УДК 37:004:316.772.5

Горбенко А. А., старш. викладач
Київський професійно-педагогічний коледж імені Антона Макаренка

КІБЕРБЕЗПЕКА ОСВІТНЬОГО СЕРЕДОВИЩА В УМОВАХ КАРАНТИНУ

Під час карантинів у закладів освіти надзвичайно гостро стоїть питання організації дистанційного навчання. Але, одночас, це серйозний виклик організації безпечного освітнього онлайн середовища.

Ураховуючи, це перед освітою постають нові завдання, пов'язані не тільки з формуванням у здобувача освіти необхідних знань і соціального самоусвідомлення, але і його розуміння власної інтегрованості у світову спільноту вже на ранніх етапах навчання, практично необмежених можливостей впливу кіберпростору на свою особистість, відпові-дальності перед собою та суспільством за власну поведінку та її (можливі) глобальні наслідки, знання та розуміння небезпек кіберпростору.

Законом України «Про основні засади забезпечення кібербезпеки України» визначаються основні поняття зазначеної проблемної галузі [1]. Зокрема, Стаття 1 Закону визначає кібербезпеку як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі».

Водночас Стаття 2 Закону пояснює: «1. Цей Закон не поширюється на: 1) відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах; ... 3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів;…».

Інакше кажучи, чинний Закон не передбачає будь-які дії з безпеки стосовно людини, яка не входить до критичної інформаційної інфраструктури держави, а людський складник інтелектуального капіталу (який набуває зростаючого значення в усьому світі) не входить до критичного ресурсу України. І це в той час, коли в усьому світі основна боротьба йде за людські та інтелектуальні ресурси, тобто за тих, хто вже завтра буде забезпечувати конкурентоспроможність країни.

Мета статті – оцінка проблем та завдань кібербезпеки учасників освітнього процесу та можливих загроз у цифровому освітньому середовищі.

Як визначається Законом «Про основні засади забезпечення кібербезпеки України» [1], «кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних».

Звертається увага на те, що кіберпростір визначається різноманіттям з'єднань, що одночасно переводить його в категорію зони ризику. Усі зростаючі розміри, охоплення і функції збільшують можливості як законослухняних громадян, так і ворожих гравців. Супернику необхід-но лише атакувати слабку ланку мережі, щоб завоювати новий плацдарм і отримати переваги [2].

Основним способом захисту від методів соціальної інженерії є навчання учасників освітнього процесу. Вони мають бути попереджені про небезпеку розкриття персональної інформації та конфіденційної інформації, а також про способи запобігання витоку даних.

Крім того, у кожного учасника, в залежності від місця та функції в освітньому процесі, повинні бути інструкції про те, як і на які теми мож-на спілкуватися із сторонніми особами стосовно персональних особливостей, яку інформацію можна надавати для служби технічної підтрим-ки, як і яку інформацію може повідомити учасник навчального процесу стороннім особам і працівникам мас-медіа. Крім того, можна виділити основні правила протидії соціальній інженерії.

Призначені для користувача облікові дані є власністю закладу освіти. Всім співробітникам в день прийому на роботу має бути роз'яснено те, що ті логіни і паролі, які їм видали (якщо це має місце), не мож-на використовувати в інших цілях (на webсайтах, для особистої пошти тощо), передавати третім особам або іншим співробітникам, які не мають на це права.

Персональні дані з результатів тестування та виконання психологіч-них і медичних обстежень можуть бути застосовані користувачами соціальної інженерії, тому потребують обережного використання.

Необхідно проводити вступні та регулярні навчання співробітників і учнів, спрямовані на підвищення знань з інформаційної безпеки.

Обов'язковою є наявність регламентів з безпеки, а також інструкцій, до яких користувач повинен завжди мати доступ.

На комп'ютерах користувачів завжди має бути актуальне антивірус-не програмне забезпечення, а також слід встановити брандмауер.

Необхідно бути пильним щодо джерела, яке запитує конфіденційні дані. Ніколи не слід відкривати вміст додатків або переходити за посиланням, не вивчивши всіх деталей. Часто адреса відправника містить помилки в назвах, а посилання мають неправдоподібний вигляд.

Варто також критично ставитися до отриманих повідомлень. Останнім часом в Україні запроваджуються спеціальні навчальні програми і курси для учнів та вчителів, які займаються питаннями безпечного Інтернету [3].

Проте нові кіберзагрози потребують і нових підходів до захисту користувачів, особливо учасників освітнього процесу. Для викладачів зак-ладів освіти особливого значення набуває не тільки знання критеріїв надійності джерел та достовірності даних і засобів їх оцінювання, а й використання ефективних педагогічних технологій формування відповідних умінь учнів і студентів, а також засоби оцінювання рівня розвитку таких умінь.

Список використаних джерел

1. Закон № 2163-VIII «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради), № 45, с. 403, 2017.

2. Z. Yan, T. Robertson, R. Yan, Sung Yong Park, S. Bordoff, Q. Chen, and E. Sprissler, «Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? », Computers in Human Behavior, ISSN: 0747-5632, Vol: 84, Page: 375-382, 2018.

3. Дементієвська Н. П. «Професійний розвиток вчителів щодо компетентностей, пов’язаних з безпечним і відповідальним використанням електронних соціальних мереж». [Електронний ресурс]. Звітна наукова конференція Інституту інформаційних технологій і засобів навчання НАПН України : матеріали наук. конф., (Київ, 28 бер. 2017 р.). НАПН України, Ін-т інформаційних технологій і засобів навч. К.: ІІТЗН НАПН України, 26-31, [Електронний ресурс]. Режим доступу: http://lib.iitta.gov.ua/id/eprint/708603.