

КОНКУРЕНТНА РОЗВІДКА ТА УПРАВЛІННЯ ЗНАННЯМИ / BUSINESS INTELLIGENCE & KNOWLEDGE MANAGEMENT

DOI: [10.18372/2225-5036.27.16516](https://doi.org/10.18372/2225-5036.27.16516)

АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ПРОТИДІЇ ЛАЗЕРНИМ СИСТЕМАМ РОЗВІДКИ

Іван Опірський, Ярослав Совин, Даценко Єгор, Усик Мирон

Національний університет «Львівська політехніка»



ОПІРСЬКИЙ Іван Романович, д.т.н., проф.

Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.

Освіта: Національний університет «Львівська Політехніка», 2008 рік.

Посада: професор кафедри захисту інформації з 2019 року.

Наукові інтереси: методи і засоби технічного захисту інформації, охорона державної таємниці, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки, математичні методи та моделі захисту інформації, технічні канали витоку інформації, спецвимірювання .

Публікації: більше 150 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.

E-mail: iopirsky@gmail.com.

Orcid ID: 0000-0002-8461-8996.



Совин Ярослав Романович, к.т.н., доц.

Рік та місце народження: 1979 рік, м. Львів, Україна.

Освіта: Національний університет «Львівська Політехніка», 2001 рік.

Посада: доцент кафедри захисту інформації з 2011 року.

Наукові інтереси: безпека вбудованих систем, апаратна криптографія, легковагова криптографія, ефективна реалізація криптографічних алгоритмів у вбудованих системах та IoT з підвищеною стійкістю до фізичних атак, атаки через сторонні канали. *Публікації:* понад 50 наукових публікацій, серед яких наукові статті, навчальний посібник, тези та матеріали доповідей на конференціях.

E-mail: sovynjarosl@gmail.com.

Orcid ID: 0000-0002-5023-8442.



Даценко Єгор Максимович, студент кафедри захисту інформації Національного університету «Львівська політехніка».

Рік та місце народження: 2002 рік, м.Сміла, Черкаська область, Україна.

Наукові інтереси: системи кібернетичного захисту інформаційних ресурсів, комп'ютерні науки.

E-mail: yehor.datsenko.kb.2019@lpnu.ua.

Orcid ID: 0000-0001-7330-9488.



Усик Мирон Юрійович, студент кафедри захисту інформації Національного університету «Львівська політехніка».

Рік та місце народження: 2002 рік, м. Львів, Львівська область, Україна.

Наукові інтереси: системи кібернетичного захисту інформаційних ресурсів, комп'ютерні науки, лазерні системи акустичної розвідки, засоби протидії лазерним системам розвідки, спецвимірювання.

E-mail: myron.usyk.kb.2019@lpnu.ua.

Orcid ID: 0000-0002-1201-4683.

Анотація. Використання лазерних систем дозволяє максимально розвинути ведення військової справи, але це може також становити велику загрозу тому, що постійно йде конкуренція між противниками, які випробовують новітні лазерні технології на людях, які воюють на іншій стороні, що суперечить протоколам про негуманну зброю. У цій статті розглянуто можливі засоби лазерних атак та які наслідки вони несуть, також оцінено теперішній стан вітчизняних розробок у даній сфері. Але дана публікація має на меті не лише опис стратегії розвитку лазерних систем розвідки та характеристичне порівняння різних представників, тут будуть описані методи захисту від них. Приведено особливості побудови та функціонування. Попри різні переваги та недоліки систем захисту, було знайдено декілька ефективних, перевірених у реальних бойових умовах, способів оборони.

Ключові слова: лазерні системи розвідки, засоби протидії лазерним системам розвідки, laser blinding weapons, counter laser blinding weapons, countering laser sniper detection system.

Вступ

На всіх етапах розвитку людської цивілізації інформація була як найважливішим об'єктом, так і засобом боротьби між людьми, народами, державами. Окремі факти здійснення інформаційного впливу на широку аудиторію можна виявити протягом усієї історії суспільства.

Зрозуміло, що в різні періоди інтенсивність застосування тих чи інших способів впливу як і досконалість його організації, дуже різняться [1,2]. Політика ведення інформаційних війн та застосування інформаційних впливів з'явилися ще у первісні часи, разом з тим маємо зазначити, що системне вивчення цих феноменів почалось лише у ХХ столітті. Інформаційна війна є тотальним явищем, де неможливим є визначення її початку та кінця.

Це наявність боротьби між державами за допомогою інформаційної зброї, тобто це відкриті то приховані цілеспрямовані інформаційні впливи держав одна на одну, з метою отримання переваги в матеріальній сфері, де інформаційні впливи – це впливи з допомогою таких засобів, використання яких дозволяє досягти задуманих цілей [3].

Проте не тільки інформаційна війна стала проблемою для України. Війна на сході України кожного дня відкриває очі військовим та дослідникам світу про підступність та ворожість Росії та її армії. Щоденно країна-агресор порушує загальноприйняті норми проведення бойових дій. До того використовувалася маса іншої зброї, реактивні піхотні вогнемети, ручні протитанкові гранатомети.

Цього разу порушення торкнулося Протоколу 4 Конвенції про негуманну зброю, про заборону або обмеження застосування окремих видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень. Перша стаття наголошує на забороні використовувати лазерну зброю, спеціально призначену для використання у бойових діях, щоб причинити постійну сліпоту незахищеним органам зору людини, при чому Росія є країною, що підписала даний протокол. Це грубе порушення заставляє задуматися про методи протидії та захисту наших військових.

Мета засобів лазерної протидії оптико-електронних приладів очевидна з їх назви. Вони створені для знаходження в автоматичному та/або ручному режимах оптичних, оптико-електронних приладів, і їх ураження.

Під даний опис потрапляє все, що подібне на оптичний приціл, тобто складається з розміщених один за одним об'єктивів, окулярів та інших складових, це самі приціли, відеокамери і т.д. В ході розбору даної статті

може виникнути питання чому саме лазери заборонені у використанні, адже на першу думку краще сліпота ніж смерть.

Так, все правильно, але відповідь існує. За останні сто років людству вдалося заборонити зброю, що вважається істотно жорстокою. Отрута, біологічна зброя, хімічна зброя, розривні кулі тощо. Причиною було те, що такі види викликають зайві травми та неприємні страждання заради невеликого військового призначення. Лазери якраз підпадають під таку причину. Широко застосовувані осліплюючі лазери можуть значно збільшити страждання протягом подальшого життя, викликані війною.

Такі системи не застосовуються по одинці, а завжди як доповнення до іншої зброї. Після пошкодження бойовим лазером, постраждалий не зможе захистити себе від зброї, що йде як основна, оскільки малоімовірно що ворог на великій відстані зможе оцінити завдану шкоду. Тому результатом виявиться більше смертей та сліпих, тим самим збільшивши страждання [5, 6, 12].

Мета засобів протидії лазерним системам оптико-електронної протидії також криється у назві – захистити техніку та органи зору учасників бойових дій від пошкодження лазером. На жаль, таких систем порівняно з системами ураження мало, але більш відомі приклади розглянуто у даній статті.

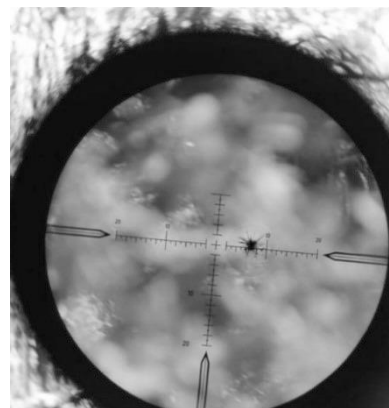


Рис. 1 Уражений лазером приціл

Як відбувається ураження лазерними системами розвідки та їх статистика в Україні

Чому саме зараз актуально розглядати розвиток та масове впровадження приладів оптичної протидії? На прикладі збройного конфлікту на сході України легко побачити збільшення випадків лазерних атак на позиції, що мало би призводити до прискіпливішої оцінки можливостей ворога та розробку нових технологій

протидії. Неодноразово місія ОБСЄ фіксувала скерування лазерного проміння у камери спостережень, що у результаті виводило їх із ладу [4]. У 2016 році від лазера постраждало 5 прикордонників, 4 з яких в ході медичних операцій та тривалої реабілітації все-таки відновили свій зір до 100%, але за словами потерпілих у них залишається невеличка пляма, яку вони все одно продовжують бачити. На місці опіку формується рубець. За словами медика, військові бачили зелено-жовтий спалах. Сам опік нагадує дію медичного лазера – його використовують для укріплення сітківки ока.

Ще 80-тих роках в Радянському Союзі розробили лазерний прилад оптико-електронної протидії. Він мав боротися зі снайперами – шукати оптику і бити по ній лазером і, відповідно, по очах бійця. На той час заявлена дальність дії приладу складала півтора кілометра при вазі у майже 60 кілограмів. Але що саме використовується у Луганській та Донецькій областях, на цей момент із впевненістю не може сказати ніхто.

Прості лазерні указки не здатні сильно нашкодити бійцям. Видимі лазери занадто помітні і втрачають ефективність на дистанції. Тому для початку потрібно провести аналітичну роботу по розпізнаванню техніки опонента. Те, що дійсно викликає занепокоєння, це невидимість такого «удару». Тобто з інфрачервоним випромінювання ситуація наступна – борець не знає, що його опромінюють і не може дізнатися, доки його зір просто не пропаде. Але якщо ж він побачив, що щось світиться і військовий не знає джерела даного світла, то туди дивитися не варто. Є небезпека того, що це буде лазер.

Розбір існуючих лазерних приладів оптичної протидії їх переваги та недоліки, принцип дії

СИЧ 5К10. Україна. Варто зазначити, що й українські розробники зброї показують позитивні результати. До прикладу можна взяти комплекс розвідки та виявлення оптичних приладів СИЧ 5К10 (рис 2). Виготовленням та випробуванням якого займається компанія Thermal Vision Technologies. Це контрснайперський комплекс, який є багатофункціональним оптико-електронним пристроєм. По характеристичних даних прилад може здійснювати моніторинг середовища цілодобово. Основна задача полягає у пошуку цілей та автоматичному виявленні прихованих та явних оптичних приладів прицілювання. Для більшого функціоналу розробники також додали можливість визначення координат і відстані об'єкта, який виявляється в складних умовах рельєфу місцевості та міських забудовах. Виконує також превентивну функцію, що є не менш важливим - це дозволяє запобігти снайперській атаці або терористичному акту ще на етапі їх підготовки [11].



Рис. 2 СИЧ 5К10

Характеристичні дані:

Дальність виявлення оптичних приладів до 2000 м, Діапазон вимірювання відстані до цілі 25 – 6000 м, похибка складає 1 м. Відстань виявлення цілей: людина – до 2500 метрів, автомобіль – до 6000 м.

Комплекс включає у себе два режими:

Пасивний режим. Розвідка територій і навколишнього оточення за допомогою телевізійного і тепловізійного модулів з метою пошуку і виявлення цілей, вимірювання відстані до них і визначення координат.

Активний режим. Лазерне сканування вручну визначених (для локалізації місця пошуку та оперативного виявлення) ділянок місцевості з метою пошуку і автоматичного виявлення прихованих оптичних приладів прицілювання і спостереження, вимірювання відстані до них і визначення координат. Одна з вагомих переваг, яку можна виділити - це спостереження теплових об'єктів (пасивні та активні джерела) в умовах обмеженої видимості (відсутності світла, наявності диму і туману).

Виявлення замаскованих оптичних приладів прицілювання і спостереження здійснюється по їх відблискам, які утворюються в результаті відбиття лазерного випромінювання від їх оптичних систем. Оптико-електронний блок містить телевізійний модуль, лазерний модуль, лазерний далекомір, GPS приймач, цифровий компас і блок управління. Керування режимами роботи комплексу та параметрами всіх модулів здійснюється дистанційно з віддаленого комп'ютера одним оператором, який повинен знаходитись у безпечному місці, щоб запобігти виявлення його локації.

На монітор віддаленого комп'ютера виводяться відео з телевізійного і тепловізійного модулів, електронна мапа місцевості з індикацією місцеположення (координат) виявлених цілей, а також режими роботи і параметри модулів.

Сферами застосування комплексу є виявлення снайперів і замаскованих оптичних приладів спостереження, охорона спеціальних зон і територій, захист об'єктів критичної інфраструктури, організація анти-терористичної діяльності, забезпечення безпеки командних і опорних пунктів, дистанційний моніторинг терористичних загроз.

«Каштан-3М». Україна. Мобільний автоматизований комплекс оптико-електронної протидії «Каштан-3М» (рис. 3) створений київським НДІ «Квант», що спеціалізуються в області розробки засобів оптико-електронного захисту і протидії високоточній зброї.

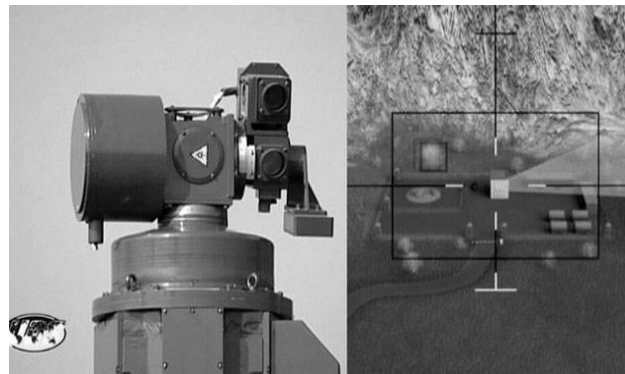


Рис. 3 «Каштан- 3М»

Комплекс призначений для захисту особливо важливих об'єктів від високоточної зброї - ракет, снарядів і авіабомб з напівактивними лазерними головками самонаведення (НЛГСН). Відповідно до результатів досліджень McKinsey & Company III виявив здатність виявляти каталізatori виникнення емоцій та почуттів у людини. Це може свідчити про те, що з часом впливати на точки зору, принципи людини стане в рази легше. Таким чином недобродушні розробники нейронних мереж зможуть досягати своєї вигоди, незважаючи на думки простих людей.

Даний комплекс володіє характеристиками, які дають змогу за короткий проміжок часу виявити противника та створення хибної лазерної цілі. Наприклад, можливість виявлення випромінювання цілевказівника противника, починаючи від 0,9 секунди. Відповідно максимальний час за котрий буде здійснено перенацілювання боеприпаса на хибну лазерну ціль складає максимум 1 секунду, що є дуже важливо в умовах проведення операції.

Принцип дії. При виявленні випромінювання/підсвічування лазерного цілевказника противника комплекс включає свій лазерний передавач, який у свою чергу підсвічує інший, випадковим чином обраний, сторонній об'єкт, це може також бути морська поверхня. Тоді він формує хибну лазерну ціль для захисту важливої інфраструктури.

Функціональні особливості:

- виявлення та пеленгація джерел лазерного випромінювання – ЛЦВ противника;
- постановка хибних лазерних цілей (активних імітаційних перешкод для систем високоточної зброї з лазерним наведенням);
- приймання цілевказівки від зовнішніх інформаційних систем і передача її до автоматизованої системи бойового управління носія чи інших систем управління;
- повністю автоматичний режим роботи;
- вибір тактики захисту в залежності від типу і кількості атакуючого боеприпасу;
- можливість зміни прийнятих рішень оператором вручну;
- реєстрацію та документування інформації про тактичну ситуацію, параметрах випромінювання лазерних цілевказників, реакціях комплексу та діях оператора;
- тренування особового складу;
- автоматичний контроль працездатності комплексу та пошук несправностей з індикацією модуля, що відмовив.

З даним комплексом було проведено багато тривалих практичних випробувань, встановлено, що абсолютно всі керовані ракети, скинуті на ціль, при використанні мобільного автоматизованого комплексу оптико-електронної протидії, відхилилися від заданих цілей ураження на безпечну відстань. За даними розробників, комплекс здатний одночасно відобразити атаку двох-трьох десятків високоточних ракет.

Подібний метод захисту не потребує використання витратних боеприпасів, зрив наведення вражаючих елементів високоточної зброї відбувається без їх вогневого ураження, що значно знижує вартість бойового застосування. В побудові комплексу закладені приймач

лазерного випромінювання і прилад постановки хибної лазерної цілі. Приймачі лазерного випромінювання - висувні, вони встановлені з кожного боку кунга. Прилад постановки хибної лазерної цілі (ХЛЦ) розміщений на основі, на даху комплексу. До складу «Каштан-3М» також входять пульт управління комплексом, засоби управління приводами постановки ХЛЦ, засоби контролю та комутації первинного електроживлення. На думку розробників, головною складовою комплексу є не його матеріальна частина, а алгоритм роботи і програмне забезпечення, створене на основі тривалого вивчення практичного досвіду використання зброї з лазерною системою наведення і тактики його застосування.

Заплановано продовження робіт з модернізації комплексу та зменшення його розмірів. За інформацією з ЗМІ, даним комплексом зацікавилася одна з країн Азії. Планується використовувати даний комплекс для захисту промислових об'єктів і командних пунктів. На сьогоднішній день вже втілено встановлення даного комплексу на перспективні зразки бронетанкової техніки, зокрема, на основні бойові танки [9].

SLD 500, CILAS, Франція

Також варто розглянути прилади, які використовують й інші передові країни світу. Одним із таких є SLD 500 від французького виробника CILAS (рис. 4). Для точного виявлення снайперської оптики на місці використовуються промислові лазери, такі як детектори Glint. Лазерний промінь наводиться в напрямку передбачуваного положення снайпера і при появі контакту з об'єктивом телескопічного прицілу або іншого оптичного приладу противника формується відбита енергія або енергія зворотного розсіювання, яка дозволяє засікти положення снайпера. Такі системи дозволяють точно і швидко визначити загрозу і ідентифікувати її з допомогою цифрової камери з високою роздільною здатністю.



Рис. 4 SLD 500, CILAS

Кожен модуль системи схожий на радар для визначення швидкості. Цей модуль розрахований на створення «зони безпеки» певної площі, при необхідності покрити більшу площу необхідно використовувати кілька модулів, пов'язаних в єдину систему.

Промінь лазера, що посилається кожним модулем, відбивається від кожної поверхні, яку він висвітлює. Спеціальний фотоприймач уловлює відбиті сигнали, і процесор системи виділяє із загальної картини

сигнали з характеристиками відповідними або близькими до відбиття від лінз оптичних прицілів. Точність така, що модуль в стані розрізнити сигнали відбиття від лінз фотоапаратів, відеокамер і біноклів.

Системою може керувати оператор або встановлювати її в повністю автоматичне виявлення для цілодобового спостереження з відеозйомкою. При виявленні загрози спливе сигнал тривоги, і SLD 500 негайно надасть своє місцезнаходження GPS і точну відстань, що дозволить командам контрнадзорів реагувати тихо і швидко. Систему можна поєднувати з різними тепловізорами для нічних операцій. Застосування цієї системи може залучати різні сфери діяльності людини. Її можна використовувати для охорони високопоставлених осіб під час виступів в публічних місцях, охорони громадських місць, де присутня велика скупчення людей. Наприклад, кілька модулів можуть бути встановлені по межах стадіону, площею. У разі появи снайпера в радіусі дії системи, його позиція тут же була б визначена класичним методом триангуляції. При цьому інші «безпечні» джерела відображень лазерного променя були б просто проігноровані. Тобто даний прилад несе важливу превентивну місію [10].

Розбір існуючих приладів протидії лазерним приладам

Починаючи з найпростіших методів, розглянемо спочатку методи, що не потребують або майже не потребують спеціального додаткового обладнання.

Метод розміщення хибних цілей. Ідея полягає у тому, що на території бойових дій будуть застосовані хибні «мішені». Як було описано вище, методи протидії оптико-електронним приладам здатні виявляти відблиски, що не є справжніми оптичними приладами, наприклад скляні пляшки, їх уламки і т.п., тому для використання даного методу потрібні справжні прилади, з складними системами лінз. Такими можуть слугувати дешева і в основному непридатна для використання в бойових діях китайська оптика.

Разом з цим, має бути дотримане правило – не використовувати реальні оптичні прилади в зоні де працюють системи оптико електронної протидії більше ніж на декілька секунд. Якщо є велика потреба, використовувати цифрові системи нагляд з дисплеєм. Це не врятує від ураження, але врятує зір оператора приладу [15, 16].



Рис. 5 Цифровий бінокль Sony DEV-5

Ще одним способом є *діафрагмування об'єктиву*. Мається на увазі, у кришці, яка закриває бленду, вирізати отвір бажано не правильної форми, малого розміру.

Очевидно, якість зображення значимо погіршиться, але це краще ніж травми від ураження лазером, або виявлення позиції ворогом. Перейдемо до технічно-наукових рішень, спеціально вироблених для протидії.

Метод сотових бленд. Сотові бленди – по своїй природі антиблікові насадки, які перешкоджають потраплянню сонячних променів на лінзи та їх подальшому відбиттю. Згідно принципів роботи лазерних систем протидії, якщо лазерний промінь не відіб'ється назад, відповідно позиція бійця не може бути виявлена. Такі бленди за розмірами мають набагато перевищувати діаметр оптики. Поверхня таких пристроїв повинна бути затемнена для зменшення повторного відбиття. Цікавим способом заміни сотової бленди є її саморобна версія за допомогою звичайної трубчастої бленди та чорних або темних трубочок для коктейлів, що щільно вкладені всередину. Таким чином виходить власна сотова бленда, що має подібні властивості, але звичайно незрівнянна з спеціально виготовленою на виробництві.



Рис. 6 Сотова бленда

Засоби звуження кута відблиску променя. На початку дані системи були розроблені для допомоги боротьби з відблисками, що видавали позицію британських військових. В цьому вони схожі на сотові бленди. Всередині знаходиться диск, що може змінювати кут свого положення. В закритому вигляді він представляє собою кришку, що захищає оптику від бруду, води та пилу. Кут змінюється за допомогою двох зовнішніх гвинтів. Він зберігає картину прицілу навіть у той час коли відкритий на декілька градусів, зберігаючи покритими більшість об'єктивних лінз [16].



Рис. 7 Звужувач кута The Sniper Hider

Метод світлофільтрів. Лазерні детектори використовують інфра-червоний діапазон, який людське око не здатне виявити. Не дарма обрана саме ця довжина хвиль – для того щоб прилад був непомітним. Але саме ця особливість приладів оптичної протидії має і недолік – якщо не допустити попадання променя на фокальну область об'єктива, то він не відіб'ється, а це у свою чергу значить не буде блику. Логічно випливає, що якщо використовувати фільтри, що поглинають світло інфра-червоного діапазону, приціл не втратить своїх характеристик, так як нам потрібен видимий діапазон для його використання, а системи виявлення не зможуть помітити оптичний або оптико-електронний прилад. Недоліком даного методу є те, що такі системи як «Сжатие» використовують комплексні діапазони. Від такого типу лазерної зброї світлофільтри не допоможуть. Також варто зазначити, що деякі фільтри не поглинають, а відбивають ІЧ-промені, тому потрібно ставити такі застосунки між лінзою та соотовою блендою, тоді ефект буде найкращим [18].



Рис. 8 Інфрачервоний світлофільтр

Використання світлофільтрів із нанесеним на них світлопоглинальним покриттям. Зменшення помітності оптико-електронного приладу досягається зменшенням ефективної площі розсіювання за рахунок використання з'ємної бленди з захисним склом, з іншого боку якого нанесено світлопоглинальне покриття, яке складає 10 % діаметра вхідної оптичної поверхні приладу, що призводить до зменшення потужності відбитого сигналу. Недоліком цього способу є те, що при застосуванні потужних зондуючих випромінювань лазерним детектором рівень пониження ефективної площі розсіювання є недостатнім.

Кутникові відбивачі. Кутникові відбивачі – конструкції форма яких є тетраедром із взаємно перпендикулярними площинами. Особливістю даної конструкції є таке переломлення направлено на нього променя, що він відбивається строго у місце з якого вийшов промінь.

Такі конструкції використовують у підвищенні помітності навігаційних знаків, радіоелектронній боротьбі, точному вимірюванні відстані до об'єктів. Яскравим прикладом є знаходження за допомогою лазера та кутникового відбивача «Лунохода-1», на Місяці. Якщо розмістити декілька таких споруджень у зоні дії лазерних засобів протидії, це значно загальмує процес виявлення справжньої оптики [17].



Рис. 9 Кутниковий відбивач

Антиблікові плівки. Дані плівки використовуються на телефонах, камерах, автомобільних стеклах та інших приладах і є досить поширеними. Принцип дії полягає у самому матеріалі плівки. Поверхневий шар являє собою пагорби різної висоти. Через дану особливість, світло потрапляючи на поверхню відбивається по різних напрямках, тобто розсіює промені. Існує два види таких плівок: на акриловій основі та на натуральній основі. Акрилова основа має декілька переваг, перша з них це висока стійкість до пошкоджень, друга це довговічність. Недоліком є помутніння матеріалу після використання акрилу. Плівки на натуральній основі є маркими, але ніяк не впливають на прозорість матеріалу, тому, напевно, підходять для оптики краще. У теорії можна використовувати музейне безблікове скло, але воно доволі дороговартісне [19].

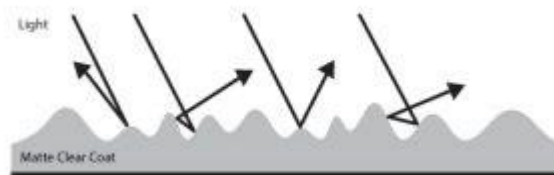


Рис. 10 Поверхня антиблікової плівки

Антилазерні окуляри. Цікавим теоретичним виходом з ситуації атаки на око снайпера можуть слугувати професійні антилазерні окуляри. Вироблені для деяких професій, таких як лазерний гравірувальник, такі окуляри мають принцип дії зав'язаний на перетворенні енергії. Скло в таких окулярах поглинає лазерне опромінення, перетворюючи енергію в тепло. Недоліком є те, що вони обмежені у довжині хвилі і обирати їх потрібно від того, який лазер використовується. Такі прилади мають свою характеристику рівня захисту, одним з найвищих є O.D:6. Він захищає очі при довжині хвилі 600-1000 нм. Важливо зазначити, що такі окуляри повністю не захищають від лазерного ураження і, очевидно, не скриють позицію снайпера.

Технології захисту майбутнього. Варто зазначити, що на даний момент розробляються електронні прилади протидії лазерному опроміненню. Принцип їх дії полягає у виявленні інфра-червоного опромінення, яке передає прилад лазерної протидії, за допомогою фотодіоду, що має малі габарити та є чутливим. Після виявлення ІЧ променів, пристрій передає сигнал на плату, яка у свою чергу передає живлення на рідкокристалічні фільтри. Вони під дією струму змінюють площину поляризації світла, яке проходить повз них. Змінюючи напругу, можна змінити кількість світла, що проходить

через фільтри. При мінімальній прозорості інфрачервоне світло не проходить взагалі. Після завершення опромінення датчики не приймають промені, і кристали стають у звичайну форму [20].



Рис. 11 Захисні окуляри

Дорогим методом є використання цифрових прицілів для снайперських гвинтівок. Цифрові приціли мають високий функціонал, порівняно з оптичними. Тепловізори, багато режимів роботи, все це дають цифрові приціли. На щастя, наявні в даний час інструменти, такі як штучний інтелект і машинне навчання, все більшою мірою здатні впоратися з цим завданням. Щоб успішно використовувати нові, передові технології для боротьби з сьогодишнім постійно мінливим ландшафтом загроз, взаємодія людини і машини-це те, над чим ми повинні працювати.



Рис. 12 Цифровий приціл

Також існують патенти, в яких принцип дії полягає у наступному – оптико-електронний прилад отримує лазерне опромінення, що реєструється спеціальним датчиком. Після цього генерується перешкоджаючий лазерний промінь, який направляється у тому самому напрямку, звідки було отримане лазерне опромінення, для дезорієнтації приладу оптико-електронної протидії. Напрямки можуть бути обрані різними, від того місця звідки прийшло опромінення до його оптичних систем. При цьому необхідно щоб довжина хвилі перешкоджаючого випромінювання була такою самою як у опромінювача. Крім того необхідно, щоб перешкоджаючий промінь потрапив на оптику у той момент часу, коли він відкритий для прийому.

Висновок

Для виробництва та належного експлуатування лазерних приладів протидії потрібні іноваційні рішення, основною задачею яких буде - не дати викрити позицію бійця (мішені) та виявлення зондуючого променя.

Вже готові розробки стратегічного виробника озброєння та військової техніки ГК «Укроборонпром»

показали на практиці, що Україна прагне аби в арсеналі війська було більше сучасного, якісного, високотехнологічного та надійного озброєння, здатного захистити державу та зберегти життя військових.

Досвід та методи захисту розвиваються по мірі появи нових приладів оптичного ураження, а бійці стають все кращими на полі бою. З розібраних у статті методів захисту від лазерів можна помітити, що спеціалізованих приладів не є багато.

Кожен з засобів має свої унікальні характеристики і не є подібними один до одного. Всі вони використовуються не за своїм основним призначенням, але автори прийшли до висновку, що розробка спеціалізованих приладів захисту від систем оптико-електронної протидії є надзвичайно важливим завданням, що має бути вирішене у найближчий час. Це зумовлено активним використанням бойових лазерних променів, у тому числі Росією проти України, а також через відсутність аналогів, створить велику зацікавленість інших країн.

Список літератури

- [1] М.М. Браїловський, І.С. Іванченко, І.Р. Опірський, В.О. Хорошко. Інформаційно-психологічне протиборство в Україні // НАУ: Науковий журнал «Безпека інформації», – том 25 №3, – Київ, 2019. – С.144-149.
- [2] Опірський І.Р. Проблематика основного постулату прогнозування НСД // Науковий збірник «Сучасна спеціальна техніка». – Київ, ДНДІ МВС України. – №2(41). – 2015р. – С.3-8.
- [3] Дудикевич В.Б., Опірський І.Р. Аналіз моделей захисту інформації в інформаційних мережах держави// Системи обробки інформації. Вісник Харківського університету повітряних сил ім. Івана Кожедуба. – Харків, 2016р. – Випуск 4(141). – С.86-89.
- [4] Окупанти застосували біля станції сліпучі лазери [Електронний доступ] Режим доступу: <https://www.ukrinform.ua/rubric-ato/3248919-okupanti-zastosovali-bila-panic-slipuchi-lazeri-ukraina-v-obse.html>.
- [5] Лазерна атака на Донбасі [Електронний доступ] Режим доступу: <https://www.radiosvoboda.org/a/donbas-realii-lazerna-ataka-na-donbasi/29619874.html>.
- [6] Blinding laser weapons: questions and answers [Електронний доступ] Режим доступу: <https://www.icrc.org/en/doc/resources/documents/misc/57jmcz.htm>.
- [7] Промінь смерті – мрія, відтворена в металі [Електронний доступ] Режим доступу: <https://armyinform.com.ua/2020/04/promin-smerti-mriya-vidtvorena-v-metali/>.
- [8] Комплекс розвідки та виявлення оптичних приладів СИЧ 5К10 [Електронний доступ] Режим доступу: <https://www.youtube.com/watch?v=5qaHkplalT&t=5s>.
- [9] Мобільний автоматизований комплекс оптико-електронного протидії «Каштан-3М» [Електронний доступ] Режим доступу: <https://ru.uos.ua/produksiya/sistemi-zashchiti/45-mobilniy-avtomatizirovanniy-kompleks-optiko-ielectronnogo-protivodeystviya-kashtan-3m>.
- [10] Системи обнаружения снайперов противника [Електронний доступ] Режим доступу: <http://newsmilitary.narod.ru/VH-antisniperteh.html>

[11] СИЧ 5К10 [Електронний доступ] Режим доступу: <https://archer.ua/ua/product/kompleks-rozvidk-i-ta-viavlenna-opticnih-priladiv-sic-5k10>.

[12] Lasers Stop Snipers Before They Fire [Електронний доступ] Режим доступу: <https://www.wired.com/2007/04/darpa-countersn/>.

[13] Laser Optical Detection System «LODS-2000» [Електронний доступ] Режим доступу: <http://uarpa.com/en-US/Laser-technology/Laser-Optical-Detection-System-LODS-2000.aspx?ID=63>.

[14] «Mobile Optical Detection System for Counter-Surveillance» [Електронний доступ] Режим доступу: <http://s3.amazonaws.com/arenaattachments/1381379/c3a4e751324dc288e976bd33d0295ea3.pdf?1509407477>.

[15] «Аналіз науково-технічних рішень щодо захисту оптичних та оптико-електронних приладів спостереження від лазерних приладів оптичної протидії» [Електронний доступ] Режим доступу: <http://perio>

dica.nadpsu.edu.ua/index.php/military_tech/article/view/539/509.

[16] «Лазер проти снайпера: протидія сучасним лазерним детекторам оптичних приладів» [Електронний доступ] Режим доступу: <https://www.ukrmilitary.com/2018/05/laser-vs-sniper.html>.

[17] Кутниковий відбивач [Електронний доступ] Режим доступу: https://uk.wikipedia.org/wiki/%D0%9A%D1%83%D1%82%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2%D0%B8%D0%B9_%D0%B2%D1%96%D0%B4%D0%B1%D0%B8%D0%B2%D0%B0%D1%87.

[18] Оптичні фільтри [Електронний доступ] Режим доступу: <https://hoayafilter.com/catalog/>.

[19] Антиблікові плівки [Електронний доступ] Режим доступу: <https://www.forceone-am.com/en/pf.html>.

[20] Електронна система протидії лазерним засобам локації та ураження [Електронний доступ] Режим доступу: <http://feltran.kpi.ua/article/view/199000>.

УДК 654.071

Opirskyy I.R., Sovyn Ia.R., Datsenko Ye. M., Usyk M.Yu.

ANALYSIS OF METHODS AND MEANS OF COUNTERING LASER INTELLIGENCE SYSTEMS

Abstract. The use of laser systems allows for the best possible development of military affairs, but it can also pose a great threat because there is constant competition between opponents who test the latest laser technology on people fighting on the other side, which contradicts the protocols on inhumane weapons. This article discusses the possible means of laser attacks and what consequences they have, as well as assesses the current state of domestic developments in this area. But this publication aims not only to describe the strategy for the development of laser reconnaissance systems and a characteristic comparison of different representatives, it will describe methods of protection against them. Features of construction and functioning are given. Despite the various advantages and disadvantages of defense systems, several effective, proven in real combat conditions, methods of defense have been found.

Key words: laser reconnaissance systems, means of counteraction to laser reconnaissance systems, laser blinding weapons, counter laser blinding weapons, countering laser sniper detection system.

UDK 654.071

Opirskyy I.R., Sovyn Ia.R., Datsenko Ye. M., Usyk M.Yu.

АНАЛИЗ МЕТОДОВ И СРЕДСТВ ПРОТИВОДЕЙСТВИЯ ЛАЗЕРНЫМ СИСТЕМАМ РАЗВЕДКИ.

Аннотация. Использование лазерных систем позволяет максимально развить ведение военного дела, но это может также представлять большую угрозу тому, что постоянно идет конкуренция между противниками, испытывающими новейшие лазерные технологии на людях, воюющих на другой стороне, что противоречит протоколам о негуманном оружии. В этой статье рассмотрены возможные средства лазерных атак и какие последствия они несут, также оценено состояние отечественных разработок в данной сфере. Но данная публикация имеет целью не только описание стратегии развития лазерных систем разведки и характеристическое сравнение разных представителей, здесь будут описаны методы защиты от них. Приведены особенности построения и функционирования. Несмотря на различные преимущества и недостатки систем защиты, было найдено несколько эффективных способов обороны, проверенных в реальных боевых условиях.

Ключевые слова: лазерные системы разведки, средства противодействия лазерным системам разведки, laser blinding weapons, counter laser blinding weapons, countering laser sniper detection system.

Опірський Іван Романович, д.т.н., професор, професор кафедри захисту інформації Національного університету «Львівська політехніка».

Opirskyy Ivan, Doctor of Technical Sciences, Professor, Professor of the Department of Information Protection of the National University "Lviv Polytechnic".

Опирский Иван Романович, д.т.н., профессор, профессор кафедры защиты информации Национального университета "Львовская Политехника".

Совин Ярослав Романович, к.т.н., доцент, доцент кафедры захисту інформації Національного університету «Львівська політехніка».

Sovyn Yaroslav, Ph.D., Associate Professor, Associate Professor of the Department of Information Protection of the National University "Lviv Polytechnic".

Совын Ярослав Романович, к.т.н., доцент, доцент кафедры защиты информации Национального университета "Львовская Политехника".

Sovyn Yaroslav, Ph.D., Associate Professor, Associate Professor of the Department of Information Protection of the National University "Lviv Polytechnic".

Даценко Єгор Максимович, студент кафедри захисту інформації Національного університету «Львівська політехніка».

Даценко Егор Максимович, студент кафедры защиты информации Национального университета "Львовская Политехника".

Datsenko Yegor, Student of the Department of Information Protection of the National University "Lviv Polytechnic".

Усик Мирон Юрійович, студент кафедри захисту інформації Національного університету «Львівська політехніка».

Усик Мирон Юрьевич, студент кафедры защиты информации Национального университета "Львовская Политехника".

Usyk Myron, Student of the Department of Information Protection of the National University "Lviv Polytechnic".