ARTICLE

DOI 10.36074/grail-of-science.17.06.2022.037

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ В ЦИФРОВОМУ ОСВІТНЬОМУ СЕРЕДОВИЩІ ЗАКЛАДУ ОСВІТИ

Яценко Оксана Іванівна
асистент кафедри комп'ютерних наук та інформаційних технологій
Житомирський державний університет імені Івана Франка, Україна

Яценко Олександр Сергійович
асистент кафедри комп'ютерних наук та інформаційних технологій
Житомирський державний університет імені Івана Франка, Україна

Анотація. *В статті зазначено роль цифрового освітнього середовища в професійній діяльності педагогічного працівника та для всебічного розвитку сучасного студента. Дано визначення поняття «інформаційна безпека» та вказано її основні складові. Наведено основні види загроз інформаційні безпеці цифрового середовища навчального закладу та методи боротьби з ними. Зроблено висновок, що для надійного захисту цифрового освітнього середовища закладу освіту всі ці заходи повинні застосовуватися комплексно, з ідентифікацією однієї або декількох осіб, відповідальних за реалізацію всіх аспектів ІБ.*

Ключові слова: *цифрове освітнє середовище, заклад освіти, інформаційна безпека, захист інформації, загрози інформаційні безпеці, методи захисту інформації*

Сукупність інформаційних ресурсів зберігання, обробки, пошуку та поширення інформації, доступ до даних на основі інформаційних технологій створює спеціальний цифровий простір, що забезпечує якісний освітній процес. У навчальному закладі цей простір формується так, що студент під час навчання має можливість здобувати прогресивні та актуальні знання, навички інтенсивного їх використання, вчиться вільно мислити, адаптуватися до суспільства, що стрімко розвивається. В університеті студент не припиняє нарощувати власні знання і навички, набуває висококваліфіковані концепції за обраною професією.

Цифрове освітнє середовище – це реальність, у якій живе сучасне суспільство. В умовах цифрового середовища в учнів та студентів формується якості та вміння, що затребувані суспільством XXI століття та визначають особистісний та соціальний статус сучасної людини: інформаційна активність та медіаграмотність, уміння мислити глобально, здатність до безперервної освіти та вирішення творчих завдань, готовність працювати у командах, комунікативність та професійна мобільність та багато інших.

Педагогічному працівнику цифрове освітнє середовище дозволяє використовувати широкий спектр сучасних інформаційних технологій, використання яких дає можливість провести будь-яке заняття на вищому технічному рівні, насичує його інформацією, допомагає швидко здійснити комплексну перевірку засвоєння знань.

Інформаційна безпека (ІБ) – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та недостовірність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [1]. Виходячи з даного визначення можна сказати, що ІБ закладу освіти включає в себе систему заходів, спрямованих на захист інформаційного освітнього простору і персональних даних від випадкового або навмисного їх пошкодження, крадіжки або внесення змін в конфігурацію системи, а також захист навчального процесу від будь-якої інформації, що носить характер пропаганди, забороненої законом та будь-яких видів реклами.

У складі інформації, що знаходиться в розпорядженні навчального закладу та потребує захисту, можна виділити такі основні групи:

– навчальні матеріали, створені авторами курсу та розміщені на внутрішніх ресурсах закладу;

– персональні дані учасників освітнього процесу;

– результати педагогічної діагностики та моніторингу навчальних досягнень слухачів;

– інформація про діяльність учасників освітнього процесу, що здійснюється з використанням певних публічних інтернет-сервісів.

Вся ця інформація може стати об'єктом крадіжки, крім того вона може бути навмисно чи випадково пошкоджена, можуть бути внесені зміни до коду навчальних програм тощо. Отже особи, відповідальні за захист даних, повинні нести відповідальність за:

– збереження цілісності та доступності даних в будь-який час для будь-якого авторизованого користувача;

– захист від будь-яких втрат або несанкціонованих змін;

– конфіденційність, недоступність для третіх осіб.

Особливістю загроз є не тільки можливість крадіжки інформації або пошкодження масивів будь-якими свідомо діючими хакерськими групами, але і сама активність учасників освітнього процесу (частіше всього студентів), що можуть навмисно або помилково нанести шкоди апаратному чи програмному забезпеченні освітнього процесу. Існує чотири групи об'єктів, що можуть піддаватися навмисному або ненавмисному впливу:

– комп'ютерна техніка та інше обладнання (можуть бути пошкоджені в результаті механічного впливу, вірусів);

– програми, що використовуються для забезпечення функціонування системи або в навчальному процесі (можуть постраждати внаслідок дії вірусів або хакерських атак);

– дані зберігаються як на жорстких дисках, так і на окремих носіях;
– персонал, відповідальний за працездатність інформаційної системи;

Загрози, спрямовані на пошкодження будь-якого з компонентів системи, можуть бути як випадковими, так і навмисними. Загрози, які не залежать від намірів персоналу, студентів або третіх осіб, включають:

– надзвичайні ситуації, такі як відключення електроенергії або повінь;
– кадрові помилки;
– збої в роботі програмного забезпечення;
– вихід з ладу обладнання;
– проблеми в роботі систем зв'язку тощо.

Всі ці загрози ІБ є тимчасовими, передбачуваними і легко усуваються діями співробітників і спецслужб.

Навмисні загрози ІБ є більш небезпечними і, в більшості випадків, непередбачуваними. Їх винуватцями можуть стати студенти, співробітники, конкуренти, треті особи з наміром вчинити кіберзлочин. Для підриву ІБ такі особи повинні бути добре знайомі з принципами роботи комп'ютерних систем і програм. Найбільш вразливими до таких загроз є комп'ютерні мережі. Порушення зв'язку між компонентами інформаційної системи може призвести до її повної непрацездатності. Наслідком таких дій може бути: порушення авторських прав, навмисне викрадення чужих розробок та персональних даних. Комп'ютерні мережі не часто піддаються зовнішнім атакам з метою впливу на свідомість дітей, але це не виключено. А найсерйознішою небезпекою буде використання шкільного обладнання для залучення дитини до злочинів і тероризму.

З точки зору проникнення в периметр ІБ і для вчинення крадіжки інформації або створення збоїв в роботі систем необхідний несанкціонований доступ. Існує кілька типів несанкціонованого доступу:

– Людський. Інформацію можна вкрасти, скопіювавши на тимчасовий носій, відправлений по електронній пошті. Крім того, при наявності доступу до сервера, зміни до баз даних можна вносити вручну.

– Програмний. В цьому випадку для крадіжки даних або організації доступу до них використовуються спеціальні програмні засоби, що можуть копіювати паролі, копіювати та перехоплювати інформацію, перенаправляти трафік, вносити зміни в роботу інших програм.

– Апаратний. Даний вид доступу пов'язаний або з використанням спеціальних технічних засобів, або з перехопленням електромагнітного випромінювання по різних каналах, в тому числі телефонних каналах.

Боротьба з різними видами атак на ІБ повинна вестися на п'яти рівнях, а робота повинна бути комплексною. Існує ряд методичних розробок, які дозволять побудувати захист навчального закладу на необхідному рівні.

1) Нормативно-правовий спосіб захисту інформації. Захист інформації ґрунтується на законах, що діють у цій сфері, які визначають її окремі масиви як такі, що підлягають захисту. Вони висвітлюють інформацію, яка повинна бути недоступна третім особам з різних причин (конфіденційна інформація, персональні дані, комерційна, офіційна або професійна таємниця). Порядок

захисту персональних даних визначається, в тому числі, законом «Про інформацію», «Про захист персональний даних», Трудовим кодексом. Вони та Цивільний кодекс допомагають розробити методологію забезпечення захисту інформації, пов'язаної з комерційною таємницею. Крім законів, необхідно виділити діючі в цій сфері ГОСТи, що визначають порядок захисту даних, методи і апаратні засоби, що використовуються для цієї мети.

2) Морально-етичні засоби забезпечення ІБ. В освітній сфері важливу роль відіграє система морально-етичних цінностей. Вона повинна лягти в основу системи заходів, що захищають від травматичної, етично некоректної, незаконної та недостовірної інформації. Для захисту від пропаганди в закладах освіти необхідно керуватись Конвенцією ООН «Про права дитини», положеннями закону «Про захист прав дитини», які визначають його права на захист від інформації, яка може завдати моральної шкоди. Необхідно створити списки документів, програм та інших джерел, які можуть травмувати психіку підлітків, щоб не допустити їх проникнення на територію навчального закладу. Це стане однією з основ інформаційної безпеки.

3) Адміністративно-організаційні заходи будуються на основі посадових інструкцій та на створенні внутрішніх правил і норм. що визначають порядок роботи з інформацією та її носіями. Це внутрішні методи, присвячені ІБ, посадовим інструкціям, спискам інформації, яка не може бути передана тощо. Крім того, закладом освіти має бути розроблений регламент, який визначає порядок взаємодії з компетентними органами за запитами про надання їм певних даних і документів. Адміністративно-організаційні заходи в закладі освіти повинні визначати порядок доступу дітей в інтернет в комп'ютерних класах, можливість захисту деяких ресурсів неоднозначного характеру від доступу дитини, а також заборону на використання власних носіїв даних.

4) Фізичні заходи. Серед фізичних заходів повинна бути передбачена система захисту доступу до приміщень, що містять носії інформації, організація контролю доступу відвідувачів, встановлення різних ступенів доступу. Крім того, заходи фізичного захисту можуть включати в себе обов'язкове резервне копіювання важливої інформації на носії, до яких немає доступу з в інтернет. Необхідно не тільки встановлювати паролі, але і регулярно їх замінювати. Неприпустимо перекладати організацію заходів фізичного захисту комп'ютерної мережі на співробітників найманих підрозділів безпеки.

5) Технічні та програмні заходи – це комплексна система захисту всієї комп'ютерної мережі. Ця система захисту повинна бути забезпечена спеціалізованими програмними продуктами, наприклад, DLP-системами і системами SIEM, що здатні виявляти всі можливі загрози безпеці і застосовувати заходи боротьби з ними. Для навчальних закладів, бюджет яких не дозволяє реалізувати професійні системи, необхідно використовувати дозволені та рекомендовані заходи захисту програмного забезпечення, зокрема антивіруси. За цю систему заходів і її реалізацію повинні відповідати керівництво навчального закладу і співробітники IT-відділів. Електронна пошта, до якої працівники та студенти мають доступ, повинна контролюватися. Оптимальним також є введення повної заборони на копіювання будь-якої інформації з жорстких дисків комп'ютерів навчального закладу. Крім того, має бути

програмне забезпечення, яке обмежує доступ дитини до певних сайтів (фільтрів вмісту).

Для надійного захисту ІС закладу освіту всі ці заходи повинні застосовуватися комплексно, з ідентифікацією однієї або декількох осіб, відповідальних за реалізацію всіх аспектів ІБ.

Список використаних джерел:

[1] Верховна Рада України. (2007, січ. 9). Закон № 537-V, Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. [Електронний ресурс] // Режим доступу: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=537-16#Text (Дата звернення: 15.05.2022).

[2] Закон України Про захист персональних даних (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481) {Із змінами, внесеними згідно із Законами № 4452-VI від 23.02.2012, ВВР, 2012, № 50, ст.564 № 5491-VI від 20.11.2012}