ПРЕДЛОЖЕНИЕ ПО АВТОМАТИЗАЦИИ ОХРАНЫ И ОБОРОНЫ РАЙОНА СТАРТОВОЙ ПОЗИЦИИ

Демешко В. С., Онищук Р. С.
Кафедра тактики и вооружения войсковой противовоздушной обороны, Военная академия РБ
Минск, Республика Беларусь
E-mail: demeka-v@mail.ru

Статья посвящена повышению уровня безопасности охраняемых объектов за счет применения автоматизированной системы охраны. Предложен облик системы автоматизированной охраны. Приведены основные показатели качества с помощью которых оценивается эффективность данной системы.

Проблема обеспечения живучести подразделений, вооруженных ЗРК малой дальности, обусловливается наличием в Вооруженных Силах иностранных государств сил специальных операций, а именно диверсионно разведывательных групп, деятельность которых предполагает целенаправленную работу по разведке, проведению диверсий и выводу из строя систем и средств ПВО. В связи с этим организация эффективного противодействия диверсионным группам в условиях современных войн и конфликтов приобретает первостепенное значение [1]. Наиболее сложной из угроз является нейтрализация проникновения на охраняемую территорию подготовленной вооруженной диверсионно разведывательной группы и недопущение применения ей по охраняемому объекту переносных средств поражения. Проведя анализ возможностей сил специальных операций иностранных государств и расчеты по оценке возможностей подразделений охраны и обороны показывают, что имеющийся штат подразделений охраны не обеспечит выполнение задачи по охране с требуемой надежностью обеспечения безопасности. [2]. Для повышения уровня безопасности охраняемых объектов одним из направлений может быть автоматизация процессов обнаружения и нейтрализации угроз, сведя до минимума степень участия человека. При этом на человека возлагаются задачи принятия решения и контрольные функции, а роль боевых средств будут выполнять роботизированные платформы, способные обнаруживать противника в любых условиях и поражать его по команде оператора. Облик системы автоматизированной охраны и её основные элементы представлены на рисунке 1.

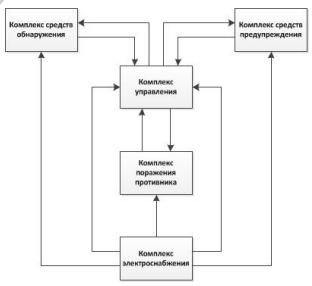

Рис. 1 – Структурная схема системы автоматизированной охраны

Особое внимание необходимо уделить комплексу средств обнаружения, который предназначен для обнаружения нарушителя в ответственном секторе и может быть построен на базе пассивных систем, работающих на разных физических принципах, и типах чувствительных элементов, воспринимающих воздействие нарушителей при пересечении их чувствительных зон, а также на базе бесплотно летательных аппаратов [2]. На рисунке 2 показан пример реализации системы охраны пассивными датчиками, которые широко применяются при охране гражданских объектов [3].

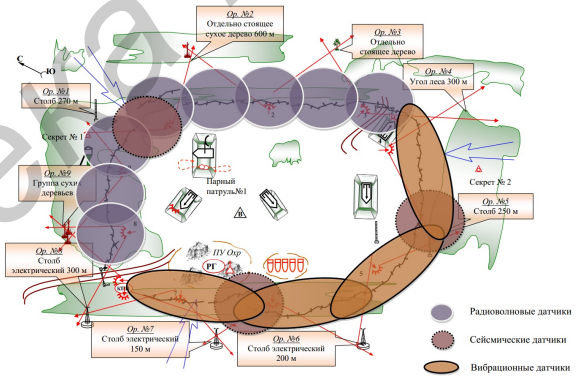

Рис. 2 – Пример реализации системы охраны пассивными датчиками

Эффективность данной системы можно оценить с помощью показателей качества, таких как: размеры зоны обнаружения; вероятность правильного обнаружения; время наработки на ложное срабатывание; помехозащищенность системы охраны; уязвимость к преодолению. Верная интерпретация этих показателей имеет первостепенное значение для проектирования и эксплуатации любой системы охраны периметра [4]. Зона обнаружения системы охраны представляет собой участок местности, в пределах которого обеспечивается обнаружение нарушителей с вероятностью правильного обнаружения не ниже заданной при фиксированном времени наработки на ложное срабатывание. Речь не идет о пространственной зоне обнаружения, поскольку в рамках исследования рассматривается система обнаружения только наземных нарушителей. При этом в зависимости от типа используемых

средств обнаружения конфигурация зоны обнаружения может изменяться. Вероятность правильного обнаружения – это вероятность наступления события, заключающегося в формировании системой охраны сигнала «Тревога» при обнаружении нарушителя. Другой важной характеристикой системы охраны является время наработки на ложное срабатывание. Время наработки на ложное срабатывание выбирается исходя из области применения системы. При использовании для охраны государственной границы или периметров важных объектов время наработки на ложное срабатывание, как правило, составляет не менее 720 ч, что означает порядка одного ложного срабатывания в течение месяца. Стремление повысить чувствительность системы неизбежно влечет за собой увеличение числа ложных тревог. Именно поэтому в пассивных системах обнаружения вторжения при оценке ситуации далеко не все тревоги вызваны вторжением. На практике разработчик системы должен поддержать требуемую вероятность обнаружения при фиксированной частоте ложных тревог (критерий Неймана-Пирсона, который, заключается, в решение о наличии сигнала на входе приемника выдается в результате сравнения с пороговым значением одной и той же величины, которая называется отношением правдоподобия). Под помехозащищенностью понимают способность пассивных систем поддерживать показатели качества, такие как вероятность обнаружения наземного противника и вероятность ложного срабатывания, на заданном уровне в условиях воздействия помех. Работа пассивных систем обнаружения происходит в условиях воздействия на чувствительные элементы датчиков преднамеренных и непреднамеренных помех естественного и искусственного происхождения. К преднамеренным помехам относятся помехи, создаваемые нарушителем с целью приведения пассивной системы в неработоспособное состояние (или ограничения ее характеристик). Возможность создания нарушителем таких помех зависит от знания им физического принципа действия таких систем, ее основных характеристик. Результатом непосредственного воздействия помех на датчики пассивной системы является ухудшение качества правильного обнаружения. Любая пассивная система обладает конечной помехозащищенностью, поэтому под воздействием значимых помеховых факторов она с определенной вероятностью может выдавать ложные тревоги. Вопрос помехозащищенности конкретного датчика определяется в основном местом и качеством его установки. Поэтому наработка одного и того же датчика на ложное срабатывание на разных объектах отличается в несколько раз. Под уязвимостью пассивных систем к преодолению понимается возможность нарушителя преодолеть зону обнаружения, не вызвав появления сигнала тревоги, в том числе с использованием специальных методов и средств пересечения рубежа или устройства нейтрализации (блокировки) системы. Уязвимость преодоления зависит от физического принципа работы конкретного датчика. Таким образом, применение автоматизированной системы охраны с использованием технических средств, позволит: повысить эффективность охраны района стартовой позиции подразделения, вооруженного ЗРК малой дальности; повысить оперативность оповещения о вторжении наземного противника за счет применения датчиков, работающих на разных физических принципах; сконцентрировать внимание личного состава из числа взвода охраны и обороны на наиболее опасных и уязвимых участках местности.

1. Подлесный, Е. А. Локальные войны и вооруженные конфликты: учеб. пособие: в 2ч. / Е. А. Подлесный, В. И. Шатько –Минск: ВАРБ, 1998.
2. Демешко, В. С. Повышение эффективности охраны стартовых позиций подразделений, вооруженных ЗРК малой дальности: дис. ... маг. техн. наук: 1–958004 / В. С. Демешко. – М., 2017.
3. Задачи и проблемы охраны объектов [Электронный ресурс]. – Режим доступа: http://www.v1electronics.ru. – Дата доступа: 15.08.2017.
4. Демешко, В. С. Расчет основных показателей качества системы автоматизированной охраны с использованием мажоритарной логики / В. С. Демешко // Актуальные проблемы современной науки: материалы 11 междунар. науч.–техн. конф., – Актобе, 19 мая 2017 г. Военный ин-т Сил воздушной обороны; редкол.: изд-во Принт-А. – Актобе, 2017. – С. 327.