сполучену з мобільним телефоном по якому передавати відео потік. При цьому фрагменти індивідуальної IP-камери через засоби мобільного оператора або через Wi-Fi канали зв'язку будуть автоматично вмонтовані у фільм-звіт.

Розглядаються напрямки використання видеофіксації переміщень об'єкта.

Перше це спостереження за об'єктом. Другий напрям це збір доказової бази присутності об'єкта в даному місті в даний час. Яка може бути використана як для звинувачення підозрюваного, так і для його захисту. Третій напрям це пошук свідків подій. Які мають мобільні телефони і знаходились в полі зору веб-камери.

Висновки:

Удосконалення системи відеоспостереження дозволяє більш ефективно реалізовувати роботу правоохоронних органів. Система дозволить підвищити ефективність діяльності поліції.

Система запатентована автором: Мордвинцев М.В., Машкаров Ю.Г. Спосіб відео документування переміщень об'єкта за допомогою системи відео фіксації. Патент на корисну модель № 73635, 2012, -4 с.

**Список бібліографічних посилань**


1. Мордвинцев Н.В., Усовершенствование систем видеонаблюдения при реализации задач правоохранительных органов. Издательский дом "Интернаука" Международный научный журнал 5 (1), 59-61
2. Мордвинцев М.В., Машкаров Ю.Г. Спосіб відео документування переміщень об'єкта за допомогою системи відео фіксації. Патент на корисну модель № 73635, 2012, -4 с.



**ОЛЕГ СТЕПАНОВИЧ ГАВРИШ**
викладач кафедри економічної та інформаційної безпеки
Дніпропетровського державного університетету внутрішніх справ


## ІНФОРМАЦІЙНІ АСПЕКТИ СУЧАСНИХ МЕТОДІВ ГІБРИДНОЇ ВІЙНИ

Основна проблема гібридної війни полягає в тому, що вона не закінчується швидко. У кіберпросторі ми повинні готуватися до тривалої війни. Більш того, засоби і методи ведення гібридної війни будуть удосконалюватися з боку противника. Потрібно залучати кращих інформаційних фахівців до цього процесу і воювати кращими методами в тісній співпраці з нашими західними партнерами. Тому що застарілими методами виграти сучасну інформаційну війну неможливо [1].

Ситуація безпеки навколо України може змінюватися динамічно. Очевидно, що в разі її загострення і виникнення значних інформаційних загроз будуть швидко прийняті необхідні політичні та управлінські рішення, затверджені нормативно-правові акти. Але, все це втрачає будь-який сенс, якщо в Україні завчасно і в необхідній кількості не будуть відібрані і

підготовлені бійці «інформаційного фронту», які вміють ефективно виконувати завдання в області кібербезпеки держави.

Аналіз ситуації показав картину, яка насторожує. На тлі поточного дефіциту справжніх фахівців ми виявили тенденцію відтоку навіть наявних кадрів. Не секрет, що в кінці минулого року звільнився в запас полковник Владислав Селезньов, який заслужив гарну репутацію серед представників ЗМІ та симпатії у численних аудиторій глядачів. Стало відомо про наміри звільнитися в запас добре відомого в закритих колах офіцера структур інформаційно-психологічних операцій, який реалізував успішний проект з протидії російської інформаційної агресії. Є інші аналогічні приклади. Отже, щось у нас не так і проблема кадрового потенціалу стає критичною. Тому потрібно щось кардинально змінювати [1].

Нещодавно натрапила на інформацію з питань підготовки та мотивації фахівців для дій в інформаційному та кіберпросторі в західних країнах. Виявляється, у них є суттєві і іноді дуже схожі з нашими проблеми. Російська інформаційна агресія також спонукала їх до перезавантаження, а в кадровому плані виникло найбільше запитань. Наприклад, ЦРУ в 2017 році був змушений відкрито оголосити про пошук значної кількості нових фахівців, які добре знають російську мову, відповідну культуру, традиції і т.д. і готові внести свій внесок у протидію деструктивним діям Російської Федерації в інформаційному просторі.

Майже одночасно спецслужба в Великобританії GCHQ (Government Communications Headquarters, тобто «Центр урядових комунікацій») була змушена визнати, що відчуває проблеми з залученням, мотивацією і змістом персоналу, в першу чергу фахівців з інформаційної безпеки (згідно з матеріалами щорічного звіту GCHQ). Причина дуже проста - урядова організація не в змозі бути конкурентною з високотехнологічними компаніями сфери бізнесу, які мають набагато більше важелів мотивації і часто пропонують в кілька разів більший рівень грошового забезпечення.

У сусідній Польщі також змушені підвищувати імідж спецслужб і одночасно вирішувати їх кадрову проблему через відкриті джерела інформації.

Подібних прикладів досить багато. Їх об'єднує одне: існує кадрова проблема, але одночасно з'являється її розуміння і бажання вирішити. Ми повинні бути вдячними, оскільки досвід сусідів дає нам шанс не «винаходити велосипед» або «наступати на граблі». У нас, в свою чергу, виявляються цілком очікувані причини проблем.

Перша і найголовніша - це неповне розуміння нових викликів в інформаційному просторі і шляхів нейтралізації їх з боку вищого політичного і військового керівництва країни. Це окрема тема для дискусії, тому залишимо її за межами цієї публікації.

Наступна проблема - процедури підготовки кадрів в навчальних закладах і подальше призначення їх після випуску на конкретні посади в силовому блоці. Виявляється, після майже чотирьох років війни ми зберігаємо якесь зачароване коло. Підготовка фахівців у вищих навчальних закладах для структур сектору безпеки і оборони здійснюється на підставі державного

замовлення. Процедура формування такого замовлення, в першу чергу, ґрунтується на штатній потребі у фахівцях певного рівня і напряму на момент їх випуску для подальшої служби в конкретних організаційних структурах (певних підрозділах спецслужб, бойових військових частинах і т.д.). Іншими словами, якщо ми очікуємо через 5 років конкретного лейтенанта-випускника, то вже сьогодні ми повинні розуміти, на яку конкретно посаду ми його призначаємо. А якщо ці посади ще не існують? Тоді в нинішньому державному замовленні ці фахівці просто не будуть передбачені і набір першокурсників не відбудеться.

Тому виникає питання, чи існує в державі чітке бачення перспективних організаційних структур? Чи не чергових департаментів або директоратів на управлінської верхівки силових структур, а саме бойових підрозділів? До речі, я знаю про низку рішень в силових структурах щодо вдосконалення та розвитку структур інформаційного протиборства, які чомусь не виконані.

Третя проблема - де і як готувати фахівців? Мені добре відома і зрозуміла проблематика стратегічних комунікацій. Наприклад, кілька років тривала дискусія про необхідність створення в Національному університеті оборони України навчально-наукового підрозділу у напрямку стратегічних комунікацій, який мав унікальний шанс стати загальнодержавним інтегратором серед силових структур держави та прикладом навіть для західних партнерів. За наявною інформацією цю ідею чомусь «спустили на гальмах» і в перспективній структурі університету такий підрозділ не розглядається.

Потрібні й інші гнучкі форми кадрового забезпечення «інформаційного фронту». Наприклад, через службу в резерві для цивільних представників сфери ЗМІ, рекламного бізнесу, відомих блогерів, «білих хакерів» і ін. Про всяк випадок, в Збройних силах України вже більше 150 000 чоловік служать в оперативному резерві і логічно бачити в їх рядах бійців інформаційного напряму.

Найголовнішим фактором успіху я вважаю питання формування цінностей, етичних норм і мотивації. Більшість необхідних спеціальностей інформаційних воїнів є високотехнологічними і добре стимульований матеріально в цивільному житті. Це не солдати піхоти, які можуть вчитися в масовому форматі в разі мобілізації. Йдеться про штучний підхід. Кожен такий фахівець є унікальним і своєрідним. Якщо ми сподіваємося отримати їх досвід і знання для безпеки держави - слід міняти наші підходи в роботі державних структур з цінними кадрами і фахівцями [2].

Здається, що нам достатньо грати в волонтерські «інформаційні війська». Досить «виїжджати» на волонтерських проектах і випрошувати допомогу у закордонних партнерів. Настає час вирішувати питання протидії інформаційному агресору на професійному рівні. Або іншими словами - інвестувати в майбутнє безпеки держави.

**Використані джерела**

1. Попова Т. Методами "красных замполитов" выиграть современную информационную войну невозможно. [Електронний ресурс] // NV.UA – 2018.

– Режим доступу: https://nv.ua/opinion/popova/hlavnaja-problema-informatsionnoho-fronta-ukrainy-2450161.html

2. Колодюк А. Информационные технологии: двигатель для Украины. [Електронний ресурс] // ZN.UA – 2018. – Режим доступу: https://zn.ua/ECONOMICS/informatsionnye_tehnologii_dvigatel_dlya_ukrainy.html

**ЕДУАРД ВОЛОДИМИРОВИЧ РИЖКОВ**
кандидат юрідичниїх наук, доцент, завідувач кафедри економічної та інформаційної безпеки, Дніпропетровського державного університету внутрішніх справ

## ДЕЯКІ ПРОБЛЕМНІ ПИТАННЯ В РОБОТІ СЕКТОРІВ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ ТЕРИТОРІАЛЬНИХ ОРГАНАХ ТА ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Відповідно до п. 2 ст. 18 Закону України «Про національну поліцію» поліцейський повинен професійно виконувати свої службові обов'язки відповідно до вимог нормативно-правових актів, посадових (функціональних) обов'язків, наказів керівництва. На практиці з реалізацією цих норм закону виникають проблеми, адже відсутній єдиний підхід до організації покладання службових обов'язків на працівників відділів та відділень поліції.

Так як специфіка роботи співробітника сектору інформаційної підтримки (далі – СІП) управління та районного відділу різниться, то й функціональні обов'язки мають бути різними. Проте це не виключає системності в підході до складання функціональних обов'язків для співробітників. З метою більш якісного виконання покладених функцій вони мають бути вичерпними та чітко визначеними. Адже зараз та робота, яку виконують працівники, залежить в певній мірі від особистого ставлення керівника відділу чи відділення, що знижує ефективність кінцевого результату.

Виходом з ситуації що склалася нами вбачається необхідність розробки типових функціональних обов'язків на рівні Департаменту інформаційно-аналітичної підтримки для працівників кожного рівня підрозділів з урахуванням їх специфіки та покладених на них завдань. Це забезпечить більш ефективне та стабільне виконання завдань підрозділами на місцях та зменшить навантаження на працівників «не своєї» роботи, що в свою чергу підвищить якість кінцевого результату.

На рівні управлінь, як на нашу думку, пропонуємо визначити доступи виключно до тих інформаційних підсистем, які необхідні для виконання покладених обов'язків. Наприклад, великою проблемою є навантаження окрім основної інформаційної підсистеми, яка підлягає наповненню - ІП «Кримінальна статистика», є ведення ІП «Єдиний облік», а саме облік та контроль прийнятих рішень за матеріалами, які розглянуті відповідно до Закону України «Про звернення громадян».

Проблемним питанням також залишається залежність працівників та їх робочого часу від внесення даних до ЄРДР. На практиці це залежить від