УДК 004

Ольга Ю. Чубукова, Ігор В. Пономаренко
Київський національний університет технологій та дизайну

ІНФОРМАЦІЙНА БЕЗПЕКА У НАВЧАЛЬНИХ ЗАКЛАДАХ УКРАЇНИ

У статті розглянуто особливості забезпечення інформаційної безпеки у навчальних закладах в сучасних умовах. Наукова новизна полягає в комплексному аналізі підходів щодо забезпечення інформаційної безпеки в навчальних закладах. Практична значимість дослідження підтверджена необхідністю розробки ефективної стратегії забезпечення інформаційної безпеки навчальних закладів, що дозволить оптимізувати навчальний процес та мінімізуватиме ризики негативних інформаційних впливів на школярів та студентів.

Ключові слова: *інформаційна безпека; захист інформації; освіта; навчальні заклади; база даних.*

Ольга Ю. Чубукова, Игорь В. Пономаренко
Киевский национальный университет технологий и дизайна

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УЧЕБНЫХ ЗАВЕДЕНИЯХ УКРАИНЫ

В статье рассмотрены особенности обеспечения информационной безопасности в учебных заведениях в современных условиях. Научная новизна заключается в комплексном анализе подходов по обеспечению информационной безопасности в учебных заведениях. Практическая значимость исследования подтверждена необходимостью разработки эффективной стратегии обеспечения информационной безопасности учебных заведений, что позволит оптимизировать учебный процесс и минимизировать риски негативных информационных воздействий на школьников и студентов.

Ключевые слова: *информационная безопасность; защита информации; образование; учебные заведения; база данных.*

Olga Yu. Chubukova, Igor V. Ponomarenko
Kyiv National University of Technologies and Design

INFORMATION SECURITY IN EDUCATIONAL STAFF OF UKRAINE

The article deals with the features of providing information security in educational institutions in modern conditions. Scientific novelty consists in a comprehensive analysis of approaches to providing information security in educational institutions. The practical significance of the research is confirmed by the need to develop an effective strategy for ensuring information security of educational institutions, which will optimize the educational process and

minimize the risks of negative informational influences on schoolchildren and students.

Keywords: *information security; information protection; education; educational institutions; database.*

Постановка проблеми та її зв'язок з важливими науковими та практичними завданнями. Активний розвиток глобального економічного середовища та національних систем відбувається в умовах інтенсивного впровадження інноваційних технологій. Інтеграція високотехнологічних електронних пристроїв у різноманітні процеси на рівні країн, видів економічної діяльності, окремих підприємств та в приватному житті населення призводить до генерування значних обсягів інформації. Окреме місце у якості джерела генерування даних посідає мережа Інтернет, що слугує інструментом створення, накопичення та передачі інформації. В зазначених умовах інформація постає у вигляді ресурсу, який можливо оцінити у грошовій формі виходячи зі специфіки даних та попиту серед окремих груп користувачів. Окремі держави намагаються заволодіти секретною інформацією інших країн, компанії використовують промисловий шпіонаж для отримання секретної інформації конкурентів, у багатьох випадках фіксуються випадки викрадення персональної інформації громадян з метою набуття певної вигоди тощо. Наведена ситуація призводить до розробки національних стратегій захисту у сфері інформаційної безпеки та активної розробки спеціалізованих продуктів, що дозволяють за допомогою апаратного та програмного забезпечення мінімізувати втрату інформаційних ресурсів країн, компаній, громадян тощо. Ринок представлених продуктів активно розвивається та має значний потенціал для зростання, оскільки відбувається безперервна еволюція методів, які націлені на незаконне заволодіння комерційною та приватною інформацією. В окремих випадках головною метою незаконно доступу до інформації є блокування доступу до неї власників або повне знищення даних, що негативно впливає на функціонування компанії у цілому або окремих систем. Виходячи з міжнародного досвіду та ситуації в Україні, в першу чергу мова йде про хакерську атаку у 2017 р. через спеціалізоване бухгалтерське програмне забезпечення M.E.Doc, слід відмітити активізацію державних заходів, які орієнтовані на запобігання незаконному порушенні інформаційної безпеки. Наприклад, після хакерських атак у 2017 р. було створено Ситуаційний центр забезпечення кібернетичної безпеки. Кабінетом Міністрів України 11 липня 2018 р. введено в дію розпорядження «Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України», а з вересня 2018 р. починають розглядатись пропозицій до плану заходів на 2019 рік. Поряд з цим, важливо приділяти увагу вирішенню питань інформаційної безпеки в

окремих видах економічної діяльності, в тому числі у сфері освіти. Специфіка функціонування навчальних закладів передбачає генерування персональної інформації учнів, студентів та педагогічних працівників, баз даних з навчальними матеріалами, поточної документації тощо. Для забезпечення ефективного функціонування навчальних структур необхідно створити дієву систему захисту інформації, яка дозволить мінімізувати ризики втрати або пошкодження відповідних даних.

Аналіз останніх публікацій з проблеми дослідження. Останні публікації стосовно дослідження підходів проблем захисту інформації були опубліковані такими авторами: І. Арістова, А. Гальчинський, П. Друкер, Я. Жаліло, О. Зощенко, Е. Лемберг, Г. Почепцов, М. Роуз, Е. Тофлер, Ф. Фукуяма та ін. Незважаючи на широкий спектр наукових праць існує потреба у проведенні комплексного дослідження підходів щодо запровадження ефективної системи захисту інформації в освітньому процесі.

Невирішені частини дослідження. Питанням забезпечення інформаційної безпеки в Україні присвячено багато праць вітчизняних вчених, проте існує потреба у дослідженні особливостей захисту даних у закладах освіти, що дозволить мінімізувати ризики втрати інформаційного середовище зазначених установ та дасть можливість захисти учнів і студентів від шкідливої інформації.

Мета дослідження полягає у вивченні особливостей забезпечення захисту інформації у закладах освіти.

Виклад основних результатів та їх обґрунтування. В розвинених країнах світу сучасна система освіти забезпечується завдяки ефективній державній політиці регулювання ключових процесів, розробці та реалізації дієвих стратегій розвитку та відповідному фінансуванні передбачених заходів, в тому числі й у сфері запровадження інноваційних технологій. В Україні окресленим питанням також приділяється певна увага, проте існує потреба у запровадженні передового досвіду окремих держав світу у сфері захисту інформації в освітніх закладах. Слід наголосити, що до освітнього процесу залучаються діти та підлітки, які дуже чутливі до сприйняття будь-якої інформації, що може пропагувати шкідливі для здоров'я, психіки та безпеки даної категорії населення цінності. Поряд з цим, потрібно забезпечити захист персональних даних школярів та студентів від заволодіння зловмисниками. В системі освіти також зберігається інформація про педагогічних та інші категорії працівників, навчальні матеріали у цифровому вигляді, фінансові та бухгалтерські дані, а також службова документація, приведені електронні матеріали також потребують захисту. Для забезпечення функціонування освітніх закладів та нормальної життєдіяльності усіх учасників навчального процесу система інформаційної безпеки повинна мінімізувати ризики пошкодження баз

даних, викрадення масивів конфіденційних відомостей, а також гарантувати неможливість проникнення в навчальні приміщення пропаганди, яка негативно впливає на свідомість учнів та школярів [1, 2].

Інформаційна безпека освітнього закладу представляє собою складну систему, яка передбачає захист наявного в організації інформаційного простору та унеможливлює пошкодження або викрадення персональних даних усіх учасників навчального процесу, а також інформації, що дозволяє установі функціонувати та має грошову, освітню, інтелектуальну цінність тощо. Забезпечення ефективного функціонування системи безпеки передбачає витрати певних грошових ресурсів у рамках розробленої стратегії захисту даних. При розробці стратегії доцільно врахувати фактори зовнішнього та внутрішнього середовища, оскільки досягнення оптимального результату можливе лише за умови знаходження рівноваги між наявними можливостями та бажаними результатами.

Розглянемо більш детально інформацію, яка знаходиться у розпорядженні навчальних закладів в Україні:

- Персональні дані учнів, студентів, викладачів та інших категорій працівників. В Україні згідно з вимогами Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1 червня 2010 р. було прийнято Закон України «Про захист персональних даних». У відповідності з представленим нормативно-правовим актом передбачається комплекс заходів захисту приватної інформації та встановлюється відповідальність за її неправомірне розповсюдження.

- Структурована навчальна інформація, що забезпечує освітній процес (бібліотеки, бази даних, навчальні програми). Захист зазначеної групи інформації здійснюється у зв’язку з необхідністю унеможливлення її часткового або повного пошкодження, тобто мінімізації ризиків порушення або повного припинення функціонування освітнього закладу на певний період часу. Поряд з цим, навчальна інформація може містити елементи інтелектуальної власності, які були розроблені працівниками освітнього закладу у рамках чинного законодавства або отримані в інших структур у відповідності з певними правовідносинами. В певних випадках освітній заклад використовує навчальну інформацію лише для власних потреб та не бажає надавати навчально-методичні розробки у користування іншим установам. Обмеження доступу до фінансової інформації здійснюється для унеможливлення махінацій з наявними коштами. В сучасних умовах запровадження систем оцінювань знань учнів та студентів за допомогою спеціалізованого програмного забезпечення важливо забезпечити їх об’єктивність, що передбачає захист представлених систем від зовнішнього втручання.

- Наукові напрацювання, які наділені ознаками інтелектуальної власності і захищені законодавством. Специфіка функціонування

навчальних установ, в першу чергу вищих навчальних закладів, передбачає проведення викладацьким персоналом наукових досліджень, активної участі в грантових програмах тощо. Отримані в процесі досліджень наукові результати, а також згенеровані в процесі дані, потребують захисту як продукти інтелектуальної власності. Особливу увагу потрібно приділяти обмеженню доступу до інформації, що генерується на етапі апробації та не отримала вигляд комплексного наукового продукту, який опублікований або запатентований відповідними науковцями [3].

Для забезпечення захисту інформації в навчальних закладах повинні бути передбачені грошові ресурси на утримання персоналу, що має відповідний рівень кваліфікації. Кількість фахівців у сфері ІТ-захисту повинна відповідати специфіці функціонування освітнього закладу, особливостям наявних баз даних, чисельності персоналу та осіб, що навчаються. До основних посадових обов'язків зазначених працівників необхідно віднести:

- забезпечення безперебійної доступності до інформації в цілому або певних її модулів в будь-який час для користувачів у відповідності з їх правами доступу;

- створення умов захисту від повної або часткової втрати інформації, несанкціонованого внесення змін у дані особами, які не мають відповідних повноважень;

- конфіденційність та недоступність даних для третіх осіб [4].

Загрози інформаційної безпеки освітніх закладів пов'язані не лише з діяльністю спеціалізованих хакерських груп, що діють у власних інтересах або виконують замовлення третьої сторони, але й пов'язані з безпосередніми учасниками навчального процесу – школярами та студентами, які випадково або навмисно можуть зіпсувати комп'ютерне обладнання, пошкодити або видалити певну інформацію, встановити шкідливе програмне забезпечення тощо. Віднесення даної категорії громадян до групи ризику пов'язане з психологічними особливостями, які притаманні дітям та підліткам: допитливість, необачність, безтурботність, підвищене почуття справедливості тощо.

Виділяються п'ять груп об'єктів, що можуть піддатися навмисному або ненавмисному впливу:

- комп'ютерна техніка та інші апаратні засоби, які можуть бути пошкоджені в результаті механічної дії, інтеграції шкідливого програмного забезпечення тощо;

- спеціалізоване програмне забезпечення, яке використовується для функціонування освітнього закладу або безпосередньо застосовується в навчальному процесі та може повністю або частково втрати функціональність внаслідок хакерських атак, активації вірусів або інших шкідливих дій;

- інформація навчальних закладів, яка зберігається на різних носіях та використовується для забезпечення функціонування зазначених установ;

- школярі та студенти, які відносяться до групи ризику внаслідок їх вразливості до негативного інформаційного впливу, що може завдати шкоди їм безпосередньо або призвести до агресивної поведінки по відношенню до оточуючих або навчального закладу [5];

- персонал навчального закладу, який під впливом зовнішніх факторів або за власними мотивами може негативно вплинути на інформаційну безпеку закладу освіти, частково або повністю знищивши інформацію, використавши її в особистих інтересах або передавши дані третім особам.

В рамках розробки ефективної стратегії інформаційної безпеки освітніх закладів доцільно виділити п’ять основних напрямів захисту даних:

1. Нормативно-правовий. Комплексна організація протидії з незаконним заволодінням даними або їх знищенням базується на чинній нормативно-правовій базі України. Серед основних нормативно правових актів необхідно виділити Закон України «Про захист персональних даних» від 1 червня 2010 р., Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р., розпорядження Кабінету Міністрів України «Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України» від 11 липня 2018 р. Поряд з цим існує ряд стандартів, інструкцій та рекомендацій, що орієнтовані на звбезпечення інформаційної безпеки, в тому числі й у навчальних закладах [6].

2. Морально-етичний. Однією з ключових функцій освітньої системи є формування в учнів та студентів системи моральних цінностей, які є позитивними орієнтирами у суспільстві. Для досягнення наведеної мети навчальним закладам необхідно реалізовувати комплекс заходів, що захищають підлітків від шкідливої інформації. Формування у школярів та судентів системи цінностей зменшує ймовірність скоєння правопорушень даною категорією населення, в тому числі на території закладів освіти [7, 8].

3. Адміністративно-організаційний. Представлений напрям передбачає розробку внутрішніх інструкцій, які регламентують особливості використання комп’ютерного обладнання, специфіку роботи з інформацією та її носіями. Крім того, необхідно сформувати правила доступу школярів та студентів до мережі Інтернет в комп’ютерних класах, порядок блокування небезпечного для даної категорії населення контенту, заборона на користування власними носіями інформації. Повинно бути

передбачено використання системи батьківського контролю над ресурсами мережі Інтернет.

4. Фізичний. У межах даного напряму передбачається формування пропускної системи згідно з рівнем доступу до приміщень, в яких розміщуються носії інформації навчального закладу. В приміщення допускаються лише авторизовані користувачі, а використання ними інформації здійснюється суворо в межах їх прав доступу до даних. Встановлені паролі повинні регулярно змінюватись з метою мінімізації ризиків заволодіння інформацією третіми особами або її знищення. До заходів фізичного захисту може бути віднесено обов'язкове копіювання важливої інформації на диски комп'ютерів, які не мають доступу до мережі Інтернет [9].

5. Технічний. Для забезпечення якісного захисту інформації в освітніх закладах необхідно використовувати спеціалізоване програмне забезпечення, яке дає можливість виявляти потенційні загрози та реалізовувати заходи боротьби з ними. В умовах недостатнього рівня фінансування заходів, які орієнтовані на забезпечення інформаційної безпеки освітніх закладів, більшість установ використовує лише антивіруси та безкоштовні програмні продукти у сфері боротьби з незаконним порушенням інформаційних систем. Передбачається встановлення фільтрів, які обмежують доступ школярів та студентів до певних ресурсів в мережі Інтернет. Потрібно встановити контроль за доступом співробітників, учнів та студентів до електронної пошти. Також необхідно запровадити заборону на копіювання певних видів інформації з комп'ютерів освітнього закладу [10].

Ефективна стратегія інформаційної безпеки передбачає комплексне використання наведених вище напрямів захисту даних. Ключова роль на етапі запобігання незаконному заволодінню інформацією відводиться посадовим особам, які безпосередньо реалізують комплекс заходів захисту даних. Поряд з навчальними закладами реалізацію виховної функції у сфері інформаційної грамотності та безпеки учнів і студентів повинні виконувати батьки.

Висновки та перспективи подальших досліджень. Ефективне функціонування вищих навчальних закладів в сучасних умовах можливе лише за умови реалізації комплексу заходів, які орієнтовані на дотримання інформаційної безпеки. Інтенсивне генерування освітніми закладами великих обсягів інформації під час навчального та наукового процесу передбачає створення умов щодо її надійного зберігання. Еволюція шкідливого програмного забезпечення для незаконного заволодіння даними вимагає від навчальних установ здійснювати комплекс заходів у рамках оптимізації стратегії забезпечення інформаційної безпеки.

Література

1. Data Security Solutions for Educational Institutions. – Retrieved from: https://www.thalesesecurity.com/solutions/industry/education.

2. Чубукова О. Ю. Складові інноваційної економіки – освіта, технологічні уклади, когнітивні технології / О. Ю. Чубукова, Н. В. Раллє // Науковий вісник Полісся. – 2016. – № 3 (7). – С. 130–133.

3. Top Cybersecurity Threats Active in the Education Sector Today – and Why You Should Care. – Retrieved from: https://www.csoonline.com/article/3250862/security/top-cybersecurity-exploits-active-in-the-education-sector-today-and-why-you-should-care.html

4. Data Security. – Retrieved from: https://library.educause.edu/topics/cybersecurity/data-security.

5. Ślusarczyk B. Sustainable Dewelopment Policies of the European Union as Expressions of Socio-Economic Seciurity / B. Ślusarczyk, A. Wolak-Tuzimek // Bezpecnostne Forum 2014 Security Forum, Zbornik Vedeckych Prac. – Wydawnictwo Belianum, Banska Bystrica, 2014. – S. 344–350.

6. Офіційний сайт Верховної Ради України [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

7. How to help young learners stay safe on the internet. – Retrieved from: https://www.britishcouncil.org/voices-magazine/how-help-young-learners-stay-safe-internet.

8. Internet Safety. – Retrieved from: https://kidshealth.org/en/parents/net-safety.html.

9. Data Copy Protection. – Retrieved from: https://www.truscont.com/solutions/data-protection.

10. Ольшанська О. В. Сучасні аспекти когнітивістики в економічному розвитку / О. В. Ольшанська // Вісник Київського національного університет технологій та дизайну. – 2014. – № 6 (81). – С. 78–82

10. Информационная безопасность образовательных учреждений [Электронный ресурс]. – Режим доступа: https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdenij.