

К вопросу повышения живучести системы охранной сигнализации к преднамеренным действиям нарушителя

Enhancing security alarm system survivability: countering deliberate intruder interference

Н.А. Рябцев¹ ©, Р.С. Дмитриев² ©

N.A. Ryabtsev¹ ©, R.S. Dmitriev² ©

^{1, 2} Федеральное казенное учреждение «Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации, г. Москва, Российская Федерация

¹ E-mail: RyabcevNA@rosgvard.ru

² E-mail: DmitrievRS@rosgvard.ru

Аннотация. В статье рассмотрены и описаны основные факторы, влияющие на живучесть системы охранной сигнализации. Авторами предложена дополнительная мера ее повышения за счет применения средств обнаружения скрытой установки. Представлены преимущества средств обнаружения, предназначенных для скрытой установки, а также описаны проводимые в данном направлении исследования. Представлен положительный эффект от применения средств обнаружения скрытой установки на живучесть системы охранной сигнализации и дальнейшие направления исследования таких средств.

Abstract. The article examines and describes the key factors affecting the survivability of a security alarm system. The authors propose an additional measure to enhance its resilience through the use of detection tools designed for covert installation. The paper highlights the benefits of detection equipment intended for covert deployment, while detailing current research initiatives in this area. Furthermore, the paper demonstrates the positive impact of employing covert installation detection tools on the overall survivability of the security alarm system, and outlines future research directions for such equipment.

Ключевые слова: система охранной сигнализации; живучесть; проникновение; внешние воздействующие факторы; преднамеренные действия нарушителя; саботаж; разрушающие воздействия; средство обнаружения; извещатель; скрытая установка

Keywords: security alarm system, survivability, intrusion, environmental factors, deliberate intruder actions, sabotage, destructive impacts, detection sensor, detector, concealed installation

ДЛЯ ЦИТИРОВАНИЯ: Рябцев Н.А., Дмитриев Р.С. К вопросу повышения живучести системы охранной сигнализации к преднамеренным действиям нарушителя // Академический вестник войск национальной гвардии Российской Федерации. – 2026. – № 2. – С. 48–52.

Под эффективностью системы охранной сигнализации следует понимать ее свойство выполнять поставленную цель в заданных условиях эксплуатации и с определенным качеством [1]. Критерием оценки эффективности такой системы является вероятность «эффективного» обнаружения несанкционированного проникновения нарушителя, которая зависит от вероятностей технического отказа, пропуска цели и преднамеренных действий нарушителя. Вероятность «эффективного» обнаружения можно определить по формуле:

$$P_{\text{зо}} = (1 - P_{\text{от}}) \times (1 - P_{\text{но}}) \times (1 - P_{\text{пд}}) \quad (1)$$

где $P_{\text{зо}}$ – вероятность «эффективного» обнаружения;

$P_{\text{от}}$ – вероятность технического отказа;

$P_{\text{но}}$ – вероятность пропуска цели;

$P_{\text{пд}}$ – вероятность преднамеренных действий нарушителя.

Вероятности технического отказа, пропуска цели и преднамеренных действий нарушителя в

большей степени зависят от живучести элементов системы охранной сигнализации (средств сбора и обработки информации, каналов передачи данных, источников электропитания, линий электропитания и иного оборудования) – способности сохранять или оперативно восстанавливать работоспособность в штатных и нештатных ситуациях. Живучесть данных элементов, в свою очередь, зависит от их устойчивости к внешним воздействующим факторам: климатическим (температура, влажность), механическим (вибрация, удары), электромагнитным (электростатические разряды, импульсные помехи, промышленные радиопомехи), а также к преднамеренным действиям нарушителя.

В большей степени от указанных факторов и особенно от преднамеренных действий нарушителя зависит живучесть первичных средств сбора и обработки информации – средств обнаружения (датчиков, извещателей, модулей), т.к. они, в отличие от других элементов системы охранной сиг-

нализации, находятся в открытом доступе. Учитывая тот факт, что средства обнаружения являются наиболее многочисленными элементами системы охранной сигнализации и составляют ее большую часть, можно сделать вывод, что их влияние на эффективность системы наиболее велико.

В настоящее время проблема обеспечения устойчивости средств обнаружения к климатическим, механическим и электромагнитным факторам в значительной степени решена за счет применения инженерно-технических идей, таких как: комбинирование независимых каналов обнаружения с различными физическими принципами действия, использование корпусов с высокими степенями защиты по ГОСТ 14254–2015, внедрение алгоритмов адаптивной фильтрации и автоматической подстройки порогов чувствительности под динамически изменяющиеся условия окружающей среды, реализация функции самотестирования с передачей сообщений на средство сбора и обработки информации. При этом проблема устойчивости средств обнаружения к преднамеренным действиям нарушителя значительно сложнее и требует особого внимания.

Преднамеренные действия нарушителя на средства обнаружения с целью нарушения их работоспособности можно разделить на два вида: разрушающие – физическое повреждение; саботаж – скрытое воздействие на конструктивные элементы [2].

При разрушающих действиях в системе охранной сигнализации формируется сигнал «Тревога», что делает их нецелесообразными при попытке проникновения нарушителя на охраняемый объект. Вместе с тем данные действия могут применяться нарушителем при проверке работоспособности системы, определении способов реагирования на сигнал «Тревога», оценки задействованных сил охраны, а также с целью отвлечения от других объектов.

При саботаже средства обнаружения сигнал «Тревога» в системе охранной сигнализации не

формируется, что делает его весьма эффективным способом проникновения на охраняемый объект [3].

Саботаж выполняется на этапе подготовки не-санкционированного проникновения на охраняемый объект лицами, знающими принципы работы и построения системы охранной сигнализации. Проникновения, предпринятые с помощью саботажа, носят преднамеренный характер и совершаются с целью хищения определенных видов материальных ценностей или для иных противоправных действий.

Саботаж характеризуется предварительной разведкой объекта с изучением архитектуры системы охранной сигнализации, а также с применением специальных технических средств и методик обхода и, как правило, влечет за собой человеческие жертвы, крупный экономический ущерб, репутационные потери и широкий общественный резонанс. Количество случаев саботажа средств обнаружения из всех элементов, входящих в систему охранной сигнализации, составляет более 50 %. Основные виды и способы саботажа средств обнаружения систематизированы и представлены в таблице 1.

Стоит отметить, что методы борьбы с указанными видами саботажа уже реализованы в серийно выпускаемых средствах обнаружения, применяющихся для охраны объектов высоких категорий значимости. Основным методом борьбы с саботажем средств обнаружения является внедрение дополнительных функций, таких как: контроль положения корпуса и зоны обнаружения относительно монтажной поверхности, отрыва от поверхности, вскрытия корпуса, использования антисаботажных зон обнаружения, защита от маскирования. Однако реализация данных функций требует значительных изменений в конструкции средств обнаружения: установки дополнительных чувствительных элементов, усложнения схемотехники и алгоритмов обработки сигналов. При этом данные решения не защищают средства обнаружения от разрушающих действий нарушителя, а также сопряжены с увеличением себестоимости изделий.

Таблица 1

Основные виды и способы саботажа средств обнаружения

Вид	Способ
Маскирование	Экранирование зоны обнаружения различными материалами, нанесение оптически непрозрачных покрытий на чувствительные элементы
Переориентация зоны обнаружения	Изменение пространственной ориентации извещателя относительно монтажной поверхности
Изменение настроек	Изменение параметров чувствительности и обнаружительной способности
Блокировка канала передачи данных	Внесение помех в линию связи со средством сбора и обработки информации, воздействие на информационные выходы
Подмена составных частей	Подмена задающего блока магнитоконтактных извещателей, использование имитаторов приемо-передающих устройств

В качестве дополнительной меры для снижения уязвимости средств обнаружения к саботажу и разрушающим действиям нарушителя можно рассмотреть их скрытую установку. Основным преимуществом предлагаемого авторами решения является возможность минимизировать вероятность обнаружения нарушителем средств обнаружения и, как следствие, снизить вероятность преднамеренных действий нарушителя и повысить живучесть системы охранной сигнализации в целом. Если нарушитель не видит средство обнаружения и не может определить его модель, физический принцип действия и зону обнаружения, возможность планирования проникновения на объект путем нарушения его работоспособности или повреждения стремится к нулю.

Кроме того, необходимо отметить следующие дополнительные преимущества скрытой установки средств обнаружения.

Психологический фактор – неопределенность относительно наличия и расположения средств обнаружения системы охранной сигнализации сдерживает потенциального нарушителя.

Защита от повреждений – позволяет снизить риск повреждения средств обнаружения в производственных или общественных местах.

Эстетическое оформление – позволяет сохранить дизайн интерьера и экстерьера охраняемого объекта, что особенно актуально для исторически значимых объектов.

Реализовать скрытую установку возможно несколькими способами: интегрируя средство обнаружения в конструкцию охраняемого объекта, используя малогабаритные корпуса или выносные чувствительные элементы, маскируя их различными материалами или под предметы интерьера.

В настоящее время в «Списке технических средств безопасности...» представлен ряд средств обнаружения, предназначенных для скрытой установки.

1. Извещатели охранные точечные магнитоконтактные ИО102-5 и ИО102-6 (рис. 1).



Рис. 1а. Извещатели охранные точечные магнитоконтактные ИО102-5



Рис. 1. Извещатели охранные точечные магнитоконтактные ИО102-6

Данные извещатели предназначены для скрытой установки в элементы открывающихся строительных конструкций. Они могут быть покрашены в цвет охраняемой конструкции, а также могут быть использованы для организации охранных устройств типа «ловушка». Извещатель ИО102-5 предназначен для установки на магнитонепроводящие поверхности, а ИО102-6 – на магнитопроводящие.

2. Извещатель охранный объемный ультразвуковой «Витрина», предназначен для охраны витрин (рис. 2).



Рис. 2. Извещатель охранный объемный ультразвуковой «Витрина»

Извещатель состоит из двух миниатюрных микрофонов, которые формируют стационарное акустическое поле внутри охраняемого объема и блока обработки сигналов. Микрофоны скрытно устанавливаются внутри охраняемого пространства по диагонали напротив друг друга, а блок обработки выносится за пределы охраняемого объема. Извещатель способен обнаружить перемещение предметов и проникновение рукой в охраняемое пространство.

3. Извещатель охранный совмещенный «Стеклопакет» (рис. 3).

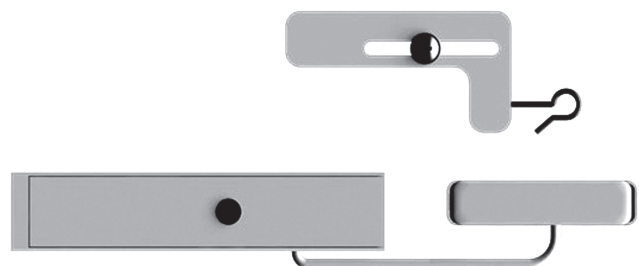


Рис. 3. Извещатель охранный совмещенный «Стеклопакет»

Извещатель предназначен для обнаружения различного рода воздействий на стеклопластиковые оконные блоки, такие как: разрушающие воздействия на раму (сверление, рез), открывание створки, разрушение стеклопакета, поворот ручки створки окна. Конструктивно извещатель состоит из: блока обработки сигнала, задающего элемента (с магнитом) и внешнего магнитоуправляемого модуля. Извещатель монтируется на торцевую часть створки окна рядом с запорным механизмом, что делает его установку скрытой. Также в 2025 году специалистами ФКУ «НИЦ «Охрана» Росгвардии разработана и освоена в серийном производстве его радиоканальная версия – «Стеклопакет-РК», входящая в состав радиоканальной системы «Ладога-А».

4. Извещатели инерционные «Метка-ПРО» исп.2 из состава радиоканальной системы «Стре-

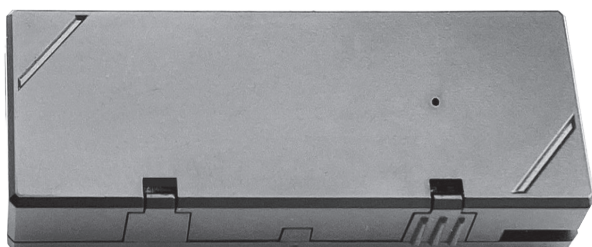


Рис. 4а. Извещатель охранный точечный магнитоконтактный «Метка-ПРО» исп.2



Рис. 4б. Извещатель охранный точечный магнитоконтактный «Грань-РК Мини»

лец-Интеграл» и «Грань-РК Мини» из состава радиоканальной системы «Ладога-А» (рис. 4).

Извещатели предназначены для охраны отдельных предметов. Формируют сигнал тревоги при попытках сместить охраняемый объект.

5. Ловушка охранно-сигнальная «Кукла-Л» (рис. 5).

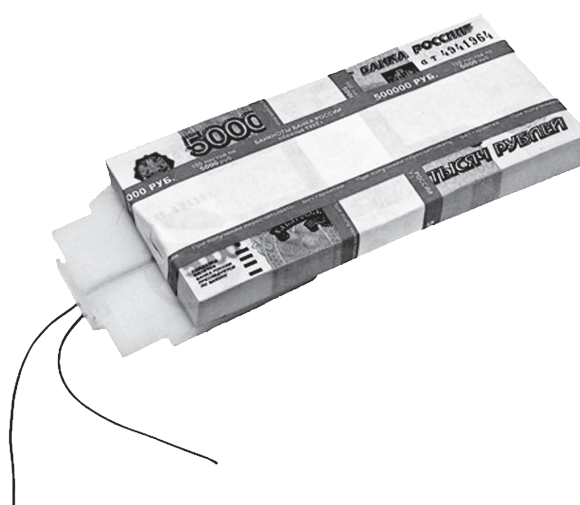


Рис. 5. Ловушка охранно-сигнальная «Кукла-Л»

Ловушка замаскирована под пачку денежных банкнот и предназначена для формирования сигнала «Тревога» ручным способом. Принцип действия данной ловушки такой же, как и у магнитоконтактных извещателей – в пачке с банкнотами находится магнит, а в площадке, на которой она расположена, – геркон. При сдвиге пачки банкнот геркон размыкает шлейф сигнализации, тем самым формируя извещение о тревоге.

При помощи описанных моделей средств обнаружения можно сформировать первый (периметр) и третий (отдельные предметы) рубежи охраны объекта, а также организовать возможность формирования сигнала «Тревога» ручным способом. Для организации второго рубежа охраны (внутренний объем помещений) в настоящее время в «Списке технических средств безопасности...» средства обнаружения, предназначенные или имеющие возможность скрытой установки, отсутствуют.

В 2026 году ФКУ «НИЦ «Охрана» Росгвардии в соответствии с Планом научной работы в войсках национальной гвардии Российской Федерации осуществляет разработку радиоволнового объемного охранного извещателя, физический принцип действия и алгоритмы обработки сигнала которого позволяют при организации второго рубежа охраны осуществлять его скрытую установку (закрывать его радиопрозрачными материалами, такими как: пластик, фанера, дерево и ткань).

В продолжение направления создания средств обнаружения скрытой установки ФКУ «НИЦ «Охрана» Росгвардии проводятся исследования нового инновационного материала – ферромагнитного аморфного микропровода [4]. Данный материал обладает уникальными особенностями – под воздействием упругих сил деформации (сжатие, растяжение, скручивание, изгиб) изменяет свое электрическое сопротивление и амплитуду своего электромагнитного сигнала. Благодаря своим раз-

мерам (диаметр до 120 мкм, длина до 100 м) и прочностным характеристикам (усилие на разрыв до 3 100 Мпа) его можно внедрять в различные материалы, что в перспективе позволит создавать средства обнаружения, интегрированные в строительные конструкции и предметы интерьера [5].

Таким образом можно утверждать, что средства обнаружения скрытой установки, по сравнению со средствами обнаружения, устанавливаемыми открыто, более защищены от преднамеренных действий нарушителя, т.к. нарушителю невозможно определить место их установки, идентифицировать их модель и физический принцип действия, определить их зону обнаружения, сформировать тактику их обхода или выбрать способы воздействия на них.

В заключение можно сделать вывод, что за счет применения средств обнаружения скрытой уста-

новки повышается живучесть системы охранной сигнализации и снижается вероятность проникновения на охраняемый объект.

Предлагаемое авторами решение применения дополнительной меры для снижения уязвимости средств обнаружения к преднамеренным действиям нарушителя, заключающейся в их скрытой установке, позволяет снизить вероятность таких действий и повысить живучесть системы охранной сигнализации в целом.

Вместе с тем, необходимо проведение научных исследований, направленных на определение тактики применения средств обнаружения скрытой установки и их конструктивных исполнений с учетом увеличения технической оснащенности, квалификации и количества подготовленных нарушителей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Членов А.Н. Моделирование системы охраны и пожарной безопасности промышленного объекта / А.Н. Членов, Н.А. Рябцев // Проблемы техносферной безопасности: материалы Международной научно-практической конференции молодых учёных и специалистов. – 2024. – № 13. – С. 36–40.

2. Рябцев Н.А. Автоматизация сбора и обработки данных в системе охранно-пожарной сигнализации промышленного объекта на основе классифицированных извещателей: дис.... канд. техн. наук: 05.13.06 / Рябцев Николай Алексеевич. – М., 2020. – 189 с.

3. Рябцев Н.А. Влияние технических средств обнаружения на уровень автоматизации системы тревожной сигнализации / Н.А. Рябцев, Т.А. Буцынская, А.Н. Членов // Проблемы техносферной безопасности: материалы Международной науч-

но-практической конференции молодых учёных и специалистов. – 2022. – № 11. – С. 213–216.

4. Umnov P.P. Amorphous glass-metal composite as element of a cement mortar reinforcing / P.P. Umnov, E.R. Rakhmatullina, M.D. Breeva [et al.] // Advanced High Entropy Materials: Abstracts of the V International Conference and School, Saint-Petersburg, 09–13.10.2023. – Saint-Petersburg: OOO "Заневская площадь", – 2023. – P. 120-121. – EDN YLFRAC.

5. Молоканов В.В. Использование особенностей деформации ферромагнитных аморфных проводов для получения новых видов изделий и материалов / В.В. Молоканов, А.В. Крутилин, Н.А. Палий, Т.Р. Чуева, П.П. Умнов // Актуальные проблемы прочности: материалы международной научной конференции. – Минск, 2022. – С. 149.

Статья проверена программой Антиплагиат. Оригинальность — 83 %.

Статья поступила в редакцию 19.02.2026; одобрена после рецензирования 06.04.2026; принята к публикации 15.05.2026.