URL: http://max-energy-saving.info/index.php?pg= law/3.html
4. Українська асоціація відновлюваної енергетики. URL: http://uare.com.ua/.

БЕЗПЕКА В ІНТЕРНЕТІ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Землянська Олена Василівна, Праховнік Наталія Артурівна, Ковтун Андрій Іванович, Ковтун Максим Андрійович
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Анотація. *Безпека інформації та персональних даних в Інтернеті є дуже важливим питанням на сьогоднішній день, адже з кожним днем росте кількість людей, які користуються глобальною мережею. Тези присвячені визначенню основних проблем захисту інформації в Інтернеті та їх вирішенню.*

Ключові слова: *Інтернет, всесвітня мережа, безпека персональних даних, конфіденційність, захист даних, проблеми захисту інформації.*

На сьогоднішній день сфера інформаційно-обчислювальних технологій торкається майже усіх аспектів нашого життя. В Інтернеті щодня здійснюються тисячі різноманітних операцій, платежів, розмов, листувань та багато інших дій, що потребують конфіденційності користувача та захисту його персональних даних.

Саме поняття інформаційної безпеки означає стан інформацій, при якому система нормально функціонує та забезпечується цілісність, конфіденційність та захищеність персональних даних, а також забезпечення доступу до них.

Можна виділити три основні принципи, які відносяться до інформаційної безпеки:

– доступ до конфіденційних даних має бути лише у авторизованих користувачів;

– повнота та достовірність інформації означають її цілісність;

– доступність інформації означає, що при виникненні потреби авторизованим користувачам може бути забезпечений доступ до певних ресурсів, на яких розміщена ця інформація.

З появою всесвітньої мережі з’явились і проблеми захисту інформації в ній, адже Інтернет та інформаційна безпека несумісні за своєю природою. Відомо, що чим легший доступ в мережу, тим гіршою є її інформаційна безпека. Користувач може навіть не дізнатися, що його дані були скопійовані, змінені або навіть зіпсовані. Існують антропогенні, техногенні та стихійні джерела загрози персональним даним.

До антропогенних джерел відносяться випадкові, або навмисні дії деяких суб’єктів. Існує два види таких дій:

– зовнішній – коли відбувається незаконне проникнення третьої особи зі сторони зовнішньої мережі;

– внутрішній – коли відбувається порушення інформаційної безпеки зсередини, наприклад працівником певної компанії.

До техногенних джерел відноситься все, що може призвести до відмови роботи програмного забезпечення або апаратної частини. Це можуть бути як застаріла система, під’єднанні до неї прилади, серверні проблеми, збої в кабельній або дисковій системі, так і програмні помилки, несправність операційної системи.

До стихійних джерел відносяться різноманітні природні катаклізми. Злива може викликати проблеми з електромережею, хуртовина проблеми зі зв`язком, а буревії можуть пошкодити або знищити необхідне для збереження або доступу до інформації обладнання.

Коли мова йде про захист персональних даних в мережі Інтернет, найчастіше мається на увазі антропогенні джерела загрози. Оскільки при передачі даних, вони мають пройти велику кількість різноманітних роутерів та серверів. На цьому шляху інформацію можуть

перехопити, пошкодити, змінити, перенаправити, або «заразити» комп'ютерним вірусом, адже вже на рівні архітектури Інтернет не має засобів захисту від злодіїв.

Захист даних насамперед необхідний для компаній та організацій, таких як банкові системи, оператори, державні організації тощо. Ще однією проблемою при забезпеченні захисту корпоративної мережі є ефективність роботи, адже при підвищенні рівня безпеки, знижується швидкість доступу, що може негативно вплинути на продуктивність роботи. Робота звичайного користувача у всесвітній мережі також потребує захисту, як зі сторони організацій, що надають доступ до Інтернету, так зі сторони сервісів, що зберігають персональні дані. Але, найважливішим є розуміння небезпеки самим користувачем, свідоме використання мережі, а також внесення у неї своєї інформації. Не зважаючи на те, що з самого заснування Інтернет не був захищеним, з часом з'явилися засоби захисту, які можна класифікувати наступним чином:

– апаратні;
– програмні;
– змішані;
– засоби організаційного характеру.

До групи апаратних засобів відносяться електронні або механічні засоби, що забезпечують захист від фізичного проникнення, або у випадку, якщо доступ все ж був отриманий, замаскувати дані для їх збереження.

Програмні засоби можуть ідентифікувати користувачів для контролю доступу, шифрувати або видаляти інформацію, тестувати контроль системи захисту даних. Рівень захисту цієї групи менший за апаратний, але більш гнучкий та дешевий, що спрощує використання та зменшує фінансові витрати на захист.

Змішані засоби захисту поєднують в собі апаратні і програмні розробки для підвищення ефективності та надійності системи. Ці засоби є найпоширенішими у використанні. До засобів організаційного характеру відносяться як контроль доступу до приміщення, так і складання та вивчення правил користування комп'ютерною мережею, а також свідоме використання власних даних у ній. Провайдери забезпечують максимальний захист інформації своїх користувачів завдяки апаратно-програмним засобам, а сучасні операційні системи мають вбудовані програмні засоби захисту, такі як брандмауер. Крім того, існує безліч антивірусів, що збільшують захищеність системи від зловмисників, завдяки своєчасному оновленню вірусних баз. Усі сервіси, що оперують персональними даними, зобов'язують користувачів до створення облікових записів для подальшої аутентифікації, що забезпечує доступ до даних лише авторизованим у системі користувачам. Незважаючи на всі заходи безпеки, користувач має і сам розуміти ризики користування мережею, адже в більшості випадків зловмисник розраховує не лише на прогалину в системі, а й на людський фактор. При дотриманні всіх правил користування мережею, ризик втрати, ушкодження або викрадення даних значно знижується, але не зникає. Саме тому при доступі в Інтернет важливо уникати надмірного розповсюдження персональних даних.

Якщо проводити аналіз проблем, що створюють реальну небезпеку в віртуальному світі, то можна сформулювати основні правила безпечної роботи в глобальній мережі Інтернет:

– використовуйте антивірусне програмне забезпечення;
– уникати підключення до публічних Wi-Fi мереж;
– для здійснення он-лайн платежів використовувати лише спеціально захищені браузери;
– завантажувати додатки лише з офіційних банківських сайтів;
– не здійснювати фінансові операції через незахищені платіжні системи у мережі Інтернет;
– не використовувати підозрілі он-лайн форми для введення персональних даних;
– для передачі конфіденційних даних або здійснення он-лайн транзакцій використовувати мобільний Інтернет або домашню мережу;

– ніколи не надавати незнайомим особам свої персональні дані та конфіденційну інформацію;

– не передавати персональні данні по електронній пошті, в чатах, за допомогою систем миттєвого обміну повідомленнями;

– не відправляти свою фотокартки чи фотокартки родичів;

– повідомляти відповідні органи у разі отримання інформації, що змусить вас почуватись некомфортно, або що має характер залякування.

Список використаних джерел

1. Безпека життєдіяльності та цивільний захист : підручник / О. Г. Левченко, О. В. Землянська, Н. А. Праховнік, В. В. Зацарний. Київ : Каравела, 2019. 268 с.
2. Безпека в мережі Інтернет. URL: http://svitppt.com.ua/informatika/osnovni-ponyattya-zahistu-informacii-bezpeka-v-merezhi-internet.htmll
3. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
4. Технології захисту інформації. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186

ПРОБЛЕМИ ОСВІТЛЕННЯ НАВЧАЛЬНИХ ПРИМІЩЕНЬ НА ЗАНЯТТЯХ З ВИРОБНИЧОГО НАВЧАННЯ

Іванова Тетяна Сергіївна
Полтавський національний педагогічний університет імені В. Г. Короленка

***Анотація**. Освітлення – це один з найважливіших чинників, який значною мірою впливає на продуктивність праці, рівень травматизму і професійних захворювань. Ось чому питання раціонального освітлення навчальних приміщень на заняттях з виробничого навчання є актуальною проблемою охорони праці.*

***Ключові слова**: освітлення, охорона праці, безпечні умови навчання та праці, працездатність людини, виробниче середовище.*

Актуальні проблеми розвитку сучасного суспільства безпосередньо пов’язані з формуванням у людини здоров’язберігаючої компетентності, екологічної безпеки та культури. Загальноосвітній навчальний заклад гарантує безпечні та нешкідливі умови навчання, режим роботи, умови для фізичного розвитку та зміцнення здоров’я, формує гігієнічні навички та засади здорового способу життя студентів. Забезпечення безпечних і нешкідливих умов навчання, праці та виховання у закладах освіти покладається на їх власника або уповноважений ним орган, керівника закладу освіти.

Керівництво і відповідальність за організацію охорони праці під час проведення навчання в майстернях навчального закладу покладається на керівника відповідно до Положення про організацію роботи з охорони праці учасників навчально-виховного процесу в установах і навчальних закладах. Він створює здорові і безпечні умови для проведення занять; наказом призначає відповідальних осіб, які зобов’язані контролювати створення безпечних умов навчання та праці, стежити за виконанням студентами цих Правил та відповідних інструкцій з охорони праці на робочому місці в майстернях; затверджує інструкції з охорони праці (безпеки життєдіяльності) для студентів під час навчання в майстернях; організовує роботу щодо забезпечення студентів справними обладнанням та пристроями; організовує проведення технічного обслуговування та ремонту обладнання в майстернях; організовує один раз на три роки навчання викладачів, майстрів, інструкторів виробничого навчання з питань охорони праці, безпеки життєдіяльності з наступною перевіркою знань відповідно до Типового положення про порядок проведення навчання і