Лубко Д.В.
кандидат технічних наук,
доцент кафедри комп'ютерних наук
Таврійський державний агротехнологічний університет
імені Дмитра Моторного

КОМП'ЮТЕРНА БЕЗПЕКА ТА СПОСОБИ ЇЇ ПОКРАЩЕННЯ

Анотація. *У роботі виконано огляд-аналіз інформаційної та комп'ютерної безпеки, сучасних проблем комп'ютерної безпеки та її актуальність на сьогодні. Крім цього пропонуються загальні рекомендації способів покращання комп'ютерної безпеки.*

Ключові слова: *інформаційна безпека, комп'ютерна безпека, проблеми комп'ютерної безпеки, способи покращення комп'ютерної безпеки.*

Lubko D. **Computer security and ways of its improvement.** *The work includes an overview and analysis of information and computer security, modern problems of computer security and its relevance today. In addition, general recommendations on ways to improve computer security are offered.*

Key words: *information security, computer security, computer security problems, ways to improve computer security.*

Актуальність дослідження. Актуальність проблеми кібербезпеки визначається кількома ключовими факторами, які включають в себе: зростанням кількості кіберзлочинності; збільшенням кількості кібератак; залежністю від технологій; поширеністю кібершпигунства; важливістю даних; розвитком технологій, тощо. У зв'язку з цими факторами кібербезпека залишається критично важливою проблемою в сучасному світі, і необхідно постійно працювати над її вдосконаленням та зміцненням для захисту інформації, систем та інфраструктури.

Сьогодні кібербезпеку (комп'ютерну безпеку) повною мірою можна вважати важливим аспектом діяльності будь-якого суспільства. В умовах існування інформаційного світового середовища, через складність та трудомісткість більшості процесів і методів захисту інформації та комп'ютерних систем від несанкціонованого доступу, а

також вразливість інформаційних систем до певних дій становить значну проблему для різних користувачів [2].

Метою дослідження є аналіз комп'ютерної безпеки та способів її покращання.

Виклад основного матеріалу. Розглянемо спочатку поняття інформаційної безпеки. *«Інформаційна безпека* – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через: негативний інформаційний вплив за допомогою, в першу чергу, несанкціо-нованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невчасної, невірогідної та упередженої інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням, є справедливими» [4].

Ще одне визначення, це те що інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [1].

Відокремлюють наступні рівні надання інформаційної безпеки [5]:

1. Рівень особи.
2. Суспільний рівень.
3. Державний рівень.

Спеціальне законодавство в галузі безпеки інформаційної діяльності представлено низкою законів. У їхньому складі особливе місце належить базовому закону України «Про інформацію», що закладає основи правового визначення найважливіших компонентів інформаційної діяльності [3]: інформації та інформаційних систем; суб'єктів – учасників інформаційних процесів; правовідносин виробників – споживачів інформаційної продукції; власників інформації – обробників і споживачів на основі відносин власності при забезпеченні гарантій інтересів громадян і держави.

До основних модулів інформаційної безпеки можна віднести: комп'ютерна безпека; захист персональних даних; захист помешкань; захист каналів та мереж зв'язку; захист документації (електронної, паперової); захист інших небезпечних погроз інформації (Рис.1).

Рис 1. Модулі інформаційної безпеки

Актуальність комп'ютерної безпеки на сьогоднішній день надзвичайно висока, і ця тема стає все більше актуальною через кілька важливих факторів. А саме, дана тема актуальна з наступних причин: збільшення кількості загроз; велика кількість даних в онлайні; залежність від технології; економічні наслідки; підрив критичної інфраструктури; загрози кібершпигунства та кібервійськового характеру; підвищення регулювання і вимог до захисту даних; масштабність обробки даних.

Загалом, комп'ютерна безпека стає необхідністю, оскільки без її належного забезпечення і свідомості користувачів із зростаючою кількістю зв'язків та даних в онлайн-середовищі наша інформація і системи піддаються серйозним ризикам.

Комп'ютерна безпека – це важлива галузь, яка займається захистом інформації, комп'ютерних систем та мереж від різноманітних загроз, які можуть призвести до несанкціонованого доступу, втрати даних, поширення вірусів і багатьох інших проблем. Проблеми комп'ютерної безпеки постійно еволюціонують і стають більш складними і небезпечними внаслідок швидкого розвитку IT-технологій.

Ось докладний огляд деяких основних проблем комп'ютерної безпеки:

1. *Віруси, черви і троянські коні.* Це види зловмисного програмного забезпечення, які можуть інфікувати комп'ютери та спричиняти різноманітні шкодливі дії. Вони можуть видаляти, модифікувати або

красти дані, а також завдавати шкоду апаратному забезпеченню або навіть перетворювати комп'ютери на засоби для атак на інші системи.

2. *Фішинг.* Атаки фішингу включають в себе ведення користувачів в обман, щоб отримати їхні паролі, особисті дані або фінансову інформацію, подаючи себе за легітимні джерела. Атакувачі можуть використовувати підроблені веб-сайти, електронні повідомлення та інші методи для обману користувачів і отримання їх особистої інформації, такої як паролі і кредитні дані.

3. *Витік даних.* Це може бути навмисне чи несприятливе розголошення конфіденційної інформації через помилки користувачів або атаки ззовні. Компанії та організації можуть стикатися з проблемами витоку конфіденційної інформації через несанкціонований доступ, помилкову настройку або атаки. Втрати даних можуть завдати серйозної шкоди компаніям і користувачам.

4. *Несанкціонований доступ.* Ця проблема включає в себе несанкціонований доступ до комп'ютерів і мереж, що може призвести до втрати даних або порушення конфіденційності. Це може бути результатом слабкого управління доступом, недоліків в програмному забезпеченні або психологічних атак. Також, це може стосуватися не тільки комп'ютерів, але й мережевого обладнання, смартфонів та інших пристроїв.

5. *DOS-атаки.* Атаки на доступність (наприклад, атаки з використанням відмови в обслуговуванні) можуть призвести до перегрузки системи або мережі, що призводить до недоступності для користувачів.

6. *Зловживання внутрішнім доступом.* Інсайдери можуть бути джерелом загроз для комп'ютерної безпеки, використовуючи свій внутрішній доступ для незаконних цілей.

7. *Слабкість паролів.* Багато користувачів використовують слабкі паролі або викладають їх в мережу, що дозволяє зловмисникам отримати доступ до їхніх облікових записів.

8. *Хакерські атаки.* Хакери намагаються незаконно отримати доступ до систем, мереж або даних з метою крадіжки, руйнування або витоку конфіденційної інформації.

9. *Дослідження на отримання інформації (OSINT).* Зловмисники використовують відкриту доступну інформацію, зокрема в соціальних

мережах і відкритих джерелах, для створення нападів або зловживання інформацією.

10. *Дефейс веб-сайтів та їх руйнування.* Зловмисники можуть стирати вміст веб-сайтів або внести зміни в них для поширення свого повідомлення або спричинення руйнування.

11. *Віртуальна приватність та захист особистих даних.* Зростання збору особистих даних та їх зловживання підштовхує до зростання проблем в сфері приватності та захисту цих даних.

12. *Загрози Інтернету речей (IoT).* Підключені до Інтернету пристрої можуть бути вразливими перед цифровими атаками, якщо не забезпечені відповідним захистом.

13. *Соціальна інженерія.* Це техніка, в якій атакуючий намагається отримати доступ до системи, обманюючи людей замість використання технічних засобів. Це може включати в себе телефонні атаки, відвідування та викрадання ідентифікаційних карток та інше. Зловмисники можуть використовувати психологічні методи, щоб обманювати користувачів.

14. *Атаки на веб-додатки.* Веб-додатки, такі як веб-сайти та онлайн-служби, піддаються атакам, таким як SQL-ін’єкція, міжсайтовий скриптінг (XSS) та інші. Ці атаки можуть дозволити зловмисникам отримувати доступ до баз даних або контролювати веб-сторінки.

15. *Атаки на вбудовані системи.* Вбудовані системи, такі як системи керування автомобілем, медичні пристрої та інші, також стають об’єктом атак. Уразливості в таких системах можуть мати серйозні наслідки для безпеки людей.

Забезпечення комп’ютерної безпеки – постійний процес, що вимагає поєднання технічних заходів і свідомості користувачів. Відсутність належного захисту може призвести до великих фінансових втрат, втрати довіри клієнтів та інших негативних наслідків.

Покращення комп’ютерної безпеки – це важлива задача, яка вимагає комплексного підходу та постійного удосконалення.

Способи покращення комп’ютерної безпеки:

Оновлення програмного забезпечення. Потрібно регулярне оновлення операційних систем, додатків та антивірусного програмного забезпечення є важливим. Виробники випускають патчі для усунення виявлених уразливостей.

Сильні паролі. Потрібно використовувати сильні паролі для всіх облікових записів. Це повинні бути довгі комбінації букв, цифр і символів, які важко вгадати. Краще використовувати фрази або парольні менеджери для збереження паролів.

Двофакторна автентифікація (2FA). Потрібно увімкнути 2FA для облікових записів, де це можливо. Це додає додатковий шар безпеки, оскільки для входу необхідно буде надіслати код з додатку або на електронну пошту, поза введенням пароля.

Фаєрволи. Потрібно встановити фаєйрволи на вашому маршрутизаторі та комп'ютері. Фаєрволи допомагають контролювати всі мережеві з'єднання.

Антивірусне програмне забезпечення. Потрібно встановити добре відоме та оновлене антивірусне програмне забезпечення для виявлення та блокування шкідливих програм.

Шифрування даних. Потрібно використовувати шифрування для збереження конфіденційної інформації. Шифрування дисків і передача даних поширює ступінь захисту.

Резервне копіювання даних. Потрібно регулярно створювати резервні копії важливих даних. В разі атаки або втрати даних ви зможете відновити інформацію.

Освіта користувачів. Потрібно навчати користувачів впізнавати фішингові атаки та інші загрози. Люди є слабким ланкою в безпеці, і освіта допомагає їм уникнути ризику.

Мережева безпека. Потрібно захищати свою домашню мережу налаштуванням бездротового пароля, вимикаючи функції WPS і обмежуючи доступ до підключених пристроїв.

Моніторинг активності. Потрібно використовувати інструменти для моніторингу активності на мережі і комп'ютерах. Вони допомагають вчасно виявляти незвичайні дії та атаки.

Регулярний аудит безпеки. Потрібно проводити регулярні аудити безпеки, щоб виявляти слабкі місця і уразливості, і виправляти їх.

Віртуалізація та контейнеризація. Потрібно використовувати віртуалізацію та контейнеризацію для ізоляції додатків та сервісів і встановлення обмежень на їхню діяльність.

Служба безпеки в мережі. Потрібно розглянути можливість використання спеціалізованих служб безпеки в мережі або звертайтеся до фахівців із комп'ютерної безпеки для консультацій.

Політика доступу. Потрібно встановити політику доступу для користувачів та обмежте доступ до системи лише необхідним особам.

Загальний принцип полягає в тому, щоб постійно підтримувати високий рівень уваги до комп'ютерної безпеки та вживати заходів для уникнення потенційних загроз.

Висновки. Усі приведені методи протидії погрозам комп'ютерної безпеки поодинці здатні запобігти як правило тільки визначеному виду погрози, при цьому ефективність цих засобів прямо залежить від кваліфікації обслуговуючого (працюючого) персоналу і від загального відношення до проблем безпеки на фірми. Тому, для створення ефективної системи комп'ютерної безпеки, у першу чергу, необхідна розробка комплексної політики безпеки на тому робочому місці де це потрібно. Така політика повинна містити в собі як організаційні заходи (навчання персоналу прийомам безпечної роботи, розмежування доступу до важливої і конфіденційної інформації, використання надійного парольного захисту, тощо) так і програмно-апаратні засоби захисту (наприклад використання міжмережевого екрану (firewall), серверного пакету комплексного антивірусного захисту, антивірусних моніторів та спам-фільтрів, тощо.

Література

1. Богуш В., Юдін О. Інформаційна безпека держави. Гол. ред. Шпак Ю.О. Київ: Видавництво «МК-Прес». 2005. 432 с.

2. Лубко Д. В., Шаров С. В. Розробка та використання сніферу як засобу забезпечення безпеки TCP з'єднань. *Системи обробки інформації*: Збірник наукових праць. Харківський університет Повітряних Сил імені Івана Кожедуба. 2017. Вип. 5(151). С. 138–144.

3. Лужецький В. А., Кожухівський А. Д., Войтович О. П. Основи інформаційної безпеки: навчальний посібник. Вінниця: ВНТУ. 2013. С. 9.

4. Фурашев В. Сутність та визначення понять «інформаційна безпека» і «безпека інформації». *Журнал «Правова інформатика»*. № 2(34). 2012. С. 51–59.

5. Bondar I. R. Informatsiina bezpeka yak osnova natsionalnoi bezpeky. Mekhanizm rehuliuvannia ekonomiky. Sumy. 2014. URL: http://www.lac.lviv.ua/fileadmin/www.lac.lviv.ua/data/kafedry/MEV/Bodnar/Bodnar_Vyb_Pub_9.pdf.