– Власники автоматизованих систем та оператори мереж передачі даних повинні створювати необхідні умови для здійснення державного контролю за забезпеченням захисту державних інформаційних ресурсів.

– Власники автоматизованих систем та оператори мереж передачі даних повинні повідомляти ДСТСЗІ СБ України про виявлені ними спроби та факти здійснення несанкціонованих дій щодо державних інформаційних ресурсів [2].

Безпека державних інформаційних ресурсів та інформаційних технологій є одними з найбільш вагомих чинників забезпечення національних інтересів держави. Державні інформаційні ресурси є першоосновою інформаційного суверенітету, за їхньою допомогою держава контролює та регулює інформаційні потоки. Це головний ресурс людської діяльності. Отже, захист державних інформаційних ресурсів повинен забезпечуватися впровадженням комплексу технічних, криптографічних, організаційних та інших заходів і засобів комплексної системи захисту інформації, спрямованих на недопущення блокування інформації, несанкціонованого ознайомлення з нею та/або її модифікації.

Список використаних джерел

1. Про Державну службу спеціального зв'язку та захист інформації України : Закон України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/3475-15

2. Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах : Закон України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/z0027-02#Text

3. Довгань О.Д. Інформаційні ресурси: національні та державні, зміст, поняття // Державне управління : інформація і право. – 2015. – № 3. – Режим доступу : //www.ippi.org.ua/sites/default/files/dovgan.pdf

---

УДК 004.056.5

ОСНОВНІ ПОНЯТТЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ПРОТИБОРСТВА

Дубиніна В. М., здобувачка вищої освіти. КБ-171
Науковий керівник**: Гур'єв В. І.,** к.т.н., доцент
Національний університет «Чернігівська політехніка»

Інформаційне протиборство - форма боротьби сторін, що представляє собою використання спеціальних (політичних, економічних, дипломатичних, військових та інших) методів, способів і засобів для впливу на інформаційне середовище протилежної сторони і захисту власної в інтересах досягнення поставлених цілей.

Основними сферами ведення інформаційного протиборства є:

−політична;

−дипломатична;

−фінансово-економічна;

−інноваційна;

−військова.

Інформаційно-психологічне протиборство – це система інформаційних і психологічних впливів на інформаційні ресурси противника, свідомість і почуття його військовослужбовців і населення, а також комплекс заходів щодо захисту власних інформаційних і психологічних ресурсів. Об'єктами інформаційно-психологічного протиборства виступають населення, армії і уряди протиборчих, дружніх і нейтральних країн. Сферою його відання можуть бути системи управління, канали зв'язку і електронні комунікації, бази і банки даних, засоби масової

інформації, свідомість і психіка людей. Будь-яка війна передбачає наявність засобів її ведення. В даному випадку необхідно вести мову про «інформаційно-психологічному зброю.

Сучасна інформатизація і комп'ютеризація різних сфер суспільного життя, збільшення енергетичних і психофізіологічних впливів на людину, ослаблення його стресостійкості, формування монотонності і своєрідної автоматичності дій, підвищення стомлюваності зробили об'єкти управління і зв'язку, енергетики і транспорту, банківську систему і військову діяльність дуже уразливими по відношенню до інформаційно-психологічного впливу. За деякими оцінками вже сьогодні ця, поки що нетрадиційна зброя, за своїми вражаючими факторами і наслідками застосування порівняна з зброєю масового ураження. А в XXI столітті інформаційно-психологічна зброя цілком ймовірно може стати найважливішим фактором стримування, прийнявши естафету від ядерних засобів озброєння.

Інформаційно-психологічне протиборство є специфічною формою сучасних війн. Воно ведеться за допомогою інформаційно-психологічної зброї і в мирний час виступає в якості найважливішого засобу соціального тиску, спрямованого на зниження морально-психологічного стану противника і дезорганізацію системи його державного і військового управління, а також стримування від прийняття рішень на використання збройної сили. У воєнний час інформаційно-психологічний протиборство направлено на те, щоб паралізувати волю військ і населення супротивника до опору, викликавши у них почуття приреченості, замішання і страху. Уже сьогодні інформаційно-психологічну зброю часто називають зброєю, яку не видно або зброєю, яка не вбиває, але перемагає.

Основними функціями інформаційно-психологічного протиборства є: дезінформація і дезорієнтація населення протиборчої країни; навіювання сумнівів у правильності політичного курсу протилежного боку; спонукання її населення до антигромадських вчинків, страйків і кампаній громадянської непокори; схилення до сумніву основних духовних цінностей і способу життя суперника; спонукання його населення до прямої зради Батьківщині або еміграції; підрив морально-психологічного стану військ противника; недопущення або мінімізація подібних дій по відношенню до власного населення і армії, їх надійний інформаційно-психологічний захист.

Здійснення цих функцій досягається рішенням на політичному і стратегічному рівнях наступних завдань: дискредитація фактів історії і політики держави - об'єкта впливу, національної самобутності його народу, діяльності в соціально-економічній, політичній, військовій та культурній сферах; підміна системи цінностей, що визначають світогляд протилежної сторони; применшення визнаних світових успіхів в науці, техніці та інших областях, перебільшення помилок, прорахунків і недоліків; створення інформаційно-психологічного клімату, що викликає почуття взаємної підозри, сумніви, побоювання і створює передумови для економічної, духовної і військової поразки, втрати волі до опору; представлення власного способу життя і системи цінностей як поведінки і світогляду майбутнього, які необхідно прийняти, щоб вижити; пропаганда форм суспільної поведінки, що роблять негативний вплив на моральний потенціал протилежної сторони; зниження ефективності всієї системи управління об'єкта впливу.

На оперативному і тактичному рівні в повсякденній діяльності ракетних військ стратегічного призначення: в процесі несення бойового чергування, підготовки і ведення бойових дій інформаційно-психологічне протиборство направлено на підрив морального духу військовослужбовців і населення супротивника, зниження за рахунок цього бойового потенціалу його збройних сил і враховує такі фактори сучасного бою: висока динаміка і напруженість бойових дій, страх, побоювання і невпевненість окремих військовослужбовців; недолік інформації, наявність чуток, дезінформації та неперевірених відомостей; наявність недосвідчених і слабо підготовлених командних кадрів і особового складу; тривале ведення бойових дій, фізична і психологічна втома особового складу; вимоги скритності і маскування дій, секретності і необхідності захисту інформації; втрати особового складу, недоліки в матеріально-побутовому забезпеченні і постачанні, збільшення захворювань і труднощі в медичному лікуванні.

У ракетних військах стратегічного призначення інформаційно-психологічне протиборство здійснюють командири, штаби, служби та органи виховної роботи. Особлива роль в цьому належить службі захисту державної таємниці ракетних військ стратегічного призначення, органам військової контррозвідки і обчислювальним відділам. Органи виховної роботи здійснюють інформаційно-виховну та психологічну роботу, беруть участь спільно з медичною службою в захисті особового складу від інформаційно-психологічного впливу противника і психологічної реабілітації військовослужбовців.

Як видно з аналізу функцій, цілей і завдань, інформаційно-психологічне протиборство по своїй суті всеохоплююче. Воно ведеться в мирний і воєнний час, на всіх рівнях і напрямках. Інформація в ньому виступає в якості зброї, ресурсу та цілі, а психологічний компонент як свого роду спосіб або засіб доставки цієї інформації. Ефективність і результативність інформаційно-психологічного протиборства залежить в кінцевому рахунку від обох цих складових. Тому в сучасних умовах надзвичайно важливо, щоб країна не залишилася осторонь від сучасних інформаційних технологій і в той же час зберегла свою унікальну самобутність, свої традиції, свій світогляд, своє емоційно-психологічну своєрідність.

Список використаних джерел

1. Панарин И. СМИ, пропаганда и информационные войны [Електронний ресурс] / И. Панарин. – Режим доступа: https://propagandahistory.ru/books/Igor-Panarin_SMI--propaganda-i-informatsionnye-voyny/28

2. Оров А.М. Основні прийоми ведення інформаційних війн в політичній сфері [Електронний ресурс] / А.М.Оров. – Режим доступа: https://ukrbukva.net/page,5,78344-Osnovnye-priemy-vedeniya-informacionnyh-voiyn-v-politicheskoiy-sfere.html

3. Сафіна С.О. Інформаційні війни сучасності [Електронний ресурс] / С.О. Сафіна. – Режим доступа: http://ukrefs.com.ua/page,2,98886-Informacionnye-voiyny-sovremennosti.html

---

УДК 004.455.1:004.056

АНАЛІЗ РОБОТИ АНТИФІШИНГОВОГО БРАУЗЕРА НА ОСНОВІ «RANDOM FOREST» І ПРАВИЛА «EXTRACTION FRAMEWORK»

Желіба Д. В., здобувач вищої освіти, гр. МКБп-201
Науковий керівник: **Ткач Ю. М.**, д.пед.н., доцент
Національний університет «Чернігівська політехніка»

Фішинг - це техніка атаки у соціальній інженерії, яка найбільш широко використовується для отримання конфіденційної інформації користувача, наприклад облікових даних для входу, інформації про кредитні та дебетові картки тощо[3]. Для захисту веб-користувачів від цих атак розробляються різні методи боротьби з фішингом, але вони не можуть захистити користувача від цих атак різними способами. У цій роботі ми пропонуємо нову техніку для ідентифікації фішингових веб-сайтів без особливих зусиль зі сторони клієнта, пропонуючи нову архітектуру браузера. У цій системі ми використовуємо правило аналізу властивостей або функцій веб-сайту, використовуючи лише URL-адресу.

Виявлення та блокування фішингової атаки надзвичайно важливо для збереження безпеки та конфіденційності користувача Інтернету. Вчені запропонували різні підходи для вирішення цієї визначної проблеми. Існує кілька алгоритмів, розроблених для виявлення фішингових сайтів. Але ними може користуватися лише спеціаліст.

Головною метою цієї роботи є аналіз технології, яка може бути легко використана кожною особою для точного виявлення нелегальних веб-сайтів у режимі реального часу. Процес виявлення здійснюється на стороні клієнта. Новизна підходу EPDB - це нещодавно