5. Закон України «Про місцеве самоврядування» [Електронний ресурс]. -Режим.доступу: http://kodeksy.com.ua/konstitutsiya_ukraini/statja-140.htm.
6. Стратегія сталого розвитку «Україна – 2020» схвалена Указом Президента України від 12 січня 2015 року № 5/2015 [Електронний ресурс]. – Режим.доступу: http://zakon3.rada.gov.ua/laws/show/5/2015.
7. Офіційний сайт Великогаївської об'єднаної територіальної громади [Електронний ресурс]. – Режим доступу: https://alt.velykogaivska-gromada.gov.ua/.

Чубукова О. Ю.
доктор економічних наук, професор,
завідувач кафедри економічної кібернетики та маркетингу
Пономаренко І. В.
кандидат економічних наук, доцент,
доцент кафедри кономічної кібернетики та маркетингу
Київський національний університет технологій та дизайну
м. Київ, Україна

ЗАХИСТ ІНФОРМАЦІЇ В ЗАКЛАДАХ ОСВІТИ У СУЧАСНИХ УМОВАХ

Особливості функціонування сучасних підприємств, установ та організацій передбачають переведення системи документообліку в електронний вигляд. Створення спеціалізованих баз даних, які містять комплексні відомості про діяльність зазначених структур та їх окремих підрозділів, інформацію про певних працівників або інших юридичних або фізичних осіб, що пов'язані з цими закладами, дає можливість швидко отримувати необхідні дані. Оптимізація діяльності здійснюється й закладами освіти, які мають великі обсяги інформації про педагогічних працівників, школярів або студентів, навчальні матеріали, поточну фінансову та іншу документацію, що дозволяє забезпечити навчальний процес, та ін. Навчальні заклади приділяють увагу забезпеченню захисту представлених інформаційних ресурсів, оскільки вони містять цінні персональні відомості про окремі категорії працівників та підлітків, а також діяльність зазначених організацій, що можуть бути вкрадені та використані третіми особами з метою отримання певного зиску, а також призведуть до матеріальної та моральної шкоди учасників освітнього процесу. Окреслені проблеми необхідно вирішувати на постійній основі, оскільки науково-технічний прогрес призводить до еволюції шкідливого програмного забезпечення та спеціалізованих шпигунських пристроїв. З метою мінізації ризиків втрати цінної інформації існує потреба у комплексному дослідженні особливостей захисту даних та реалізації передового досвіду у сфері протидії кіберзлочинам в практичній діяльності закладів освіти [1].

В окреслених умовах керівництву освітніх закладів необхідно розробити ефективну стратегію інформаційної безпеки, що повинна містити наступні етапи:

1. Визначення місця інформаційної безпеки в системі забезпечення функціонування освітнього закладу. На даному етапі необхідно врахувати ключові особливості функцінування конкретного освітнього закладу, наявні ресурси та можливості. Важливо застосувати індивідуальний підхід для кожного навчального закладу, в рамках нормативного-правових актів держави, що дозволить побудувати ефективну систему інформаційного захисту за умови оптимального використання наявних ресурсів.

2. Виявлення наявних ризиків. На основі індивідуальних ризків освітньої установи та з урахуванням її специфічних потреб необхідно провести комплексний аналіз можливих загроз. При побудові системи кібербезпеки навчального закладу виявлені у ході дослідження ризики необхідно врахувати, що дасть можливість забезпечити високий рівень інформаційної безпеки.

3. Розробка та запровадження політики безпеки. На основі чинного законодаства та передового досвіду у сфері інформаційної безпеки необхідно розробити та запровадити систему інфомаційного захисту. Інноваційна система передбачає не лише використання новітніх підходів та інструментів, але й використання елементів попередньої системи інформаційної безпеки, які є актуальними в сучасних умовах та довели своє ефективність і доцільність використання у майбутньому.

4. Управління безпекою. Важливу роль у забезпеченні ефективного функціонування системи інформаційної безпеки відіграють працівники різних ланок управління. На рівні керіництва уповноважена особа відповідає за розробку та виконання стратегічних заходів щодо забезпечення кібербезпеки освітніх закладів. На рівні системних адміністраторів посадові обов’язки передбачають тестування та перевірку системи, а також виконання щоденних адміністративних заходів. Керівники вищих рівнів контролюють виконання підлеглими посадових обов’язків щодо забезпечення інформаційної безпеки в закладах освіти.

5. Програмний захист інформації. На даному етапі проводиться класифікація потенційних загроз комп’ютерному програмному забезпеченню за умови використання шкідливого софту. На оснвові отриманих результатів створюється або вдосконалюється система кібербезпеки від вірусів та іншого шкідливого програмного забезпечення.

6. Фізичний захист інформаційної системи. Поряд з боротьбою з шкідливим програмним забезпеченням, необхідно розробити комплекс заходів стосовно мінімізації ризиків пошкодження або знищення комп’ютерного обладнання, в

першу чергу мова йде про сервери, яке займається обробкою та збереженням відповідної інформації.

7. Створення системи доступу. У відповідності з рівнем доступу до інформації у навчальному закладі кожній з категорій користувачів надаються різні права для роботи з даними. В даному випадку можуть використовуватись різноманітні стратегії налаштування прав доступу до інформації або запобігання щодо її використання [2].

Отже, закладам освіти необхідно приділяти значну увагу питанням захисту інформації, яка генерується в процесі їх діяльності. Необхідно мінімізувати ризик втрати даних, що пов’язані як безпосередньо з діяльністю установ, так і з приватним життям усіх учасників навчального процесу. Безперервна еволюція шкідливих програм передбачає постійне вдосконалення захисту даних.

Література:

1. Cyber security in education [Електронний ресурс]. – Режим доступу: https://edtechnology.co.uk/Article/cyber-security-in-education.
2. Why Information Security In Education? [Електронний ресурс]. – Режим доступу: https://nces.ed.gov/pubs98/safetech/chapter1.asp.