УДК 378:004

СУЧАСНИЙ ОСВІТНІЙ ПРОЦЕС І КІБЕРБЕЗПЕКА

Костікова М. В., доцент, канд. техн. наук, доцент кафедри інформатики та прикладної математики, Харківський національний автомобільно-дорожній університет

Анотація. В матеріалі розглянута проблематика кібербезпеки у навчальному середовищі і надані пропозиції щодо її розв'язання. Акцентовано, що найбільш значущими серед кіберзагроз для учасників навчально-виховного процесу є методи соціальної інженерії, знання яких та протидія яким можуть бути найбільш ефективними для забезпечення кібербезпеки.

Ключові слова: кібербезпека, навчальне середовище, кіберзагроза, суб'єкт освітнього процесу, соціальна інженерія.

Розвиток цифрового інформаційного суспільства все більше набуває динамічності. Швидкість розповсюдження інформації потребує постійного, пильного контролю, адже в сучасному світі з'явилось безліч нових загроз, таких як дезінформація, маніпуляція, пропаганда, фейкові новини, вірусні атаки що заполонили цифрову площину. Отже, інфосфера стає дедалі більш вразливою щодо стороннього кібернетичного впливу [1].

На сучасному етапі новітніх інформаційних технологій актуального значення набуває кібербезпека, що містить у собі міжвідомчий характер у глобалізованому світі. Адже кібербезпека є правозахисним проявом сучасного віртуального світу на тлі інноваційного розвитку інформаційних технологій в системі законного капіталу [2]. При розбудові національної системи кібербезпеки Україна враховує як кращий міжнародний досвід, так і особливості свого соціально-економічного, політичного, культурного та історичного розвитку.

На теперішній час гостро стоїть питання щодо захисту цифрової інформації, комп'ютерних мереж, операційних систем, серверів, баз даних, приватних і державних установ від несанкціонованого втручання сторонніх осіб. Тому цілком природною є необхідність створення надійної системи кібернетичної безпеки та її постійного удосконалення. Питання кібербезпеки гостро стоять з того часу, як комп'ютерна техніка перестала бути лише прерогативою великих наукових центрів. З появою та поширенням локальних і глобальних мереж змінилося розуміння кібербезпеки, відповідних трендів, проблем і задач.

Навчальне середовище є одним з наріжних каменів освіти. Внаслідок переходу до дистанційного та гібридного навчання, освітній сектор України стикнувся з великим спектром кіберзагроз. Усвідомлення цих загроз може допомогти вишам та їхнім співробітникам захистити себе та своїх студентів від цих уразливостей. В установах вищої освіти циркулюють великі обсяги персональних даних і фінансової інформації про студентів, викладачів, співробітників, а також інформації про наукові дослідження. Це робить їх привабливою ціллю для кіберзлочинців. Людський фактор, тобто помилки співробітників або студентів через необізнаність або зневажання елементарними правилами кібергігієни лежать в основі більшості успішно реалізованих кібератак.

Ознаки кіберзагроз в галузі освіти можна розділили за дев'ятьма критеріями: загрози через людський фактор, крадіжка персональних даних, загрози на пристрої IoT, програми-вимагачі або зловмисне програмне забезпечення, фінансова вигода, шпигунство, фішинг, DDoS-атаки, загрози на CMS. Знання основних загроз освітніх мереж і систем, розуміння поширених способів злому і витоків конфіденційних даних

студентів, викладачів та інших співробітників дозволить вибирати й застосовувати навчальним закладам найбільш ефективні інструменти і стратегії на всіх рівнях кіберзахисту. Кібербезпека є спільною відповідальністю для всіх, а її успіх залежить від обізнаності про мотиви та методи зловмисників, дотримання належної кібергігієни кожним та контролем за дотриманням вимог.

Крім того, у кожного суб'єкта освітнього процесу, в залежності від функції та місця в освітньому процесі, повинні бути інструкції про те, на які теми і як можна спілкуватися із сторонніми особами стосовно персональних особливостей, яку інформацію можна надавати для служби технічної підтримки, яку і як інформацію може повідомити учасник навчального процесу стороннім особам і працівникам мас-медіа. Крім того, необхідно дотримуватися наступних дев'яти типових правил протидії імовірним загрозам [3].

1. Призначені для користувача облікові дані є власністю навчального закладу. 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 можна використовувати в інших цілях (на web-сайтах, для особистої пошти тощо), повідомляти іншим співробітникам, які не мають на це права або третім особам. Наприклад, співробітник на час відпустки може передати власні авторизовані дані своєму колезі для того, щоб той зміг виконати деяку роботу або подивитися певні дані в момент його відсутності. Персональні дані з результатів тестування та виконання психологічних і медичних обстежень можуть бути застосовані користувачами соціальної інженерії (метод одержання необхідного доступу до інформації, заснований на особливостях психології людей), тому потребують обережного використання.

2. Необхідно проводити вступні та регулярні навчання учнів і співробітників, спрямовані на підвищення знань з інформаційної безпеки. Проведення таких інструктажів дозволить суб'єктам освітнього процесу мати актуальні дані про існуючі методи соціальної інженерії, а також не забувати основні правила з інформаційної безпеки.

3. Обов'язковою є наявність регламентів з безпеки, а також інструкцій, до яких користувач повинен завжди мати доступ. В інструкціях повинні бути описані дії суб'єкта освітнього процесу при виникненні тієї чи іншої ситуації. Наприклад, у регламенті можна прописати, що необхідно робити і куди звертатися при спробі третьої особи запросити конфіденційну інформацію або облікові дані.

4. На комп'ютерах користувачів завжди має бути актуальне антивірусне програмне забезпечення, а також слід встановити брандмауер.

5. У корпоративної мережі навчального закладу або об'єднання закладів необхідно використовувати системи виявлення та запобігання атак. Необхідно також використовувати системи запобігання витоку конфіденційної інформації. Усе це дозволить знизити ризик виникнення фішингових атак.

6. Необхідно щонайбільше обмежити права користувача в системі. Наприклад, можна обмежити доступ до web-сайтів і заборонити використання знімних носіїв, які можуть бути використані за межами навчального закладу.

7. Необхідно бути пильним щодо джерела, яке запитує конфіденційні дані. Представники Міністерства освіти і науки навряд чи будуть телефонувати до школи, щоб дізнатися дані щодо конкретного учня або студента. Якщо людину просять ввести особисті дані – краще окремо зайти на сайт компанії, наприклад, банку. Ще краще – для уточнення інформації зателефонувати на офіційний номер установи.

8. 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.

9. Критично відноситися до отриманих повідомлень: наскільки правдоподібною

може бути інформація про те, що принц з африканської країни або американський мільярдер міг залишити вам спадщину?

Рекомендується повідомляти про такі небезпеки інших членів сімей, насамперед, літніх людей, які не мають досвіду користування електронними засобами та не обізнані з питань соціальної інженерії.

Проте нові кіберзагрози потребують і нових підходів до захисту користувачів, особливо учасників освітнього процесу.

Для викладачів закладів 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. Нам потрібно знати, як захистити себе і своїх учнів від кібератак. Можливі ситуації, коли наші учні опиняться кіберзлочинцями, проте можливі й інші – в яких вони вже будуть жертвами. Молодь швидко освоює цифрові програми, деякі навіть вміють їх зламувати, однак життєвого досвіду у них все ж замало. Вони можуть бути недостатньо проникливі і мудрі, щоб розпізнати всі небезпеки онлайн-світу, з якими їм доведеться зіткнутися. Тому викладачі зобов'язані захистити своїх учнів і розповісти їм про кібербезпеку, щоб вони могли захиститися в Інтернеті.

Кібербезпека – захищеність життєво важливих інтересів громадянина і людини, суспільства та держави під час використання кіберпростору. Питання кібербезпеки у сучасному освітньому процесі є актуальним, широко обговорюється та знайшло відображення у багатьох публікаціях. Так у джерелах [4, 5] ця проблематика знайшла своє глибоке освітлення.

Інформатизація та цифровизація в наш час проникають у всі сфери діяльності держави, суспільства, бізнесу, науки, освіти та окремої людини. Тому пошук шляхів забезпечення кібербезпеки (зокрема, розробка відповідних технологій) стали важливим аспектом діяльності ІТ-сфери.

Таким чином, проблеми кібербезпеки не зводяться лише до технічних аспектів захисту інформаційних ресурсів, вони у повному обсязі мають включати такі види захисту: правові, інформаційні, технічні, організаційні та психологічні. Загрози учасникам навчально-виховного процесу з боку кіберпростору можуть бути як пасивні та активні, тому необхідно розробляти адекватні засоби захисту та життєстійкості системи «суб'єкт освітнього процесу – засоби навчання – середовище».

Список літератури

1. Доценко С. О., Лебедєва В. В. Роль і місце кібербезпеки в освітній діяльності. *Дистанційна освіта: Реалії та перспективи*: матеріали І всеукраїнської науково-практичної конференції (м. Харків, 12 грудня 2018). Харків, 2018. С. 12–15.

2. Лісовська Ю. П. Кібербезпека: ризики та заходи: навч. посібник. Київ: Видавничий дім «Кондор», 2019. 272 с.

3. Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. *Інформаційні технології і засоби навчання.* 2019. Том 70, № 2. С. 313–331. URL: https://www.researchgate.net/publication/332716122_KIBERBEZPEKA_V_CIFROVOMU_NAVCALNOMU_SEREDOVISI (дата звернення 19.09.2022).

4. Закон України № 2163-VIII «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, с. 403). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 20.09.2022).

5. Кібербезпека. Аспект 1: соціальні мережі. *Міністерство оборони України: офіційний веб сайт.* URL: https://www.mil.gov.ua/ukbs/shhodenni-kiberzagrozi/kiberbezpeka-aspekt-1-soczialni-merezhi.html (дата звернення 20.09.2022).