

## НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ ДЛЯ РАДИАЦИОННО-ОПАСНЫХ ОБЪЕКТОВ

© 2018 К.Г. Терехов

АО «ФЦНИВТ «СНПО «Элерон», Москва, Россия

Безопасность объектов атомной отрасли невозможно обеспечить без применения систем контроля и управления доступом на радиационно-опасном объекте (СКУД РОО). В статье рассматриваются особенности проектирования и эксплуатации оборудования, входящего в состав РОО: турникеты, радиационные мониторы, средства интеллектуального видеонаблюдения, биометрические сканеры и т.д. Указаны меры противодействия несанкционированным действиям нарушителя на контрольно-пропускных пунктах (КПП), описаны способы обнаружения запрещенных к проносу веществ, электронные удостоверения личности. Приводятся варианты защиты информационных активов от несанкционированного доступа в СКУД. Отмечены перспективы развития СКУД. Минимизация роли персонала охраны при соответствующем развитии функциональных возможностей СКУД позволяет защититься от ошибок или умышленных действий, сократить время контроля параметров доступа, повысить качество контроля при сокращении финансовых затрат, обеспечить эффективное противодействие подготовленному внешнему и внутреннему нарушителю.

*Ключевые слова:* Глобальная ядерная безопасность, радиационно-опасный объект, атомная отрасль, человеческий фактор, СКУД, КПП, радиоактивные вещества, контрольно-пропускной пункт, классы аппаратуры обнаружения, классификация объектов поиска, досмотровое оборудование.

Поступила в редакцию: 25.07.2018

Вопросы глобальной ядерной безопасности кроме хорошо известных проблем, связанных с экологическим загрязнением окружающей среды в результате радиационных аварий [1], радиационного и радиационно-экологического контроля, осуществляемых как в штатной работе, так и при аварийных ситуациях [2, 3], включают также защиту от угроз, связанных с действиями нарушителя радиационно-опасных объектов (РОО). В атомной отрасли это АЭС, технологические и исследовательские реакторы, заводы по работе с ядерными и радиоактивными материалами, предприятия для получения изотопов, хранилища радиоактивных отходов и т.д. Для локализации угроз РОО, связанных с человеческим фактором (несанкционированный доступ, хищения с целью терроризма и другими случаями) объекты атомной отрасли оснащают специальными техническими средствами – системами контроля и управления доступом (СКУД) [4].

Актуальным вопросом для специалистов, занимающихся изысканием, проектированием, строительством и монтажом СКУД РОО, является определение перспективных направлений развития этих систем. Согласно многолетнему опыту АО «ФЦНИВТ «СНПО «Элерон» по проектированию, монтажу и эксплуатации СКУД на объектах атомной отрасли они должны удовлетворять следующими тактико-техническими требованиями [5]:

- обеспечивать автоматическое противодействие попыткам несанкционированного действия (НСД) на контрольно-пропускных пунктах (КПП);
- удостоверять личность проходящих лиц по двум и более признакам, в том числе биометрическим;
- выявлять наличие запрещенных предметов и веществ (ЗПВ) у проходящих лиц, преимущественно в автоматическом режиме;
- обеспечивать защиту аппаратных средств СКУД и информационных активов от

НСД на КПП.

Рассмотрим современные технологические методы и средства, позволяющие реализовать вышеуказанные требования.

## ПРОТИВОДЕЙСТВИЕ НСД НА КПП

Под несанкционированными действиями понимается совершение или попытка совершения диверсии, хищения ядерных материалов, ядерных установок, несанкционированного доступа, проноса (провоза) запрещенных предметов, вывода из строя или нарушения функционирования инженерно-технических средств физической защиты [6].

Наиболее вероятными целями (угрозами) нарушителей на охраняемом объекте могут быть:

1) хищение радиоактивных, ядерных материалов для возможного дальнейшего их применения, распространения технологий производства РВ в зарубежных странах или с целью шантажа;

2) вывод из строя (подрыв) элементов объекта, содержащих радиоактивные вещества (РВ), с целью создания аварийной ситуации на охраняемом объекте;

3) захват объекта с целью завладения хранящимися РВ, в том числе и для демонстрации силы террористических (преступных) элементов;

4) блокирование или вывод из строя объекта или отдельных его элементов для привлечения внимания общественности к выдвигаемым экстремистскими группами экологическим, экономическим, политическим и иным требованиям с целью усложнения социально-политической обстановки в данном регионе;

5) нападение на личный состав караула и боевых постов с целью завладения оружием и захвата отдельных военнослужащих в качестве заложников;

6) сбор и хищение информации о назначении объекта, о количестве и номенклатуре хранящихся специзделий, графиках и порядке их транспортировки и т.п.

Автоматизация выявления НСД на КПП и в зонах контроля пропускных устройств (ПУ) СКУД достигается посредством применения шлюзовых конструкций, оснащенных весоизмерительными устройствами, различными датчиками защиты от проникновения, а также интеллектуальными средствами телевизионного наблюдения, которые обеспечивают:

– детектирование перемещения (проброса) запрещенных предметов через зону контроля;

– обнаружение оставленных предметов;

– проверку установленного порядка прохождения зоны контроля.

От данного перечня задач зависит конфигурация КПП, конструкции автоматических пропускных устройств (АПУ), используемых средств досмотра и т.д.

Перспективным также является использование интеллектуальных средств видеонаблюдения для автоматического выявления НСД. В настоящее время возможности видеонализа существенно возросли, чему во многом способствует переход на цифровые видеокамеры высокой четкости. Перспективные средства видеонаблюдения и оценки ситуации способны в автоматическом режиме не только детектировать движение в указанных областях кадра, обнаруживать оставленные предметы, осуществлять многокамерное сопровождение объекта, измерять статические и динамические биометрические признаки контролируемых лиц, но также определять эмоциональное состояние людей.

Применение интеллектуальных средств видеонаблюдения совместно с быстродействующими управляемыми преградами позволит существенно увеличить пропускную способность КПП за счет отказа от ручного досмотра с применением часового.

Таким образом, существенная минимизация роли персонала охраны при соответствующем развитии функциональных возможностей СКУД позволяет защититься от ошибок или умышленных действий, сократить время контроля параметров доступа, повысить качество контроля при сокращении финансовых затрат, обеспечить эффективное противодействие подготовленному внешнему и внутреннему нарушителю.

## ОБНАРУЖЕНИЕ ЗАПРЕЩЕННЫХ К ПРОНОСУ ПРЕДМЕТОВ И ВЕЩЕСТВ (ЗПВ)

Проблема автоматизации процедур досмотра проходящих лиц на предмет выявления ЗПВ в настоящее время является наиболее трудноразрешимой. Можно констатировать, что с определенным качеством может решаться задача обнаружения ядерных материалов, радиоактивных веществ, металлосодержащих предметов. Вместе с тем перечень запрещенных веществ достаточно обширен и включает в себя взрывчатые, наркотические, отравляющие, психотропные и тому подобные вещества. В этой связи интересным техническим решением, направленным на автоматизацию обнаружения ЗПВ, является совмещение аппаратуры обнаружения со средствами биометрического контроля. Например, возможно рассматривать совместное функционирование газоаналитического оборудования для обнаружения следов взрывчатых, наркотических и психотропных веществ на руках контролируемых лиц с биометрическими сканерами отпечатка пальца или геометрии кисти руки.

В настоящий момент развитие металлообнаружителей идет по пути увеличения точности локализации предметов поиска в пространстве портала [7], улучшения селективности по признакам, позволяющим отличить предмет поиска от предмета личного пользования, а также улучшения показателей помехоустойчивости, надежности, чувствительности. В то же время не прекращается поиск путей автоматизации процедур выявления металлических предметов и их идентификации, что позволит снизить роль человеческого фактора и существенно сократить время досмотра.

Визуализацию скрытых предметов можно осуществить с помощью радиовидения. В этой связи актуальным является повышение интеллектуальности алгоритмов обработки изображений, полученных в различных диапазонах длин волн (сантиметровом, миллиметровом, терагерцевом и др.).

В области обнаружения РВ становится все более очевидно, что простого детектирования недостаточно, например, согласно [8] требуется обнаружение количества РВ, превышающего значение минимально значимой активности, которая для разных нуклидов существенно различается. Кроме того, опыт эксплуатации оборудования обнаружения РВ показывает, что срабатывание детекторов приводит к длительной процедуре поиска и выявления причин, поэтому перспективным на сегодня направлением является замена радиационных мониторов, определяющих лишь факт превышения над фоновым уровнем, соответствующей спектрометрической аппаратурой, способной обнаруживать, идентифицировать и локализовать в пространстве РВ.

Отметим, что в задачу обнаружения ЗПВ входит также пресечение выноса конфиденциальных документов и материальных ценностей с территории предприятия.

Перспективным решением, уже используемым в некоторых СКУД, является нанесение на документы и материальные ценности RFID-идентификаторов (подобных тем, что используются в торговле и логистике). Активный радиочастотный идентификатор, представляющий собой наклейку, позволит отслеживать местонахождение предметов и документов в реальном времени.

## УДОСТОВЕРЕНИЕ ЛИЧНОСТИ [9]

В связи с запланированным массовым введением электронных удостоверений личности перспективным является использование информации с указанных носителей для ее внесения в базу данных СКУД в автоматическом режиме. Это, в свою очередь, улучшит

качество и ускорит процедуру регистрации абонентов и изготовления пропускных документов.

В настоящее время в СКУД критически важных объектов активно используются устройства биометрической верификации. Однако практика показывает, что любую самую совершенную биометрическую систему может дискредитировать достаточно большое значение вероятности ложного задержания. Особенно это проявляется при массовом проходе. В основном ошибка считывания биометрических параметров объясняется внутрииндивидуальной вариабельностью измеряемых признаков, которая может быть учтена при использовании соответствующих адаптивных решающих правил.

Вместе с тем для достижения требуемых значений вероятностей ошибок первого и второго рода необходимо иметь механизмы расчета и управления порогами обнаружения и режимами биометрического контроля, что достигается посредством статистического анализа считываемых биометрических данных.

С точки зрения психологии пользователей и увеличения пропускной способности СКУД предпочтительно использовать бесконтактные биометрические технологии контроля, например по радужной оболочке глаза, по рисунку вен на руках, по 3D-геометрии лица и др.

Также является перспективным использование активных RFID-пропусков для бесконтактной идентификации. Особенно преимущество этой технологии проявляется в аварийных ситуациях в условиях свободного прохода, когда сохраняется возможность зарегистрировать всех лиц, покинувших охраняемую зону.

Важнейший фактор минимизации рисков безопасности и нарушения приватности, связанных с биометрическими системами, – защита биометрических шаблонов, хранящихся в базе данных системы. Эта проблема становится все более актуальной в связи с широким использованием биометрической идентификации в повседневной жизни, что ведет к появлению слабезащищенных баз данных с биометрическими шаблонами.

## ЗАЩИТА ИНФОРМАЦИОННЫХ АКТИВОВ ОТ НЕСАНКЦИОНИРОВАННЫХ ДЕЙСТВИЙ (НСД) В СКУД

С целью защиты информационных активов от хищения и несанкционированного изменения в СКУД могут использоваться, например:

- разделение защищаемой информации по нескольким центрам принятия решения;
- ресурсное резервирование оборудования СКУД;
- защита локальных центров принятия решения от несанкционированного доступа с помощью самого оборудования СКУД с обеспечением возможности его автономной работы;
- проведение аналитической работы в автоматическом режиме с целью выявления отклонений в технических характеристиках оборудования, информационных атак на активы и других незначительных отклонений от штатного функционирования, которые могут свидетельствовать о нарушениях или подготовительных мероприятиях к ним.

Классические методики защиты информации предполагают необходимость наличия в составе программного обеспечения сертифицированных функций обеспечения безопасности информации, а также применение сертифицированного базового программного обеспечения.

Подводя итог вышесказанному, направления совершенствования СКУД РОО [10] нацелены на получение следующих результатов:

- 1) повышение степени автоматизации процессов контроля и управления доступом с целью сокращения эксплуатационных затрат;
- 2) обеспечение надежности и безотказности оборудования СКУД, достигаемое за счет применения бесконтактных технологий и новых материалов;
- 3) внедрение в состав СКУД современных биометрических технологий и автоматических средств досмотра проходящих лиц;

4) развитие и совершенствование программного обеспечения СКУД, направленные как на решение задачи построения адаптивных (интеллектуальных) СКУД, так и на обеспечение защиты информационных активов системы [11].

5) Комплексование технологического оборудования (шлюз и радиационный монитор или шлюз и металлообнаружитель с радиационным монитором).

#### СПИСОК ЛИТЕРАТУРЫ

1. *Елохин, А.П.* Автоматизированные системы контроля радиационной обстановки окружающей среды: учеб. пособие для вузов [Текст] / А.П. Елохин. – Москва : МИФИ, 2012. – 316 с.
2. *Елохин, А.П.* Методы и средства систем радиационного контроля окружающей среды: Монография [Текст] / А.П. Елохин ; М-во образования и науки Российской Федерации, Нац. исслед. ядерный ун-т «МИФИ». – Москва : НИЯУ МИФИ, 2014. – 519 с.
3. *Елохин, А.П.* Основы экологии и радиационно-экологического контроля окружающей среды: учеб. пособие для вузов [Текст] / А.П. Елохин, А.И. Ксенофонтов, И.В. Пырков. – Москва : Изд-во «Тривант», 2016. – 680 с.
4. ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».
5. *Попов, М.Н.* Основные направления развития систем контроля и управления доступом в ФГУП «СНПО «Элерон» [Текст] / Попов М.Н., Горбачевич Н. – Каталог «СКУД. Антитерроризм», 2013. – С.42-43.
6. Постановление Правительства РФ от 19.07.2007 N 456 (ред. от 18.05.2017) «Об утверждении Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов».
7. *Терехов, К.Г.* Особенности выбора современных металлообнаружителей для особоопасных объектов [Текст] / К.Г. Терехов // Международная молодежная научная конференция «Полярное сияние 2009». Ядерное будущее: технологии, безопасность и экология: сборник тезисов докладов. – Москва : НИЯУ МИФИ, 2009. – С.132-133.
8. Правила радиационной безопасности при эксплуатации атомных станций (ПРБ АС-99). СП 2.6.1.28-2000. Москва 2000.
9. *Портной, Е.О.* некоторых особенностях систем контроля и управления доступом [Текст] / Е. Портной // Директор по безопасности. – 2011. – № 10.
10. *Иванов, П.Д.* Анализ состояния и перспективы развития систем контроля и управления доступом в России [Текст] / П.Д. Иванов, И.Д. Суверина // Инженерный журнал: наука и инновации. – 2014. – Вып. 10.
11. *Терехов, К.Г.* Системный подход к оснащению КПП СФЗ средствами автоматического контроля объектов поиска [Текст] / К.Г. Терехов, С.И. Журин // Спецтехника и связь № 5-6. – 2012. – С.19-23.

#### REFERENCES

- [1] Elokhin A.P. Avtomatizirovanny`e sistemy` kontrolya radiacionnoj obstanovki okruzhayushhej sredy`: ucheb. posobie dlya vuzov [Automated Systems for Monitoring the Radiation Environment of the Environment]. Nacional`ny`j issledovatel`skij yaderny`j universitet «МИФИ» [Textbook for High Schools. National Research Nuclear University "MEPI"]. Moscow. MEPI, 2012. 316 p. (in Russian).
- [2] Elokhin A.P. Metody` i sredstva sistem radiacionnogo kontrolya okruzhayushhej sredy`: Monografiya [Methods and Means of Radiation Monitoring Systems of the Environment]. The Monograph, 2014. 520 p. (in Russian).
- [3] Elokhin A.P., Ksenofontov A.I., Pyrkov I.V. Osnovy` e`kologii i radiacionno-e`kologicheskogo kontrolya okruzhayushhej sredy`: ucheb. posobie dlya vuzov [Bases of Ecology and Radiation-Environmental Control of the Environment]. Textbook for High Schools. Moscow. Publishing House «Tvant». 2016. 680 p. (in Russian).
- [4] GOST R 51241-2008 «Sredstva i sistemy` kontrolya i upravleniya dostupom. Klassifikaciya. Obshhie texnicheskie trebovaniya. Metody` ispy`tanij» [GOST R 51241-2008 «Means and Systems of Access Control and Management. Classification. General Technical Requirements. Methods of Testing»] (in Russian).
- [5] Popov M.N., Gorbachevich N. Osnovny`e napravleniya razvitiya sistem kontrolya i upravleniya dostupom v FGUP «SNPO «E`leron» [The Main Directions of the Development of Access Control Systems in FCS&HT "SNPO" Eleron]. Katalog «SKUD. Antiterrorizm» [Catalog «Anti-terrorism»]. 2013. P. 42-43 (in Russian).
- [6] Postanovlenie Pravitel`stva RF ot 19.07.2007 N 456 (red. ot 18.05.2017) [Decree of the Government of

- the Russian Federation No. 456 of 19.07.2007]. Ob utverzhdenii Pravil fizicheskoy zashhity` yaderny`x materialov, yaderny`x ustanovok i punktov xraneniya yaderny`x materialov [Approval of the Rules for the Physical Protection of Nuclear Materials, Nuclear Installations and Nuclear Storage Facilities] (in Russian).
- [7] Terekhov K.G. Osobennosti vy`bora sovremenny`x metalloobnaruzhitelej dlya osoboopasny`x ob`ektov [Features of Choice of Modern Metal Detectors for Dangerous Objects]. Mezhdunarodnaya molodezhnaya nauchnaya konferenciya «Polyarnoe siyanie 2009». Yadernoe budushhee: texnologii, bezopasnost` i e`kologiya: sbornik tezisov dokladov [International Youth Scientific Conference «Polar Lights 2009». Nuclear Future: Technology, Safety and Ecology: a Collection Of Abstracts]. Moskva, NIYaU MIFI [MoscowNNIU MEFhI]. 2009. P. 132-133 (in Russian).
- [8] Pravila radiacionnoj bezopasnosti pri e`kspluatacii atomny`x stancij (PRB AS-99). SP 2.6.1.28-2000. Moskva 2000 [Rules for Radiation Safety in the Operation of Nuclear Power Plants (PWB-99). SP 2.6.1.28-2000. Moscow 2000] (in Russian).
- [9] Portnoy E. O nekotory`x osobennostyax sistem kontrolya i upravleniya dostupom [Some Features of Access Control Systems]. Direktor po bezopasnosti [Director of Security]. 2011. № 10 (in Russian).
- [10] Ivanov P.D., Suverina I.D. Analiz sostoyaniya i perspektivy` razvitiya sistem kontrolya i upravleniya dostupom v Rossii [Analysis of the State and Prospects of Development of Access Control Systems in Russia]. Inzhenerny`j zhurnal: nauka i innovacii [Engineering Journal: Science and Innovations]. 2014. № 10 (in Russian).
- [11] Terekhov K.G., Zhurin S.I. Sistemny`j podxod k osnashheniyu KPP SFZ sredstvami avtomaticheskogo kontrolya ob`ektov poiska [A systematic Approach to Equipping the Check Point of the SFZ with Automatic Monitoring of Search Objects]. Specztexnika i svyaz` [Special Equipment and Communication]. 2012. № 5-6. P. 19-23 (in Russian).

## Directions of Access Control Systems Improving for Radiation Hazardous Facilities

**K.G. Terekhov**

*JSC FCS&HT "SNPO "Eleron", 14, Gen. Belova str., Moscow, 115563, Russia*

*ORCID iD: 0000-0002-5161-6337*

*WoS Researher ID: O-3704-2018*

*e-mail: gunper@mail.ru*

**Abstract** – The safety of nuclear facilities is not possible without the use of access control systems at a radiation hazardous facility (ACS ROO). The article deals with the design and operation of equipment included in the ROO: turnstiles, radiation monitors, intelligent video surveillance, biometric scanners, etc. Measures to counter unauthorized actions of the offender at checkpoints are described, methods for detecting substances banned to penetration, electronic identity cards are described. The article provides options for protecting information assets from unauthorized access to the ACS. Prospects for the development of the ACS have been noted. Minimizing the role of security personnel with the corresponding development of the ACS functionality allows us to protect ourselves from mistakes or deliberate actions, reduce the time for monitoring access parameters, improve the quality of control while reducing financial costs, and provide effective counteraction to the prepared external and internal violator.

*Keywords:* Global nuclear safety, radiation hazardous facility, nuclear industry, human factor, access control system, checkpoint, radioactive substances, detection equipment classes, classification of search objects, inspection equipment.