ДЕЯКІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗАКЛАДУ ОСВІТИ

Олеся Олексюк

Тернопільський обласний комунальний інститут післядипломної педагогічної освіти

Питання безпеки інформаційних систем закладів освіти у період широкого впровадження новітніх інформаційних технологій в освітній процес є одними з найактуальніших та мало досліджених питань. Вивчення проблеми негативного впливу інформаційних технологій та засобів масової комунікації на формування, розвиток, та здоров'я школярів нині потребує нагального вивчення. Освітньому закладу для успішного функціонування й розвитку усіх підсисистем, організації ефективного управління ними необхідно своєчасно та адекватно реагувати на виклики та ризики зовнішнього середовища. А сучасність ставить перед системою освіти нові завдання й вимагає оновлення педагогічних стратегій освітнього процесу, які б нівелювали вказані негативні впливи.

Безпека освітньої галузі є невіддільною складовою загальнодержавної системи безпеки, що характеризується великою кількістю взаємопов`язаних аспектів. Проаналізуємо основні поняття інформаційної безпеки. Питання інформаційної безпеки досліджували науковці В. Лужецький, О. Войнович, А. Дудатьє,в О. Спірін, В. Ковальчук, О. Соснін та ін. Оскільки термін безпека багатогранний його тлумачення залежить від наукової області, в якій він вивчається. У психології розкривають безпеку через стан захищеності психіки від зовнішніх і внутрішніх загроз. У юриспруденції – як систему встановлених законом правових норм, що гарантують захист особи і суспільства, забезпечення їх нормальної життєдіяльності, прав і свобод. Мовознавці у тлумачному словнику української мови дають визначення терміну «безпека - стан, коли кому-чому-небудь ніщо не загрожує».

У сучасному світі постійно зростає роль інформації. А сукупність усіх інформаційно комунікаційних технологій створює потужний дидактичний інструмент для забезпечення освітніх процесів. Проте існує тенденція до збільшення загроз несанкціонованого втручання в роботу інформаційних систем.

Поняття «інформаційна безпека» перебуває у процесі формування. Під ним часто розуміють безпосередньо захист інформації, і особливо – захист таємної, комерційної інформації, інформації з обмеженим доступом, персональних даних тощо. У Національній доктрині інформаційної безпеки України інформаційну безпеку визначають як стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. У законі України Про інформацію під захистом інформації розуміють сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї. Отже поняття «інформаційна безпека» і «захист інформації» не є синонімічними, безпека інформації – це стан захищеності інформації від потенційних загроз, а захист інформації – це діяльність (комплекс заходів), спрямована на забезпечення інформаційної безпеки» [2].

Визначальними принципами інформаційного законодавства є:

- гарантованість права на інформацію;
- відкритість, доступність інформації й свобода обміну інформацією;
- об'єктивності, достовірності, повноти і точності інформації;
- мінімізації негативного інформаційного впливу та негативних наслідків функціонування інформаційно-комунікативних технологій;
- недопущення незаконного розповсюдження, використання і порушення цілісності інформації;
- законність отримання, використання, поширення й зберігання інформації.

Отже поняття інформаційної безпеки містить не лише технічний, адміністративний, організаційний аспекти захисту інформації та безпеки інформаційних систем, а й гуманітарний – забезпечення інформаційної безпеки споживачів інформації, тобто інформаційної безпеки особистості.

Недотримання у навчальному закладі правил інформаційної безпеки може призвести до небажаних наслідків [1, 3]:

− знищення або пошкодження важливих даних закладу освіти (документація, навчальні матеріали, відомості про оцінювання навчальних досягнень);

− несанкціоноване одержання і розповсюдження персональних даних учнів, учителів, адміністрації;

− проникнення небажаного контенту усередину навчальної мережі;

− зростання витрат на інформаційну безпеку навчального закладу;

− публікація особистих даних дітей на сайтах закладу освіти.

У закладі освіти необхідно передбачити систему заходів, щоб мінімізувати зазначенні інформаційні загрози. Безпеку інформаційного середовища закладу освіти розглядають у таких аспектах: фізичному, технічному, адміністративному, організаційному, освітній. Фізичний аспект передбачає обмеження доступу сторонніх осіб до приміщень школи, у яких знаходяться комп'ютери, сервери, комутаційне обладнання; технічний – використання пристроїв і програмних засобів, призначених для захисту операційних систем та мереж (фільтрації контенту); адміністративний – включає в себе керівні принципи та політики закладу щодо використання інформаційних даних та технологій; організаційний реалізується через систему управління доступу користувачів до ресурсів та систем, яка включає ідентифікацію та автентифікацію користувачів; освітній передбачає формування базових знань з інформаційної безпеки в усіх учасників освітнього процесу

Якщо взяти за основу походження загроз, то їх можна класифікувати як внутрішні та зовнішні. Внутрішні загрози більшою мірою стосуються інформаційної безпеки та виникають як несистематичні порушення безпеки, пов'язані з діяльністю некомпетентних або недоброчесних користувачів. Зовнішні загрози стосуються кібербезпеки і спричиняються внаслідок дій вірусів хакерських атак, шахрайських маніпуляцій, надсилання спаму тощо. У контексті зовнішніх загроз постає питання відповідальних за розгортання та технічний супровід інформаційно-освітніх середовищ закладів середньої освіти. В

університетах і коледжах зазначені завдання виконують окремо створені підрозділи (центри обслуговування комп'ютерних мереж, відділи дистанційного навчання) [3]. У загальноосвітніх школах проблема залишається невирішеною. Зазвичай завдання щодо технічного супроводу комп'ютерної мережі виходять за межі посадових обов'язків учителів інформатики. На нашу думку, вирішення цієї проблеми, потребує уваги державних органів.

Отож, в сучасних умовах безпека інформаційно-комунікаційного середовища закладу середньої освіти може бути забезпечена тільки комплексною системою захисту, що здійснюватиметься безперервною, цілеспрямовано, мобільно, адекватно сучасним викликам. Зазначена проблема потребує уваги як науковців, педагогів практиків, адміністрації. Подальші дослідження вбачаємо у вивченні проблеми захисту свідомості дітей від деструктивного інформаційного впливу та формування інформаційної культури усіх учасників освітнього процесу.

Література

1. Биков В.Ю. Проблеми і завдання розвитку комп'ютерно-технологічної платформи інформаційно-освітнього простору // Освітній україноцентризм Георгія Філіпчука : зб. наук. пр. / [редкол.: Н. Нічкало (голова), та ін. ; упоряд.: Н. Нічкало, О. Боровік] ; НАПН України ; Ін-т пед освіти і освіти дорослих НАПН України. –К. : Богданова А.М., 2016.– С. 514-522.

2. Лужецький В. А. Інформаційна безпека: навч.посіб. / В. А. Лужецький, О. П. Войнович, А. В. Дудатьєв. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – 240 с.

3. Олексюк В. Стан сформованості компетентностей з інформаційної безпеки майбутніх учителів інформатики [Електронний ресурс] / В. Олексюк, О. Олексюк // Інформаційні технології і засоби навчання. – 2017, Вип.62(6), С. 277-291. – Режим доступу до ресурсу: https://journal.iitta.gov.ua/index.php/itlt/article/view/1906/1285