Вестник Евразийской науки / The Eurasian Scientific Journal https://esj.today

2022, №1, Том 14 / 2022, No 1, Vol 14 https://esj.today/issue-1-2022.html

URL статьи: https://esj.today/PDF/21SAVN122.pdf

Ссылка для цитирования этой статьи:
Царькова, Е. Г. К вопросу создания автоматизированных систем управления экологической безопасностью потенциально опасных объектов городского хозяйства / Е. Г. Царькова // Вестник евразийской науки. — 2022. — Т. 14. — № 1. — URL: https://esj.today/PDF/21SAVN122.pdf

For citation:
Tsarkova E.G. On the issue of creating automated environmental safety management systems for potentially hazardous urban facilities. *The Eurasian Scientific Journal*, 14(1): 21SAVN122. Available at: https://esj.today/PDF/21SAVN122.pdf. (In Russ., abstract in Eng.).

УДК 504

Царькова Евгения Геннадьевна
ФКУ «Научно-исследовательский институт Федеральной службы исполнений наказаний», Москва, Россия
Научный сотрудник НИЦ-1
ФГБОУ ВО «Тверской государственный университет», Тверь, Россия
Кандидат физико-математических наук
E-mail: university69@mail.ru
РИНЦ: https://elibrary.ru/author_profile.asp?id=252048

К вопросу создания автоматизированных систем управления экологической безопасностью потенциально опасных объектов городского хозяйства

Аннотация. Вопросы обеспечения экологической безопасности потенциально опасных объектов городского хозяйства в настоящее время приобретают особую значимость. Высокую опасность представляет реализация террористических акций на потенциально опасных объектах городского хозяйства, а также деструктивные воздействия нарушителей на потенциально опасные объекты посредством сетевых кибератак. В работе рассматриваются современные методы обеспечения экологической безопасности потенциально опасных объектов городского хозяйства с использованием средств автоматизации. Рассматриваются методы повышения экологической безопасности за счет создания и использования автоматизированных систем управления безопасностью природно-техногенных систем. Исследуются методы повышения эффективности комплексной системы безопасности потенциально опасных объектах городского хозяйства, рассматриваются возможности автоматизации рассматриваемых процессов с применением системы поддержки принятия решений для управления безопасностью потенциально опасных объектах городского хозяйства. Описаны подходы к формированию моделей угроз безопасности объекта, в том числе с учетом влияния обстановки и внешних воздействий на вероятность и способы реализации негативных воздействий. Предложен алгоритм отсева угроз безопасности из полного перечня потенциальных негативных воздействий. В качестве отдельной категории негативных воздействий рассмотрены угрозы кибератак на компоненты информационно-телекоммуникационной сети потенциально опасных объектах городского хозяйства, предложена модель компьютерной безопасности потенциально опасного объекта. Показана возможность использования разработанных алгоритмов, схем, структур, процессов и методов в создании автоматизированной системы поддержки принятия решений для анализа уязвимости потенциально опасных объектов городского хозяйства, в том числе, для определения наиболее перспективных направлений развития и модернизация системы защиты

потенциально опасных объектов городского хозяйства, а также для автоматизации процессов управления и функционирования экологически безопасных природно-техногенных систем.

Ключевые слова: экологическая безопасность объектов городского хозяйства; угрозы безопасности; негативные воздействия; комплексная система безопасности; кибербезопасность; сетевые эпидемии

Введение

Вопросы обеспечения безопасности на потенциально опасных объектах городского хозяйства, химически опасных объектах, в настоящее время приобретают особую значимость. Сегодня на территории Российской Федерации размещено более 10 тысяч химически опасных объектов (ПОХО), относящихся к топливно-энергетическому комплексу, химической, горнодобывающей и перерабатывающей промышленности, к различным отраслям городского хозяйства. Порядка 70 % из них находятся на территориях с населением более 100 тысяч человек, в том числе, в городской черте [1]. Объекты химического профиля, взаимодействующие с различными химическими веществами, составляют значительную долю потенциально опасных объектов техносферы. Ряд химических веществ в силу своей токсичности несут значительную потенциальную опасность для населения населенных пунктов и окружающей среды и могут приводить к поражениям живых организмов различной степени тяжести, включая летальные исходы.

Согласно Методике прогнозирования масштабов заражения сильнодействующими ядовитыми веществами при авариях (разрушениях) на химически опасных объектах и транспорте [1] к химически опасным объектам относятся объекты, на которых хранятся, перерабатываются, используются или транспортируются опасные химические вещества, аварии на котором или разрушение которого может повлечь гибель или химическое заражение людей, сельскохозяйственных животных или растений, а также химическое заражение окружающей природной среды. Более 50 % организаций указанных выше отраслей народного хозяйства применяют аммиак и хлор. Используемые на предприятиях химической, металлургической, нефтехимической и промышленности, на объектах городского хозяйства токсичные химические вещества (ТХВ) содержатся как в сырье, так и во вспомогательных материалах, а также отходах производства; кроме того, транспортные средства, участвующие в перевозке токсически опасных грузов, также являются источником угроз экологической безопасности.

Перечень видов химических опасных объектов проиллюстрирован на рисунке 1.

Вероятность возникновения чрезвычайных ситуаций (ЧС) на таких объектах приводит к появлению угрозы заражения территорий площадью 300 тысяч квадратных километров с населением более 50 миллионов человек с зоной химического заражения, включающей не только место непосредственного разлива опасных веществ, но и местность, над которой распространится облако зараженного воздуха с поражающими концентрациями.

Сегодня особую опасность представляет реализация террористических акций на территории ПООГХ. В современных условиях терроризм стал проблемой мирового международного уровня. Глобальный характер современного терроризма обусловлен развитием средств коммуникации, увеличением, в силу различных причин, миграционных потоков, плотным контактом различных сообществ, отличающихся мировоззрением,

[1] РД 52.04.253-90. Методика прогнозирования масштабов заражения сильнодействующими ядовитыми веществами при авариях (разрушениях) на химически опасных объектах и транспорте.

религиозными традициями и политическими позициями. Социальная, религиозная, политическая напряженность является благодатной почвой для пополнения рядов террористических организаций. Производственный терроризм в виде диверсионных акций экстремистских группировок на потенциально опасных объектах городского хозяйства служит предпосылкой для реализации широкого спектра угроз. В связи с этим задачи обеспечения антитеррористической безопасности на ПООГХ, в том числе, за счет создания эффективной системы физической защиты территории объекта, в настоящее время приобретают особую значимость [2–4].

Рисунок 1. *Перечень химически опасных объектов (составлено автором)*

Общая совокупность угроз на ПООГХ принимает вид разнообразных негативных воздействий (НВ), которые могут иметь различную природу и способы реализации. Актуальная задача повышения эффективности комплексных систем безопасности потенциально опасных объектов городского хозяйства требует разработки новых алгоритмов и моделей управления безопасностью, а также подходов к описанию информационных процессов и структур ПООГХ.

Несмотря на широкое изучение проблемы построения комплексной системы безопасности объектов различной ведомственной принадлежности, до сих пор сохраняется актуальность решения вопроса о способах выбора ее оптимальной структуры и создания эффективных алгоритмов для обеспечения максимально надежной защиты ПООГХ, возможной в заданных условиях эксплуатации. Целью данного исследования является разработка моделей для анализа негативных воздействий для построения системы поддержки принятия решений (СППР) управления безопасностью ПООГХ. Создание такой СППР требует проведения работ по формированию модели предметной области и модели угроз ПООГХ, а также формализации описания возникающих в ходе функционирования потенциально опасного объекта информационных процессов [5; 6].

Методы

Отправной точкой построения комлексной системы безопасности потенциально опасного объекта городского хозяйства является создание модели угроз, в частности, составление перечня негативных воздействий, характерных для данного объекта, а также анализ уязвимости ПООГХ с определением актуального перечня угроз (негативных воздействий), проводимый с учетом модели нарушителя.

Построение алгоритма формирования перечня и ранжирования по значимости НВ играет важную роль в создании СППР управления безопасностью ПООГХ. Разработанный в ходе данного исследования алгоритм формирования полного перечня угроз с учетом действий нарушителей различных типов и формирование сценариев реализации негативных воздействий со стороны нарушителя представлен на рисунке 2.

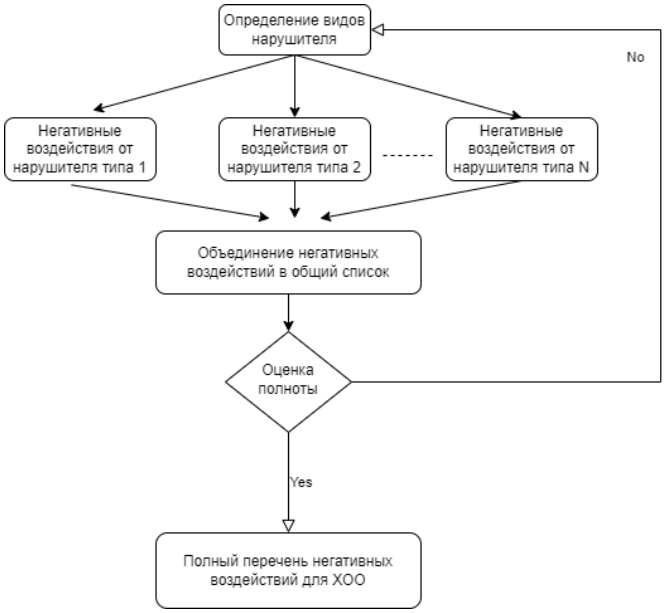

Рисунок 2. *Алгоритм формирования полного перечня НВ ПООГХ (составлено автором)*

Для представления модели угроз изначально необходимо определить полный перечень потенциальных угроз ПООГХ. При этом возможность реализации угрозы на ПООГХ в значительной степени зависит от обстановки и характеристик потенциальных нарушителей — факторов, учет которых неоходим в ходе создания моделей и алгоритмов для СППР управления безопасностью ПООГХ [4–6]. Подход к формированию модели угроз для модельного производственного объекта представлен на рисунке 3.

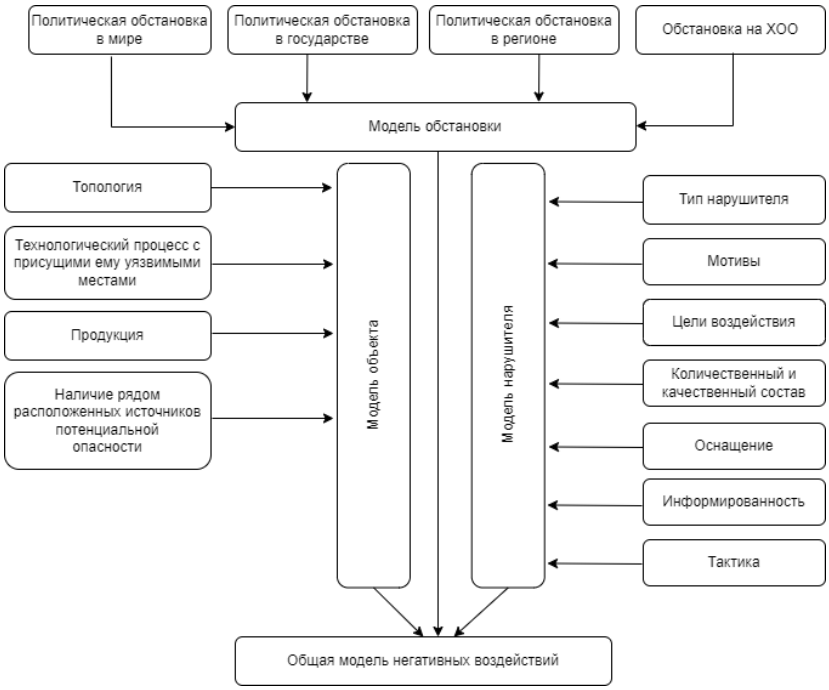

Рисунок 3. *Схема построения модели угроз ПООГХ [5]*

21SAVN122
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Потенциально опасный объект городского хозяйства может подвергаться различным негативным воздействиям, вероятность возникновения и способы реализации которых зависят от целей нарушителя. В работе М. Гарсиа [7] приведена методика определения угроз безопасности, включающая следующие этапы (рис. 4):

Рисунок 4. *Схема методики определения угроз безопасности ПООГХ [7]*

Угроза безопасности ПООГХ M_y в общем случае может быть представлена следующей моделью:

$$M_y =< O, A_t, P_l >, \quad (1)$$

где O — часть ПООГХ, на которую направлено негативное воздействие; A_t — показатель привлекательности реализации негативного воздействия для потенциального нарушителя; P_l — матрица потенциальных потерь, возникающих вследствие реализации негативного воздействия на ПООГХ (рис. 5).

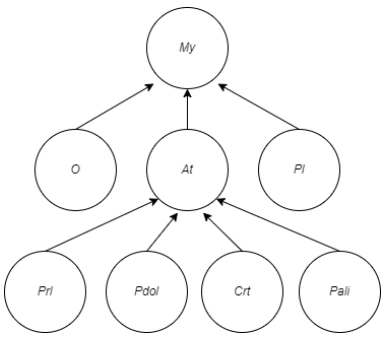

Рисунок 5. *Схема общей модели угрозы безопасности ПООГХ [5]*

Отдельную категорию угроз представляют негативные воздействия, связанные с информационной безопасностью автоматизированных систем управления, используемых на ПООГХ (АСУ ПООГХ). Кибербезопасность автоматизированных систем управления ПООГХ — важный аспект создания системы защиты потенциально опасных объектов. Для современных систем безопасности, образованных сложными техническими комплексами, которые объединены в единую систему с помощью интеграционных алгоритмов и сетевых технологий, высок риск возникновения деструктивных воздействий в форме реализации киберугроз. Подобного рода воздействия могут приводить как к нарушению технологических процессов, протекающих с использованием АСУ[2], так и к сбоям в системе комплексной безопасности ПООГХ, снижающим эффективность ее функций [8; 9].

[2] Громов Ю.Ю., Дидрих И.В., Иванова О.Г., Ивановский М.А., Однолько В.Г. Информационные технологии: учеб. пособие. Тамбов: изд-во ТГТУ, 2015. — 192 с.

Средства электронно-вычислительной техники, используемые на ПООГХ, как правило, представляют собой совокупность физических и виртуальных устройств, подключенных к единой информационно-телекоммуникационной сети передачи данных. Разработка моделей информационной безопасности ПООГХ — важный компонент в создании СППР управления безопасностью потенциально опасного объекта. Для описания динамики развития сетевых киберэпидемий с участием распространенных в настоящее время программных деструктивных воздействий в форме сетевых червей в такой системе может быть использована детерминированная модель распространения эпидемии — SIR-модель (Susceptible-Infected-Removed model) [9–12]. Данная модель пригодна при математическом моделирования сетевых киберэпидемий и кроме того, позволяет анализировать факторы, которые обеспечивают затухание сетевых эпидемий. В рассматриваемой модели различные хосты компьютерной сети ПООГХ могут находиться в одном из трех состояниях: уязвимом (s), зараженном (i), невосприимчивом (r), при этом $s + i + r = N$, где N — постоянное количества хостов сети предприятия. Предполагается, что узлы сети становятся неуязвимыми только в случаем полного излечения от инфекции [12–14].

Результаты

Введем постоянную среднюю скорость «иммунизации» сети за счет использования антивирусного программного обеспечения, проводимую в единицу времени, через γ и введем следующие обозначения[3]: $I = \frac{i}{N}, R = \frac{r}{N}, S = \frac{s}{N}$.

Тогда

$$\begin{cases} \frac{dS(t)}{dt} = -\beta I(t)S(t), \\ \frac{dI(t)}{dt} = \beta I(t)S(t) - \gamma I(t), \\ \frac{dR(t)}{dt} = \gamma I(t) \end{cases} \quad (2)$$

На рисунке 6 приведены графики функций $S(t)$, $I(t)$, $R(t)$, полученные в соответствии с моделью (2) при следующих значениях параметров: $S(0) = S_0 = 4.7$, $I(0) = I_0 = 0.3$, $R(0) = R_0 = 0.01$, $\beta = 0.5, \gamma = 0.1, T = 10$.

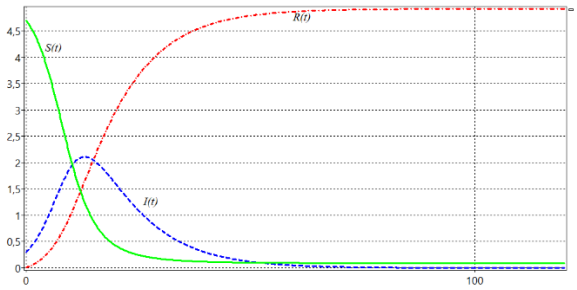

Рисунок 6. *Графики зависимости S(t), I(t), R(t) от времени (составлено автором)*

[3] Семыкина, Н.А. Математические модели в информационной безопасности: учебно-методическое пособие / Н.А. Семыкина, И.А. Шаповалова. — Тверь: Тверской государственный университет, 2020. — 126 с.

В рассматриваемой модели учитывается пороговое значение, являющееся необходимым условием распространения эпидемии. На участке возрастания функции *I(t)* ее производная положительна. Функция *S(t)* непрерывно уменьшается, поскольку увеличивается количество инфицированных узлов сети. Таким образом, для возникновения сетевой киберэпидемии необходимо, чтобы было выполнено условие:

$$S(0) > \frac{\gamma}{\beta} \equiv \rho. \tag{3}$$

Величина γ — характеристика запаздывания реакции специалиста по защите информации на возникновение инцидента, влекущего необходимость загрузки необходимых «заплат», β — показатель улучшения технических характеристик компьютерной сети и возможностей нарушителя, реализующего киберугрозу [15]. Так, нарушитель имеет возможность делать паузы в цикле размножения для избегания ситуации создания катастрофически растущего трафика, что снижает скорость инфицирования. В реальных условиях посредством инсталляции антивирусного программного обеспечения, установки межсетевых экранов и «заплат» приобретают «иммунитет» не только узлы сети, являющиеся инфицированными (*I*), но и уязвимые (*S*).

Упростим модель. Полагая среднюю скорость иммунизации примерно одинаковой для узлов данных типов и равной малой величине γ, получаем:

$$\begin{cases} \dfrac{dI(t)}{dt} = \beta I(t)\big(1 - R(t) - I(t)\big) - \gamma I(t), \\ \dfrac{dR(t)}{dt} = \gamma\big(1 - R(t)\big). \end{cases} \tag{4}$$

С учетом условия развития эпидемии получаем:

$$R(t) = 1 - e^{-\gamma t}. \tag{5}$$

Из выражения (4) следует, что в случае, когда время достаточно велико, эпидемию теоретически возможно преодолеть. Однако, время может оказаться неприемлемо большим [16].

На рисунке 7 приведены графики динамики развития эпидемии в соответствии с моделью (4) при заданных значениях параметров: $I(0) = I_0 = 0.01$, $R(0) = R_0 = 0$, $T = 10$.

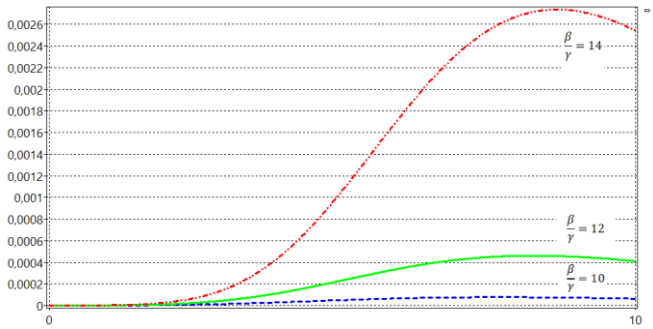

Рисунок 7. *Динамика развития киберэпидемии согласно модели (3) (составлено автором)*

Для построения системы защиты компьютерной сети ПООГХ от деструктивных воздействий введем в процесс динамики сетевой эпидемии управляющее воздействие, равное коэффициенту $\gamma = \gamma(t)$, рассматривая его как кусочно-непрерывную при $t \in [0, T]$ функцию управления, которая удовлетворяет ограничению:

21SAVN122
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

$$0 \le \gamma(t) \le Y_{\max} \le 1, t \in [0, T]. \quad (6)$$

Здесь $Y_{\max}$ — максимальная норма управления, которая характеризует технические и экономические возможности предприятия по организации защиты информации в сети ПООГХ.

Целью управления в рассматриваемой задаче является минимизации функционала, выражающего количество узлов системы, невосприимчивых к заражению, в конечный момент времени *T*. Так, полагая в качестве необходимого условие, чтобы большинство узлов хостов сети ПООГХ (например, более 85 %) в конечный момент времени были невосприимчивы к заражению, получаем следующую задачу оптимального управления процессом защиты компьютерной сети ПООГХ от вирусов: требуется минимизировать функционал

$$J(\gamma) = A \max\left\{\left(0{,}85N(T) - R(T)\right), 0\right\}^2 \to \min, \quad (7)$$

где $N(T) = S(T) + I(T) + R(T)$ — количество хостов в компьютерной сети ПООГХ в конечный момент времени, A > 0 — штрафной коэффициент, при динамических условиях (4), ограничении на управление (6). Для решения данной задачи может быть применена ее дискретная аппроксимация с использованием явных разностных схем[4] и построены численные траектории [17].

Использование приведенной модели в СППР позволяет не только прогнозировать развитие компьютерных эпидемий на ПООГХ, но и осуществлять поиск оптимальных управляющих воздействий для их нейтрализации [18].

Обсуждение

Таким образом, в работе сформулированы общие подходы к формированию моделей угроз, а также построения информационных процессов и структур системы безопасности потенциально опасных объектов народного хозяйства, включая информационную безопасность. Предложенный подход, представленные модели, а также способы отсева негативных воздействий могут быть использованы для анализа уязвимости СФЗ в СППР, в том числе, для определения наиболее перспективных направлений развития и модернизация системы защиты потенциально опасных объектов городского хозяйства, а также при автоматизации процессов управления и функционирования экологически безопасных природно-техногенных систем.

[4] Golubev M.O. Gradient projection method for convex function and strongly convex set ifac-papersonline // Elsevier Science Publishing Company, Inc., Андреева Е.А., Цирулева В.М. Вариационное исчисление и методы оптимизации: учеб. пособие для вузов. — Тверь: ТвГУ, 2004. 575 с.

ЛИТЕРАТУРА

1. Никитенко Ю.В. Управление экологическим риском химически опасных объектов: монография / Ю.В. Никитенко. — Воронеж: ВУНЦ ВВС «ВВА», 2014. — 68 с.
2. Бояринцев А.В. Проблемы антитерроризма: угрозы и модели нарушителя/ А.В. Бояринцев, А.Г. Зуев, А.В. Ничиков. — СПб.: ЗАО «НПП «ИСТА-Системс», 2008. — 220 с.
3. Novikov D A. Mathematical model of information process of protection of the social sector / Novikov D.A., Tsarkova E.G., Dubrovin A.S., Soloviev A.S. // Journal of Physics: Conference Series, Voronezh, 18–20 декабря 2017 года. — Voronezh: Institute of Physics Publishing, 2018. — P. 012041. — DOI 10.1088/1742-6596/973/1/012041.
4. Душкин А.В., Жукова М.А., Родин С.В., Сумин В.И. // Управление контролем целостности эталонной автоматизированной информационной системы вневедомственной охраны // Вестник Воронежского института ФСИН России. 2013, № 1 С. 51–55.
5. Сумин В.И. Разработка моделей и алгоритмов информационных структур и процессов объектов особой важности / В.И. Сумин, Д.Ю. Чураков, Е.Г. Царькова // Промышленные АСУ и контроллеры. — 2019. — № 4. — С. 30–39.
6. Чибунин, В.М. Возможности комплексной системы видеонаблюдения «Безопасный город» при использовании правоохранительными органами / В.М. Чибунин // Современный ученый. — 2020. — № 5. — С. 274–278.
7. Гарсиа М. Проектирование и оценка систем физической защиты / М. Гарсиа. — М.: Мир, 2003. — 386 с.
8. Dubrovin A.S. Analysis and visualization in graph database management systems / A.S. Dubrovin, O.V. Ogorodnikova, E.G. Tsarkova [et al.] // Journal of Physics: Conference Series: Current Problems, Voronezh, 07–09 декабря 2020 года. — Voronezh, 2021. — P. 012059. — DOI 10.1088/1742-6596/1902/1/012059.
9. Громов Ю.Ю., Ивановский М.А., Дидрих В.Е., Иванова О.Г., Мартемьянов Ю.Ф. Методы анализа информационных систем. М.: Изд-во МИНЦ «Нобелистика», 2012. — 220 с.
10. Громов Ю.Ю., Тютюник В.М. Меры количества и качества информации // Информационные системы и процессы. — Изд-во МИНЦ «Нобелистика». — Тамбов. — М.; СПб.; Баку; Вена; Гамбург, том 11, С. 4-8.
11. Кравченко А.С., Родин С.В., Смоленцева Т.Е. Аппаратно-программные средства и информационные процессы защиты систем предоставления пользователям доступа к программным ресурсам // Современные проблемы науки и образования. — 2015. — № 1.
12. Сумин В.И., Смоленцева Т.Е., Апсалямова Р.Д., Сахаров С.Л. Информационные процессы сложных систем // Актуальные проблемы деятельности подразделений УИС: сборник материалов Всероссийской научно-практической конференции. Федеральная служба исполнения наказаний, ФКОУ ВПО «Воронежский институт ФСИН России», 2016. — С. 154–156.

13. Сумин В.И., Дураков С.Г., Чулюков В.А. Построение информационного процесса обучения на основе адаптивной модели: Вестник ВИ ФСИН России, № 2/2012. — С. 62–64.

14. Optimal management of website under adverse impacts conditions / D. Churakov, E. Tsarkova, T. Vorotnikova, A. Belyaev // Journal of Physics: Conference Series: Applied Mathematics, Computational Science and Mechanics: Current Problems, Voronezh, 11–13 ноября 2019 года. — Voronezh: Institute of Physics Publishing, 2020. — P. 012113. — DOI 10.1088/1742-6596/1479/1/012113.

15. Кунижева, Л.А. Математическая модель распространения цепной эпидемии сетевых вирусов на предфрактальном графе / Л.А. Кунижева // Моделирование, оптимизация и информационные технологии. — 2019. — Т. 7. — № 4(27). — С. 45–46. — DOI 10.26102/2310-6018/2019.27.4.012.

16. Zou C.C., Gong W., Towsley D. Code Red worm propagation modeling and analysis // 9th ACM Symposium on Computer and Communication Security. Washington DC, 2002. P. 138–147.

17. Kephart J.O., White S.R. Directed-graph epidemiological models of computer viruses // Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy. Oakland, California, 1991. P. 343–359.

18. Захарченко А. Черводинамика: причины и следствия // Защита информации. Конфидент, 2004. № 2, С. 50–55.

Tsarkova Evgeniya Gennadievna
Research Institute of the Federal Penitentiary Service of Russia, Moscow, Russia
Tver State University, Tver, Russia
E-mail: university69@mail.ru
RSCI: https://elibrary.ru/author_profile.asp?id=252048

On the issue of creating automated environmental safety management systems for potentially hazardous urban facilities

Abstract. The issues of ensuring the environmental safety of potentially hazardous urban facilities are currently becoming particularly important. The implementation of terrorist actions at potentially dangerous urban facilities, as well as the destructive effects of violators on potentially dangerous objects through network cyber attacks, is a high danger. The paper discusses modern methods of ensuring environmental safety of potentially hazardous urban facilities using automation tools. The methods of improving environmental safety through the creation and use of automated safety management systems of natural and man-made systems are considered. The methods of increasing the effectiveness of the integrated security system for potentially hazardous urban facilities are investigated, the possibilities of automating the processes under consideration with the use of a decision support system for managing the safety of potentially hazardous urban facilities are considered. The author proposes an approach to the formation of models of threats to the security of an object, including taking into account the influence of the situation and external influences on the probability and methods of implementing negative impacts, and also develops an algorithm for screening out security threats from a complete list of potential negative impacts. As a separate category of negative impacts, the article considers the threats of cyberattacks on the components of the information and telecommunications network of potentially dangerous urban facilities, a model of computer security of a potentially dangerous object is proposed. The possibility of using the developed algorithms, schemes, structures, processes and methods in creating an automated decision support system for analyzing the vulnerability of potentially hazardous urban facilities, including for determining the most promising areas of development and modernization of the protection system of potentially hazardous urban facilities, as well as for automating the management and functioning of environmentally safe natural and man-made systems, is shown.

Keywords: environmental safety of urban facilities; security threats; negative impacts; integrated security system; cybersecurity; network epidemics