ISSN 2413–9599 (Print)
ISSN 2541–870X (Online)

www.radioprom.org

DOI: 10.21778/2413-9599-2020-30-3-127-134
УДК 621.391

Математические модели характеристик своевременности реагирования на проникновение в охраняемую зону при блокировании информации в комплексах физической защиты

С. В. Скрыль[1], С. А. Винокуров[2], Т. Б. Ходырев[3], А. В. Мазин[4], Д. А. Холод[1]

[1] ФГБОУ ВО «Московский государственный технический университет им. Н. Э. Баумана», Москва, Россия
[2] Воронежский институт МВД России, Воронеж, Россия
[3] Федеральная служба войск национальной гвардии Российской Федерации, Москва, Россия
[4] ФГБОУ ВО «Московский государственный технический университет им. Н. Э. Баумана», Калужский филиал, Калуга, Россия

Данная статья является первой в серии статей, посвященных вопросам обеспечения физической защиты судов и иных плавсредств с ядерными энергетическими установками и радиационными источниками в период их стоянки в портах. Рассматриваются принципы построения и функционирования мобильных комплексов физической защиты морских портов как нового класса комплексных автоматизированных систем безопасности. Определяется блокирование информации в комплексе как наиболее серьезная уязвимость таких систем. Констатируется малое количество данных по вопросам защиты информации от блокирования в комплексных и интегрированных системах безопасности и их отсутствие в системах рассматриваемого класса. Определяется основная причина нынешнего состояния теории и практики защиты информации от блокирования в комплексах физической защиты морских портов – отсутствие методического аппарата математического моделирования, адекватно оценивающего эффективность противодействия проникновению в охраняемые зоны при блокировании информации в такого рода охранных системах. Приводится формальная интерпретация исследуемых процессов. Рассматривается концептуальная модель нарушения режима охраны территории и акватории порта. Приводятся математические модели частных показателей своевременности реагирования на действия нарушителей на отдельных этапах реализации угрозы проникновения в охраняемую зону. Обосновывается интегральный показатель своевременности реагирования на проникновение в охраняемую зону при блокировании информации в комплексах физической защиты морских портов.

Ключевые слова: комплексы физической защиты, противодействие проникновению в охраняемые зоны при блокировании информации комплексов физической защиты, своевременность реагирования на проникновение в охраняемую зону

Для цитирования:
Математические модели характеристик своевременности реагирования на проникновение в охраняемую зону при блокировании информации в комплексах физической защиты / С. В. Скрыль, С. А. Винокуров, Т. Б. Ходырев, А. В. Мазин, Д. А. Холод // Радиопромышленность. 2020. Т. 30, № 3. С. 127–134. DOI: 10.21778/2413-9599-2020-30-3-127-134

Mathematical models of characteristics of timely response to penetration into a protected area by blocking information in physical protection complexes

S.V. Skryl[1], S.A. Vinokurov[2], T.B. Khodyrev[3], A.V. Mazin[4], D.A. Kholod[1]

[1] Bauman Moscow State Technical University, Moscow, Russia
[2] Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, Russia
[3] Federal service of the national guard of the Russian Federation, Moscow, Russia
[4] Bauman Moscow State Technical University, Kaluga branch, Kaluga, Russia

This article is the first in a series of articles devoted to the issues of physical protection of ships and other watercraft with nuclear power plants and radiation sources during their stay in ports. The principles of construction and functioning of mobile complexes of physical protection of seaports as a new class of integrated automated security systems are considered. The blocking of information in the complex is determined as the most serious vulnerability of such systems. A small amount of data on information protection from blocking in complex and integrated security systems and their absence in systems of the class under consideration is stated. The main reason for the current state of the theory and practice of information protection against blocking in the complexes of physical protection of seaports is determined, which is the lack of a methodological apparatus for mathematical modeling that adequately evaluates the effectiveness of countering penetration into protected areas by blocking information in such security systems. A formal interpretation of the processes under study is given. A conceptual model of violation of the protection regime of the port territory and water area is considered. Mathematical models of particular indicators of the timeliness of response to the actions of violators at individual stages of the penetration into the protected area threat are presented. An integral indicator of timeliness of response to penetration into a protected area by blocking information in the complexes of physical protection of seaports is substantiated.

Keywords: complexes of physical protection, counteraction to penetration into protected areas by blocking information of complexes of physical protection, timeliness of response to penetration into a protected area

For citation:
Skryl S.V., Vinokurov S.A., Khodyrev T.B., Mazin A.V., Kholod D.A. Mathematical models of characteristics of timely response to penetration into a protected area by blocking information in physical protection complexes. Radio industry (Russia), 2020, vol. 30, no. 3, pp. 127–134. (In Russian). DOI: 10.21778/2413-9599-2019-30-3-127-134

Введение

Интенсивное развитие ядерной энергетики и расширение ее инфраструктуры наряду с неоспоримыми преимуществами порождает и целый ряд проблем, связанных с обеспечением ее защиты от различного рода угроз, и в первую очередь от угрозы ядерного терроризма [1]. Ядерный терроризм может быть охарактеризован как наиболее опасная по тяжести последствий форма терроризма, так как он сопряжен с массовой гибелью людей и радиационным заражением огромных территорий. Наиболее доступным способом реализации угрозы ядерного терроризма является организация аварий на объектах ядерной энергетики: АЭС, судах с ядерными энергетическими установками, объектах хранения, переработки и транспортирования ядерных отходов, веществ и материалов.

В связи с этим Национальный антитеррористический комитет акцентирует внимание на ряде недостатков в обеспечении безопасности береговой ядерной инфраструктуры, связанных с ее уязвимостью при проникновении террористических групп, использующих маломерные суда. Было указано на актуальность физической защиты судов и иных плавсредств с ядерными энергетическими установками и радиационными источниками в период их стоянки в портах [2]. Это, в свою очередь, обусловливает необходимость решения ряда задач по своевременному обнаружению и реагированию на несанкционированные действия и нейтрализации нарушителей [3].

Для эффективного решения этих задач разработан и внедряется в эксплуатацию новый класс комплексных автоматизированных систем безопасности – мобильные комплексы физической защиты морских портов (КФЗ). КФЗ представляют собой систему технических средств наблюдения, охраны и противодействия нарушителям,

способную обеспечивать защиту объектов морских портов, любых категорий судов и плавсредств со стороны суши и воды, а также осуществлять мониторинг охраняемой территории и акватории морского порта.

КФЗ обеспечивает:

- оптическое обнаружение и сопровождение малых надводных целей в охраняемой зоне;
- гидроакустическое обнаружение и сопровождение подводных целей в охраняемой зоне;
- автоматическое оповещение и определение параметров движения целей (курса, скорости, глубины);
- передачу данных на центральный пост управления охраняемого объекта и скоростной патрульный катер;
- выдачу данных целеуказания для средства поражения пловцов-нарушителей;
- нелетальное воздействие на обнаруженных и классифицированных подводных нарушителей;
- обнаружение объектов на границах охраняемых территорий.

Управление охранным оборудованием в КФЗ реализуется через его локальную вычислительную сеть, обеспечивающую передачу, обработку и накопление информации оборудования охранной сигнализации, охранного телевидения, мониторинга окружающей обстановки, контроля и управления доступом с целью обеспечения безопасности охраняемой территории и акватории [4].

Методический аппарат математического моделирования противодействия проникновению в охраняемые зоны

Одной из наиболее серьезных уязвимостей КФЗ при реализации им своей основной функции – управления охранным оборудованием – является блокирование информации [5]. Блокирование информации в КФЗ вызывает его неработоспособность, т. е. невыполнение им своей целевой функции, состоящей в обеспечении физической защиты охраняемой территории и акватории. Как следствие, невыполнение этой функции может иметь серьезные последствия.

Это обусловливает высокие требования к мерам противодействия такого рода угрозам, которые должны исключать возможность нарушения работоспособности КФЗ [6].

Низкий уровень проработки вопросов защиты информации от блокирования в комплексных и интегрированных системах безопасности и отсутствие проработки этих вопросов в комплексах физической защиты ставят крайне актуальную на сегодняшний день проблему – проблему защищенности информации от блокирования в КФЗ. Среди факторов, обусловливающих нынешнее состояние теории и практики защиты информации от блокирования в комплексах физической защиты, следует отметить отсутствие методического аппарата математического моделирования, адекватно оценивающего эффективность противодействия проникновению в охраняемые зоны при блокировании информации в КФЗ.

Рассмотрим основные принципы построения таких моделей. При этом будем исходить из того, что адекватность оценки эффективности противодействия проникновению в охраняемые зоны при блокировании информации в КФЗ определяется формальной интерпретацией как самого эффекта противодействия, так и соответствующих угроз нарушения режима охраны территории и акватории порта.

Для формальной интерпретации эффекта противодействия проникновению в охраняемые зоны при блокировании информации в КФЗ определим условие, когда противодействие реализуется эффективно. Будем полагать, что таким условием является ситуация, когда время $\tau_{(р)}$ реагирования на такого рода угрозу не превышает время $\tau_{(п)}$ блокирования информации в КФЗ и последующего проникновения нарушителей на охраняемую территорию, т. е.

$$\tau_{(р)} \le \tau_{(п)}, \qquad (1)$$

Так как $\tau_{(р)}$ и $\tau_{(п)}$ являются случайными величинами, выполнение условия (1) следует рассматривать как случайное событие. Вероятность $P(\tau_{(р)} \leqslant \tau_{(п)}$ этого события следует рассматривать как характеристику своевременности реагирования на угрозу проникновения в охраняемую зону в результате блокирования информации в КФЗ. Данная характеристика может рассматриваться в качестве показателя E – эффективности противодействия такого рода угрозам:

$$E = P(t_{(р)} \le t_{(п)}). \qquad (2)$$

Очевидно, что выражение (2) является простейшей математической абстракцией, основанной на предположении о статистической независимости случайных величин времени $\tau_{(п)}$ реализации нарушителем своих действий и времени $\tau_{(р)}$ реагирования на его действия. Приводимая ниже концептуальная модель нарушения режима охраны территории и акватории порта позволяет уточнить условия своевременного реагирования на угрозу проникновения в охраняемую зону (выражения (3) и (4)) исходя из ограничений на возможности реагирования на определенные этапы действий нарушителей.

Концептуальная модель нарушения режима охраны территории и акватории порта определяет субъект нарушения режима охраны, его квалификацию, мотивацию, цели, этапы действий и временные рамки. Подобная модель рассматривается как предпосылка к формальной интерпретации действий нарушителя.

В общем виде содержание концептуальной модели нарушения сводится к следующему:

1. Субъектом нарушения режима охраны территории и акватории порта в случае, если нарушение носит форму проникновения в охраняемую зону, является внешний нарушитель, а в случае, если нарушение носит форму блокирования информации в КФЗ, субъектом является внутренний нарушитель. Наличие внутреннего нарушителя обусловлено двумя обстоятельствами:
   - автономным характером функционирования как КФЗ в целом, так и его подсистемы управления, исключающим возможность несанкционированного доступа (НСД) к информационным процессам в комплексе через внешние управляющие или информационные ресурсы;
   - наличием в составе программного обеспечения подсистемы управления комплекса физической защиты достаточно эффективных как системных, так и прикладных программных средств защиты информации от НСД, предполагающих возможность доступа к информации в КФЗ лишь ограниченной категории его должностных лиц.
2. Действия и внешнего, и внутреннего нарушителей, в том числе и действия в отношении информационных ресурсов и информационных процессов КФЗ, являются противоправными, а сами нарушители квалифицируются как злоумышленники.
3. Имеет место целевая мотивация такого рода действий.
4. Целевой функцией внутреннего нарушителя является блокирование информации в КФЗ.
5. Целевой функцией внешнего нарушителя является несанкционированный доступ в охраняемую зону.
6. Целевые функции нарушителей реализуются в четыре этапа:
   - этап доступа к аппаратным и программным средствам КФЗ (этап 1);
   - этап анализа состояния охраняемой зоны (этап 2);
   - этап блокирования информации в КФЗ (этап 3);
   - этап проникновения в охраняемую зону (этап 4).
7. Соотношения между моментом времени $t_{(\text{нп})\text{i}}$ начала действий нарушителя и моментом времени $t_{(\text{нр})\text{i}}$ начала реагирования КФЗ следующие:
   - для этапов доступа к аппаратным и программным средствам КФЗ и анализа состояния охраняемой зоны существует временной интервал определенной длины между рассматриваемыми моментами времени:
   $$t_{(\text{нр})\text{i}} - t_{(\text{нп})\text{i}} > 0; \quad (3)$$
   - для этапов блокирования информации в КФЗ и проникновения в охраняемую зону длина временного интервала между рассматриваемыми моментами времени близка нулю:
   $$t_{(\text{нр})\text{i}} - t_{(\text{нп})\text{i}} \approx 0. \quad (4)$$
8. Для внутреннего нарушителя характерно многократное (за исследуемый период) выполнение противоправных действий. При этом кратность несанкционированного доступа внутренним нарушителем к информации КФЗ определяется его возможностями по обеспечению скрытности своих действий. Вероятность многократного несанкционированного доступа к информации КФЗ с увеличением кратности существенно снижается.
9. Для внешнего нарушителя характерно однократное (за исследуемый период) выполнение противоправных действий.

В выражениях (3) и (4) переменная i идентифицирует этап противоправных действий ($i = 1, 2, 3, 4$).

На основе рассмотренной концептуальной модели формируются функциональные модели угроз нарушения режима охраны территории и акватории порта и реагирования на такого рода угрозы. В свою очередь, на основе этих функциональных моделей формируются математические модели временных характеристик $\tau_{(\text{р})}$ и $\tau_{(\text{п})}$.

Воспользовавшись рассмотренной формальной интерпретацией исследуемых процессов, сформируем аналитические модели показателя своевременности реагирования на действия нарушителей при реализации ими соответствующих этапов противоправных действий. При этом в основу положим существующий в методологии защиты информации методический аппарат для исследования своевременности реализации мер обеспечения безопасности информации [7].

Математической интерпретацией показателя (2) своевременности реагирования на действия нарушителей на этапах 3 и 4 является событие, соответствующее соотношению (4) между моментом времени начала действий нарушителя и моментом времени начала реагирования КФЗ. В этом случае

для математического представления (2) достаточно одного условия – условия (1).

Это позволяет воспользоваться сходством представления данного показателя и функции распределения вероятностей [8] и определить данный показатель исходя из представления (2) в виде

$$e_{\text{j}} = P(\bar{\tau}_{(\text{p})\text{j}} \le \tau_{(\text{п})\text{j}}) = 1 - P(\tau_{(\text{п})\text{j}} < \bar{\tau}_{(\text{p})\text{j}}) = 1 - \int_0^{\bar{\tau}_{(\text{p})\text{j}}} f_{(\text{п})\text{j}}(z)\,dz, \quad (5)$$

где $f_{(\text{п})\text{j}}$ – функция плотности вероятности случайной величины времени $\tau_{(\text{п})\text{i}}$ реализации нарушителем j-го, $j = 3, 4$, этапа; $\bar{\tau}_{(\text{p})\text{j}}$ – среднее значение случайной величины времени $\tau_{(\text{p})\text{j}}$ реагирования на действия нарушителя по реализации j-го этапа.

Оценивая законы распределения времени $\tau_{(\text{п})\text{j}}$ и времени $\tau_{(\text{p})\text{j}}$, примем во внимание тот факт, что обе эти случайные величины представляют собой композицию времени реализации отдельных функций, выполняемых нарушителями в процессе проникновения в охраняемую зону, и функций, выполняемых в процессе противодействия проникновению. Согласно представленным в [9] функциональным моделям число последовательно композиционно связанных функций, реализующих эти процессы, является достаточным для того, чтобы, в соответствии с теоремой Линдеберга и Ляпунова [10], рассматривать время $\tau_{(\text{п})\text{j}}$ и время $\tau_{(\text{p})\text{j}}$ реализации исследуемых процессов как случайные величины, распределенные по нормальному закону.

Это позволяет представить выражение (5) для определения показателей e_{j} своевременности реагирования на действия нарушителя по блокированию информации в КФЗ и проникновения в охраняемую зону в виде

$$e_{\text{j}} = erf\left(\frac{\bar{\tau}_{(\text{п})\text{j}} - \bar{\tau}_{(\text{p})\text{j}}}{\sigma_{\text{j}}}\right), \quad (6)$$

где $\bar{\tau}_{(\text{п})\text{j}}$ и σ_{j} – среднее значение и среднеквадратическое отклонение случайной величины $\tau_{(\text{п})\text{j}}$, соответственно; $erf(x) = \frac{2}{\pi}\int_0^x e^{-z^2}\,dz$ – функция ошибок [8].

В отличие от (5), математической интерпретацией показателя (2) своевременности реагирования на действия нарушителей на этапах 1 и 2 является событие, соответствующее соотношению (3) между моментом времени начала действий нарушителя и моментом времени начала реагирования КФЗ. В этом случае математическое представление (2) основывается на трех условиях своевременности реагирования на такого рода угрозы:

$$t_{(\text{нп})\text{k}} + t_{(\text{п})\text{k}} > t_{(\text{нр})\text{k}}, \quad (7)$$

$$t_{(\text{нр})\text{k}} + t_{(\text{p})\text{k}} > t_{(\text{нп})\text{k}}, \quad (8)$$

$$t_{(\text{нр})\text{k}} + t_{(\text{p})\text{k}} \le t_{(\text{ну})\text{k}} + t_{(\text{п})\text{k}}, \quad (9)$$

где k идентифицирует этап противоправных действий ($k = 1, 2$).

Согласно этим условиям, показатель своевременности реагирования на действия нарушителя по доступу к аппаратным и программным средствам КФЗ анализу состояния охраняемой зоны представляется в виде

$$e_{\text{k}} = P(t_{(\text{нп})\text{k}} + \tau_{(\text{п})\text{k}} > t_{(\text{нр})\text{k}}, t_{(\text{нр})\text{k}} + \tau_{(\text{p})\text{k}} > t_{(\text{нп})\text{k}}, t_{(\text{нр})\text{k}} + \tau_{(\text{p})\text{k}} \le t_{(\text{ну})\text{k}} + \tau_{(\text{п})\text{k}}). \quad (10)$$

Соответствующая выражению (10) функция распределения вероятностей представляется следующим образом [11]:

$$\begin{aligned} e_{\text{k}} &= P(t_{(\text{нп})\text{k}} + \tau_{(\text{п})\text{k}} > t_{(\text{нр})\text{k}}, t_{(\text{нр})\text{k}} + \tau_{(\text{p})\text{k}} > t_{(\text{нп})\text{k}}, \\ &\quad t_{(\text{нр})\text{k}} + \tau_{(\text{p})\text{k}} \le t_{(\text{нп})\text{k}} + \tau_{(\text{п})\text{k}}) = \\ &= \int_0^{\omega} dt \int_0^{t+\bar{\tau}_{(\text{п})\text{k}} - \bar{\tau}_{(\text{p})\text{k}}} f_{1\text{k}}(u) f_{2\text{k}}(t)\,du - \int_0^{\omega} dt \int_0^{t} f_{1\text{k}}(u) f_{2\text{k}}(t)\,du = \\ &= \int_0^{\omega} f_{2\text{k}}(t)\left[\frac{F_{1\text{k}}(t + \bar{\tau}_{(\text{п})\text{k}} - \bar{\tau}_{(\text{p})\text{k}})}{R_{1\text{k}}} - F_{1\text{k}}(0)\right] dt - \\ &\quad - \int_0^{\omega} f_{2\text{k}}(t)\left[\frac{F_{1\text{k}}(t)}{R_{2\text{k}}} - F_{1\text{k}}(0)\right] dt = \\ &= \int_0^{\omega} f_{2\text{k}}(t)\left[\frac{F_{1\text{k}}(t + \bar{\tau}_{(\text{п})\text{k}} - \bar{\tau}_{(\text{p})\text{k}})}{R_{1\text{k}}} - \frac{F_{1k}(t)}{R_{2\text{k}}}\right] dt, \end{aligned} \quad (11)$$

где $f_{1\text{k}}$, $f_{2\text{k}}$ – плотности распределения случайных величин $t_{(\text{нр})\text{k}}$ и $t_{(\text{ну})\text{k}}$, соответственно; $F_{1\text{k}}(x)$ – соответствующая закону распределения $f_{1\text{k}}$ функция распределения случайных величин, ограничивающих размер области выполнения условий (7–9); $R_{1\text{k}}$, $R_{2\text{k}}$ – нормировочные коэффициенты для усеченных распределений, соответствующих плотностям $f_{1\text{k}}$ и $f_{2\text{k}}$, ω – время, в течение которого может проявиться хотя бы одна угроза.

Выразив $t_{(\text{нп})\text{k}}$ через $t_{(\text{нр})\text{k}}$ и устремив w в бесконечность, выражение (11) запишем в виде

$$e_{\text{k}} = \int_0^{\infty} f_{2\text{k}}(t)\left[\frac{1}{R_{1\text{k}}} F_{\text{k}1}(t + \bar{\tau}_{(\text{п})\text{k}} - \bar{\tau}_{(\text{p})\text{k}}) - \frac{1}{R_{2\text{k}}} F_{1\text{k}}(t)\right] dt. \quad (12)$$

При оценке законов распределения времени $t_{(\text{п})\text{k}}$ и времени $t_{(\text{p})\text{k}}$ воспользуемся теми же основаниями, что и в случае математического представления (5) и (6) показателей своевременности реагирования на действия нарушителя по блокированию информации в КФЗ и проникновения в охраняемую зону. Это позволяет рассматривать время $t_{(\text{п})\text{k}}$ и $t_{(\text{p})\text{k}}$ как случайные величины, распределенные по нормальному закону, а выражение (12) представить в виде [12]

$$e_{\text{k}} \approx \frac{1}{R_{1\text{k}}}\left[\frac{\bar{\tau}_{(\text{п})\text{k}} - \bar{\tau}_{(\text{p})\text{k}}}{4R_{1\text{k}}\sigma}\left[1 + erf\left(\frac{\bar{\tau}_{(\text{o})\text{k}}}{\sigma\sqrt{2}}\right)\right] + \right.$$
$$\left. + \frac{1}{4R_{2\text{k}}}\exp\left(\frac{\bar{\tau}^{2}_{(\text{o})\text{k}}}{2\sigma^{2}}\right) - \frac{1}{8}\left[1 + erf\left(\frac{\bar{\tau}^{2}_{(\text{o})\text{k}}}{2\sigma^{2}}\right)\right]\right], \quad (13)$$

где $\bar{\tau}_{(\text{o})\text{k}}$, σ_{k} – среднее значение и среднеквадратическое отклонение случайной величины времени обнаружения действий нарушителя по реализации k-го этапа проникновения в охраняемую зону, соответствующее длительности временного интервала $t_{(\text{нр})\text{k}} - t_{(\text{нп})\text{k}}$;

$$R_{1\text{k}} = \frac{1}{2}\left(1 - erf\left(\frac{\bar{\tau}_{(\text{п})\text{k}} - \bar{\tau}_{(\text{p})\text{k}} - \bar{\tau}_{(\text{o})\text{k}}}{\sigma_{\text{k}}\sqrt{2}}\right)\right);$$

$$R_{2\text{k}} = \frac{1}{2}\left(1 + erf\left(\frac{\bar{\tau}_{(\text{o})\text{k}}}{\sigma_{k}\sqrt{2}}\right)\right).$$

Полагая, что своевременность реагирования на проникновение в охраняемую зону при блокировании информации КФЗ характеризует состояние обеспечения своевременности реагирования на всех этапах действий нарушителя, соответствующий показатель представим в виде

$$E = \left(1 - \prod_{\text{i}=1}^{4}(1 - e_{\text{i}})\right). \quad (14)$$

Выражения (6), (13) и (14) являются математическими моделями характеристик своевременности реагирования на проникновение в охраняемую зону при блокировании информации КФЗ. В своей совокупности они представляют собой эффективный инструмент адекватной оценки возможностей КФЗ по противодействию проникновениям в охраняемые зоны в широком диапазоне способов и средств осуществления нарушителем своих действий, включая применение беспилотных летательных аппаратов и средств радиоэлектронной борьбы. В следующих статьях данной серии будут приведены результаты вычислительных экспериментов с разработанными математическими моделями, а также соответствующий методический аппарат, позволяющий научно обосновывать требования к характеристикам применяемых в КФЗ мер противодействия проникновениям в охраняемые зоны.

Выводы

В результате анализа определена концепция теории и методологии построения методического аппарата математического моделирования, получены адекватные средства оценивания и эффективного противодействия проникновению в охраняемые зоны при блокировании информации в КФЗ. Приведена формальная интерпретация исследуемых процессов. Построена концептуальная модель нарушения режима охраны территории и акватории порта. Предложены математические модели частных показателей своевременности реагирования на действия нарушителей на отдельных этапах реализации угрозы проникновения в охраняемую зону. Обоснован интегральный показатель своевременности реагирования на проникновение в охраняемую зону при блокировании информации в КФЗ.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Федеральный закон* от 06.03.2006 № 35-ФЗ «О противодействии терроризму» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru (дата обращения: 27.07.2020).
2. *Временное положение* по оснащению портовых средств инженерно-техническими средствами охраны. Утверждено распоряжением Росморречфлота от 29.07.2005, № ВР-211-р [Электронный ресурс]. URL: https://sudact.ru/law/rasporiazhenie-rosmorrechflota-ot-29072005-n-vr-211-r-ob/vremennoe-polozhenie-po-osnashcheniiu-doosnashcheniiu/ (дата обращения: 27.07.2020).
3. *Распоряжение* Правительства Российской Федерации от 02.11.2009 № 1629-р «О Перечне объектов, подлежащих обязательной охране полицией» [Электронный ресурс]. URL: https://legalacts.ru/doc/rasporjazhenie-pravitelstva-rf-ot-02112009-n-1629-r/ (дата обращения: 27.07.2020).
4. *Рекомендации* Р 78.36.038-2013 «Построение и техническое обслуживание локально-вычислительной сети в пределах пункта централизованной охраны». М.: НИЦ «Охрана» МВД России, 2012. 27 с.
5. *Кулаков В.Г., Гаранин М.В.* Информационная безопасность телекоммуникационных систем. (Технические аспекты) М.: Радио и связь, 2004. 304 с.
6. *Белова Е.А., Ходырев Т.Б.* Организация защиты информации в системах физической защиты критически важных объектов // Общественная безопасность, законность и правопорядок в III тысячелетии: сборник материалов Всероссийской научно-практической конференции. Воронеж: Воронежский институт МВД России, 2013. С. 142–144.
7. *Скрыль С.В., Багаев Д.А.* Своевременность как базовый показатель качества защиты информации // Вопросы защиты информации. 2009. № 2(85). С. 61–63.
8. *Вентцель Е.С.* Теория вероятностей. М.: Наука, 1969. 576 с.
9. *Зарубин В.С., Ходырев Т.Б., Зарубин С.В.* Использование структурных моделей для формализованного представления процессов защиты информационных процессов в комплексах физической защиты // Вестник Воронежского института ФСИН России. 2015. № 4. С. 28–31.
10. *Вентцель Е.С., Овчаров Л.А.* Теория вероятностей и ее инженерные приложения. М.: Высшая школа, 2000. 480 с.

11. *Оценка* своевременности реагирования на угрозы как важный элемент кибербезопасности: теоретические основы и исследовательская модель / С. Скрыль, М. Сычев, А. Сычев, Т. Мещерякова, А. Ушакова, Э. Абачараева, Е. Смирнова // Креативность в интеллектуальных технологиях и науке о данных. CITY&DS. 2019. Интеллектуальные технологии в социальной инженерии. Data Science in Social Networks Analysis and Cybersecurity, Communications in Computer and Information Science 1084, Part 2. Springer Nature Switzerland AG 2019, pp. 258–269.
12. *Оценка* защищенности информации от вирусных атак: существующий и перспективный методический аппарат / С.В. Скрыль, А.М. Сычев, Т.В. Мещерякова, В.И. Арутюнова, Д.А. Голубков // Промышленные АСУ и контроллеры. 2018. № 9. С. 51–62.

REFERENCES

1. Federal law No. 35-FZ of March 6, 2006 *"O protivodeistvii terrorizmu"* [On countering terrorism]. Official Internet portal of legal information. (In Russian). Available at: http://pravo.gov.ru (accessed: 27.07.2020).
2. Temporary provision for equipping port facilities with engineering and technical security equipment. Approved by the order of Rosmorrechflot of 29.07.2005, no. BP-211-R. (In Russian). Available at: https://sudact.ru/law/rasporiazhenie-rosmorrechflota-ot-29072005-n-vr-211-r-ob/vremennoe-polozhenie-po-osnashcheniiu-doosnashcheniiu/ (accessed 27.07.2020).
3. Order of the Government of the Russian Federation of 02.11.2009 No. 1629-R «On the List of objects subject to mandatory police protection». (In Russian). Available at: https://legalacts.ru/doc/rasporjazhenie-pravitelstva-rf-ot-02112009-n-1629-r/ (accessed 27.07.2020).
4. Recommendations P 78.36.038-2013 «Construction and maintenance of a local computer network within a point of centralized protection». Moscow, SIC «Protection» of the Ministry of internal Affairs of Russia Publ., 2012, 27 p. (In Russian).
5. Kulakov V.G., Garanin M.V. Information security of telecommunication systems. (Technical aspects). Moscow, Radio and communications Publ., 2004. 304 p. (In Russian).
6. Belova E.A., Khodyrev T.B. Organization of information protection in systems of physical protection of critical objects. *Public security, law and order in the third Millennium: collection of materials of the all-Russian scientific and practical conference.* Voronezh, Voronezh Institute of the Ministry of internal Affairs of Russia Publ., 2013, pp. 142–144. (In Russian).
7. Skryl S.V., Bagaev D.A. Timeliness as a basic indicator of the quality of information protection. *Information security issues,* 2009, no. 2 (85), pp. 61–63. (In Russian).
8. Wentzel E.S. Probability Theory. Moscow, Nauka Publ., 1969, 576 p. (In Russian).
9. Zarubin V.S., Khodyrev T.B., Zarubin S.V. Use of structural models for formalized representation of information process protection processes in physical protection complexes. *Vestnik Voronezhskogo instituta FSIN Rossii,* 2015, no. 4, pp. 28–31. (In Russian).
10. Wentzel E.S., Ovcharov L.A. probability Theory and its engineering applications. Moscow, Higher school Publ., 2000, 480 p. (In Russian).
11. Skryl S., Sychev M., Sychev A., Meshcheryakova T., Ushakova A., Abacharayeva E., Smirnova E. Assessment of timely response to threats as an important element of cybersecurity: theoretical foundations and research model. // Creativity in smart technologies and data science. CITY&DS. 2019. Intelligent technologies in social engineering. Data Science in Social Networks Analysis and Cybersecurity, Communications in Computer and Information Science 1084, Part 2. Springer Nature Switzerland AG 2019, pp. 258–269.
12. Skryl S.V., Sychev A.M., Meshcheryakova T.V., Arutyunova V.I., Golubkov D.A. Assessment of information security from virus attacks: existing and prospective methodological apparatus. *Industrial ACS and controllers,* 2018, no. 9, pp. 51–62. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Скрыль Сергей Васильевич, д.т.н., профессор, Московский государственный технический университет имени Н.Э. Баумана, 105005, Москва, ул. 2-я Бауманская, д.5, стр. 1, тел.: +7 (495) 632-22-47, e-mail: skryl@bmstu.ru.
Винокуров Станислав Анатольевич, к.т.н., доцент, заместитель начальника по учебной работе, Воронежский институт Министерства внутренних дел Российской Федерации, 394065, Воронеж, просп. Патриотов, 53. тел.: +7 (473) 247-67-07, e-mail: vinokurovvs@yandex.ru.
Ходырев Тимофей Борисович, адъюнкт, старший инспектор по особым поручениям, Федеральная служба войск национальной гвардии Российской Федерации, 111250, Москва, Красноказарменная ул., 9А, стр. 4, тел.: +7 (916) 607-97-31, e-mail: tim-hod@yandex.ru.
Мазин Анатолий Викторович, д.т.н., профессор, заведующий кафедрой, Московский государственный технический университет им. Н.Э. Баумана, Калужский филиал, 248000, Калуга, ул. Баженова, д.2, тел.: +7 (910) 915-58-25, e-mail: mazinav@yandex.ru.
Холод Денис Александрович, аспирант, ассистент, Московский государственный технический университет имени Н.Э. Баумана, 105005, Москва, ул. 2-я Бауманская, д.5, стр. 1, тел.: +7 (499) 263-69-55, e-mail: dekholod@yandex.ru.

AUTHORS

Sergey V. Skryl, D.Sc. (Engineering), professor, Bauman Moscow State Technical University, 5, str. 1, ulitsa 2-ya Baumanskaya, Moscow, 105005, Russia, tel.: +7 (495) 632-22-47, e-mail: skryl@bmstu.ru.
Stanislav A. Vinokurov, Ph.D. (Engineering), associate professor, deputy head for academic affairs, Voronezh Institute of the Ministry of Internal Affairs of Russia, 53, prospekt Patriotov, Voronezh, 394065, Russia, tel.: +7 (473) 247-67-07, e-mail: vinokurovvs@yandex.ru.

Timofey B. Khodyrev, junior scientific assistant, senior inspector for special assignments, Federal service of the national guard of the Russian Federation, 9a, str. 4, ulitsa Krasnokazarmennaya, Moscow, 111250, Russia, tel.: +7 (916) 607-97-31, e-mail: tim-hod@yandex.ru.
Anatoliy V. Mazin, D.Sc. (Engineering), professor, head of the Department, Bauman Moscow State Technical University, Kaluga branch, 2, ulitsa Bazhenova, Kaluga, 248000, Russia, tel.: +7 (910) 915-58-25, e-mail: mazinav@yandex.ru.
Denis A. Kholod, postgraduate student, assistant, Bauman Moscow State Technical University, 5, str. 1, ulitsa 2-ya Baumanskaya, Moscow, 105005, Russia, tel.: +7 (499) 263-69-55, e-mail: dekholod@yandex.ru.

Поступила 30.04.2020; принята к публикации 26.07.2020; опубликована онлайн 07.09.2020.
Submitted 30.04.2020; revised 26.07.2020; published online 07.09.2020.