Фактори підвищення вразливості ІО ВНЗ до агресії та шляхи їх мінімізації

Пелещишин Андрій
Кафедра СКІД
НУ "Львівська політехніка"
Львів, Україна
apele@ridne.net

Корж Роман
Кафедра СКІД
НУ "Львівська політехніка"
Львів, Україна
korzh@lp.edu.ua

The paper presents ways of minimizing vulnerabilities of the information image of university to a purposeful aggression

Ключові слова: вищий навчальний заклад (ВНЗ), інформаційний образ (ІО), мережева агресія.

Суттєвими факторами, що впливають на вразливість ІО ВНЗ до агресії є:

- бюрократична структура ВНЗ і слабкість мобілізаційного ресурсу;
- прогалини в ІО ВНЗ;
- низька комунікативна компетентність працівників підрозділів.

Розглянемо ці фактори та зменшення їхнього впливу шляхом використання запропонованих у роботі підходів.

Дж. Аркілла і Д. Ронфельд у політологічному аспекті здійснили моделювання протистояння класичних ієрархічних організаційних структур та соціальних груп у формі мереж. Вони дійшли таких висновків:

- ієрархіям важко боротися з мережами;
- треба стати мережею, щоби змагатися з мережею;
- той, хто опановує мережеву форму першим, отримує значну перевагу.

Звичайно, проектування таких висновків на «мікрорівень» протистоянь у соціальних середовищах Інтернету потребує критичного ставлення, проте загалом вони дають важливі орієнтири щодо організаційного забезпечення мережевої агресії.

Так, чітко відображено необхідність якомога швидшого виявлення агресії, поки ідея агресії залишається ідеєю окремих людей, а не у певний спосіб сформованої спільноти, та високої швидкості реагування на неї. Для цього доцільно використовувати розроблені вище підходи до визначення важливості та інтенсивності критичних дискусій.

Другим, і з певних причин, складнішим, аспектом є організація «соціальної мережі захисників» на основі доволі традиційної ієрархічної структури сучасного українського ВНЗ. На практиці інколи бюрократичні перепони, неготовність до певного зменшення формальної дистанції між управлінцями і виконавцями, страх і небажання прийняття публічних управлінських рішень та просто коментування своїх дій призводить до неможливості створення таких соціальних груп. Їхня імітація завжди виглядає програшно на тлі добре вмотивованого і мережево організованого агресора і стає додатковим негативним подразником для соціуму та об'єктом критики.

Для усунення указаних вище внутрішніх проблем доцільно передбачати діяльність працівників з формування та захисту ІО ВНЗ як одне з обов'язкових виробничих завдань, з відповідною системою мотивацій.

Водночас вкрай важливим є формування повноцінного реєстру підрозділів, який включає повний перелік асоційованих з ВНЗ структур (тобто таких, для яких $DepAs(Dep_i) \le 0,4$ [1] у тому числі усіх дружньо налаштованих організацій які діють як віртуальні спільноти. Такі організації фактично підлягають обліку двічі – як асоційований підрозділ і як віртуальна спільнота. Критично важливим є включення в число

асоційованих підрозділів студентських спільнот, які лояльні до ВНЗ. Такий підхід забезпечує формування згаданої вище «соціальної мережі захисників» як мобілізаційного ресурсу. Використання його здійснюється згідно зі сформованим в умовах агресії розподілом зон відповідальності.

Другим фактором ризику для ВНЗ є наявність прогалин у його інформаційному образі. Відсутність представництва ВНЗ в окремих значимих спільнотах сповільнює виявлення агресивних матеріалів аж до моменту набуття ними значного суспільного резонансу. Реакція ВНЗ безпосередньо у такому разі є вже неефективною, адже входження буде відбуватися у спільноту з сформованим негативним ставленням. Основним індикатором прогалини за тематикою є низьке значення показника $CoverTh(Th_i) < 0.1$. Для таких тематик існують авторитетні спільноти, у яких не беруть участі представники ВНЗ. Відповідно входження в такі спільноти є важливим організаційним випереджувальним заходом для захисту ІО ВНЗ.

Ще одним фактором ризику для ВНЗ традиційно є недостатня компетентність працівників у питаннях соціомережевих комунікацій. Як наслідок, залучення працівників до побудови ІО ВНЗ часто породжує непорозуміння в спільнотах (невдала комунікація, стилістично неправильні повідомлення, нетипова поведінка), що породжує додаткову вразливість ВНЗ агресора. Агресор може задіяти в своїх інтересах негативні настрої в межах таких спільнот.

Головним індикатором такої некомпетентності є комплекс соціально-комунікативних характеристик [2]. Зведемо ці характеристики в комплексний показник мережевої компентності:

$$DepComp(Dep_i) = \frac{\sum_{x \in DC} DCx(Dep_i) DAU^{(DCx)}}{\sum_{x \in DC} DAU^{(DCx)}}$$

де $DC = \{CU, CC, CF, CD, CW, CM, PU, PW\}$ – множина позначень соціально-комунікативних характеристик підрозділу, $DAU^{(DCx)}$ - множина вагових коефіцієнтів для кожної з характеристик, визначається експертами (інформаційним підрозділом ВНЗ). Прийнятним варіантом визначення $DAU^{(DCx)}$ є присвоєння їм однакової величини.

Генератори, які є зонами відповідальності підрозділів, для яких $DepComp(Dep_i) < 0,5$, потребують додаткового контролю з боку інформаційного підрозділа на предмет цілеспрямованої агресії, а сам підрозділ – додаткового навчання прийомам ефективної діяльності в ССІ.

Крім цього показника для виявлення ризиків слід також використовувати показники комунікативної складності освітньої спільноти та комунікативної цінності, а саме результативність $Result(Gen_i, T_0, T_1)$ та продуктивність $Prod(Gen_i, T_0, T_1)$ інформаційної діяльності підрозділа [3-4].

Література

[1] А. Пелещишин, Р. Корж, О. Трач Визначення комплексу показників віртуальної спільноти для вищих навчальних закладів, Східно–Європейський журнал передових технологій, №2/2, С. 16-23, 2014.

[2] R. Korzh, A. Peleshchyshyn, Y. Syerov, and S. Fedushko, "University's Information Image as a Result of University Web Communities' Activities," Advances in Intelligent Systems and Computing, Csit 2016, Proceedings Paper vol. 512, pp. 115-127, 2017.

[3] R.Korzh , A. Peleshchyshyn , S. Fedushko , Yu. Syerov “Protection of University Information Image from Focused Aggressive Actions”, Advances in Intelligent Systems and Computing: Recent Advances in Systems, Control and Information Technology, Proceedings of the International Conference SCIT 2016, May 20-21, 2016, Warsaw, Poland. Springer, 2017, Volume 543, pp 104-110.

[4] O. Trach, V. Vus, O. Tymovchak-Maksymets, “Typical algorithm of stage completion when creating a virtual community of a HEI”, Proceedings of the XIIIth International Conference “Modern Problems of Radio Engineering, Telecommunications and Computer Science” (TCSET'2016), 2016, pp. 849-851.