9. Дембіцька С. В. Охорона праці в галузі та цивільний захист: [навч. посіб.] / С. В. Дембіцька, О. В. Кобилянський. – Вінниця : ВНТУ, 2017. – 130 с.
10.Кобилянський О. В. Охорона праці в робочій професії: [навч. посіб.] / О. В. Кобилянський. – Вінниця: ВДТУ, 2001. – 127 с.
11.Захисне екіпірування із композитних матеріалів [Електронний ресурс]. - Режим доступу: http://spetsperchatka.ru/perchatki-kevlarovie/548-perchatki-kevlarovie.html
12.Кириченко В. І. Охорона праці під час виконання робіт з підвищеною небезпекою: [навч. посіб.] / В. І. Кириченко, О. В. Кобилянський. – Вінниця: Поліграф, 2004. – 140 с.

Гнатюк Андрій Констянтинович, студент групи ЕПА-17м, факультет електроенергетики та електромеханіки, Вінницький національний технічний університет, Вінниця
Хайнацький Дмитро Сергійович, студент групи ЕПА-17м, факультет електроенергетики та електромеханіки, Вінницький національний технічний університет, Вінниця

Hnatiuk Andriy K., student of the group EPA-17m, Department of electromechaniks and electricity, Vinnytsia National Technical University, Vinnytsia.
Khainatskyi Dmytro S., student of the group EPA-17m, Department of electromechaniks and electricity, Vinnytsia National Technical University, Vinnytsia.

УДК 57.011

А. О. Гоголкіна

ЗАХИСТ ДАНИХ В СФЕРІ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ

Вінницький національний технічний університет

Проаналізовано проблемні питання щодо захисту даних в сфері телекомунікаційних послуг та методи боротьби з ними.
Ключові слова: захист інформації, Wi-Fi, VPN, шифрування, загроза.

DATA PROTECTION IN TELECOMMUNICATION SERVICES

Problematic issues concerning data protection in the field of telecommunication services and methods of dealing with them were analyzed.
Keywords*:* information protection, Wi-Fi, VPN, encryption, threat.

Посилення уваги до питань захисту інформації обумовлене зростанням доступу до неї. У нинішньому інформаційному столітті нові покоління електронно-обчислювальних машин з'являються з надзвичайною швидкістю. Збільшується пам'ять машин, змінюється їх структура й операційна система. Творці нової обчислювальної техніки намагаються за певними параметрами суміщати нову техніку із застарілою. Зазначимо, що операційні системи завжди відрізнялися недосконалістю та складністю своєї документації. Навіть найпоширеніша операційна система Windows, не зважаючи на регулярне відновлення, не позбавлена помилок. Це викликає особливу тривогу, тому що сучасна індустрія досить сильно залежить від роботи комп'ютерної мережі. Ситуація ускладнюється ще й зростанням кількості витончених вірусних атак[1].

На даний час досить актуальним є питання захисту та шифрування даних, адже здебільшого вся інформація знаходиться в електронному вигляді.

Для гарантованої безпеки функціонування інформаційної мережі застосовуються різні протоколи шифрування конфіденційної інформації, електронні підписи, здійснюється сертифікація інформації. Заборона на несанкціоноване переміщення даних між локальною мережею міжнародної компанії та глобальною мережею може забезпечуватися спеціальними комп'ютерами або програмами [2].

Є багато різних методів для боротьби з перехопленням цифрових даних. Основні з них розглянемо нижче.

Багато з нас користуються громадським Wi-Fi , не підозрюючи, що це легкий спосіб перехоплення даних. Просто потрібно не користуватися громадським Wi-Fi. На жаль, всі ми знаємо, що часом без нього обійтися не можна. У таких випадках віддавайте перевагу Wi-Fi з паролем. Хоча закрита точка – не завжди безпечна. Тому при підключенні перевіряйте, чи існують серед доступних точки-клони. Якщо існують, є ризик того, що одна з них створена зловмисником.

Якщо Ви пересилаєте через громадську точку доступу будь-які конфіденційні дані, обов'язково зашифруйте інформацію. В цьому Вам можуть допомогти окремі сервіси шифрування текстів чи безпечні месенджери, наприклад Telegram. Нещодавно шифрування посилив і месенджер WhatsApp. У браузері переконайтеся, що використовуєте зашифроване з'єднання. В адресному рядку таке з'єднання підписано як HTTPS.

Відмінний варіант захисту від перехоплення – використання віртуальної приватної мережі (VPN). Якщо у Вас налаштований власний VPN-тунель, наприклад, провідний до домашнього ПК, то спроби перехопити дані на цьому маршруті будуть для хакера безперспективними. Якщо особистого VPN у Вас немає, можна скористатися сервісами, які його надають. Зазвичай, це коштує грошей, оскільки тунель здається користувачеві в оренду. Проте, є і безкоштовні рішення. Наприклад, сервіси Cyber Ghost або HotspotShield дають безкоштовний VPN з обмеженою швидкістю доступу. А ось Tor для проведення онлайн-платежів або пересилання чогось конфіденційного використовувати не рекомендується. Це, в першу чергу, анонімайзер, а не засіб підвищення приватності. Тобто, дані в ньому перехопити можуть, але не можуть зрозуміти, звідки ці дані[3].

Порушниками охорони інформації, насамперед, виявляються користувачі і робітники інформаційної системи, які мають до неї доступ. Основними причинами порушення захисту інформації є: безвідповідальність, самовпевненість і корисливий інтерес персоналу. За даними статистики, 81,7 % порушень допускається службовцями компанії, які мають доступ до інформаційної системи, і тільки 17,3 %- сторонніми особами (у тому числі 1 % припадає на випадкових осіб). Отже, головне джерело порушень безпеки інформації знаходиться всередині самих інформаційних систем, тож для будь-якої з них внутрішній захист має бути обов'язковим[4].

Однією з найбільших загроз інформаційних систем є ураження вірусними програмами, що проникають через різні носії інформації, особливо через глобальні інформаційні мережі. За словами Володимира Тихонова, спеціаліста служби консалтингу "Лабораторії Кас-перського", у 2006 році було зафіксовано 7 великих вірусних епідемій. Епідемії 2006 року він ділить на такі групи: черв'як, черв'яки сімейств Baie та Warezov, серед яких багато поштових черв'яків, а також варіант троянця-шифрувальника Єрсосіе. У 2006 році з'явилось біля 60 тис. нових вірусів, що на 41 % більше, ніж у 2005 році[5].

Оператори мережі та постачальники послуг повинні вжити всіх належних технічних і організаційних заходів для того, щоб забезпечити фізичну і програмну безпеку мережі, послуг і даних, які вони збирають і обробляють, та унеможливити будь-яке несанкціоноване втручання або перехоплення комунікаційних повідомлень[6].

Абоненти телекомунікаційних послуг повинні бути проінформованими про ризики зламу безпеки мереж та про спосіб, у який вони можуть обмежити ризики безпеки для своїх повідомлень[7].

Таким чином, захист інформації в наш час Є нагальною потребою не лише для великих фірм, а й для звичайних людей.

У цілому всі названі і багато інших проблем можуть бути вирішені тільки в результаті створення нормально функціонуючої національної системи технічного захисту інформації. Розвиток і становлення такої системи може бути реалізовано тільки шляхом об'єднання зусиль різних міністерств, відомств, організацій, установ, підприємств, а також зусиль провідних вчених, інженерів і практиків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України № 2594-IУ від 31 травня 2005 р. "Про внесення змін до Закону України "Про захист інформації в автоматизованих системах" // Відомості Верховної Ради України. — 2005. — № 26. — Ст. 347.

2. Закон України № 80/94 — ВР від 5 липня 1994 р. "Про захист інформації в інформаційно-телекомунікаційних системах" // Відомості Верховної Ради України. — № 31. — 1994. — Ст. 286.

3. Системи оброблення інформації Розроблення систем. Терміни та визначення: ДСТУ 2941-94. — К: Держстандарт України. — 1995. — 20 с.

4. Системи оброблення інформації Основні поняття. Терміни та визначення: ДСТУ 2938-94. — К: Держстандарт України, 1995. — 32 с.

5. Закон України "Про інформацію" № 267 від 2 жовтня 1992 р. // Відомості Верховної Ради України. — № 48. — 1992 — Ст. 650.

6. Закон України "Про Концепцію Національної програми інформатизації" № 228-ІУ від 4 лютого 1998 р. // Відомості Верховної Ради України. — № 27 — 28. — Ст. 182.

7. Закон України № 74/98 від 4 лютого 1998 р. "Про Національну програму інформатизації" // Відомості Верховної Ради України. — № 27-28. — Ст. 181.

Гоголкіна Анастасія Олександрівна - студентка групи ТКС-17мі, факультет інфокомунікацій, радіоелектроніки та наносистем, Вінницький національний технічний університет, Вінниця, e-mail: tknastya@ukr.net

Науковий керівник: ***Томчук Микола Антонович***, кандидат технічних наук, доцент кафедри Безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, Вінниця, e-mail: tomchuk.mykola@gmail.com

Gogolkina Anastasia A., – student of the group TKC-17mi, the faculty of Infocommunications, electronics and nanosystems, Vinnytsia national technical University, Vinnytsia, e-mail: tknastya@ukr.net

Supervisor: ***Tomchuk Mykola A.***, Cand. Sc. (Eng.), Assistant Professor of Department of Health and Safety Studies, Vinnitsa National Technical University, Vinnytsia, e-mail: tomchuk.mykola@gmail.com