УДК 621.391

А.О. Феклістов

Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

СУЧАСНІ ПОГЛЯДИ НА ПРАВИЛА БЕЗПЕКИ ПІД ЧАС ВИКОРИСТАННЯ ВІЙСЬКОВОСЛУЖБОВЦЯМИ ТЕЛЕКОМУНІКАЦІЙНИХ СОЦІАЛЬНИХ МЕРЕЖ

Розглядаються сучасні погляди на правила безпеки під час використання військовослужбовцями телекомунікаційних соціальних мереж за досвідом збройних сил провідних країн світу.

Ключові слова: *телекомунікаційна соціальна мережа, правила безпеки поведінки військовослужбовців.*

Вступ

Постановка проблеми у загальному вигляді. Одним з напрямків розвитку сучасних засобів інформаційної боротьби (ІБ) в провідних країнах світу є активне застосування можливостей сучасних телекомунікаційних соціальних мереж, соціальних медіа (далі – соціальних мереж) для інформаційного впливу на великі аудиторії. Соціальні мережі як засіб глобальної комунікації набуває особливої значущості для військових різних країн, у тому числі для Збройних Сил (ЗС) України.

Слід відзначити, що у світі соціальних мереж уявлення про правду може бути таким ж могутнім, як і сама правда. Тому спроможність оперативно та відкрито контактувати із масовою аудиторією несе низку ризиків, пов'язаних з безпекою військовослужбовців, військових колективів та військових операцій. Таким чином, набуває актуальності задача визначення сучасних поглядів на правила безпеки під час застосування військовослужбовцями соціальних мереж.

Аналіз літератури. Комплексний огляд результатів сучасних досліджень математичних моделей соціальних мереж як моделей інформаційного впливу, управління та протиборства наведений в [1]. Відзначимо, що соціальні мережі слід розглядати як засіб ІБ, концептуальні засади, основні положення та складові якої наведені в [2 – 6].

Основним джерелом інформації щодо визначення сучасних поглядів на поведінку військовослужбовців у соціальних мережах, у тому числі в інформаційних операціях, є відкриті керівні документи, що розміщені в мережі Інтернет [7 – 13].

Мета статті є визначення сучасних поглядів на правила безпеки під час застосування військовослужбовцями соціальних мереж за досвідом збройних сил передових країн світу.

Викладення матеріалів досліджень

Соціальні мережі є одним з засобів інформаційних операцій, які представляють собою комплекс заходів щодо маніпулювання інформацією з метою досягнення й утримання переваги через впливи на інформаційні процеси в системах іншої сторони. Застосування соціальних мереж слід віднести до таких складових ІБ як комп'ютерно-телекомунікаційна та інформаційно-психологічна боротьба (рис. 1) [3, 6].

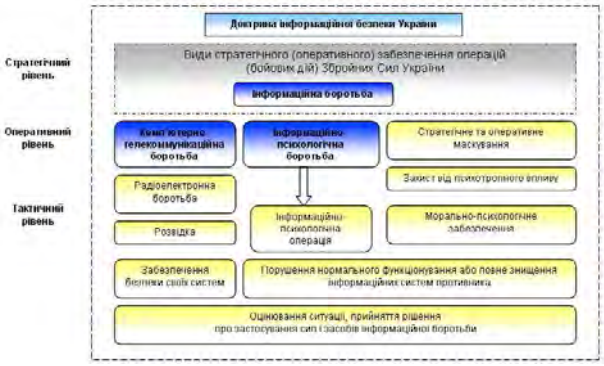

Рис. 1. Складові системи ІБ ЗС України

Потрібно відзначити, що на даний час ЗС України вже активно застосовують соціальні мережі в повсякденній діяльності. Відкриті та функціонують представництва офіційного сайту Міністерства оборони (МО) України (www.mil.gov.ua) в соціальних мережах Facebook, YouTube та ВКонтакте (рис. 2).

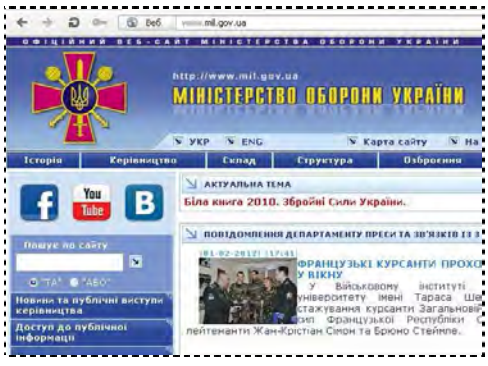

Рис. 2. Посилання на представництва в соціальних мережах Facebook, YouTube та ВКонтакте на офіційному сайті МО України (www.mil.gov.ua)

В той же час залишається актуальним задача розробки правил поведінки військовослужбовців та членів їх родин під час використання даних ресурсів

з урахуванням особливостей діяльності військових колективів.

В якості одного з можливих підходів щодо вирішення цієї задачі пропонується розглянути результати аналізу основних положень “Керівництва по соціальним медіа ЗС США” ("U.S. Army Social Media Handbook", далі – керівництва), яке було розроблено у відділі Інтернету та соціальних медіа департамента зовнішніх зв’язків Пентагону та офіційно прийнято у лютому 2010 року (рис. 3) [7].

Рис. 3. Керівництво по соціальним медіа ЗС США

Керівництво визначає основні правила поведінки військовослужбовців в соціальних мережах, таких, наприклад, як Facebook, Twitter Flickr та YouTube. Вимоги документа спрямовані на усвідомлення військовослужбовцями, членами їх родин, командирами військових колективів важливості та особливостей публічного оприлюднення інформації щодо їх діяльності.

При цьому інформація може бути ризикованою (чутливою) або безпечною. Наприклад: повідомлення “Військовослужбовець “Джон” знаходиться в місці “Кандагар” в таборі “Дельта” в Афганістані” має ризиковану (чутливу) інформацію, в той час як повідомлення “Військовослужбовець нашого підрозділу відправлений в Афганістан” може вважатися безпечною інформацією.

Вважається, що якщо військовослужбовець не готовий розповісти щось перед своїми колегами або написати на стіні свого дому, то не слід оприлюднювати цю інформацію і в соціальних мережах. Відносно поведінки командирів дане правило полягає в тому, що якщо командир не бажає сказати щось перед строєм, то він не повинен розміщувати це повідомлення і в соціальні мережі.

Контроль безпеки поведінки в соціальних мережах здійснюється по відношенню до окремого військовослужбовця, його родини та знайомих, військового колективу, командира військового колективу, військової операції та спрямований на пропаганду, створення позитивного іміджу збройних сил у населення та збереження конфіденційної інформації та військової таємниці.

Аналіз керівництва показує, що основні правила безпеки поведінки військовослужбовців умовно можливо поділити на 2 групи:

1) правила безпеки, які рекомендується виконувати військовослужбовцями, командирами та в цілому військовими колективами;

2) правила безпеки, які забороняють визначені дії військовослужбовцям, командирам та в цілому військовим колективам.

Розглянемо стислий зміст даних правил.

1. Правила безпеки поведінки, які рекомендується виконувати військовослужбовцями, командирами та в цілому військовими колективами (“ДОЗВОЛЕНО”).

1.1. Працювати в соціальних мережах, якщо це не порушує політику безпеки військового колективу та базові принципи військового правопорядку.

1.2. Ділитися своїм досвідом та знаннями із майбутніми військовослужбовцями та розповідати про життя в армії.

1.3. Дотримувати субординацію по відношенню до командира (начальника).

1.4. Знати політику безпеки військового колективу: що можливо та не можливо робити під час використання соціальних мереж.

1.5. Вимикати мобільні телефони, що мають функцію GPS-приймача, під час безпосередньої участі у військовій операції.

1.6. Встановити опції безпеки щодо перегляду даних у режимі “тільки для друзів”.

1.7. Перевіряти фото-, аудіо- та відеоматеріали перед їх розміщенням та переконатись, що вони не несуть ризикованої (чутливої) інформації, що може бути небезпечною після розповсюдження.

1.8. Переконатися, що родина військовослужбовця та його знайомі усвідомили політику щодо безпеки операції.

1.9. Координувати свою діяльність з офіцером по зв’язкам із засобами масової інформації у разі отримання запросів від недержавних блогів щодо оплати розміщення матеріалів у мережі.

1.10. Визначити членів військового колективу, які будуть відповідальні за розміщення матеріалів на офіційних сторінках в соціальній мережі та переконатися, що ці особи пройшли всі тренінги (інструктажі) по безпеці операцій.

1.11. Переконатися, що зміст матеріалів для розміщення, затверджений командиром або уповноваженим органом відповідно до діючих вимог щодо безпеки.

1.12. Здійснювати моніторинг перебування у соціальних мережах та переконатися, що зовнішні користувачі не розміщують ризикованої (чутливої) інформації на вашому офіціальному представництві (наприклад, дошці об’яв на Facebook) та не порушують безпеку операцій.

1.13. Розробляти методичні матеріали та проводити регулярні тренінги (інструктажі) по безпеці операцій в соціальних мережах з військовослужбовцями та членами їх родин.

1.14. Буди пильними та ніколи не бути самозадоволеними у питаннях, що стосуються безпеки операцій.

2. Правила безпеки, які забороняють визначені дії військовослужбовцям, командирам та в цілому

військовим колективам ("ЗАБОРОНЕНО").

2.1. Розповсюджувати інформацію, яка має ознаки конфіденційності та (або) військової таємниці.

2.2. Розміщувати інформацію про заплановані та поточні військові операції.

2.3. Критикувати та сваритися на керівництво, негативно висловлюватися про своїх командирів (начальників).

2.4. Публікувати відверті висловлення близьких та рідних.

2.5. Додавати в "друзі" свого командира (начальника).

2.6. Коментувати, розміщувати або робити посилання на матеріали, що порушують політику безпеки військового колективу або правила поведінки військовослужбовця.

2.7. Використовувати програми соціальних мереж, які містять інформацію про місцезнаходження, переміщення, тренування або чергування в місцях дислокації, коли інформація про точні географічні координати впливає на проведення військової операції.

2.8. Розміщувати фотографії, що містять дані із географічним положенням, на сайтах, що мають сервіс публічного оприлюднення фотографій, наприклад, таких як Flickr та Picasa.

2.9. Розкривати ризиковану (чутливу) інформацію про себе (наприклад, розклади та місця проведення події).

2.10. Включати матеріали, що містять дані про авторські права та торгівельні марки, на свої сторінки в соціальних мережах.

2.11. Використовувати службове становище та (або) повноваження для просування себе в мережі для досягнення особистих або фінансових переваг.

2.12. Зупинятся працювати щодо захисту безпеки військових операцій.

В цілому, наведені правила безпеки поведінки під час використання військовослужбовцями соціальних мереж потребують подальшої адаптації відповідно до чинних вимог законодавства України та керівних документів ЗС України.

Висновки

В статті визначені основні правила безпеки під час використання військовослужбовцями соціальних мереж за досвідом збройних сил передових країн світу. Результати досліджень можуть бути використані під час розробки методичних рекомендацій та керівних документів в інтересах ЗС України та використовуватися під час організації та проведення заходів міжнародного співробітництва (наприклад, спільних (багатонаціональних) навчань із оприлюдненням їх результатів в електронних засобах масової інформації, у тому числі соціальних мережах).

Список літератури

1. Губанов Д.А. Социальные сети: модели информационного влияния, управления и противоборства / Д.А. Губанов, Д.А.Новиков, А.Г. Чхартишвили; под ред. Д.А. Новикова. – М.: Издательство физ.-мат. лит-уры. – 2010. – 228 с.

2. Рось А.О. Концептуальні засади моделювання інформаційної боротьби / А.О. Рось, І.В. Замаруєва, В.Л. Петров // Наука і оборона. – 2000. – № 2. – С. 46-53.

3. Толубко В.Б. Складові інформаційної боротьби / В.Б. Толубко, А.О. Рось // Наука і оборона. – № 2. – 2002. – С. 23-28.

4. Жук С.Я. Тенденції та перспективи розвитку інформаційної боротьби й інформаційної зброї / С.Я. Жук, В.О. Чмельов, Т.М. Дзюба // Наука і оборона. – № 2. – 2006. – С. 35-41.

5. Пєвцов Г.В. Забезпечення інформаційної безпеки регіону: проблема, концепція та шляхи її реалізації / Г.В. Пєвцов, О.М. Черкасов. – Х: Видавництво ХарРІ НАДУ "Магістр". – 2008. – 138 с.

6. Феклістов А.О. Сучасні погляди на місце інформаційних операцій в системах інформаційної боротьби / А.О. Феклістов // Системи озброєння та військова техніка. – Х.: ХУПС, 2010. – Вип. 2(22). – С. 25-27.

7. U.S. Army Social Media Handbook. January. – 2011. – 39 p.

8. Joint Publication 3-13.2 Psychological Operations. 07 January 2010. – 125 p.

9. Information Operations. Air Force Doctrine Document 2-5. 11 January 2005. – 54 p.

10. Joint Publication 3-13 Information Operations. 13 February 2006. – 136 p.

11. UK Joint Warfare Publication 3-80. Information Operations. – 2002. – 55 p.

12. UK Joint Doctrine Publication 3-90. Civil-Military Co-operation (CIMIC). – 2006. – 47 p.

13. Neil Chuka A Comparison of the Information Operations doctrine of Canada, the US, the UK, and NATO // Canadian Army Journal. – Vol. 12.2 Summer 2009. – P. 91-99.

Надійшла до редколегії 3.11.2011

Рецензент: д-р техн. наук, проф. А.М. Сотніков, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

СОВРЕМЕННЫЕ ВЗГЛЯДЫ НА ОПРЕДЕЛЕНИЕ ПРАВИЛ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ВОЕННОСЛУЖАЩИМИ ТЕЛЕКОММУНИКАЦИОННЫХ СОЦИАЛЬНИХ СЕТЕЙ

А.А. Феклистов

Рассматриваются современные взгляды на определение правил безопасности при использовании военнослужащими телекоммуникационных социальных сетей на основе опыта вооруженных сил передовых государств.

Ключевые слова: *телекоммуникационная социальная сеть, правила безопасности поведения военнослужащих.*

THE MODERN VIEWS ON SECURITY GUIDELINES IN SOCIAL NETWORKS FOR MILITARY PERSONNEL

A.O. Feklistov

The article considers modern views on security guidelines in social networks for military personnel based on the armed forces experience of progressive countries.

Keywords: *social network, security guidelines for military personnel.*