое явление «скулшутинг» [2]. Автором рассмотрены факторы, способствующие совершению вооруженных нападений на образовательные учреждения; выявлены признаки, присущие вооруженным нападениям на образовательные учреждения и террористическим актам.

Безопасность обеспечивается совокупностью организационно-технических мероприятий, направленных на усиление защищенности образовательного учреждения. Например, полагается, что пожарная безопасность обеспечена, если величина пожарного риска не превышает нормативной величины. Если обратиться к угрозе проявления террористической активности, то, например, для критически важных объектов (объектов энергетики, оборонных предприятий и т.д.) безопасность обеспечена, если вероятность ликвидации угрозы больше вероятности успешного завершения террористической атаки [3, 4]. При этом используется вероятностно-временной анализ динамики террористической атаки и реакции на атаку сил реагирования. Эффективность инженерных систем антитеррористической защиты выражается в величине финансовых затрат на достижение требуемого уровня защищенности. Требуемый уровень защищенности определяется категорированием объектов защиты.

В целях установления требований по обеспечению антитеррористической защищенности объектов (территорий) с учетом возможных последствий совершения террористических актов, проводится категорирование объектов (территорий), относящихся к сфере деятельности Министерства просвещения [5].

Категории образовательных учреждений определяются на основе двух параметров: численность населения и прогнозируемое количество пострадавших. Каждой категории соответствует набор мероприятий по обеспечению антитеррористической защищенности объектов (таблица) [5].

Однако категорирование образовательных учреждений, определяя состав средств защиты, не определяет количественные характеристики системы антитеррористической защищенности.

В связи с этим необходимо рассмотреть вопрос о модернизации инженерно-технических средств защиты объектов [6]. Модернизация системы антитеррористической защищенности предполагает:

- Система должна «вписываться» в существующие системы комплексной безопасности образовательных учреждений региона. Система должна функционировать в рамках систе-

Категории опасности объектов

| Категория опасности | Пострадавшие люди в здании, N | Численность населения в населенном пункте, H | Мероприятия по обеспечению антитеррористической защищенности объектов |
|---------------------|---------------------------------|--|---|
| 1 категория | $N > 1100$ | $H > 10\ 000$ | <ol style="list-style-type: none"> 1) мероприятия по категории 2; 2) оборудование контрольно-пропускных пунктов при въезде (въезде) на прилегающую территорию объекта; 3) оснащение въездов на объект средствами снижения скорости и противотаранными устройствами; |
| 2 категория | $N > 1100$ | $H < 10\ 000$ | <ol style="list-style-type: none"> 1) мероприятия по категории 3; 2) оборудование объектов системами контроля и управления доступом; 3) оснащение въездов воротами, обеспечивающими жесткую фиксацию их створок в закрытом положении; |
| | $801 < N < 1100$ | $H > 100\ 000$ | |
| 3 категория | $801 < N < 1100$ | $H < 100\ 000$ | <ol style="list-style-type: none"> 1) мероприятия по категории 4; 2) оснащение объектов системами видеонаблюдения, охранной сигнализацией; 3) обеспечение охраны объектов сотрудниками охранных организаций; 4) оборудование основных входов контрольно-пропускными пунктами; 5) оснащение стационарными и ручными металлоискателями; |
| | $501 < N < 800$ | $H > 10\ 000$ | |
| | $100 < N < 500$ | $H > 100\ 000$ | |
| 4 категория | $501 < N < 800$ | $H < 10\ 000$ | <ol style="list-style-type: none"> 1) разработка плана эвакуации; 2) обеспечение пропускного и внутриобъектового режимов; 3) оснащение системами передачи тревожных сообщений; 4) оборудование системами оповещения и управления эвакуацией; 5) оснащение объектов системами наружного освещения; 6) проведение практических занятий, инструктажа о порядке действий, учений и тренировок по реализации планов обеспечения антитеррористической защищенности объекта; |
| | $100 < N < 500$ | $H < 100\ 000$ | |
| | $N < 100$ | при любом H | |

мы более высокого уровня, например системы «Безопасный город», так как образовательное учреждение в общем случае не в состоянии обеспечить функционирование системы защиты. Кроме того, и это главное, образовательное учреждение не в состоянии самостоятельно ликвидировать террористическую угрозу. Однако образовательное учреждение в состоянии

снизить ущерб, обусловленный террористической атакой. Инженерная система антитеррористической защиты призвана минимизировать ущерб, связанный с террористической атакой.

- Модернизация инженерно-технической системы обеспечения безопасности, ориентирована на поднятие среднего уровня антитеррористической защищенности образовательных учреждений в регионе. Образовательные учреждения региона находятся в разных условиях. Поэтому уровень угрозы будет различаться. Уровень защищенности должен соответствовать уровню угрозы.

- Модернизация систем, происходит в условиях ограниченных финансовых и временных ресурсов региона. Система должна учитывать условия конкретного учреждения и конкретного региона.

- Модернизация системы антитеррористической защищенности предполагает:

- количественную оценку угроз каждого образовательного учреждения;
- количественную оценку антитеррористической защищенности с учетом:

- а) уровня подготовки персонала;

- б) уровня подготовки контингента;

- в) существующей системы физической защиты объекта;

- г) территориального размещения объекта.

Количественная оценка антитеррористической защищенности образовательного учреждения характеризуется величиной предотвращенного риска [7] в условиях террористической атаки и включает:

1. Оценку соответствия угроз и защищенности для каждого образовательного учреждения в регионе. Ранжирование учреждений по оценкам соответствия;

2. Оценку эффективности модернизации;

3. Оптимизация модернизации с учетом существующих ресурсов.

Таким образом, новые условия требуют существенной модернизации системы комплексной безопасности образовательных учреждений. В том числе, в части антитеррористической защищенности. Модернизация осуществляется на основе количественных оценок уровня угроз и уровня защищенности. Количественная оценка уровня угроз рассчитывается методом свертки критериев, характеризующих террористическую угрозу образовательным учреждениям. К рассматриваемым критериям относятся: контингент сотрудников и учащихся; балансовая стоимость объекта; численность населения в регионе, где расположен объект; количество выпускников.

Количественная оценка уровня защищенности будет зависеть от количественной оценки уровня инженерно-технических средств защиты объекта. Учитывая имманентную неопределенность параметров террористической атаки, количественная оценка антитеррористической защищенности образовательного учреждения характеризуется величиной предотвращенного риска [7]. Количественно анализируется антагонистический конфликт между нарушителем (террористом) и реципиентами риска (учащиеся и сотрудники образовательного учреждения) в условиях террористической атаки [8]. Реципиенты риска противопоставляют нарушителю управляемую экстренную эвакуацию, динамика которой определяется инженерно-техническими средствами.

Эффективность инженерно-технических систем антитеррористической защиты образовательных учреждений характеризуется величиной финансовых затрат на увеличение предотвращенного риска в процессе террористической атаки.

Литература

1. Давыдов Д.Г., Хломов К.Д. Массовые убийства в образовательных учреждениях: механизмы, причины, профилактика // Национальный психологический журнал. 2018. № 4. С. 62–76.

2. Вторушина В.В. Вооруженные нападения на образовательные учреждения в России: причины, квалификация и личность преступника // *Право и управление*. 2023. № 2. С. 300–304.
3. Боровский А.С., Тарасов А.Д. Интегрированный подход к разработке общей модели функционирования систем физической защиты объектов // *Тр. ИСА РАН*. 2011. Т. 61. Вып. 1. С. 3–14.
4. Боровский А.С., Тарасов А.Д. Приближенная оценка защищенности потенциально-опасных объектов // *Программные продукты и системы*. 2013. № 3. С. 235–243.
5. Постановление Правительства РФ от 2 августа 2019 г. № 1006 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)».
6. Колодкин В.М., Копелев С.М., Варламов Д.В. Интеллектуальные средства защиты людей в зданиях в условиях чрезвычайных ситуаций // *Безопасность в техносфере: сб. ст. / М-во науки и высш. образования РФ, ФГБОУ ВО «Удмуртский государственный университет». Междунар. ассоц. специалистов пожар., пром. и экол. безопасности; науч. ред. В.М. Колодкин. — Ижевск: Удмуртский университет. 2022. Вып. 15. С. 6–14.*
7. Бочков А.В. О методе синтеза рисков в управлении безопасностью структурно-сложных системам // *Надежность*. 2020. № 1. С. 57–67.
8. Нечаев Ю.И. и др. Онтологический синтез управленческих решений в условиях антагонистических конфликтов // *Препринты ИПМ им. М.В. Келдыша*. 2018. № 179. С. 1–22.

УДК: 614.8

ПРОГНОЗИРОВАНИЕ ВЕРОЯТНОСТИ ВОЗНИКНОВЕНИЯ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ НА ПРЕДПРИЯТИЯХ НЕФТЕПЕРЕРАБАТЫВАЮЩЕГО КОМПЛЕКСА В СОВРЕМЕННЫХ УСЛОВИЯХ

*В.В. Артюхин, С.Ю. Бутузов, О.А. Морозова
(ВНИИ ГОЧС (ФЦ), Академия ГПС МЧС России)*

В работе предлагаются некоторые подходы к построению модели прогнозирования вероятности возникновения чрезвычайных ситуаций (ЧС) на предприятиях нефтеперерабатывающего комплекса в современных условиях. В основе подхода лежит моделирование с помощью биномиального распределения. Исходными данными модели являются открытые данные о возникновении ЧС на территории Российской Федерации за период 2022–2023 гг.

На территории Российской Федерации зарегистрировано около 80 тысяч опасных производственных объектов (ОПО) нефтегазового комплекса, из которых нефтехимической и нефтегазоперерабатывающей промышленности и объектов нефтепродуктообеспечения составляют примерно 5 % (4096 объектов по данным [1] за 2021 год). Основными видами аварий являются взрыв (с разрушением технических устройств и сооружений), пожар, выброс