

Программные продукты и системы

DOI 10.15827/0236-235X

/ О программном
эмуляторе
квантовых
алгоритмов

/ Метод
решения задач
кибербезопасности

/ Управление
настройками
сетевой
инфраструктуры

/ О нейросетевой
диагностике
заболеваний



№1

ТОМ 37

2024

Научно-исследовательский институт
«Центрпрограммсистем»

Программные продукты и системы

НАУЧНЫЙ ЖУРНАЛ

2024, том 37, № 1
(год издания тридцать седьмой)

Главный редактор
Г.И. САВИН, академик РАН

SOFTWARE & SYSTEMS

Research Journal

2024, vol. 37, no. 1

Editor-in-Chief
G.I. SAVIN, Academician of the Russian Academy of Sciences

Research Institute CENTERPROGRAMSYSTEM

© ПРОГРАММНЫЕ ПРОДУКТЫ И СИСТЕМЫ
Научный журнал

2024. Т. 37. № 1
DOI: 10.15827/0236-235X.142

Главный редактор

Г.И. САВИН, академик РАН

Научные редакторы номера:

Н.А. СЕМЕНОВ, д.т.н., профессор

А.Н. СОТНИКОВ, д.ф.-м.н., профессор

Издатель НИИ «Центрпрограммсистем»
(г. Тверь, Россия)

Учредитель В.П. Куприянов

Журнал зарегистрирован в Роскомнадзоре
3 марта 2020 г.

Регистрационное свидетельство ПИ № ФС 77-77843

Подписной индекс в каталоге
Урал-Пресс 70799

ISSN 0236-235X (печатн.)

ISSN 2311-2735 (онлайн)

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Семенов Н.А. – заместитель главного редактора, д.т.н., профессор Тверского государственного технического университета (г. Тверь, Россия)

Сотников А.Н. – заместитель главного редактора, д.ф.-м.н., профессор, заместитель директора Межведомственного суперкомпьютерного центра РАН (г. Москва, Россия)

Афанасьев А.П. – д.ф.-м.н., профессор Московского физико-технического института (технического университета), заведующий Центром распределенных вычислений Института проблем передачи информации РАН (г. Москва, Россия)

Баламетов А.Б. – д.т.н., профессор Азербайджанского научно-исследовательского и проектно-исследовательского института энергетики (г. Баку, Азербайджан)

Борисов В.В. – д.т.н., профессор филиала Национального исследовательского университета «МЭИ» в г. Смоленске (г. Смоленск, Россия)

Голенков В.В. – д.т.н., профессор Белорусского государственного университета информатики и радиоэлектроники (г. Минск, Беларусь)

Елизаров А.М. – д.ф.-м.н., профессор Института математики и механики им. Н.И. Лобачевского Казанского федерального университета (г. Казань, Россия)

Еремеев А.П. – д.т.н., профессор Национального исследовательского университета «МЭИ» (г. Москва, Россия)

Кузнецов О.П. – д.т.н., профессор Института проблем управления РАН (г. Москва, Россия)

Мамросенко К.А. – к.т.н., доцент Московского авиационного института (национального исследовательского университета), руководитель Центра визуализации и спутниковых информационных технологий НИИСИ РАН (г. Москва, Россия)

Палюх Б.В. – д.т.н., профессор Тверского государственного технического университета (г. Тверь, Россия)

Сулейманов Д.Ш. – академик АН Республики Татарстан, д.т.н., профессор Казанского государственного технического университета (г. Казань, Республика Татарстан, Россия)

Татарникова Т.М. – д.т.н., доцент, профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина) (г. Санкт-Петербург, Россия)

Ульянов С.В. – д.ф.-м.н., профессор, ведущий научный сотрудник Объединенного института ядерных исследований (г. Дубна, Россия)

Хорошевский В.Ф. – д.т.н., профессор Московского физико-технического института (технического университета) (г. Москва, Россия)

Шабанов Б.М. – д.т.н., чл.-корр. РАН, директор Межведомственного суперкомпьютерного центра РАН (г. Москва, Россия)

Язенин А.В. – д.ф.-м.н., профессор Тверского государственного университета (г. Тверь, Россия)

АССОЦИИРОВАННЫЕ ЧЛЕНЫ РЕДАКЦИИ

Национальный исследовательский университет «МЭИ», г. Москва, Россия

Технологический институт Южного федерального университета, г. Таганрог, Россия

Тверской государственный технический университет, г. Тверь, Россия

АДРЕС ИЗДАТЕЛЯ И РЕДАКЦИИ

Россия, 170024,
г. Тверь, просп. Николая Корыткова, д. 3а
Телефон (482-2) 39-91-49
Факс (482-2) 39-91-00
E-mail: red@cps.tver.ru
Сайт: www.swsys.ru

Дата выхода в свет 16.03.2024 г.
Отпечатано ИПП «Фактор и К»
Россия, 170100, г. Тверь, ул. Крылова, д. 26
Выпускается один раз в квартал
Год издания тридцать седьмой
Формат 60×84 1/8. Объем 132 стр.
Заказ № 4. Тираж 1000 экз. Цена 550,00 руб.

© SOFTWARE & SYSTEMS

Research journal

2024, vol. 37, no. 1

DOI: 10.15827/0236-235X.142

Editor-in-chief

G.I. SAVIN, Academician of RAS

Science editors of the issue:

N.A. Semenov, Dr.Sc. (Engineering), Professor

A.N. Sotnikov, Dr.Sc. (Physics and Mathematics), Professor

Publisher Research Institute

CENTERPROGRAMSYSTEM (Tver, Russian Federation)

Founder V.P. Kupriyanov

The journal is registered with the Federal Service
for Supervision of Communications, Information Technology
and Mass Communications (Roskomnadzor)
March 3rd, 2020

Registration certificate IIII № ФС 77-77843

ISSN 0236-235X (print)

ISSN 2311-2735 (online)

EDITORIAL BOARD

Semenov N.A. – Deputy Editor-in-Chief, Dr.Sc. (Engineering), Professor of the Tver State Technical University (Tver, Russian Federation)

Sotnikov A.N. – Deputy Editor-in-Chief, Dr.Sc. (Physics and Mathematics), Professor, Deputy Director of the Joint Supercomputer Center of the Russian Academy of Sciences (Moscow, Russian Federation)

Afanasiev A.P. – Dr.Sc. (Physics and Mathematics), Professor of the Moscow Institute of Physics and Technology, Head of Centre for Distributed Computing of Institute for Information Transmission Problems (Moscow, Russian Federation)

Balametov A.B. – Dr.Sc. (Engineering), Professor of the Azerbaijan Scientific-Research & Design-Prospecting Power Engineering Institute (Baku, Azerbaijan)

Borisov V.V. – Dr.Sc. (Engineering), Professor of the MPEI Branch in Smolensk (Smolensk, Russian Federation)

Golenkov V.V. – Dr.Sc. (Engineering), Professor of the Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Elizarov A.M. – Dr.Sc. (Physics and Mathematics), Professor of the N.I. Lobachevsky Institute of Mathematics and Mechanics of the Kazan Federal University (Kazan, Russian Federation)

Eremeev A.P. – Dr.Sc. (Engineering), Professor of the National Research University "Moscow Power Engineering Institute" (Moscow, Russian Federation)

Kuznetsov O.P. – Dr.Sc. (Engineering), Professor of the Institute of Control Sciences of the Russian Academy of Sciences (Moscow, Russian Federation)

Mamrosenko K.A. – Ph.D. (Engineering), Associate Professor of the Moscow Aviation Institute (National Research University), Head of the Center of Visualization and Satellite Information Technologies SRISA RAS (Moscow, Russian Federation)

Palyukh B.V. – Dr.Sc. (Engineering), Professor of the Tver State Technical University (Tver, Russian Federation)

Suleimanov D.Sh. – Academician of TAS, Dr.Sc. (Engineering), Professor of the Kazan State Technical University (Kazan, Republic of Tatarstan, Russian Federation)

Tatarnikova T.M. – Dr.Sc. (Engineering), Associate Professor, Professor of the St. Petersburg Electrotechnical University "LETI" (St. Petersburg, Russian Federation)

Ulyanov S.V. – Dr.Sc. (Physics and Mathematics), Professor of the Dubna International University for Nature, Society and Man (Dubna, Russian Federation)

Khoroshevsky V.F. – Dr.Sc. (Engineering), Professor of the Moscow Institute of Physics and Technology (Moscow, Russian Federation)

Shabanov B.M. – Dr.Sc. (Engineering), Corresponding Member of the RAS, Director of the Joint Supercomputer Center of the Russian Academy of Sciences (Moscow, Russian Federation)

Yazenin A.V. – Dr.Sc. (Physics and Mathematics), Professor of the Tver State University (Tver, Russian Federation)

ASSOCIATED EDITORIAL BOARD MEMBERS

National Research University "Moscow Power Engineering Institute", Moscow, Russian Federation
Technology Institute at Southern Federal University, Taganrog, Russian Federation
Tver State Technical University, Tver, Russian Federation

EDITORIAL BOARD AND PUBLISHER OFFICE ADDRESS

Nikolay Korytkov Ave, 3a, Tver, 170024, Russian Federation

Phone: (482-2) 39-91-49 **Fax:** (482-2) 39-91-00

E-mail: red@cps.tver.ru

Website: www.swsys.ru

Release date 16.03.2024

Printed in printing-office "Faktor i K"

Krylova St. 26, Tver, 170100, Russian Federation

Published quarterly. 37th year of publication

Format 60×84 1/8. Circulation 1000 copies

Prod. order № 4. Wordage 132 pages. Price 550,00 rub.

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

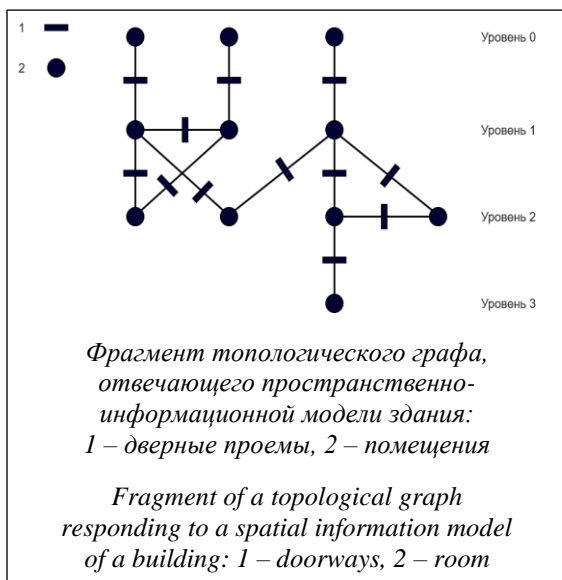
Конкретизируем временной горизонт террористической атаки на уровне порядка 10 минут. Пространственный горизонт системы антитеррористической защищенности ограничим территорией с охватом внешнего контура ОУ.

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, L .

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, помещенного 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 защищен 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

СОДЕРЖАНИЕ

| | |
|---|-----|
| Ulyanov, S.V., Ulyanov, V.S. Software emulator of quantum algorithms for sophisticated simulation on conventional computer | 5 |
| Альдарф Алаа, Шакер Алаа, Бессмертный И.А. Анализ времени выполнения теста неравенства Белла для поиска информации..... | 18 |
| Болденков А.С., Ганджа Т.В., Дмитриев В.М. Структура сетевой многоуровневой компьютерной модели в формате метода компонентных цепей для реализации сетевых виртуальных лабораторий | 24 |
| Фаткиева Р.Р., Судаков А.С. Автоматическое конфигурирование маршрутизаторов для управления настройками сетевой инфраструктуры | 34 |
| Павлов П.А., Коваленко Н.С. Синхронный режим распределенных вычислений при непрерывном выполнении блоков ограниченного числа копий программного ресурса..... | 43 |
| Полтавцева М.А., Зегжда Д.П. Моделирование информационных процессов систем управления большими данными для решения задач кибербезопасности..... | 54 |
| Колоденкова А.Е., Верещагина С.С. Программная реализация алгоритмов диагностирования электрооборудования (на примере анализа характера гармонических колебаний)..... | 62 |
| Хусаинов Р.М., Талипов Н.Г., Катасёв А.С., Шалаева Д.В. Интеллектуальная система анализа транспортных потоков в автоматизированных системах управления дорожным движением | 69 |
| Солдатов Е.С. Информационная поддержка принятия решений при мониторинге состояния криогенного оборудования | 77 |
| Московская Е.Д., Бургов Е.В., Московский А.Д., Гревцова Н.А. Система распознавания, отслеживания и описания поведения муравьев на видеозаписи, сделанной в полевых условиях | 83 |
| Чернышев Л.О., Матвеев Ю.Н. Модификация алгоритма фронтального моделирования последствий аварийных выбросов на основе эмпирико-статистического подхода | 95 |
| Колодкин В.М., Варламова Д.М., Шакиров А.Д. Риск-ориентированный подход к проектированию системы антитеррористической защищенности образовательных учреждений | 105 |
| Дударов С.П., Макляев И.В., Леметюнен Ю.А., Гусева Е.В., Кареткин Б.А., Евдокимова С.А. Моделирование биотехнологических процессов с использованием математического аппарата искусственных нейронных сетей | 113 |
| Мосин С.Г. Нейросетевая диагностика заболеваний сердечно-сосудистой системы на основе data-driven-метода | 122 |

C O N T E N T

| | |
|---|-----|
| <i>Ulyanov, S.V., Ulyanov, V.S.</i> Software emulator of quantum algorithms for sophisticated simulation on conventional computer..... | 5 |
| <i>Aldarf, Alaa, Shaker, Alaa, Bessmertny, I.A.</i> Analyzing the time of Bell inequality test for information retrieval | 18 |
| <i>Boldenkov, A.S., Gandzha, T.V., Dmitriev, V.M.</i> The structure of a network multilevel computer model in terms of the component circuit method for implementing network virtual laboratories | 24 |
| <i>Fatkieva, R.R., Sudakov, A.S.</i> Method of automatic configuration of routers | 34 |
| <i>Pavlov, P.A., Kovalenko, N.S.</i> Synchronous distributed computing at continuous execution of blocks of a limited number of program resource copiess..... | 43 |
| <i>Poltavtseva, M.A., Zegzhda, D.P.</i> Modeling information processes of big data management systems to solve cybersecurity problems | 54 |
| <i>Kolodenkova, A.E., Vereshchagina, S.S.</i> Software implementation of algorithms for electrical equipment diagnostics (by the example of harmonic oscillation analysis) | 62 |
| <i>Khusainov, R.M., Talipov, N.G., Katasev, A.S., Shalaeva, D.V.</i> Intelligent system for analyzing traffic flows in automated traffic control systems..... | 69 |
| <i>Soldatov, E.S.</i> Information support for decision making when monitoring the condition of cryogenic equipment | 77 |
| <i>Moskovskaya, E.D., Burgov, E.V., Moscovsky, A.D., Grevtsova, N.A.</i> A system for recognizing, tracking and describing ant behavior on video footage taken in the field..... | 83 |
| <i>Chernyshev, L.O., Matveev, Yu.N.</i> Modifying the algorithm for frontal modeling of accidental release consequences based on the empirical and statistical approach..... | 95 |
| <i>Kolodkin, V.M., Varlamova, D.M., Shakirov, A.D.</i> Risk-oriented approach to designing an anti-terrorist protection system of educational institutions..... | 105 |
| <i>Dudarov, S.P., Maklyaev, I.V., Lemetyuynen, Yu.A., Guseva, E.V., Karetkin, B.A., Evdokimova, S.A.</i> Modeling biotechnological processes using a mathematical apparatus of artificial neural networks..... | 113 |
| <i>Mosin, S.G.</i> Neural network diagnosis of the cardiovascular diseases based on data-driven method | 122 |