Список використаних джерел

1. Апарат для електрохімічної очистки природних і сточних вод ТЕЦ: пат. 684 Україна, МПК 6 С 02 F 1/46. N 2000052671; Заявл. 11.05.2000; Опубл.16.10.2000, Бюл. N5.
2. Спосіб очистки води: пат. 31413 Україна, МПК 6 С 02 F 1/46. N 98084602; Заявл. 26.08.1998; Опубл. 15.12.2000, Бюл. № 74-II.
3. Хенли Э. Дж., Кумамото Х. Надежность технических систем и оценка риска: пер. с англ. Москва: Машиностроение, 1984. 528 с.
4. «Дослідження з обґрунтування комп'ютерних моделей та програмно-апаратного комплексу для оцінювання ризиків та загроз виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури із застосуванням геоінформаційних технологій» («Модель Геоінформ Ризик НС»), номер держреєстрації ОИЧ U 007224 Міністерства внутрішніх справ (2014-2016). 240 с.

ЦИФРОВА БЕЗПЕКА КОМП'ЮТЕРНИХ СИСТЕМ

Близнюк М. М.
д.п.н, професор,
Вакуленко Н. В.
аспірантка,
Дебре О. С.
аспірант
кафедра виробничо-інформаційних технологій та безпеки життєдіяльності
Полтавський національний педагогічний університет імені В.Г. Короленка
м. Полтава

Ми живемо в епосі інформаційно-комунікаційних технологій. Поширення інформаційних технологій та повсюдне впровадження електронних способів зберігання та обробки даних дозволило підняти ефективність роботи з інформацією на небачений рівень. Це спричинило нові проблеми, пов'язані із забезпеченням безпеки даних. На жаль, більшість користувачів, які працюють з тими чи іншими електронними пристроями, мають дуже поверхневе уявлення про можливі небезпеки та про ті ситуації, з якими вони можуть зіткнутися.

Метою даної публікації є актуалізація уваги до цифрової безпеки комп'ютерних систем, можливі проблеми та існуючі небезпеки, причинами яких можуть бути як самі користувачі, так і недостатньо продумані рішення розробників програмного забезпечення та матеріальної частини обладнання.

Цифрова безпека представляє собою поєднання інструментів та звичок, які користувачі можуть використовувати, уникнення контролю за їхніми діями в Інтернет, доступ або втручання в їх електронну інформацію та втручання у їх електронні пристрої та програми [7, с.4].

Різні аспекти проблематики цифрової безпеки комп'ютерних систем досліджуються в працях вітчизняних та закордонних науковців, зокрема: організаційні, технічні, теоретичні і практичні аспекти використання

інформаційних технологій (В. Биков, М. Жалдак, В. Кухаренко, М. Моісеєва, Н. Морзе, В. Олійник, Є. Полат, В. Солдаткін, С. Ющик); питання кібербезпеки та стратегії розвитку інноваційної ери (П. Біленчук, О. Кобилянський, М. Малій, Р.Перелигіна, Т.Тарасевич); проблеми формування інформаційної культури та компетентності фахівців (Н. Баловсяк, О. Барановська, В. Биков, М. Головань, Т. Сіткар, Ю. Туранов).

Інформаційна складова. Безпека – це комплекс заходів, що дозволяє виконувати певні завдання без стороннього втручання. Мета справжньої інформаційної безпеки – захист конфіденційності, цілісності та доступності інформації, що зберігається в електронному вигляді, причому такий захист повинен мати прийнятну вартість. Конфіденційність – це захист інформації від людей, яким заборонено доступ до неї. Цілісність означає те, що дані не можуть змінюватись тими, хто не має для цього відповідних прав. Доступність говорить про те, що до даних або сервісів завжди забезпечений доступ для тих, кому на це дано права.

Поширення персональних комп'ютерів призвело до того, що їх користувачам (або одному з них) самим доводиться займатися питаннями адміністрування, а отже, і відповідати за безпеку цих систем. Інформація, що зберігається в комп'ютерах та інших електронних пристроях, наприклад у смартфонах, планшетах, цифрових фотоапаратах, має певну важливість і цінність. В одних випадках завдання забезпечення інформаційної безпеки полягає у збереженні доступу до ваших цифрових даних, в інших - у створенні умов її недоступності всім іншим.

Нові технології можуть представляти небезпеку для користувачів, якщо вони не будуть використовуватись з обережністю. Міжнародний досвід свідчить, що кілька репресивних урядів та могутніх корпорацій використали сучасні технології спостереження, щоб розшукати журналістів (як професійних, так і цивільних громадян), та покарати їх за роботу. Останні виклики у сфері ЗМІ різних країн також показують, що злом електронної пошти та акаунтів активістів громадянського суспільства в соціальних мережах, прослуховування телефонних розмов та інші види кіберзлочинів стають традиційними у боротьбі зі свободою слова та інформації. Небезпека також виявляється у вигляді крадіжок особистих даних користувачів цифрових технологій (особисті дані, документи) та фізичне виявлення людини (геолокація, IP адреси тощо).

Разом з тим, користуючись новими медіа, не допустимими є такі технічні ризики як, крадіжку та підбір паролів, персональних даних, розпізнавання IP-адреси та встановлення особи, крадіжку даних із комп'ютера користувачів та ін.

Ніякий набір запобіжних заходів та поради не можуть повністю гарантувати вашу безпеку та безпеку даних, але дотримання основних принципів цифрової безпеки може допомогти зберегти безпеку користувача та безпеку джерел інформації.

Помилково думати, що *використання програмних засобів та правильних методик роботи з даними гарантує повний захист вашої інформації*. На

практиці доводиться піклуватися ще й про фізичну безпеку системи, що полягає в обмеженні фізичного доступу до апаратури, що використовується. Простіше кажучи, необхідно подбати про те, щоб ніхто не вкрав важливий компакт-диск, жорсткий диск ноутбука або flash-диск, на якому записаний персональний електронний ключ користувача.

Трапляється, що для доступу до необхідних даних зловмисники користуються методами соціального інжинірингу: лунає дзвінок на робоче місце нібито від інженера служби підтримки компанії з проханням повідомити пароль, до поштової скриньки надходить фальшиве повідомлення з посиланням, що веде на підроблений сайт банку працівника, і ін.

Необхідно постійно пам'ятати, що рівень безпеки будь-якої системи визначається найслабшою ланкою. Іншим аспектом цифрової безпеки можна вважати наявність *достатнього рівня технічних знань та постійне відстеження пов'язаних із нею новин*. Наприклад, кілька років тому в Інтернеті був дуже популярний сервіс фальшивих новин, що дозволяє виготовити псевдоновий гумористичний або навіть образливий текст у дизайні відомого Інтернет-видання і надіслати посилання жертві розіграшу. Для маскування на початку адресного рядка пишеться URL видання, після чого слідує знак @, а потім вже реальна адреса сторінки. Якщо ж друга адреса вказується, скажімо, у вигляді IP-адреси, то це ще більше збільшує ймовірність того, що адреса цього сайту не буде помічена. Досить часто жертва жарту не сумнівається, що у розіграші винне саме те видання, під чию новину підроблено повідомлення, і, не вникаючи в технічні подробиці та призначення символу «@» в URL, надсилає гнівні листи на адресу відповідної редакції.

Зберігання та передача даних. Аутентифікація – це процес визначення особи користувача за наданою їм інформацією. Вона необхідна для розмежування доступу до даних та сервісів. Існують різні способи автентифікації користувачів – і паролі, ключові файли, електронні ключі, що вже стали класичними, і поки що не дуже широко поширені, наприклад біометрія і такі нестандартні методи, як аналіз нейронною мережею тимчасових характеристик ключової фрази, що вводиться користувачем.

Паролі – один із найпростіших та найпоширеніших способів аутентифікації. Сучасним користувачам доводиться працювати з кількома десятками систем, кожна з яких вимагає авторизації. При виробленні паролів слід дотримуватись наступних базових правил. Паролі повинні бути достатньої довжини (не менше 8 символів, а краще не менше 10) і бути випадковими поєднаннями літер у різних регістрах, цифр, а також додаткових символів. Рекомендується періодично змінювати паролі. При цьому бажано, щоб вони не повторювалися для різних систем. І вже зовсім неприпустимо, коли, наприклад, пароль у форумі збігається з паролем у пошті, вказаній у профайлі користувача.

Алгоритми шифрування. Авторизація не є єдиним способом обмеження доступу до інформації, оскільки не передбачає захисту самих даних у процесі зберігання. Шифрування – це мистецтво перетворювати інформацію те щоб

вона ставала незрозумілою, і навіть вміння виконувати зворотний процес. За допомогою шифрування забезпечується безпека під час зберігання та передачі даних. Алгоритм шифрування є математичною функцією, що приймає певне значення і повертає результат. Сучасні функції шифрування дуже складні та розробляються, тестуються та аналізуються протягом декількох років. Для того, щоб алгоритм шифрування став обґрунтовано суворим, він повинен відповідати найважливішій вимогі - не допускати визначення прихованих даних без знання ключа та обчислення ключа на основі зашифрованих даних.

Програмне забезпечення. Сучасне програмне забезпечення є складним комплексом, який часто містить мільйони рядків коду. Але незважаючи на те, що вибір методик та технологій розробки, що дозволяють створювати подібні програми, дуже великий, не існує рішень, які повністю гарантують відсутність будь-яких помилок. Згідно з результатами низки досліджень, навіть програми, що піддавалися серйозному та всебічному тестуванню, можуть містити від однієї до семи помилок різного рівня на тисячу рядків коду. В одних випадках вони нешкідливі і призводять лише до некоректного відображення тієї чи іншої частини інтерфейсу, а в інших провокують глобальні вірусні епідемії. Ситуація посилюється тим, що є помилки, експлуатація яких зловмисниками або шкідливими програмами не передбачає жодних дій з боку користувачів.

Розробники програмного забезпечення регулярно випускають латки або нові версії програм, що дозволяють усунути знайдені вразливості. Рекомендується встановлювати такі оновлення, оскільки з моменту виявлення помилки і до її використання в якомусь вірусі може пройти лише кілька днів. У деяких випадках, наприклад, для операційної системи Windows, оновлення може здійснюватися в автоматичному або напівавтоматичному режимі

Комп'ютерні віруси. Комп'ютерні віруси – це програми, які вміють розмножуватися та впроваджувати свої копії в інші програми, тобто заражати вже наявні файли. У принципі, не всі шкідливі програми є вірусами – деякі з них є мережевими хробаками і поширюються за допомогою різних мереж, не будучи частиною інших файлів. В окрему групу виділяють троянські програми, які самі не розмножуються, свої копії не розсилають та використовуються зазвичай для розкрадання секретної чи важливої інформації.

Сучасні шкідливі програми не тільки загрожують конфіденційності, цілісності та доступності інформації, але можуть призводити до поломки апаратної частини комп'ютерів. Так, кілька років тому був поширений вірус, який надсилав деякий документ, що зберігається на жорсткому диску, по випадковому e-mail з адресної книги користувача. Цим випадковим документом міг виявитися і нешкідливий реферат, завантажений з Мережі, і такий нешкідливий фінансовий документ.

Комп'ютери, заражені вірусами або троянськими програмами, становлять загрозу не тільки для своїх користувачів, оскільки поширюють мережевих черв'яків і є джерелами вірусів. Останнім часом заражені машини нерідко застосовуються для розсилки спаму чи організації розподілених атак на web-сайти, що вже неодноразово призводило до перебоїв у роботі низки

ресурсів на кілька годин і навіть доби. Використання антивірусу разом з резидентним модулем (монітором) і антивірусними базами, що регулярно оновлюються, а також спеціальних програм, призначених для боротьби зі шпигунським програмним забезпеченням, значно знижує загрозу зараження комп'ютера шкідливими програмами.

Загрози, що виходять з Інтернету. Інтернет – це не тільки потужне інформаційне середовище, але й місце, що є небезпечним для всіх його користувачів. Серед загроз, що виходять із мережі, – віруси та мережеві черв'яки, експлуатація вразливостей у програмах, спам та різні види шахрайських прийомів.

Безпечна робота в Інтернеті має на увазі не лише коректну поведінку та регулярну установку оновлень використовуваного програмного забезпечення, включаючи операційну систему, а й застосування персонального брандмауера. При цьому необхідно забезпечувати фільтрацію як вхідних, так і вихідних з'єднань.

Іншим джерелом мережної небезпеки є протоколи, оскільки більшість з них передають інформацію у відкритому, нешифрованому вигляді, – до них відносяться, наприклад, протокол HTTP, поштові протоколи SMTP і POP3, FTP, протоколи сімейства ICQ та багато інших. Пароль, набраний при авторизації на сайті, важлива бесіда в системі обміну повідомленнями або особистий лист можуть бути перехоплені зловмисником у вашій локальній мережі або на одному з проміжних вузлів мережі. Рішення полягає у використанні захищених протоколів, які не тільки дозволяють шифрувати інформацію, що передається в Мережі, але й мають надійні механізми аутентифікації одержувача та відправника даних.

Завдання забезпечення безпеки для сучасного користувача комп'ютерних систем полягає в мінімізації небезпеки та можливої шкоди, яка може бути завдана зловмисниками, діями самого користувача або виходом з ладу апаратури.

Час диктує свої умови, і сучасний персональний комп'ютер не може обійтися без таких програм, як антивірус, брандмауер і утиліта для видалення шпигунських програм. Світ постійно змінюється, виявляються нові проблеми та з'являються засоби для їх вирішення. Необхідно бути в курсі того, що відбувається, оперативно реагувати на виявлені вразливості у програмах, які використовує користувач. Надійні ще вчора алгоритми шифрування завтра можуть стати під натиском обчислювальної потужності або випадково виявленої помилки. Постраждати при цьому можете не лише користувач, а й інші люди, співробітники, а також організація чи установа.

Навіть серфінг у мережі або участь, здавалося б, у безневинному опитуванні може мати дуже сумні наслідки. Кілька років тому на одному відомому розважальному сайті з'явився тест із низкою питань особистого та інтимного характеру, результат якого надсилався, всупереч очікуванням, не на вказану користувачем адресу, а безпосередньо людині, яка надіслала це посилання. Здогадатися про можливі наслідки такої ситуації неважко. Вихід

один – бути пильним та ставитись до проблеми забезпечення своєї інформаційної безпеки з усією відповідальністю.

Список використаних джерел

1. Концепція технічного захисту інформації в Україні. URL: http://zakon1.rada.gov.ua/cgibin/laws /main.cgi?nreg=1126-97-%EF.
2. Биков В. Ю, Буров О. Ю., Гуржій А. М., Жалдак М. І., Лещенко М. П., Литвинова С. Г., Луговий В. І., Олійник В. В., Спірін О. М., Шишкіна М.П. Теоретико-методологічні засади інформатизації освіти та практична реалізація інформаційно-комунікаційних технологій в освітній сфері України : монографія. Наук. ред. В. Ю. Биков, С. Г. Литвинова, В. І. Луговий. Київ: Компринт, 2019. 214 с.
3. Біленчук П. Д., Кобилянський О. Л., Малій М. І., Перелигіна Р. В., Тарасевич Т. Ю. [та ін.] Електронне суспільство. Електронне право. Кібербезпека: стратегія розвитку інноваційної ери. Монографія. За заг. ред. П. Д. Біленчука і Т. Ю. Тарасевич. Київ: УкрДГРІ, 2020. 388 с.
4. Близнюк М.М. Е-суспільство: цифрове майбутнє України: монографія / П.Д. Біленчук, М.М. Близнюк, О.Л. Кобилянський, Ю.І. Ковальчук та ін. : за ред. проф. П.Д. Біленчука. Київ: УкрДГРІ, 2018. 216 с
5. Вохидов А., Рахмонбердиева Н., Пулотов С. Цифровая безопасность (руководство для журналистов) /Под общей редакцией Каршибоева Н., Душанбе. 2015. 126 с.

ПРАВОВІ АСПЕКТИ ПРОХОДЖЕННЯ МЕДОГЛЯДІВ ПРАЦІВНИКАМИ ТРАНСПОРТНОЇ ГАЛУЗІ

Піскунова Л.Е.
к.с.-г.н, доцент кафедри Загальної екології та безпеки життєдіяльності,
Зубок Т.О.
к.с.-г.н,, доцент кафедри Охорони праці та інженерії середовища
Національний університет біоресурсів і природокористування України
м. Київ

Медичний огляд працівників проводять для того, щоб визначити стан їхнього здоров’я, можливість виконання трудових обов’язків, а також для своєчасного виявлення гострих чи хронічних професійних захворювань, встановлення у разі необхідності медичних протипоказань щодо здійснення окремих видів робіт та попередження виникнення і розповсюдження інфекційних хвороб.

Реалізація конституційного права працівників на охорону життя і здоров'я в процесі трудової діяльності, належні, безпечні і здорові умови праці визначаються і регулюються основними положеннями Закону України «Про охорону праці» від 21.11.2002 № 229-IV. Стаття 17 Закону гарантує право працівників, зайнятих на важких роботах, роботах із шкідливими або небезпечними умовами праці, на проходження попереднього медичного