УДК 004.492.3

Микита Андрійович Єременко,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Метод двофакторної автентифікації як засіб боротьби з шахраями в мережі інтернет

Завдяки розвитку мережі Інтернет, глобального покриття бездротовими мережами, а також збільшенню їх швидкості, кількість користувачів мережі Інтернет значно зростає кожного року. В Україні, за даними дослідження, станом на 2019 рік проживає 25,6 мільйонів Інтернет-користувачів, що складає 58% всього населення [1].

У наш час, майже у кожного користувача банківських послуг є доступ до онлайн-банкінгу, а деякі навіть зберігають увесь свій капітал на банківських рахунках до яких є доступ через мережу Інтернет. У вересні 2019 року обсяг грошей на гривневих рахунках в українських банках виріс на 3,1% – до 571,8 млрд грн [2]. Люди зберігають більше 290,78 млрд грн на своїх поточних банківських рахунках, до яких є доступ за допомогою Інтернет-банкінгу або мобайл-банкінгу [3]. У 2019 році зареєстровано близько 6000 злочинів, скоєних в сфері використання високих інформаційних технологій. З них майже тисяча – злочини, скоєні в сфері кібербезпеки [4]. Для захисту від несанкціонований доступу до банківського акаунту через Інтернет або мобільний банкінг передбачено багато систем ідентифікації користувача. Ці системи забезпечують достатній захист від доступу шахраїв, але зазвичай вони не включені без завдання. Для значного зменшення можливості кібератак шляхом фішингу, брутфорсу, соціальної інженерії та ін. дієвим рішенням стане встановлення двофакторної автентифікації.

Двофакторна автентифікація – це різновид багатофакторної автентифікації, яка полягає у підтвердженні особистості користувача за допомогою двох, незалежних один від одного, факторів. Першим фактором зазвичай є пароль або PIN-код[5].

Розглянемо існуючі фактори автентифікації:

1) знань – що знає користувач (ПІН, пароль, кодове слово, відповідь на секретне питання і т. д.);

2) власності – що належить користувачеві (ключ, паспорт, смарт-картка, маркер безпеки, USB флеш, смартфон та інший мобільний пристрій);

3)біометрії – це частина користувача (відбитки пальців, райдужна оболонка, голос, геометрія обличчя);

4) розташування – місцеперебування людини (наприклад, IP-адреса або супутникова навігаційна система);

5) часу – певний період часу під час якого ви можете увійти в систему.

Двофакторна автентифікація у багатьох сучасних сервісах встановлена за замовчуванням. На великій кількості криптогаманців її неможливо вимкнути.

Багато людей вже стикалися з двофакторною перевіркою, наприклад, коли користувач спробує увійти у свою сторінку в соціальній мережі з іншого комп'ютера або телефону і в цей момент, служба, підозрює, що це спроба несанкціонованого доступу, та вимагає у користувача ввести код, який був надісланий на телефон.

Слід розуміти, що двофакторона автентифікація це не завжди гарантія повної безпеки. Є досить багато методів взлому двофакторної автентифікації, деякі з них складні і дорогі,а деякі достатньо примітивні.

Розглянемо найбільш вживані методи взлому:

1. Соціальна інженерія – маніпулювання людьми через виконання дій, або розголошення конфіденційної інформації іншим способом, ніж як через засоби технічного руйнування баз даних[6].

2. Фішинг – вид шахрайства побудований на надсиланні листа, ніби від банку чи іншої установи, в якому міститься посилання де пропонується ввести код двофакторної автентифікації чи надати біометричні данні.

3. Перехоплення смс чи дзвінка з кодом підтвердження – код автентифікації надходить до телефону користувача він перенаправляється на пристрій зловмисника.

4. Використання cookies-файлів – заволодіння cookies-файлами жертви та подальше їх використання. В cookies-файлах зберігається ідентифікаційна інформація. На багатьох ресурсах за наявністю cookies користувачу не потрібно вводити пароль чи код двофакторної автентифікації.

5. Крадіжка, підробка приладу чи іншого фактору автентифікації – метод який найчастіше використовується для обходу двофакторної автентифікації. Це може бути крадіжка телефону, ключ-картки, також можлива підробка біометричних даних людини.

В результаті аналізу були розглянуті методи двох факторної автентифікації, як засіб боротьби з шахраями в мережі інтернет. Був проведений порівнювальний аналіз найпопулярніших факторів та методів автентифікації.

В результаті роботи, було виявлено, що найбільш безпечний фактор це біометрія. Біометрія завжди знаходиться поряд зі користувачем і її важко викрасти. Її можливо підробити, але це достатньо складний процес яких потребує великих фінансових вкладань. Потрібно розуміти, що двофакторна автентифікація не забезпечує стовідсоткового захисту, але є найкращім засобом для запобігання несанкціонованого входу. Для більшої безпечності можливо встановити багатофакторну автентифікацію. Вона перевіряє одночасно три чи більше факторів. Тому для значного зменшення вірогідності несанкціонованого входу до особистих кабінетів з важливою інформацією, таких як онлайн чи мобайл банкінг, електронна поштова скринька, соціальні мережі, онлайн-кабінети різних фінансових організацій, потрібно використовувати усі вбудовані в ці системи засоби захисту, особливо багатофакторну автентифікацію. Розуміння принципів механізмів, недоліків і вразливостей роботи двофакторної автентифікації значно полегшать правоохоронним органам процес ідентифікації зловмисника, а також дасть змогу отримати доступ до їх акаунтів.

Список бібліографічних посилань

1. У 2018 інтернет-користувачів стало 4 млрд, з них понад 3 млрд користуються соцмережами – дослідження // hromadske : сайт. URL: https://hromadske.ua/posts/u-2018-internet-koristuvachiv-stalo-4-mlrd-z-nih-ponad-3-mlrd-koristuyutsya-socmerezhami-doslidzhennya (дата звернення: 08.10.2019).
2. В НБУ сообщили, сколько денег держат украинцы в банках // delo.ua : сайт. 10.10.2019. URL: https://delo.ua/econonomyandpoliticsinukraine/v-nbu-soobschili-skolko-deneg-derzhat-ukraincy-v-359118/ (дата звернення: 08.10.2019).

3. Сколько денег украинцы держат в банках (инфографика) // finance.ua : сайт. 23.10.2019. URL: https://news.finance.ua/ru/news/-/458606/skolko-deneg-ukraintsy-derzhat-v-bankah-infografika (дата звернення: 08.10.2019).
4. Кибератаки на Украину и разоблачение хакеров: полиция подвела итог за год. URL: https://www.segodnya.ua/ukraine/kiberataki-na-ukrainu-i-razoblachenie-hakerov-policiya-podvela-itog-za-god-1199708.html (дата звернення: 09.10.2019).
5. Двухфакторная аутетификация // ITpedia : сайт. URL: https://ru.itpedia.nl/2018/09/10/two-factor-authenticatie-2fa/ (дата звернення: 10.10.2019).
6. Немного о 2FA: Двухфакторная автентификация // habr : сайт. 25.02.2016. URL: https://habr.com/ru/company/1cloud/blog/277901/l (дата звернення: 10.10.2019).
7. Демчук В. П. Соціальна інженерія: виклики та перспективи боротьби в українському контексті // Українське право : сайт. 01.11.2017. URL: https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_demchuk_Social_engineering_perspectives_of_the_struggle_in_ukrain/ (дата звернення: 10.10.2019).

Одержано 25.10.2019