УДК 654.924

DOI: 10.51522/2307-0382-2021-233-10-69-76

**СЕРГЕЙ АЛЕКСАНДРОВИЧ
ДЕНИСЬЕВ**

преподаватель кафедры организации режима
и надзора в уголовно-исполнительной
системе Академии ФСИН России,
подполковник внутренней службы,
denisevser@rambler.ru,
<https://orcid.org/0000-0002-9451-7507>

Рязань

SERGEY A. DENISIEV

Lecturer of the Department of Organization
of Regime and Supervision in the Penitentiary
System of the Academy of the FPS of Russia,
Lieutenant Colonel of the Internal Service,
denisevser@rambler.ru,
<https://orcid.org/0000-0002-9451-7507>

Ryazan

Повышение эффективности интегрированных систем безопасности на охраняемых объектах уголовно- исполнительной системы

Improving the efficiency of integrated security systems
at guarded facilities of the penal system

Аннотация. В статье рассматриваются актуальные вопросы организации функционирования систем охранно-тревожной сигнализации, охранного телевидения, контроля и управления доступом, входящих в состав интегрированной системы безопасности объекта УИС.

Цель исследования – предметный анализ проблем, складывающихся в процессе оборудования техническими средствами охраны и надзора пульта управления техническими средствами охраны, помещения дежурного помощника начальника колонии, контрольно-пропускного пункта по пропуску людей, запретной зоны объекта УИС. Предметом статьи выступили реализованные и возможные интеграционные связи на программном и аппаратном уровнях между системой охранно-тревожной сигнализации, системой охранного телевидения, системой контроля и управления доступом. Методологическую основу исследования составили статистический метод, анализ, синтез, индукция, системно-структурный, формально-логический методы.

Обоснованы выводы о необходимости оборудования помещения дежурного помощника начальника колонии автоматизированным рабочим местом интегрированной системы безопасности; оборудования калиток для прохода в запретную зону считывателями бесконтактных карт для управления электромеханическим замком. Кроме того, высказаны предложения о необходимости обязательного информирования начальника караула о тревожной ситуации, возникающей в системе контроля и управления доступом на контрольно-пропускном пункте по пропуску людей; о целесообразности рассмотрения возможности верификации тревожных событий в запретной зоне посредством установки купольных видеокамер на наблюдательных вышках.

Практическое значение итогов работы заключается в том, что высказанные предложения могут

быть учтены при внесении возможных изменений в нормативные акты, регулирующие инженерно-техническое обеспечение объектов УИС.

Ключевые слова: инженерно-технические средства охраны и надзора, интегрированная система безопасности, система охранно-тревожной сигнализации, система охранного телевидения, система контроля и управления доступом, начальник караула, дежурный помощник начальника колонии, приборы приемно-контрольные охранно-пожарные.

Abstract. The article discusses topical issues of organizing the functioning of security and alarm systems, CCTV, access control and management systems, which are part of the integrated security system of a penal system facility.

The purpose of the study is a substantive analysis of the problems arising in the process of equipping with technical means of security and supervision the control panel for technical means of protection, the premises of the duty-assistant of the head of the colony, the checkpoint for the passage of people, the restricted areas of a penal system facility. The subject of the article is the realized and possible integration links at the software and hardware levels between the security and alarm system, the CCTV system, the access control and management system. The methodological basis of the research was formed by the statistical method, analysis, synthesis, induction, system-structural and formal-logical methods.

The conclusions on the need to equip the premises of the duty-assistant to the head of the colony with an automated workstation of the integrated security system have been substantiated; to equip the gates for access to the restricted area with proximity card readers to control an electromechanical lock. In addition, proposals were made on the need of mandatory informing the chief of the guard about the alarming situation arising in the biometric control and access control system at the checkpoint for the passage of people; on the feasibility of considering the possibility of verifying alarming events in the restricted area by installing dome cameras on observation towers.

The practical significance of the work results lies in the fact that the conclusions we have declared can be used to reequip integrated security systems used at the penal system facilities.

Key words: engineering and technical means of security and supervision, an integrated security system, a security and alarm system, a security television system, a control and access control system, the chief of the guard, an assistant to the head of the colony, security and fire control devices.

Для цитирования

Денисьев С. А. Повышение эффективности интегрированных систем безопасности на охраняемых объектах уголовно-исполнительной системы // Ведомости уголовно-исполнительной системы. 2021. № 10. С. 69–76.

05.12.13 Системы, сети и устройства телекоммуникаций (технические науки)
Systems, networks and telecommunication devices (technical sciences)

Н овое тысячелетие ознаменовалось переходом от аналоговых систем сбора и обработки информации к цифровым (компьютеризированным). В течение последних 20 лет происходит планомерное внедрение в эксплуатацию интегрированных систем безопасности (далее – ИСБ) на охраняемых объектах уголовно-исполнительной системы (УИС). В настоящее время наиболее широкое распространение нашли такие системы безопасности, как ИБК «Пахра», «Тобол-ИСБ», ИСО «Орион», ИСБ «Рубеж-08» и «Рубеж-09», «Микрос-02», «КОДОС», «Синергет-КСБО».

Введение в эксплуатацию на объектах УИС новой аппаратуры требовало пересмотра ведомственной нормативной базы по применению инженерно-технических средств охраны и надзора (ИТСОН), что привело к разработке и утверждению 17.06.2013 приказа Минюста России № 94 «О внесении изменений в приказ Министерства юстиции Российской Федерации от 4 сентября 2006 г. № 279 „Об утверждении Наставления по оборудованию инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы“», в котором происходит

закрепление концептуальных положений, касающихся модернизации ИТСОН.

В приказе Минюста России от 04.09.2006 № 279 «Об утверждении Наставления по оборудованию инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы» в редакции от 17.06.2013 (далее – Наставление) раскрываются требования, предъявляемые к ИСБ, перечисляются системы, входящие в её состав:

- система охранно-тревожной сигнализации (далее – СОТС);
- система контроля и управления доступом (далее – СКУД);
- система охранного телевидения (далее – СОТ);
- система оперативно-диспетчерской связи (далее – СОДС);
- система громкоговорящей связи (далее – СГТС) [1].

Данные системы согласно требованиям Наставления должны иметь интеграционные связи между собой двух видов – программную и аппаратную.

Цель данной интеграции очевидна: автоматизировать работу системы и минимизировать влияние человеческого фактора.

Интеграция на программном уровне подразумевает использование программного обеспечения, гарантирующего выполнение различных макрокоманд (как пользовательских, созданных установщиками или пользователями ИСБ, так и подготовленных разработчиками специального программного обеспечения). Интеграция на программном уровне производится между СОТС, СКУД, СОТ в любом сочетании.

Обзор публикаций по вопросу, посвященному применению ИСБ на объектах УИС, показал, что данная тематика нашла свое отражение у таких авторов, как А. Ю. Бырков, С. В. Белокуров [2], В. В. Винокуров [3], А. С. Гаврилов [4],

В. С. Подгурский, А. В. Паринов [5], В. А. Спирин, О. С. Спирина [6]. Анализ данных работ выявил, что они, как правило, отображают описательные, констатирующие вопросы организации оборудования ИСБ объектов УИС. Вместе с тем проблематика уже существующего порядка применения СОТС, СКУД, СОТ, входящих в состав ИСБ, а также возможные пути их взаимодействия, масштабирования своего отражения в литературе, к сожалению, не получили.

Остановимся на следующих важных вопросах.

Традиционно на объектах УИС было два рабочих места, куда поступала вся информация от технических средств охраны и надзора:

- пульт управления техническими средствами охраны (далее – ПУТСО);
- помещение дежурного помощника начальника колонии (далее – ДПНК), дежурного помощника начальника следственного изолятора (далее – ДПНСИ).

В помещении ДПНК (ДПНСИ) приходит информация от СОТС, установленной на внутренней территории учреждения, а также СОТС, находящейся за пределами учреждения (здание штаба, административное здание). Необходимо отметить, что в большинстве учреждений УИС отсутствует автоматизированное рабочее место (далее – АРМ) ИСБ в помещении ДПНК (ДПНСИ). Вместо него устанавливаются приборы приемно-контрольные охранно-пожарные (далее – ППКОП) и удаленный монитор ИСБ с графической схемой СОТС периметра объекта УИС. Суммарная информационная емкость ППКОП достаточно большая и может достигать 100 и более шлейфов сигнализации.

Данный факт считаю проблемным по нескольким причинам:

– наиболее значимым является отсутствие документирования информации, поступающей от СОТС внутренней территории объекта. Возникают самые простые вопросы, на которые нет ответа, например: «Во сколько сработала тревожная кнопка в медицинской части? Был ли поставлен под охрану тот или иной шлейф СОТС?»;

– отсутствует наглядность предоставляемой информации от СОТС, что снижает оперативность принятия решений ДПНК (ДПНСИ);

– отсутствует видеоверификация тревожных событий (при наличии видеокамер в местах установки периферийных элементов СОТС).

По моему мнению, необходимо постепенное расширение уже действующих комплексов ИСБ на объектах УИС, а именно разработка и внедрение комплексов АРМ ИСБ ДПНК (ДПНСИ). Такие комплексы должны иметь возможность реализации удобного графического интерфейса отображения состояния СОТС внутренней территории. Для исправительных учреждений он должен иметь следующие постраничные графические схемы: здание штаба, территория и здание ШИЗО-ПКТ, жилая зона, производственная зона. Конечно, при разработке АРМ ИСБ ДПНК (ДПНСИ) возникнет вопрос об интеграции уже существующих СОТ внутренней территории объекта с СОТС, проектируемых АРМ.

Далее хотелось бы остановиться на актуальных вопросах применения СКУД ИСБ на объектах УИС.

В соответствии с подпунктом 7 пункта 23 Наставления [7] СКУД устанавливается в местах перехода рубежей охраны (контрольно-пропускные пункты, далее – КПП, калитки и ворота в ограждениях зон и территорий, двери режимных помещений). Интеграция между подсистема-

ми СОТС, СКУД, СОТ осуществляется на программном уровне.

Важно подчеркнуть, что практика применения СКУД на КПП по пропуску людей формируется таким образом, что сами комплексы не осуществляют управление электромеханическими замками дверей проходного коридора, решение о предоставлении доступа и управление замками дверей осуществляет часовой КПП. В связи с этим СКУД на КПП учреждений УИС не совсем правильно считать полноценной системой контроля и управления доступом, а необходимо воспринимать как систему контроля доступа (без автоматического управления), помогающую часовому КПП осуществлять идентификацию.

Очевидным также является то, что заявленные в Наставлении интеграционные связи СКУД на программном уровне с подсистемами СОТС и СОТ ИСБ являются концептуальными, их конкретные алгоритмы взаимодействия не прописаны. Наверное, тут можно задаться вопросом: «Какими они могут быть?»

Одна интеграционная связь между СОТС и СКУД на КПП существует достаточно давно, но только на аппаратном уровне и никак не связана с ИСБ: при срабатывании кнопки тревожной сигнализации у часового КПП происходит блокирование системы открывания замков дверей проходного коридора. Данная схема, как правило, выполняется специалистами группы инженерно-технического обеспечения связи и вооружения учреждения с помощью реле, без использования устройств промышленного изготовления. Разблокировку производит начальник караула. При этом необходимо отметить, что в Наставлении не указано место установки кнопки разблокировки электропитания замков.

В современных ИСБ реализована на программном уровне функция блокиров-

ки электромеханических замков, установленных на КПП по пропуску людей, в случае возникновения тревожной ситуации в СКУД. Однако не все учреждения идут по пути ее реализации. У часового КПП есть возможность, нажав кнопку «Разблокировать», прекратить режим тревожной ситуации и восстановить управление замками. Очевидно, что это решение он не должен принимать самостоятельно. Думается, необходимо обязательное (автоматическое) информирование начальника караула, то есть контроллер СКУД посредством «сухих контактов» должен выдать сигнал «Тревога» на ППКОП или АРМ ИСБ в комнате начальника караула. Часовому КПП необходимо дожидаться прибытия начальника караула с целью выработки решения о предоставлении допуска. В условиях объектов УИС, где помещения часового КПП и начальника караула смежные, такой алгоритм легко реализуем, в противном случае он требует более глубокого логического осмысления, так как проход начальника караула через двери проходного коридора невозможен – они остаются заблокированными.

Отдельно хотелось бы остановиться на пропускном режиме в запретную зону охраняемого объекта УИС.

В ограждениях запретных зон объекта (в местах примыкания к зданиям КПП и к ограждениям контрольных площадок) согласно подпункту 10 пункта 29 Наставления для действующих постоянных объектов УИС устраиваются калитки для прохода на тропы нарядов и ворота (калитки) для проезда (прохода) на контрольно-следовые полосы. Калитки для прохода на тропу специалистов ИТО устраиваются в противопобеговых заграждениях (в местах их примыкания к зданию КПП). Все ворота оборудуются запорными и замковыми (калитки – замковыми) устройствами и блокируются средствами сигнализации [7].

Вполне уместно говорить о необходимости оборудования калиток считывателями бесконтактных карт (с двух сторон) и электромеханическим замком, имеющим возможность открывания с помощью ключа. По моему мнению, организуемая СКУД должна включать в себя все калитки запретной зоны, входные двери на площадку для построения караула. Данное дооборудование СКУД учреждений УИС, прежде всего, ускорит действие резервных групп караула и дежурной смены при чрезвычайных обстоятельствах, позволит документировать время прохода сотрудников в запретную зону охраняемого объекта.

При этом в ряде учреждений УИС продолжает действовать архаичный способ прохода в запретную зону – калитки необходимо открывать одним из имеющихся на связке ключей. Безусловно, в этих условиях время выдвижения резервной группы караула № 1 во внешнюю запретную зону при чрезвычайных обстоятельствах будет только возрастать. Аналогичная ситуация имеет место быть для сотрудников дежурной смены учреждения при проходе их во внутреннюю запретную зону.

Ложные срабатывания охранных извещателей на периметре являются серьезной проблемой. Большинство сигналов тревог, которые поступают на ПУТСО, оказываются ложными. Проверка тревожной ситуации на охраняемом объекте с помощью СОТ решает проблему, предлагая возможность убедиться в обоснованности сигнала тревоги дистанционно и в кратчайшие сроки. В настоящее время видеоверификация на объектах УИС осуществляется с помощью стационарных видеокамер, установленных во внутренней запретной зоне, в автоматическом (там, где установлена ИСБ) или ручном режиме.

Представляется интересным вариант верификации тревожных событий с помощью установки купольных видеокамер на наблюдательных вышках.

В большинстве купольных камер есть поддержка тревожных входов / выходов (Alarm I/O), что дает возможность управлять купольной камерой по событиям, получаемым от сторонних систем или извещателей, объединенных с камерой на уровне «сухих контактов». Алгоритм управления купольной камерой и взаимодействие тревожных входов и выходов задается через веб-интерфейс камеры. Тактика применения купольной камеры в результате воздействия на нее событий сводится к заранее заданным точкам предустановки (Presets).

Помимо аппаратной интеграции существует и программная, без привязки к количеству тревожных входов. Например, в составе интегрированной системы охраны «Орион» с программным модулем «Видеосистема Орион Про» камера видеонаблюдения BOLID VCI-529 в сочетании с контроллером периметровых извещателей «С2000-Периметр» успешно решает проблему совместимости систем периметрального охранного видеонаблюдения и периметральных извещателей компаний «ЮМИРС», «СТ-Периметр», «Фортеза» по интерфейсу RS-485, а также любых других видов технических средств охраны, используя интеграцию на уровне «сухих контактов» [8].

На основании вышеизложенного можно полагать, что на охраняемом объекте УИС возможно создать систему видеoverификации тревожных событий с помощью купольных видеокамер, установленных на наблюдательных вышках. Данную систему возможно организовать как с помощью аппаратной интеграции с существующей СОТС объекта, так и с программной интеграции в составе ИСБ,

обеспечивающей управление купольными камерами (например, ИСО «Орион»).

Что мы получаем в результате? При срабатывании охранного извещателя в запретной зоне охраняемого объекта УИС купольная видеокамера поворачивается в направлении зоны обнаружения датчика с заранее заданными величинами углов поворота, наклона и оптического увеличения (зума). Далее часовой оператор ПУТСО переходит в ручной режим управления камерой.

Возникает вопрос: «Какие плюсы могут быть в результате использования купольной видеокамеры для верификации тревожных событий на периметре объекта УИС?» Очевидно, что в результате реального побега через запретную зону охраняемого объекта мы получим следующие преимущества:

- часовому ПУТСО не придется переключаться между стационарными видеокамерами, установленными во внутренней и внешней запретных зонах объекта;
- возможность получения крупного плана нарушителя;
- непрерывное видеосопровождение нарушителя в запретной зоне, а также за ее пределами.

По моему мнению, предложенный способ верификации может существенно повысить эффективность СОТС и системы охраны в целом.

Итак, подводя итоги данной статьи, перечислим сделанные выводы:

- в помещении ДПНК (ДПНСИ) вместо установленных ППКОП необходимо оборудование АРМ ИСБ с целью документирования информации, поступающей от СОТС, повышения качества наглядности;
- калитки для прохода в запретную зону необходимо оборудовать считывателями бесконтактных карт (с двух сторон) и электромеханическим замком, имеющим возможность открывания с помо-

щью ключа, с целью повышения оперативности действий караула при чрезвычайных обстоятельствах, документирования информации о проходах;

- необходимо обязательное (автоматическое) информирование начальника караула о тревожной ситуации, возникающей в СКУД на КПП по пропуску людей;

- целесообразно рассмотреть возможность верификации тревожных событий посредством установки купольных видеокамер на наблюдательных вышках с целью повышения эффективности СОТ системы охраны.

В заключении хотелось бы отметить, что предлагаемые возможные пути дооборудования технических средств охраны и надзора, новые интеграционные связи между СОТС, СОТ, СКУД – это лишь попытка автора высказать свою точку зрения на проблему повышения эффективности применения ИСБ на объектах УИС. Заявленные умозаключения следует считать дискуссионными, требующими тщательной апробации в реальных условиях эксплуатации на базе охраняемого объекта УИС.

1. О внесении изменений в приказ Министерства юстиции Российской Федерации от 4 сентября 2006 г. № 279 «Об утверждении Наставления по оборудованию инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы» : приказ Минюста России от 17.06.2013 № 94. Доступ из СПС «Гарант».

2. *Бычков А. Ю., Белокуров С. В.* Обзор интегрированных систем безопасности, эксплуатируемых на охраняемых объектах УИС // Актуальные проблемы деятельности подразделений УИС : сб. материалов Всерос. науч.-практ. конф. (26 мая 2016 г.). Воронеж, 2016. С. 225–227.

3. *Винокуров В. В.* Особенности применения интегрированных систем безопасности в учреждениях УИС // Техника и безопасность объектов уголовно-исполнительной системы : сб. материалов Междунар. науч.-практ. межведомственной конф. (19–20 окт. 2016 г.). Воронеж, 2016. С. 8–10.

4. *Гаврилов А. С.* Применение интегрированных систем безопасности в учреждениях УИС // Ведомости уголовно-исполнительной системы. 2016. № 11 (174). С. 40–42.

5. *Подгурский В. С., Паринов А. В.* Использование сетевых технологий в интегрированных системах безопасности на примере КСБО «Синергет» // Актуальные проблемы деятельности подразделений УИС : сб. материалов Всерос. науч.-практ. конф. (26 мая 2016 г.). Воронеж, 2016. С. 39–43.

6. *Спирин В. А., Спирина О. С.* Изучение интегрированных систем безопасности, применяемых в уголовно-исполнительной системе, как фактор повышения практической направленности повышения квалификации // Профессиональное образование и наука. 2019. № 4 (9). С. 109–111.

7. Об утверждении Наставления по оборудованию инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы (с изменениями и дополнениями) : приказ Минюста России от 04.09.2006 № 279 // Docviewer : [сайт]. URL: <https://clck.ru/WbGUf> (дата обращения: 03.04.2021).

8. *Озеров Е. В.* Поворотная камера на периметре. Тактика применения на примере BOLID VCI-529 // Алгоритм безопасности. 2017. №4. С. 16–17. URL: https://bolid.ru/files/411/607/ab_4_2017_Bolid_v_02.pdf (дата обращения: 02.08.2021).

1. On amendments to the order of the Ministry of Justice of the Russian Federation dated September 4, 2006 No. 279 «On approval of the Manual on equipping the penal system objects with engineering and technical means of security and supervision» : Order of the Ministry of Justice of Russia dated June 17, 2013 No. 94. Access from Legal Reference System «Garant».

2. Byrkov, A. Yu., Belokurov, S. V. (2016) Overview of integrated security systems operated at guarded objects of the penal system // Actual problems of the activities of penal system subdivisions : collection of articles of the All-Russian Scientific-Practical Conf. (May 26, 2016). Voronezh, pp. 225–227.

3. Vinokurov, V. V. (2016) Features of the use of integrated security systems in the institutions of the penal system // Technical equipment and safety of objects of the penal system : collection of materials of the Intern. Scientific-Practical Interdepartmental Conf. (October 19-20, 2016) Voronezh, pp. 8–10.

4. Gavrilov, A.S. (2016) Application of integrated security systems in the institutions of the penal system // Bulletin of the penal system. 11 (174), 40–42.

5. Podgurskiy, V. S., Parinov, A. V. (2016) Use of network technologies in integrated security systems on the example of Integrated security system «Synerget» // Actual problems of the activities of the penal system divisions : collection of materials All-Russian Scientific-Practical Conf. (May 26, 2016). Voronezh, pp. 39–43.

6. Spirin, V. A., Spirina, O. S. 2019. Study of integrated security systems in the penal system, as a factor in improving the practical orientation of professional development // Professional education and science. 204 (9), 109–111.

7. On approval of the Manual on equipping the facilities of the penal system with engineering and technical means of guarding and supervision : Order of the Ministry of Justice of Russia dated 04.09.2006 No. 279 (as amended). Docviewer : [site]. URL: <https://clck.ru/WbGUf> [Accessed 3rd April 2021].

8. Ozerov, E. V. (2017) Rotary camera on the perimeter. Application tactics on the example of BOLID VCI-529 // Security algorithm. 4, 16–17. URL: https://bolid.ru/files/411/607/ab_4_2017_Bolid_v_02.pdf [Accessed 2th August 2021].