УДК: 621.396.962 DOI: 10.53816/23061456_2022_11–12_61

ПРОБЛЕМА УВЕЛИЧЕНИЯ ФУНКЦИОНАЛЬНОЙ СЛОЖНОСТИ ИНТЕГРИРОВАННЫХ СИСТЕМ БЕЗОПАСНОСТИ

THE PROBLEM OF INTEGRATED PHYSICAL SECURITY SYSTEMS FUNCTIONAL COMPLEXITY INCREASING

Канд. тех. наук В.Г. Сосунов, канд. тех. наук И.В. Логинов

Ph.D. V.G. Sosunov, Ph.D. I.V. Loginov

Академия ФСО России

В статье рассмотрен процесс непрерывного развития интегрированных систем безопасности. Существующие тенденции развития таких систем приводят к развитию проблемы увеличения структурно-функциональной сложности системы и соответственно усложнения процессов ее управления. Проявления проблемы, заключающейся в значительном увеличении количества технических средств охраны, характеризуются масштабным изменением требований к профессиональным качествам персонала. Результатом такого процесса является специализация среди сотрудников охраны и появление категорий операторов технических средств охраны (ТСО), администраторов ТСО, проектировщиков, непосредственно не решающих задачу охраны, а только ее обеспечивающих. Выполнено описание основных характеристик проблемы усложнения вследствие увеличения количества функциональных подсистем и снижения времени между модернизациями. Представлены направления совершенствования процессов управления функциональным развитием интегрированных систем безопасности.

Ключевые слова: система физической защиты, интегрированная система безопасности, ресурсоемкость, непрерывное развитие, сложность, интеграция, модернизация.

The article considers the process of continuous development of integrated security systems. The existing trends in the development of such systems lead to the development of the problem of increasing the structural and functional complexity of the system and, accordingly, complicating its management processes. The manifestations of the problem, consisting in a significant increase in the number of technical means of protection, are characterized by a large-scale change in the requirements for the professional qualities of personnel. This, in turn, leads to specialization among security personnel and the emergence of categories of technical security eqipment (TSE) operators, TSE administrators, designers who do not directly solve the problem of protection, but only provide it. The description of the main characteristics of the problem of complication due to an increase in the number of functional subsystems and a decrease in the time between upgrades is carried out. The directions of improving the processes of managing the functional development of integrated security systems are presented.

Keywords: physical protection system, integrated security system, resource intensity, continuous development, complexity, integration, modernization.

Введение

В настоящее время в сфере обеспечения физической безопасности объектов наблюдается процесс активного развития интегрированных систем безопасности (ИСБ) [1, 2]. На первом этапе происходит объединение функций охранной сигнализации и телевидения с функциями контроля и управления доступом. Следующим шагом интегрируются функциональные подсистемы безопасности из списка в более чем 60 разнотипных подсистем безопасности. Изменение функций и назначений предприятий и организаций, территорий, акваторий и объектов, на которых оно расположено, списка угроз безопасности и возможных целей нарушителей, уровня оснащенности и технических возможностей нарушителей обосновывает необходимость непрерывного развития системы безопасности [3]. Для ее реализации возникает необходимость выстраивания рационального процесса управления с учетом неопределённости внешних и внутренних факторов [4, 5]. Значимое количество вариантов модернизации и ограничение лимитов ресурсов, выделяемых на совершенствование систем охраны, обосновывает решения ряда оптимизационных задач: выбор наилучших направлений модернизации, планирование программ развития, распределение ограниченных ресурсов, выделяемых на направления функциональные подсистемы [6, 7] в условиях значительного усложнения интегрированных систем охраны. Задача синтеза оптимальных ИСБ под конкретные угрозы в принципе решена [8], существующие подходы к построению интегрированных систем безопасности привели к значительному усложнению их структурно-функциональной сложности и значительному росту объемов потоков тревожных и информационных сообщений, что обуславливает актуальность рассмотрения проблемы масштабирования системы охраны с учетом ограничений на человеческие ресурсы при нарастании угроз физической безопасности.

Увеличение функциональной сложности интегрированных систем охраны: тенденции

В настоящее время происходит быстрое совершенствование технических средств, применяемых при проникновении на объекты, что приводит к расширению возможностей типовых нарушителей и актуализации дополнительных угроз безопасности, в том числе связанных с информационно-техническими воздействиями. Это обуславливает увеличение уровня значимости междисциплинарной проблемы масштабируемости развития интегрированной системы безопасности.

Развитие интегрированных систем безопасности путем последовательной модернизации функциональных подсистем и постепенного наращивания новых функциональных возможностей (например, внедрение видеоаналитики, термометрии, контроля посетителей) привело к существенному изменению их принципов организации и методов построения. Современные интегрированные системы безопасности представляют собой сложные многофункциональные системы, включающие десятки подсистем (по ГОСТ Р 57674-2017, ГОСТ Р 23704-2009) и решающие задачи не только обеспечения физической защиты объекта, но и реализующие дополнительные функции обеспечения безопасности: противопожарную безопасность, оповещение персонала и управления эвакуацией посетителей при возникновении экстренных ситуаций; обеспечения функционирования систем жизнеобеспечения и т.д. В основе инфраструктуры систем охраны лежат высокопроизводительные компьютерные сети. Наблюдаются следующие эффекты комплексирования при организации систем защиты:

– положительные: потенциальное повышение согласованности использования возможностей систем безопасности; снижение ресурсоемкости функционирования (уменьшение количества основного и вспомогательного персонала службы безопасности); снижение расходов на общие составляющие (транспортные коммуникационные сети, управляющие модули); возможность создания единого центра технического обслуживания;

– отрицательные: повышение структурной и функциональной сложности; повышение требований к квалификации персонала, увеличение сроков обучения сотрудников.

Наблюдаемая структурно-функциональная сложность организации интегрированной системы безопасности проявляется в следующих аспектах, затрудняющих управление функциональным развитием:

– структурная и функциональная сложность. В состав рассматриваемых систем безопасности может входить до десятков-сотен тысяч разнотипных компонентов (датчиков, средств связи и преобразования, исполнительных механизмов), программных средств аналитической обработки и интеграции;

– непрерывная эволюция. Значительная длительность жизненного цикла ИСБ, в течение которого сменяются несколько поколений функциональных подсистем. Объектовые системы безопасности развиваются вместе с объектами, на которых расположены предприятия, и соответственно могут функционировать десятки лет;

– высокая интенсивность смены поколений компонентов (организационных, технических и методических), затрудняющая управление развитием сложных интегрированных систем. Объективная сложность объекта управления приводит к проблеме синтеза длительно функционирующих систем из множества компонентов различных поколений, находящихся к тому же на разных стадиях жизненного цикла.

Проблема структурно-функциональной сложности ИСБ происходит от типового процесса модернизации, предусматривающего внедрение новых технических средств (интеграции дополнительных подсистем). Исторически в состав системы входит множество необслуживаемых датчиков с высокой наработкой до отказа и незначительное количество пультовых приборов, требующих обслуживания. Пример: исходное состояние ИСБ, в которую интегрирована система охранно-пожарной сигнализации с системой контроля и управления доступом (СКУД) включает тысячи датчиков с наработкой на отказ и ложное срабатывание, достигающие 100 000 часов и 10 000 часов соответственно. Общая трудоемкость обслуживания системы в процессе эксплуатации была относительно незначительной и сводилась к проведению регламентных работ, и замене вышедших из строя датчиков. Появление новых технических средств (видеокамер, тепловизоров, интеллектуальных средств аналитики) кардинально изменило ситуацию. Во-первых, данные средства имеют значительно меньшую наработку на отказ и требуют технического обслуживания в процессе эксплуатации (сотни датчиков с наработкой на отказ и ложное срабатывание порядка 1000 часов). Во-вторых, возможности ее адаптации под внешние требования приводят к дополнительной нагрузке по ее настройке. Возникают дополнительные процессы обслуживания, которые не предусматриваются, например — управление версиями. Вопросы автоматизации управления, в частности за счет их интеграции, оставлены на втором плане. В такой ситуации экспоненциальный рост количественного состава технических средств систем безопасности приводит к коллапсу возможности управления системой из-за превышения порога структурной сложности, что является одним из аспектов проблемы масштабируемости ИСБ.

Длительный жизненный цикл интегрированных систем безопасности в целом и снижение времени эксплуатации отдельных технических средств в ее составе приводят к проблеме излишней ресурсоемкости процессов технической поддержки в рамках жизненного цикла. Она заключается в излишних затратах человеческих, временных и материальных ресурсов на сопряжение и замену унаследованных технических средств в составе интегрированной системы безопасности, что затрудняет развитие при росте угроз безопасности. Наблюдается типовая ситуация, при которой сопровождение уже существующих систем охраны не позволяет внедрять новые технические средства охраны из-за недостаточности выделенных ресурсов. При этом отсутствует возможность замены всей системы одномоментно. Перспективное состояние ИСБ при этом может характеризоваться следующими показателями:

– количество подсистем охраны — до 70;

– срок службы датчика — менее 3 лет (морально устаревает);

– срок службы базового программного обеспечения — менее года;

– период обновления программных компонентов — раз в несколько месяцев (а в перспективе будут обновляться как любые программные средства — то есть еще чаще);

– необходимость поддержки сопутствующей инфраструктуры (телекоммуникационная сеть, вычислительное ядро).

При этом новые технологии характеризуются значительно увеличенной стоимостью по сравнению с ранее использовавшимися образцами.

В результате в условиях ограниченных ресурсов это приводит либо к стагнации (поддержка существующей функциональности системы охраны без возможности внедрений новых функций), либо к деградации интегрированной системы охраны (внедрение новых функций без возможности поддержки старых на заданном уровне).

Увеличение функциональной сложности интегрированных систем охраны: следствия

Усложнение структурно-функционального состава интегрированных систем охраны приводит к расширению профессиональных требований к персоналу охраны (рис. 1) и требует уточнения содержания минимальных знаний и навыков в области охраны [9]. В рамках системы охраны первоначально выделяется две основные категории: сотрудники охраны и техники ТСО, выполняющие задачи по техническому обслуживанию имеющегося оборудования. Увеличение количества функций пультового оборудования приводит к вводу в типовой штат подразделений охраны специальных должностей, ответственных за работу с ТСО, — операторов ТСО. Таким образом, происходит разделение функций охраны и контроля состояния сигналов от ТСО. Основных причин две: изменение характера взаимодействия с ТСО, необходимости непрерывного наблюдения за подаваемыми сигналами, и необходимости наличия специальных навыков по эксплуатации пультового оборудования ТСО. Следует отметить, что в комплексных системах типа «безопасный город», взаимодействующих в онлайн режиме со множеством разнородных информационных систем, для обеспечения непрерывного информационного обмена, требуется инженер (программист) в составе дежурной смены.

С другой стороны, развитие ИСБ привело к увеличению сложности процессов ее эксплуатации. Изначально для большинства вариантов применения ИСБ после ее ввода в эксплуатацию было достаточно техника ТСО, решающего задачи технического обслуживания датчиков и пультовых устройств. Объединение множества функциональных подсистем охраны, систем видеонаблюдения, в том числе на базе компьютерных сетей, привело к необходимости администрирования информационных систем безопасности, обеспечивающих компьютерных и телекоммуникационных сетей, и соответственно наличия выделенного инженера (администратора) ТСО. Снижение промежутков времени между модернизациями функциональных подсистем с параллельным увеличением количества функциональных компонентов приводит к непрерывной эволюции состава интегрированной системы безопасности. И здесь уже сам постоянный характер деятельности определяет необходимость наличия специалиста-проектировщика, ответственного за модернизацию ИСБ (включая формирование требований, работу с поставщиками, тестирование при вводе в эксплуатацию).

Рассмотрим изменение характера применения ТСО в интегрированных системах охраны. В настоящее время ввод новых датчиков охраны, в первую очередь от системы видеоаналитики, привел к значительному их росту: на одну камеру может быть до 10 сенсоров видеоанализа — количество датчиков n увеличивается на порядок. С другой стороны, надежность новых датчиков

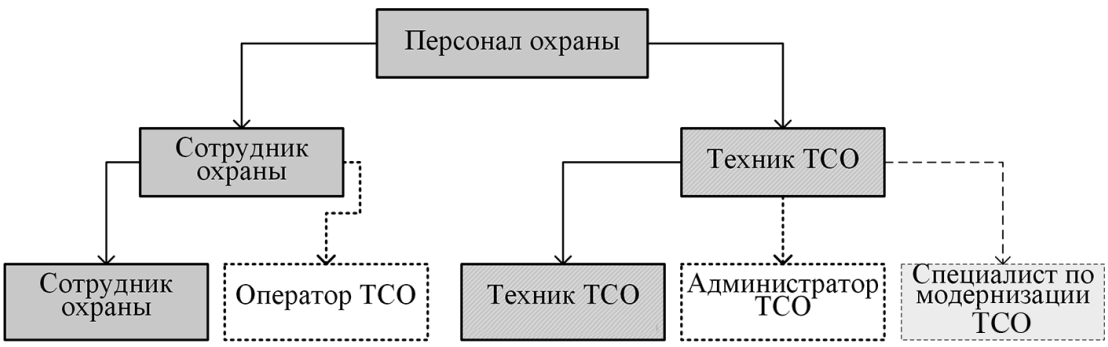


Рис. 1. Изменение профессионального состава персонала охраны при усложнении интегрированных систем охраны

(обнаружения, идентификации) значительно меньше. Если датчики вскрытия имеют наработку на ложное срабатывание $\bar{t}_{л} = 10000$ и более часов, то средства видеоаналитики даже наработку $\bar{t}_{л} = 1000$ при требуемых показателях обнаружения практически не демонстрируют. Соответственно интенсивность ложных срабатываний начинает превышать разумные пределы: $\lambda_{л} = \lambda_{л}\left(n, \bar{t}_{л}\right)$ — до 10 и более срабатываний в час (рис. 2). Психоэмоциональные и физиологические способности человека при этом ограничены возможностью реагирования на 30–60 тревожных сообщений в час. При этом действия сил охраны в большинстве случаев ориентированы на единичные случаи реагирования. Возникает два основных психолого-физиологических следствия: повышение утомляемости (и загруженности) сотрудника охраны и снижение воспринимаемого эффекта опасности от поступающего тревожного сообщений.

Решение данной проблемы промышленность видит в развитии средств снижения воспринимаемой сложности интерфейсов интегрированных систем охраны. В рамках концепции Physical security information management (платформы для интеграции и управления комплексами безопасности) предлагается комплексировать потоки тревожных сообщений и тем самым кардинальным образом снизить их интенсивность до разумного предела [10]. Крупнейшие мировые лидеры в данном направлении: CNL Software Ltd, Genetec Inc, Hexagon AB, Johnson Controls International Plc, NEC Corp., NICE Ltd., Qognify Ltd., Robert Bosch GmbH, Verint Systems Inc., Vidsys Inc., Tyco international, AxxonSoft, Intergraph Corporation, Milestone System, PRYSM Software. Среди национальных разработок следует отметить ESM, R-PLATFORMA, Интегра 4D-Планета Земля, интеллект которых отличает развитие функций ситуационно-аналитического анализа ситуации безопасности на основе единой системы тревог и поддержки принятия регламентированных решений. При этом достижение эффекта в повышении ситуативной осведомленности о состоянии безопасности объекта с минимизацей потоков тревожных и информативных сообщений должно быть подтверждено практическими результатами — снижением интенсивности ложных срабатываний при обеспечении заданной вероятности обнаружения угроз установленных типов.

С другой стороны, структурно-функциональное усложнение интегрированных систем охраны приводит к существенному увеличению ресурсоемкости процессов их сопровождения. В общем случае ресурсоемкость складывается из процессов эксплуатации и модернизации: $R = R_{э} + R_{м}$. Ресурсоемкость эксплуатации включает в себя затраты на техническое обслуживание, ремонт, администрирование и зависит прямо пропорционально от количества технических средств: $R_{э} = O_1\left(n\right)$. Ресурсоемкость модернизации (развития) включает затраты на новые технические средства охраны, зависит линейно от интенсивности поступления заявок на модернизацию (рис. 3, *а*) и от сложности системы (квадратично зависит от количества компонентов): $R_{м} = O_2\left(\lambda_{м}\right) + O_3\left(n^2\right)$, где интенсивность

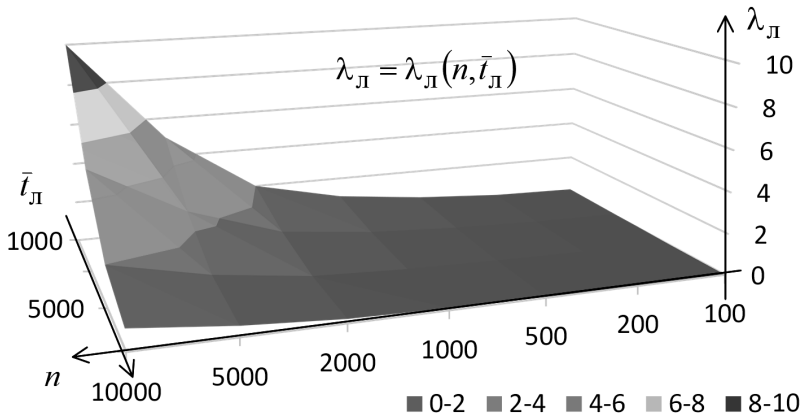
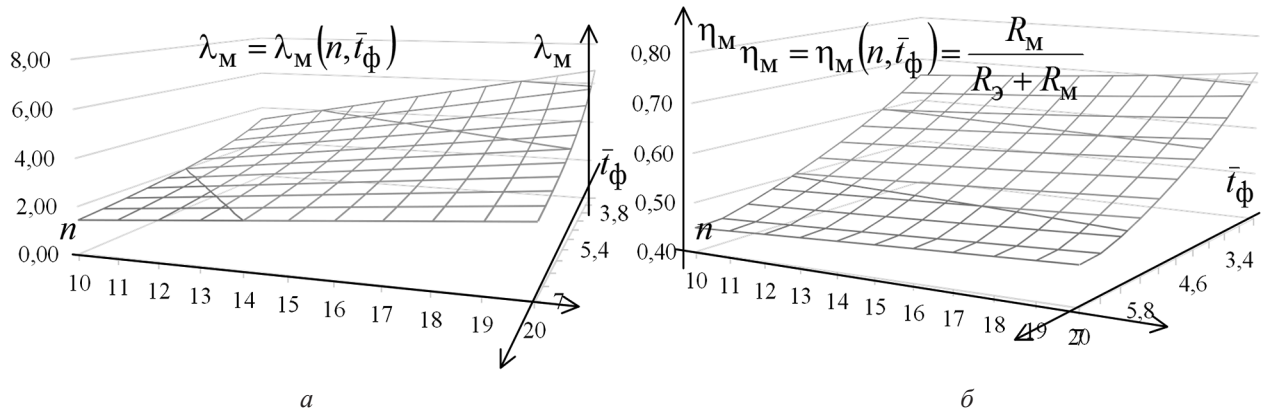


Рис. 2. График изменения интенсивности ложных срабатываний при усложнении интегрированной системы охраны



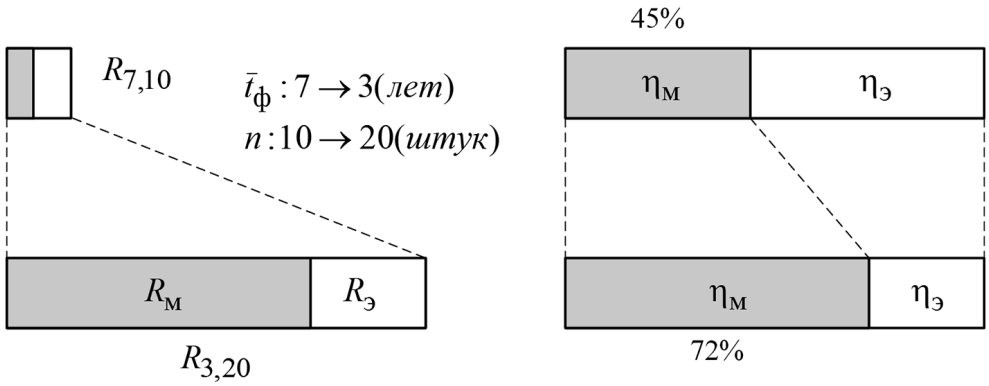
а *б*

Рис. 3. График изменения: а — интенсивности заявок на модернизацию ИСБ; б — доли ресурсов на модернизацию в общем объеме ресурсов

поступления заявок на модернизацию — $\lambda_м = n / \bar{t}_ф$. Наблюдаемое изменение количества компонентов и снижение времени между модернизациями приводит к изменению распределения доли ресурсов, затрачиваемых на разные статьи расходов (рис. 3, *б*; 4, *б*):

$$\eta_м = \eta_м\left(n, \bar{t}_ф\right) = \frac{R_м}{R_э + R_м}.$$

В целом наблюдается значительное увеличение ресурсоемкости сопровождения ИСБ в процессе их эксплуатации как на модернизацию функциональных подсистем охраны, так и на техническое обслуживание (эталонный пример на рис. 4, *а*). Причем за счет компьютеризации технических систем охраны начинает существенно возрастать объем трудоемких высококвалифицированных работ (проектирование, обоснование требований, разработка методик испытаний). Решением указанной проблемы является использование PSaaS-подхода (Physical Security as a Service) — передача услуг охраны полностью или частично на аутсорсинг. В этом случае трудоемкие задачи передаются поставщикам охранных услуг, где за счет эффекта масштаба может быть достигнуто снижение ресурсоёмкости, например: администрирование центра обработки данных (ЦОД) на 30 и 300 видеосерверов не требует увеличения ресурсов администрирования на порядок. Однако в таком подходе есть недостатки: стандартизация охранных услуг только начата (на 2021 год действует только три ГОСТ), практики распределения рисков между поставщиком и потребителем охранных услуг не наработаны, вопросы контроля предоставления услуг также не проработаны.



а *б*

Рис. 4. График изменения: а — потребности в ресурсах на эксплуатацию ИСБ; б — долей ресурсов на модернизацию и эксплуатацию ИСБ

Увеличение функциональной сложности интегрированных систем охраны: решения

Проблема обеспечения непрерывного развития сложных технических систем характерна для многих областей применения. В настоящее время выделен класс киберфизических систем, характеризующихся наличием выделенных технических средств и функционирующих в вычислительном пространстве программных компонентов. Современные интегрированные системы безопасности относятся к такому классу сложных систем, и соответственно пути решения известных проблем являются аналогичными. Наряду со стандартными механизмами снижения сложности, такими как стандартизация, унификация, можно выделить следующие направления совершенствования процессов управления:

– переход к управлению развитием интегрированных систем безопасности на основе моделей объекта управления. Все технические подсистемы охраны должны быть идентифицированы и установлены для противодействия угрозам для борьбы с которыми они созданы (создаются). Должны быть определены метрики расчета эффекта противодействия угрозам и периодически выполняться расчет значений эффективности;

– ограничение функционального разнообразия технических подсистем охраны. Данный механизм предполагает обоснованный выбор необходимости ввода новой функциональной подсистемы и периодической проверки необходимости функционирования действующих систем;

– внедрение технических подсистем с высокими эргономическими характеристиками. Новые системы должны быть проще (по применению, знаниям, навыкам) и лучше с точки зрения ситуативной осведомленности. Проверка реальных оценок освояемости, требований к квалификации персонала, времени применения должна проводиться при сравнении альтернативных вариантов новых систем;

– минимизация технического персонала в составе службы охраны — с точки зрения службы охраны весь персонал, кроме сотрудников охраны, является непроизводственным — не сможет противодействовать инциденту в кризисной ситуации. Целесообразно наделять сотрудников охраны нештатными обязанностями, чтобы оптимизировать не задействованный на решении задач охраны большую часть времени персонал.

Выводы

В настоящей статье рассмотрена проблема увеличения функциональной сложности интегрированных систем безопасности: постепенный рост количества функциональных подсистем охраны, устройств сигнализации, пультов охраны, камер и программных средств видеонаблюдения приводит к изменению принципов организации ИСБ. Отмечается, что наблюдается изменение профессионального состава персонала охраны при усложнении интегрированных систем охраны, появление новых должностных обязанностей и рост ресурсоемкости сопровождения и модернизации. Решение проблемы в условиях ограниченных ресурсов может быть достигнуто ограничением функционального разнообразия технических подсистем охраны с повышением их эргономических характеристик.

Литература

1. Peida Xu, Yong Deng, Xiaoyan Su, Xin Chen, and Sankaran Mahadevan. An evidential approach to physical protection system design. Safety Science, 65(0): 125-137, 2014. ISSN 0925-7535. doi: http://dx.doi.org/10.1016/j.ssci.2014.01.003.URL.

2. Garcia Mary Lynn. The design and evaluation of physical protection systems. 2001. 336 p.

3. Patrick T. Hester. Facility protection optimization under uncertainty. Phd thesis. 2007. 173 p.

4. Cody Harrison Fleming. Safety-driven Early Concept Analysis and Development. Phd thesis. 2015. 230 p.

5. Zou Bowen, Yang Ming, Yoshikawa Hidekazu, Lu Honghing. Evaluation of physical protection systems using an integrated platform for analysis and design // IEEE Transactions on systems, mans and cybernetics systems. 2017. Vol. 47. No 11. Pp. 2945–2955.

6. Dejan Cakija, Zeljko Ban, Marin Golub, Dino Cakija. Optimizing physical protection system using domain experienced exploration method // Automatika, Journal for Control, Measurement,

Electronics, Computing and Communications. 61: 2. 2020. Pp. 207–218.

7. Рыжова В.А. Проектирование и исследование комплексных систем безопасности. — Санкт-Петербург. НИУ ИТМО. 2012. 157 с.

8. Костин В.Н. Модернизация структуры физической защиты критически важных объектов информатизации на основе выбора эффективных решений // Вестник компьютерных технологий. 2019. Т. 25. № 12. С. 757–765.

9. Coole, Michael & Brooks, David & Treagust, David. (2015). The Physical Security Professional: Formulating a Novel Body of Knowledge. Journal of Applied Security Research. 10. 385-410. 10.1080/19361610.2015.1038768.

10. PSIM системы в России: признаки, эффекты, перспективы. Мнения экспертов (2020). Системы безопасности. № 5. С. 70–78.

References

1. Peida Xu, Yong Deng, Xiaoyan Su, Xin Chen, and Sankaran Mahadevan. An evidential approach to physical protection system design. Safety Science, 65(0): 125-137, 2014. ISSN 0925-7535. doi: http://dx.doi.org/10.1016/j.ssci.2014.01.003.URL.

2. Garcia, Mary Lynn. The design and evaluation of physical protection systems. 2001. 336 p.

3. Patrick T. Hester. Facility protection optimization under uncertainty. Phd thesis. 2007. 173 p.

4. Cody Harrison Fleming. Safety-driven Early Concept Analysis and Development. Phd thesis. 2015. 230 p.

5. Zou Bowen, Yang Ming, Yoshikawa Hidekazu, Lu Honghing. Evaluation of physical protection systems using an integrated platform for analysis and design // IEEE Transactions on systems, mans and cybernetics systems. Vol 47, No 11, November 2017. Pp. 2945–2955.

6. Dejan Cakija, Zeljko Ban, Marin Golub, Dino Cakija. Optimizing physical protection system using domain experienced exploration method // Automatika, Journal for Control, Measurement, Electronics, Computing and Communications. 61: 2. 2020. Pp. 207–218.

7. Ryzhova V.A. Design and research of complex phisical protection systems. — St. Petersburg. NIU ITMO. 2012. 157 p.

8. Kostin V.N. Modernization of the structure of physical protection of critical informatization objects based on the choice of effective solutions // Bulletin of Computer Technologies. 2019. Vol 25. No. 12. Pp. 757–765.

9. Coole, Michael & Brooks, David & Treagust, David. (2015). The Physical Security Professional: Formulating a Novel Body of Knowledge. Journal of Applied Security Research. 10. 385-410. 10.1080/19361610.2015.1038768.

10. PSIM systems in Russia: signs, effects, prospects. Expert opinions 2020). Security Systems. No 5. Pp. 70–78.