Роль кібербезпеки у процесі навчання інформатики учнів закладів загальної середньої освіти

Любчик О.О.
студент
ВДПУ імені Михайла Коцюбинського
Косовець О.П.
кандидат педагогічних наук, старший викладач
кафедри математики та інформатики
ВДПУ імені Михайла Коцюбинського
kosovets.op@vspu.edu.ua

У широкому розумінні поняття «кібербезпека» – це сукупність методів захисту систем підключених до мережі інтернет, а саме програмного та апаратного забезпечення, та даних від кіберзагроз. Вона використовується для захисту урядових інформаційних мереж, центрів обробки а зберігання іфнормації, персональних комп'ютерів та багатьох інших компю'теризованих систем від несанкціонованого доступу.

Кібербезпека в освітньому процесі – це також сукупність методів захисту, зокрема, освітніх систем підключених до мережі інтернет, програмного та апаратного забезпечення для реалізації навчального процесу, персональних даних учнів, вчителів і корпоративних даних про школу від кіберзагроз.

До кібератак необхідно готуватись заздалегідь, щоб забезпечити гарний захист від атак спрямованих на видалення, доступ, заміну, викрадення чи знищення навчального матеріалу та персональної інформації про учасників навчального процесу. Також існує загроза, що при викраденні важливих відомостей, зловмисники можуть вимагати кошти або певні послуги для того, щоб повернути інформацію власнику та впливати на репутацію учня, вчителя, школи. Кібербезпека також грає важливу роль в запобіганні атак, які мають на меті пошкодити або вплинути на процес навчання інформатики при дистанційній та змішаній формі організації, змінити налаштування роботи пристроїв тощо.

Кібербезпека особливо важлива у час розвитку цифрових технологій, будь-які організації, як урядові так і приватні, намагаються покращити результати своєї роботи шляхом зменшення часу на опрацювання даних. Тому більшість організацій активно впроваджують цифрові технологіїї в робочий процес, що призводить до збору великої бази персональних даних про користувачів відповідних систем. Зібрані персональні дані підлягають опрацюванню та використовується за необхідності у вигляді нав'язливої реклами у соціальних мережах, умесенджерах, у публічних групах та ін.

Зібрана персональна інформація, наприклад про учнів та вчителів, становить інтерес для різних зловмисників. Це відомості про стан здоров'я, про банківські рахунки, персональна та корпоративна інформація, все це приваблює хакерів та шахраїв.

Кібербезпеку можна поділити на декілька основних розділів: 1) безпека додатків; 2) безпека інформації або даних; 3) безпека мережі; 4) аварійне відновлення/планування безперевної роботи; 5) оперативна безпека; 6) хмарна безпека; 7) безпека критичної інфраструктури; 8) фізична безпека; 9) навчання правил інформаційної та кібербезпеки усіх учасників освітнього процесу.

Підтримувати кібербезпеку в умовах постійного виникнення нових кіберзагроз є проблемою усіх закладів освіти. Традиційні підходи при яких захист комп'ютерних систем націлювався лише на найвідоміші загрози, і не звертати увагу на менш відомі не надавали хорошого захисту. Щоб постійно бути захищеним в цифровому просторі потрібно використовувати систему моніторингу та оцінки ризиків в реальному часі.

Кіберзагрози мають багато різних форм, але для захисту в мережі необхідно постійно слідкувати за сучасними тенденціями та технологіями, а також постійно проводити розвідку для виявлення все нових типів загроз, які поділяються на:

- шкідливе програмне забезпечення – це будь-яка програма чи файл яка може бути використана для завдання шкоди користувачу комп'ютера. До них відносяться віруси, хробаки, шпигунські програми та трояни;
- програми-вимагачі – цей тип загрози зашифровує інформацію на пристрої користувача, і потім пропонує відновити доступ, до цієї інформації після оплати;
- соціальна інженерія – це атака яка заснована на взаємодії між шахраями та учнями / вчителями, щоб заволодіти конфіденційною іфнормацією, змінити засоби її захисту чи змусити користувачів порушити правила збереження цієї інфомрації в безпеці;
- фішинг – різновид соціальної інженерії підчас якої учням надсилаютсья шахрайські електронні листи, що схожі на повідомлення від авторитетних організацій чи відомих джерел про різноманітні виграші, подарунки та призи. Зазвичай їх використовують для отримання данних входу або інформації про кредитну карту;
- атака «людина посередині» – це атака, під час якої зловмисник прослуховує і перехоплює повідомлення між двома співрозмовниками.

Інші поширені атаки включають бот-мережі, атаки із завантаженням, комплекти експлойтів, зловживання, атаки вішінгу, атаки заповнення

облікових даних, атаки міжсайтових сценаріїв (XSS), атаки ін'єкції SQL, компроміс ділової електронної пошти (BEC) та експлойти нульового дня.

Скорочення кількості кібератак найближчим часом не очікується. Також збільшується кількість можливих точок входу для атак, наприклад, з появою Інтернету речей та різноманітних гаджетів, освітніх платформ, навчальних веб-сервісів, розвиткок електронного навчання збільшує потребу в захисті мереж і пристроїв.

Найбільш проблемним елементом кібербезпеки є постійний розвиток загроз кібербезпеці. По мірі впровадження сучасних освітніх цифрових технологій постійно відбувається знаходження нових шляхів для кібератаки. Доволі складно не відставати від цих тенденцій та постійно оновлювати способи захисту інформації, а саме антивірусні програми або апаратні засоби захисту інформації.

До того ж з часом кількість конфіденційної інформації про учнів лише збільшується, дані про акаунти користувачів та дані для входу, і чим більше їх накопичується, тим більше вона приваблює зловмисників. Або наприклад організації, що зберігають переважну кількість інформації у хмарі можуть стати жертвами програм вимагачів. Тому, саме від поведінки в мережі інотернет учасників освітнього процесу залежить запобігання таких ситуацій.

Список використаних джерел

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

2. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. К.: ДУТ, 2015. 288 с.

3. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони: підручник. Одеса.: ОНАЗ ім. О.С. Попова, 2019. 320 с.

4. Гур'єв В.І., Мехед Д.Б., Ткач Ю.М., Фірсова І.В. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека». Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с. : іл.