Список використаних джерел:

1. Зброя масового ураження: інформаційна війна – хто і як переможе? / Військова панорама. – Режим доступу: http://wartime.org.ua/
2. Гусаров В. Кремль розпочав нову інформаційну операцію проти України [Електронний ресурс] / В. Гусаров. – Режим доступу: http:// osvita.mediasapiens.ua/material/34281
3. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення // Information technology. Вісник НАДУ – 1'2015. – С. 136-141.
4. Кухаренко Р. Інформаційні війни в українському контексті // [Електронний ресурс] / Р. Кухаренко. – Режим доступу: http:// http://www.global-analityk.com/

Рудюк М.С., Бойчук В.В.

студенти,
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

СУЧАСНІ ОСОБЛИВОСТІ ВЕДЕННЯ ІНФОРМАЦІЙНИХ ВІЙН

Сучасна швидкість розповсюдження, подачі інформації, завдяки інформаційним технологіям та ефективність її сприйняття, дозволяє наслідки від «розкидання з літаків пропагандистських листівок» помножити у мільйони разів.

Тепер перекручування, підміна змісту інформації, трактування подій і фактів на певну користь стає основою страшної, руйнівної зброї, спрямованої на маніпулювання свідомістю як населення окремої країни, так і взагалі світової спільноти.

Широкомасштабне, цілеспрямоване проведення таких дій на державному рівні, сприяло появі терміну «інформаційна війна».

Досить часто під цим поняттям розуміють – всеохоплюючу, цілісну стратегію реалізації інформаційно-психологічного впливу на противника, що обумовлена зростаючою значущістю і цінністю інформації у питаннях командування, управління і політики.

Як зазначають аналітики, з масовим впровадженням інформаційних технологій і використанням інформаційної зброї метою війни стало не знищення супротивника, а цілеспрямоване керування ним. Іншими словами, інформаційні технології в наш час зробили, як видавалось, не можливе – «дистанційне управління противником» при мінімальному насильстві і кровопролитті. Тепер завдання знешкодження супротивника полягає не в знищенні живої сили, а в підриві світогляду населення, руйнуванні інфраструктури держави, зокрема збройних сил, у підриві авторитету керівництва держави тощо.

Причини проведення інформаційної війни можуть бути різні. Зокрема, територіальні зазіхання. Масована, цілеспрямована пропагандистко-підривна інформація, врешті решт повинна спровокувати місцеві референдуми, відокремити частину території від своєї країни, а далі поглинання території інформаційною країною-агресором.

Крім того, досить часто інформаційна війна може бути пов’язана із забезпеченням ринку збуту для своєї економіки. У цьому випадку інформаційна війна стає складовою частиною конкурентної боротьби.

Відхід від класичних війн, на користь інформаційних, спостерігається і у відношеннях міх країнами – світовими лідерами. Переваги отримує той, хто контролює більше інформаційного простору та застосовує ефективніші інформаційні технології.

Багато фахівців зазначають, що за своїм характером інформаційна війна займає положення між «холодною» війною, що включає, зокрема, економічне протистояння, і реальними бойовими діями за участю збройних сил. Результатом інформаційної війни є порушення функціонування елементів інфраструктури супротивника (пунктів управління, ракетних і стартових позицій, аеродромів, портів, систем зв'язку, складів і т.п.), а на відміну від «гарячої» війни із застосуванням звичайних озброєнь і (або) зброї масового ураження її цілями є не матеріальні, а «ідеальні» об'єкти (знакові системи) або їх матеріальні носії. У той же час руйнування таких об'єктів і систем може здійснюватися зі збереженням їх матеріальної основи.

Серйозною перевагою інформаційної зброї багато експертів вважають її відносну дешевизну в порівнянні з іншими видами озброєнь, оскільки в неї не треба вкладати енергію для знищення противника. Передбачається, що противник має всі необхідні засоби для власного знищення, тому ефективність застосування інформаційної зброї полягає в тому, щоб «допомогти» противнику спрямувати наявні у нього засоби проти самого себе – створити ефект саморуйнування.

Концепція сучасної інформаційної війни розроблена порівняно недавно. На думку окремих фахівців, використання інформаційної війни стало можливим в результаті «кібернетичної революції», яка спричинила масове впровадження у всі сфери життя різних інформаційних систем, заснованих на застосуванні електронних пристроїв.

Небезпека інформаційних війн, як виду інформаційного протиборства полягає ще й в тому, що не існує загальновизнаних юридичних, моральних норм та обмежень на способи і засоби ведення інформаційної війни, вони обмежені тільки міркуваннями ефективності.

Як відмічають аналітики, найважливішим принципом ведення інформаційної війни є прагнення агресора безперервно розширювати контрольований інформаційний простір, діючи в обхід сформованих моральних норм і правил, свідомо порушуючи всі соціальні обмеження і розмиваючи моральні установки.

Проведення інформаційної війни можуть забезпечувати як створені владою структури, так і окремі спільноти, групи та особи. Інформаційна війна стає безперервною і проводиться не тільки під час збройних конфліктів, але і в мирний час.

Список використаних джерел:

1. Зброя масового ураження: інформаційна війна – хто і як переможе? / Військова панорама. – Режим доступу: http://wartime.org.ua/

2. Гусаров В. Кремль розпочав нову інформаційну операцію проти України [Електронний ресурс] / В. Гусаров. – Режим доступу: http:// osvita.mediasapiens.ua/material/34281

3. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення // Information technology. Вісник НАДУ – 1'2015. – С. 136-141.

4. Кухаренко Р. Інформаційні війни в українському контексті // [Електронний ресурс] / Р. Кухаренко. – Режим доступу: http:// http://www.global-analityk.com/

Сеньків М.П., Янковська О.С.

студенти,

Навчально-науковий інститут інформаційної безпеки

Національної академії Служби безпеки України

РЕФОРМУВАННЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Необхідність нових підходів до організації діяльності органів державної влади обумовлена в першу чергу тими динамічними змінами, які відбувалися за ці роки в нашій державі, її зовнішньо- і внутрішньополітичній сфері.

Правоохоронні органи в цьому контексті мають особливе значення, оскільки від їхньої роботи залежить існування громадянських інститутів у країні, забезпечення стабільності, в тому числі й політичної. Служба безпеки України посідає окреме місце в системі правоохоронних органів.

Варто зазначити що Україна зробила низку заходів по реформуванню СБ України і державних органів в цілому. Зокрема шляхом розосередження повноважень, а саме відокремлення певних підрозділів від підпорядкування СБ України, у самостійні органи державної влади: департамент пограничної служби у окремий орган Державну прикордонну службу, департамент зовнішньої розвідки у Службу зовнішньої розвідки, департамент спеціального зв'язку та захисту інформації у Державну службу спеціального зв'язку та захисту інформації.

Але залишилось ряд проблем і вимог, які стоять перед нашою державою на порозі інтеграції в європейські та євроатлантичні структури. Відповідно для успішного просування у ці структури Україна повинна виконати ряд вимог, узгодити як своє законодавство, так і структурну організацію державних органів зі стандартами, які знайшли своє відображення в рекомендаціях ПАРЄ.

Основною проблемою, яка стосується реформування Служби безпеки України, є недоліки в структурно функціональному аспекті її організації та невідповідність європейським стандартам.

Вагомим аргументом на користь реформування Служби безпеки України є рекомендації ПАРЄ №1402 від 1999 року «Контроль над внутрішніми службами безпеки в країнах – членах Ради Європи», зокрема, відзначено, що єдиним завданням служб безпеки є захист національної безпеки. Настановою розділу А «Про організацію внутрішніх служб безпеки» дослівно рекомендовано: «…Економічні питання або боротьба з організованою