Научная статья
УДК 004; DOI: 10.61260/2218-13X-2024-3-127-138

МОДЕЛИРОВАНИЕ ПОСЛЕДСТВИЙ ЗАТОРОВЫХ СИТУАЦИЙ НА ЗАГЛУБЛЕННЫХ ЭЛЕМЕНТАХ (АВТОМОБИЛЬНЫЕ ТОННЕЛИ) ДОРОЖНО-ТРАНСПОРТНОЙ СЕТИ В РЕЗУЛЬТАТЕ ГИПОТЕТИЧЕСКОЙ КОМПЬЮТЕРНОЙ АТАКИ

✉**Комаров Валерий Валерьевич.**
АНО ДПО «Центр повышения квалификации «АИС», Москва, Россия
✉***vinnipux1@rambler.ru***

Аннотация. Целью исследования является разработка модели количественной оценки масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры в сфере транспорта.

Методы исследования заключаются в обобщении и анализе существующего методического обеспечения организации работы постоянно действующей комиссии субъекта критической информационной инфраструктуры при категорировании объектов в сфере транспорта в интересах перехода от качественных к количественным процедурам обоснования показателей категории значимости.

В рамках задачи обеспечения безопасности сложных технических систем при управлении заглубленными элементами дорожно-транспортной сети (автомобильные тоннели) синтезирована параметризованная модель объекта критической информационной инфраструктуры, функционирующего в условиях проведения в отношении него компьютерных атак. Предложен подход к расчету основных показателей категории значимости объекта критической информационной инфраструктуры в сфере транспорта. Полученные результаты позволяют обоснованно сформировать технические требования к создаваемым или модернизируемым системам обеспечения безопасности значимых объектов критической информационной инфраструктуры, осуществляющих управление системами жизнеобеспечения объектов транспортной инфраструктуры.

Практическая значимость заключается в решении задач количественного обоснования отнесения информационных системы, систем автоматизированного управления, информационно-телекоммуникационных сетей, функционирующих в сфере транспорта, к значимым объектам критической информационной инфраструктуры с использованием количественной оценки спрогнозированных последствий для жизни и здоровья участников дорожного движения от компьютерных инцидентов на обеспечивающих системах в автомобильных тоннелях.

Ключевые слова: критическая информационная инфраструктура, объект критической информационной инфраструктуры, категорирование, методика, модель, оценка возможностей реализации угрозы, ущерб

Для цитирования: Комаров В.В. Моделирование последствий заторовых ситуаций на заглубленных элементах (автомобильные тоннели) дорожно-транспортной сети в результате гипотетической компьютерной атаки // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 3. С. 127–138. DOI: 10.61260/2218-13X-2024-3-127-138.

Scientific article

MODELING THE CONSEQUENCES OF TRAFFIC SITUATIONS ON DEEP ELEMENTS (VEHICLE TUNNELS) OF THE ROAD TRANSPORT NETWORK AS A RESULT OF A HYPOTHETICAL COMPUTER ATTACK

✉**Komarov Valeriy V.**
ANO DPO «Center for Advanced Training «AIS», Moscow, Russia
✉***vinnipux1@rambler.ru***

Abstract. The purpose of the study is to develop a model for quantifying the scale of possible consequences in the event of computer incidents at critical infrastructure facilities in the transport sector.

Summery and analysis of the existing methodological support for organizing the work of a permanent commission of a subject of critical information infrastructure when categorizing objects of critical information infrastructure in the transport sector in the interests of the transition from qualitative to quantitative procedures for substantiating indicators of the category of significance.

A parameterized evolutionary model of a critical information infrastructure object operating under conditions of computer attacks computer attacks has been trained. An approach to calculating the main indicators of the category of significance of a critical information infrastructure object in the field of transport is proposed. The results obtained make it possible to reasonably formulate technical requirements for the systems being created or modernized to ensure the security of significant objects of critical information infrastructure that manage the life support systems of transport sector objects.

The main results are creation of a methodology for solving problems of quantitative justification for classifying information systems, automated control systems, information and telecommunication networks operating in the field of transport as significant objects of critical information infrastructure using a quantitative assessment of the predicted consequences for the life and health of drivers from computer incidents on supporting systems in tunnels for cars.

Keywords: critical information infrastructure, critical information infrastructure object, categorization, methodology, model, assessment the possibilities of implementing threats, damage

For citation: Komarov V.V. Modeling the consequences of traffic situations on deep elements (vehicle tunnels) of the road transport network as a result of a hypothetical computer attack // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 3. P. 127–138. DOI: 10.61260/2218-13X-2024-3-127-138.

Введение

Важным этапом обеспечения безопасности критической информационной инфраструктуры (КИИ) в сфере транспорта является процедура категорирования информационных систем, автоматизированных систем управления и информационно-телекоммуникационных сетей, обеспечивающих управленческие, технологические, производственные, финансово-экономические и (или) иные процессы объекта транспортной инфраструктуры. Правила проведения категорирования объектов КИИ и перечень показателей критериев значимости объектов КИИ Российской Федерации и их значений утвержден постановлением Правительства Российской Федерации[1].

[1] Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений: постановление Правительства Рос. Федерации от 8 февр. 2018 г. № 127. URL: http://publication.pravo.gov.ru/Document/View/0001201802130006 (дата обращения: 15.06.2024).

В процессе определения информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей для внесения их в перечень объектов КИИ, подлежащих категорированию, субъекты КИИ в транспортной сфере вынуждены действовать интуитивно, без соответствующего методического и аналитического аппарата принятия решений. Определение значения показателей критерия значимости осуществляется экспертным методом. Оценка значения показателя критерия значимости должна быть прогнозной с использованием статистических данных [1]. Однако методы прогнозирования возможных последствий компьютерных атак на объекты КИИ в сфере транспорта не опубликованы [2].

Субъекты КИИ в сфере транспорта исходят из необходимости обеспечения транспортной связанности территории страны с одновременным обеспечением транспортной безопасности[2].

В частности, транспортная система Москвы рассматривается совместно с транспортной системой Московской обл. как единый московский транспортный узел [3]. Таким образом, можно рассматривать влияние заторовых ситуаций на территорию как минимум двух субъектов Федерации.

Важнейшим элементом уличной дорожной сети являются автомобильные тоннели. Возникновение заторовой ситуации в автомобильном тоннеле может привести к негативным последствиям в социальной сфере и сфере обеспечения безопасности (прекращение или задержка движения автомобилей оперативных служб)[3]. Соответственно, организации, обслуживающие информационную инфраструктуру автомобильных тоннелей, относят к объектам КИИ, нарушение работы которых в результате воздействия компьютерной атаки может привести к возникновению заторовых ситуаций в автомобильном тоннеле: автоматических систем регулирования дорожного движения (светофоры, информационные табло) и системы транспортной безопасности тоннеля. Аналогичная позиция отражена в документах Министерства транспорта Российской Федерации и согласована с Федеральной службой по техническому и экспертному контролю (ФСТЭК) России[4].

В такой ситуации из процесса категорирования объектов КИИ выпадают вспомогательные системы автомобильных тоннелей, нарушение работоспособности которых не оказывает непосредственного влияния на пропускную способность автомобильного тоннеля и принимаются решения постоянно действующих комиссий по категорированию о неприменимости к ним показателя «Прекращение или нарушение функционирования объектов транспортной инфраструктуры, транспортных средств, в том числе высокоавтоматизированных транспортных средств, оцениваемых в размере территории, на которой недоступны транспортные услуги и/или в количестве необслуженных пассажиров». Это приводит к необоснованному решению об отсутствии необходимости присвоения категории значимости либо исключения таких информационных систем и автоматизированных систем управления из объектов КИИ. В результате не принимается дополнительных мер обеспечения безопасности от компьютерных атак в отношении вышеуказанных систем [4].

Вместе с тем законодательством Российской Федерации предусмотрен показатель категории значимости «Причинение ущерба жизни и здоровью людей». На данный показатель существенное влияние оказывает состав газовоздушной среды внутри тоннеля. Источником загрязнения газовоздушной среды служат отработавшие газы двигателей

[2] О транспортной безопасности: Федер. закон от 9 февр. 2007 г. № 16-ФЗ. URL: http://government.ru/docs/all/98356/ (дата обращения: 15.06.2024).

[3] ГОСТ Р 56521–2015. Тоннели автомобильные. Требования безопасности. URL: https://docs.cntd.ru/document/1200122432 (дата обращения: 15.06.2024).

[4] Перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере транспорта (утв. Минтрансом 15 мая 2023 г., согласовано с ФСТЭК России 5 мая 2023 г.). URL: https://mintrans.gov.ru/documents/7/12506 (дата обращения: 15.06.2024).

внутреннего сгорания транспортных средств, находящихся внутри автомобильного тоннеля[5]. Экстремальные загрязнения в следствии чрезвычайных ситуаций (пожар транспортных средств[6], разлив сильнодействующих ядовитых веществ и т.д.) выходят за рамки данного исследования, так как не являются последствиями компьютерных атак на информационную инфраструктуру автомобильного тоннеля. Соответственно, следует рассматривать процесс обеспечения безопасной газовоздушной среды как критический, а системы автоматизации, обеспечивающей его выполнение, как объекты КИИ [5].

В составе выхлопных газов двигателей внутреннего сгорания транспортных средств наибольшую угрозу для жизни и здоровья человека представляют следующие соединения:

1. Монооксид углерода (угарный газ), химическая формула – CO. Повышенную опасность несет отсутствие запаха и слабое поглощение бумажными и угольными фильтрами системы вентиляции салона автомобилей.

2. Диоксид азота, химическая формула – NO_2.

На показатели газовоздушной среды тоннеля оказывают следующие факторы:

– количество двигателей внутреннего сгорания;

– режим работы двигателя внутреннего сгорания;

– класс экологичности двигателей внутреннего сгорания;

– геометрические и аэродинамические характеристики тоннеля;

– объем естественного подпора внешнего воздуха.

Проектными решениями на строительство тоннеля длиной более 350 м при однонаправленном движении транспортных средств предусматривается система принудительной вентиляции[7]. Отдельно нужно учитывать необходимость компенсации поршневого эффекта вентиляции проезжающих через автомобильный тоннель транспортных средств, так как в случае возникновения заторовых ситуаций в тоннеле он перестает оказывать влияние на состав газовоздушной смеси [6]. Постоянная работа принудительной вентиляции не целесообразна в силу экономических (стоимость электроэнергии, моторесурс и т.д.) и экологических (акустический шум, вибрации) причин, что приводит к необходимости применения систем управления с использованием технических средств газоанализа[8]. В научных работах такие системы относят к классу киберфизических, так как они имеют в своем составе датчики изменения физических/химических параметров окружающей среды, исполнительные устройства (вентиляторы), воздействующие на физические параметры окружающей среды и цифровую диспетчерскую систему управления (автоматизированную систему управления) [7, 8].

Методы исследования

Объектом исследования стала система управления вентиляцией и контроля параметров газовоздушной среды Волоколамского транспортного тоннеля. С целью разработки методики оценки негативных последствий от компьютерных атак на системы вентиляции и газоанализа тоннеля была разработана модель изменения параметров загрязнения газовоздушной среды внутри тоннеля и проведена оценка максимального

[5] ГОСТ 31967–2012. Двигатели внутреннего сгорания поршневые. Выбросы вредных веществ с отработавшими газами. Нормы и методы определения // Электронный фонд правовой и нормативно-технической документации. URL: http://www.docs.cntd.ru (дата обращения: 15.06.2024).

[6] Р НП «АВОК» 7.6–2013. Рекомендации «АВОК». Определение параметров продольной системы вентиляции автодорожных тоннелей. URL: http://vniipo-help.ru/data/uploads/r-np-avok-7.6-2013-rekomendacii-avok.-opredelenie-parametrov-prodolnoj-sistemy-ventilyacii-avtodorozhnyh-tonnelej.pdf (дата обращения: 15.06.2024).

[7] СП 298.1325800.2017. Системы вентиляции тоннелей автодорожных. Правила проектирования // Электронный фонд правовой и нормативно-технической документации. URL: http://www.docs.cntd.ru (дата обращения: 15.06.2024).

[8] ОДН 218.5.016–2002. Показатели и нормы экологической безопасности автомобильной дороги // Электронный фонд правовой и нормативно-технической документации. URL: http://www.docs.cntd.ru (дата обращения: 15.06.2024).

времени нахождения людей в тоннеле в случае компьютерного инцидента из-за действий нарушителя (компьютерной атаки).

Моделирование основано на предположении о вмешательстве нарушителя в работу автоматизированных систем управления вентиляционного оборудования и контроля параметров газовоздушной среды Волоколамского транспортного тоннеля и определяется как некорректное отображение показаний датчиков о превышении допустимого уровня угарного газа и диоксида азота, то есть нарушении целостности информации или блокировки возможности передачи команды на изменение режима работы двигателей системы вентиляции (включение, увеличение скорости вращение лопастей вентилятора), то есть нарушении доступности, что можно отнести к нарушению устойчивого функционирования объекта КИИ в киберпространстве [9].

Необходимо отметить, что нарушитель имеет возможность синхронизировать проведение компьютерной атаки с пиковой нагрузкой на пропускную способность автомобильного тоннеля. Используя визуальное наблюдение за заторовой ситуацией на въездах и выездах из тоннеля, общедоступные данные о заторовой ситуации в средствах массовой информации, а также данные специализированных ресурсов типа «Яндекс Пробки» либо прогнозные промежутки времени, связанные с гидрометеорологическими прогнозами (снегопад, ливни, туманы) или внешними событиями в городе (массовые мероприятия, плановые ремонты дорожной сети и т.д.), нарушитель способен нанести компьютерной атакой максимальный ущерб жизни и здоровью людей, оказавшихся в момент компьютерной атаки в тоннеле. В таких случаях деструктивное воздействие следует рассматривать как целевую компьютерную атаку [10]. При моделировании учитывается факт взаимосвязи систем газоанализа и принудительной вентиляции [11].

В соответствии с методическим документом ФСТЭК России[9] проведем оценку уровней возможностей потенциального нарушителя по реализации данной угрозы безопасности информации. Успешная компьютерная атака автоматизированных систем управления вентиляционного оборудования и контроля параметров газовоздушной среды автомобильного тоннеля осуществима при наличии у нарушителя следующих минимальных возможностей:

– использование свободно распространяемых средств реализации угроз;

– устойчивые навыки по использованию средств реализации угроз и повышению эффективности их применения;

– устойчивые навыки эксплуатации известных уязвимостей;

– навыки самостоятельного сбора информации, планирования и реализации сценария компьютерной атаки;

– знание и понимание особенностей функционирования автоматизированных систем управления вентиляцией и систем газоанализа, включая встроенные механизмы защиты;

– организация групповой работы.

Соответственно, для подобной целевой компьютерной атаки минимально необходим потенциал нарушителя, обладающего средними возможностями (тип Н3) и использование общедоступных каналов информационного обмена [12–16].

Моделирование проводилось с учётом конструктивных особенностей Волоколамского транспортного тоннеля и модели развития экстремальной ситуации, вызванной реализацией киберугрозы – компьютерной атакой [17].

Результаты исследования и их обсуждение

В соответствии с проектным решением движение в тоннеле разделено на правый и левый тоннель (проезд), с обустройством шести рамповых участков для естественной

[9] Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 5 февр. 2021 г.). URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 15.06.2024).

вентиляции по каждому тоннелю. Учитывая, что площадь рамповых участков и естественная вентиляция (рециркуляция) воздуха на каждом участке имеют разные значения, то расчёт проводился по каждому участку[10] в отдельности с учётом длины и площади рамповых участков, скорости горизонтального подпора и вертикального выдува воздуха на участках. Также для расчёта использовались дополнительные данные, полученные опытным путём, такие как скорость движения автотранспорта и расстояние между автомобилями.

Исходные данные:

1. Длина тоннеля – 1 170 м.
2. Сечение тоннеля – 70 м^2.
3. Объём тоннеля – 81 900 м^3.
4. Количество полос – 3 шт.
5. Длина автомобиля – 5 м.

В атмосферном воздухе максимальная разовая предельно допустимая концентрация CO=5,0 мг/м^3 [11].

В атмосферном воздухе максимальная разовая предельно допустимая концентрация NO_2=0,2 мг/м^3.

Значения предельно допустимой концентрации CO в тоннеле в соответствии с СНиП 32-04-97 «Тоннели железнодорожные и автодорожные»[12].

Количество автомобилей, зарегистрированных в Москве по классам экологичности двигателей, взяты в соответствии с данными Аналитического агентства «Автостат»[13] (табл. 1).

Распределение норм выбросов CO и NO_2 по классам экологичности двигателей приведены в табл. 2.

Таблица 1

Распределение автомобилей соответствующих классов экологичности в автопарке Москвы

Класс экологичности	Количество автомобилей данного класса
Евро 0	13,3 %
Евро 1	2,4 %
Евро 2	5,8 %
Евро 3	10,9 %
Евро 4	35,3 %
Евро 5	29,5 %
Евро 6	2,8 %

Характеристики участков по каждому тоннелю (в соответствии с проектной документацией) приведены в табл. 3.

[10] Транспортная развязка Ленинградского и Волоколамского шоссе в районе станции метро «Сокол» 1 этап 1-го пускового комплекса», Транспортная развязка Ленинградского и Волоколамского шоссе в районе станции метро «Сокол» 2 этап 1-го пускового комплекса» Корректировка. Системы жизнеобеспечения Волоколамского тоннеля: рабочая документация. Обозначение 14-047-Р-ВТ-ВД.ГЧ1. Лист 1. Т. 3.2.13. Кн. 13. Подраздел 2. Раздел 3.

[11] Об утверждении санитарных правил и норм СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания: постановление Главного государственного санитарного врача Рос. Федерации от 28 янв. 2021 г. № 2. URL: http://publication.pravo.gov.ru/Document/View/0001202102030022 (дата обращения: 15.06.2024).

[12] СП 122.13330.2012. СНиП 32-04-97. Тоннели железнодорожные и автодорожные. URL: https://docs.cntd.ru/document/1304138944 (дата обращения: 15.06.2024).

[13] Структура автопарка Рос. Федерации и Москвы по экологическим классам. URL: https://www.autostat.ru/infographics/38282/ (дата обращения: 15.06.2024).

Таблица 2

Нормирование выбросов CO и NO_2 по классам экологичности двигателей

Класс	Выделение CO, г/км	Выделение NO_2, г/км
Евро-0	2,75	–
Евро-1	2,72	0,1
Евро-2	2,2	0,15
Евро-3	2,3	0,2
Евро-4	1	0,08
Евро-5	1	0,06
Евро-6	1	0,06

Таблица 3

Характеристики участков по каждому тоннелю

Левый тоннель						
Значения	Рамповый участок левого тоннеля					
Участок №	1	2	3	4	5	6
Площадь рампы, $м^2$	652,2	674,2	672,2	191,5	1120,9	768,8
Длина участка, м	96,5	97,7	90,2	218,5	348,3	320,5
Скорость вертикального выдува воздуха на участке, м\с	0,48	0,20	0,13	0,07	0,07	0,01
Скорость горизонтального подпора воздуха на участке, м\с	1,6	0,7	0,4	0,2	0,2	0,1
Правый тоннель						
Значения	Рамповый участок правого тоннеля					
Участок №	1	2	3	4	5	6
Площадь рампы, $м^2$	307,7	479,7	465,5	665,3	743,5	266,6
Длина участка, м	239,9	148,3	126,3	149,9	333,6	96,6
Скорость вертикального выдува воздуха на участке, м\с	0,1	0,1	0,1	0,1	0,1	0,48
Скорость горизонтального подпора воздуха на участке, м\с	0,1	0,1	0,1	0,2	0,3	1,6

Расчёт проводился исходя из:

1) числа автомобилей каждого класса экологичности, находящихся на каждом из участков тоннеля, и зависит от скорости автомобильного потока, так как происходит сокращение дистанции между автомобилями при снижении скорости. Минимальная дистанция достигается в заторовых ситуациях, что приводит к максимальному количеству транспортных средств в тоннеле. Расчет количества автомобилей, находящихся в тоннеле, в зависимости от скорости потока приведен в табл. 4;

2) количества выделяемых автомобилями вредных веществ (CO и NO_2) за время проезда каждого участка и всего тоннеля;

3) концентрации CO и NO_2 в тоннеле, исходя из количества автомашин, одновременно находящихся в тоннеле и скорости их движения;

4) скорости естественной вентиляции тоннеля на каждом участке в соответствии проектной документацией;

5) увеличения числа людей, одновременно находящихся в тоннеле, за счёт минивэнов, пассажирских автобусов, такси и микроавтобусов и концентрации CO / NO_2 в тоннелях, за счёт грузовых автомобилей (массой до и более 12 т), не оказывает существенного влияния на достижение критических (опасных для здоровья людей) показателей концентрации вредных веществ.

Площадь рамповых участков составляет 19 % для левого тоннеля и 25 % для правого тоннеля от общей плошали тоннелей, при расчёте не учитывался первый (въездной) рамповый участок правого тоннеля, так как он не имеет закрытой части.

Пересчет выделенных CO и NO_2 на объем тоннеля в зависимости от скорости потока транспортных средств приведен в табл. 5.

Таблица 4

Распределение количества транспортных средств в зависимости от скорости

Скорость движения, км/час	Время проезда в тоннеле, мин	Длина машины, м	Расстояние между автомобилями, м	Количество машин в тоннеле, шт	Проектные данные CO, мг/м^3
5	36	5	2	1286	60,1
10	18	5	5	900	58,1
20	9	5	10	600	50,4
40	4,5	5	20	360	26,5
60	3	5	30	257	19,4
80	2,25	5	40	200	17,5

Таблица 5

Масса вредных веществ, поступивших в газовоздушную смесь тоннеля

Скорость, км/ч	Масса CO во всём тоннеле, г	Масса NO_2 во всём тоннеле, г
5	5769,86	88,83
10	4038,90	62,18
20	2692,60	41,45
40	1615,56	24,87
60	1153,97	17,77
80	897,53	13,82

В соответствии с расчётом, учитывая площадь рамповых участков и скорость естественной вентиляции (горизонтальный подпор и вертикальный выдув воздуха), количество и скорость движения автомобилей, а также массу выделяемого CO и NO_2 за время проезда участков, кратность воздухообмена (рециркуляции воздуха) на участках № 1–3 и № 5 левого тоннеля и № 6 правого тоннеля составляет от 1 до 4 раз. Таким образом, за время проезда автомобилями данных участков при скорости в 5 км/ч, концентрация вредных веществ будет равна естественному фону.

На участках № 4 и № 6 левого тоннеля и № 1 правого тоннеля уровень концентрации CO и NO_2 превышает значения естественного фона в 1–2 раза.

Таким образом, при скорости 5 км/ч в тоннеле единовременно находятся 771 автомобиль, которые создают концентрацию CO=23 мг/м^3 и NO_2=0,99 мг/м^3 при нахождении минимум 771 чел. в тоннеле в течение 22 мин.

Согласно СНиП 32-04–97 «Тоннели железнодорожные и автодорожные» нахождение в течение указанного времени без включения принудительной вентиляции и получение данных доз CO и NO_2 может привести к причинению вреда здоровью человека, а принимая во внимание, что число людей, подверженных или страдающих лёгочными (в том числе астмой) и сердечно-сосудистыми заболеваниями, составляет от 2,5 % до 30 % населения, то можно предположить наличие минимум 15 чел., подверженных данным заболеваниям, то объем вредных веществ может спровоцировать не только ухудшение самочувствия, но и привести к летальному исходу.

Заключение

В статье предложено рассматривать автоматизированную систему управления газоанализа и вентиляции заглубленного элемента дорожной сети (автомобильного тоннеля) Москвы (субъект Российской Федерации) как киберфизическую систему. Обосновано рассмотрение ее как объекта КИИ, функционирующей в сфере транспорта. Указана взаимосвязь последствий компьютерных инцидентов (нарушение целостности и доступности информационных сервисов) по показателям критериев значимости в части транспортной недоступности в пределах субъекта Федерации и причинением вреда здоровью человека. В ходе исследования выявлены и описаны особенности функционирования таких объектов, предложена модель расчета количественных показателей категорий значимости объекта КИИ в условиях деструктивного воздействия компьютерной атаки.

Полученные результаты были использованы при проведении категорирования Лефортовского, Волоколамского, Алабяно-Балтийского, Гагаринского, Новокутузовского тоннелей Москвы. Правильность результатов категорирования, полученных на основании предложенного подхода, подтверждена ФСТЭК России при проверке сведений о результатах категорирования и мероприятий государственного контроля за обеспечением безопасности значимых объектов КИИ в 2023 г.

Предложенный подход может быть использован при актуализации законодательства страны, а также в ходе мониторинга результатов категорирования КИИ в сфере транспорта.

Возможно использование данного методического подхода для расчета показателей категории значимости аналогичных систем в заглубленных сооружениях других видов транспорта (железнодорожный, метрополитен, внеуличный и т.д.) и подземных рудниках горнодобычи [18].

Список источников

1. Модель оценки ущерба от инцидентов информационной безопасности / М.О. Таныгин [и др.] // Безопасность информационных технологий. 2021. № 2. С. 98–106. DOI: 10.26583/bit.2021.2.09.

2. Состояние и перспективы развития методического обеспечения технической защиты информации в информационных системах / С.В. Соловьев [и др.] // Вопросы кибербезопасности. 2022. № 1 (53). С. 41–57. DOI: 10.21681/2311-3456-2023-1-41-57.

3. Савченко-Бельский В.Ю., Мальцева М.В. Проблемы и перспективы развития транспортной системы Московской агломерации // Транспортное дело России. 2022. № 1. С. 124–127. DOI: 10.52375/20728689_2022_1_124.

4. Актуальные вопросы проблематики оценки угроз компьютерных атак на информационные ресурсы значимых объектов критической информационной инфраструктуры / С.В. Скрыль [и др.] // Безопасность информационных технологий. 2021. Т. 28. № 1. С. 84–94. DOI: 10.26583/bit.2021.1.07.

5. Салкуцан А.А., Гавдан Г.П., Полуянов А.А. Методика определения критических процессов на объектах информационной инфраструктуры // Безопасность информационных технологий. 2020. Т. 27. № 2. С. 18–34. DOI: 10.26583/bit.2020.2.02.

6. Волков В.П., Наумов С.Н., Пирожкова А.Н. Тоннели и метрополитены. М.: Изд-во «Транспорт», 1975. 551 с.

7. Обеспечение информационной безопасности киберфизических объектов на основе прогнозирования и обнаружения аномалий их состояния / В.И. Васильев [и др.] // Системы управления, связи и безопасности. 2021. № 6. С. 90–119. DOI: 10.24412/2410-9916-2021-6-90-119.

8. Проблемные вопросы применения аналитических средств безопасности киберфизических систем предприятий ТЭК / Н.В. Нашивочников [и др.] // Вопросы кибербезопасности. 2019. № 5 (33). С. 26–33. DOI: 10.21681/2311-3456-2019-5-26-33.

9. Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 52–61.

10. Лапсарь А.П., Назарян С.А., Владимирова А.И. Повышение устойчивости объектов критической информационной инфраструктуры к целевым компьютерным атакам // Вопросы кибербезопасности. 2022. № 2 (48). С. 43–51. DOI: 10.21681/2311-3456-2022-2-39-51.

11. Гендлер С.Г. Проблемы проветривания транспортных тоннелей // Горный информационно-аналитический бюллетень. 2005. № S2. С. 282–295.

12. Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 91–103. DOI: 10.31854/1813-324X-2020-6-4-91-103.

13. Соловьев С.В., Язов Ю.К. Информационное обеспечение деятельности по технической защите информации // Вопросы кибербезопасности. 2021. № 1 (41). С. 69–79. DOI: 10.21681/2311-3456-2021-1-69-79.

14. Маслова М.А. Анализ и определение рисков информационной безопасности // Научный результат. Информационные технологии. 2019. Т. 4. № 1. С. 31–37. DOI: 10.18413/2518-1092-2019-4-1-0-5.

15. Суханов И.Д., Рыбкина О.В. Новые подходы к моделированию угроз безопасности информации. Научно-техническое и экономическое сотрудничество стран АТР в XXI веке: труды Всерос.науч.-практ. конф. Хабаровск, 2021. Т. 1. С. 277–282.

16. Кузьмин В.Н., Менисов А.Б. Исследование путей и способов повышения результативности выявления компьютерных атак на объекты критической информационной инфраструктуры // Информационно-управляющие системы. 2022. № 4. С. 29–43. DOI: 10.31799/1684-8853-2022-4-29-43.

17. Гаськова Д.А., Массель А.Г. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры // Вопросы кибербезопасности. 2019. № 2 (30). С. 42–49. DOI: 10.21681/2311-3456-2019-2-42-49.

18. Гришин Е.Л., Зайцев А.В., Кузьминых Е.Г. Обеспечение безопасных условий деятельности сотрудников по фактору вентиляция в подземных рудниках при работе техники, оснащенной двигателями внутреннего сгорания // Недропользование. 2020. Т. 20. № 3. С. 280–290. DOI: 10.15593/2712-8008/2020.3.8.

References

1. Model' ocenki ushcherba ot incidentov informacionnoj bezopasnosti / M.O. Tanygin [i dr.] // Bezopasnost' informacionnyh tekhnologij. 2021. № 2. S. 98–106. DOI: 10.26583/bit.2021.2.09.

2. Sostoyanie i perspektivy razvitiya metodicheskogo obespecheniya tekhnicheskoj zashchity informacii v informacionnyh sistemah / S.V. Solov'ev [i dr.] // Voprosy kiberbezopasnosti. 2022. № 1 (53). S. 41–57. DOI: 10.21681/2311-3456-2023-1-41-57.

3. Savchenko-Bel'skij V.Yu., Mal'ceva M.V. Problemy i perspektivy razvitiya transportnoj sistemy Moskovskoj aglomeracii // Transportnoe delo Rossii. 2022. № 1. S. 124–127. DOI: 10.52375/20728689_2022_1_124.

4. Aktual'nye voprosy problematiki ocenki ugroz komp'yuternyh atak na informacionnye resursy znachimyh ob"ektov kriticheskoj informacionnoj infrastruktury / S.V. Skryl' [i dr.] // Bezopasnost' informacionnyh tekhnologij. 2021. T. 28. № 1. S. 84–94. DOI: 10.26583/bit.2021.1.07.

5. Salkucan A.A., Gavdan G.P., Poluyanov A.A. Metodika opredeleniya kriticheskih processov na ob"ektah informacionnoj infrastruktury // Bezopasnost' informacionnyh tekhnologij. 2020. T. 27. № 2. S. 18–34. DOI: 10.26583/bit.2020.2.02.

6. Volkov V.P., Naumov S.N., Pirozhkova A.N. Tonneli i metropoliteny. M.: Izd-vo «Transport», 1975. 551 s.

7. Obespechenie informacionnoj bezopasnosti kiberfizicheskih ob"ektov na osnove prognozirovaniya i obnaruzheniya anomalij ih sostoyaniya / V.I. Vasil'ev [i dr.] // Sistemy upravleniya, svyazi i bezopasnosti. 2021. № 6. S. 90–119. DOI: 10.24412/2410-9916-2021-6-90-119.

8. Problemnye voprosy primeneniya analiticheskih sredstv bezopasnosti kiberfizicheskih sistem predpriyatij TEK / N.V. Nashivochnikov [i dr.] // Voprosy kiberbezopasnosti. 2019. № 5 (33). S. 26–33. DOI: 10.21681/2311-3456-2019-5-26-33.

9. Zaharchenko R.I., Korolev I.D. Metodika ocenki ustojchivosti funkcionirovaniya ob"ektov kriticheskoj informacionnoj infrastruktury, funkcioniruyushchej v kiberprostranstve // Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli. 2018. T. 10. № 2. S. 52–61.

10. Lapsar' A.P., Nazaryan S.A., Vladimirova A.I. Povyshenie ustojchivosti ob"ektov kriticheskoj informacionnoj infrastruktury k celevym komp'yuternym atakam // Voprosy kiberbezopasnosti. 2022. № 2 (48). S. 43–51. DOI: 10.21681/2311-3456-2022-2-39-51.

11. Gendler S.G. Problemy provetrivaniya transportnyh tonnelej // Gornyj informacionno-analiticheskij byulleten'. 2005. № S2. S. 282–295.

12. Maksimova E.A. Kognitivnoe modelirovanie destruktivnyh zloumyshlennyh vozdejstvij na ob"ektah kriticheskoj informacionnoj infrastruktury // Trudy uchebnyh zavedenij svyazi. 2020. T. 6. № 4. S. 91–103. DOI: 10.31854/1813-324X-2020-6-4-91-103.

13. Solov'ev S.V., Yazov Yu.K. Informacionnoe obespechenie deyatel'nosti po tekhnicheskoj zashchite informacii // Voprosy kiberbezopasnosti. 2021. № 1 (41). S. 69–79. DOI: 10.21681/2311-3456-2021-1-69-79.

14. Maslova M.A. Analiz i opredelenie riskov informacionnoj bezopasnosti // Nauchnyj rezul'tat. Informacionnye tekhnologii. 2019. T. 4. № 1. S. 31–37. DOI: 10.18413/2518-1092-2019-4-1-0-5.

15. Suhanov I.D., Rybkina O.V. Novye podhody k modelirovaniyu ugroz bezopasnosti informacii. Nauchno-tekhnicheskoe i ekonomicheskoe sotrudnichestvo stran ATR v XXI veke: trudy Vseros.nauch.-prakt. konf. Habarovsk, 2021. T. 1. S. 277–282.

16. Kuz'min V.N., Menisov A.B. Issledovanie putej i sposobov povysheniya rezul'tativnosti vyyavleniya komp'yuternyh atak na ob"ekty kriticheskoj informacionnoj infrastruktury // Informacionno-upravlyayushchie sistemy. 2022. № 4. S. 29–43. DOI: 10.31799/1684-8853-2022-4-29-43.

17. Gas'kova D.A., Massel' A.G. Tekhnologiya analiza kiberugroz i ocenka riskov narusheniya kiberbezopasnosti kriticheskoj infrastruktury // Voprosy kiberbezopasnosti. 2019. № 2 (30). S. 42–49. DOI: 10.21681/2311-3456-2019-2-42-49.

18. Grishin E.L., Zajcev A.V., Kuz'minyh E.G. Obespechenie bezopasnyh uslovij deyatel'nosti sotrudnikov po faktoru ventilyaciya v podzemnyh rudnikah pri rabote tekhniki, osnashchennoj dvigatelyami vnutrennego sgoraniya // Nedropol'zovanie. 2020. T. 20. № 3. S. 280–290. DOI: 10.15593/2712-8008/2020.3.8.

Информация о статье:
Статья поступила в редакцию: 27.07.2024; одобрена после рецензирования: 27.08.2024;
принята к публикации: 30.08.2024
Information about the article:
The article was submitted to the editorial office: 27.07.2024; approved after review: 27.08.2024;
accepted for publication: 30.08.2024

Сведения об авторах:
Комаров Валерий Валерьевич, преподаватель АНО ДПО «Центр повышения квалификации «АИС» (111123, Москва, ул. Плеханова, д. 4а), сертифицированный ведущий аудитор ISO/IEC 27001, e-mail: vinnipux1@rambler.ru, https://orcid.org/0009-0000-9872-9358

Information about the authors:
Komarov Valeriy V., teacher of the Autonomous non-profit organization of additional professional education «Center for advanced training «AIS» (111123, Moscow, Plekhanova str., 4a), ISO/IEC 27001 lead auditor, e-mail: vinnipux1@rambler.ru, https://orcid.org/0009-0000-9872-9358