УДК 004.056

І. А. Смоляк

ЮРИДИЧНІ АСПЕКТИ ВИКОРИСТАННЯ HONEYPOT

Вінницький національний технічний університет

Анотація

Проаналізовано використання програмних засобів під назвою "Honeypot" в аспектах юридичних ризиків з однієї сторони для особи яка застосовує такі засоби, так і для особи, яка здійснює "напад" на останні. Двояка природа таких інструментів залишає сіру зону межі відповідальності для осіб, які здійснюють захист інформації.

Ключові слова: захист інформації, доступ, honeypot, відповідальність.

Abstract

The use of Honeypot in terms of legal risks on the one hand for the person applying such means and for the person who carries out the "attack" on the latter is analyzed. The dual nature of such tools leaves a gray area of responsibility for persons engaged in the protection of information.

Keywords: information protection, access, honeypot, responsibility.

Вступ

У комп'ютерній термінології Honeypot - це механізм комп'ютерної безпеки, встановлений для виявлення, відхилення або, певним чином, протидії спробам несанкціонованого використання інформаційних систем. Як правило, Honeypot складається з даних (наприклад, на мережевому сайті), які, здається, є законною частиною сайту, яка містить інформацію або ресурси, що представляють цінність для зловмисників. Він фактично ізольований, контрольований і здатний блокувати або аналізувати зловмисників [1]. Інформаційна система, і Honeypot, як можлива частина такої системи, повинна мати певні засоби захисту, оскільки таким чином забезпечується схоронність, цілісність та певні фактичні межі такої мережі, що особливо важливо в юридичному аспекті.

Результати дослідження

У Вітчизняному законодавстві за із несанкціонованого доступу в інформаційну систему передбачається адміністративна та кримінальна відповідальність, тобто за здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем (ст. 212-6 Кодексу про Адміністративні правопорушення [2]), та за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 Кримінального кодексу України [3]).

Проаналізувавши вищевказані статті, можна зробити висновок, що в їх диспозиціях містяться фрази "незаконний доступ" та "несанкціоноване втручання". Тому інформаційним системам для того, щоб бути під охороною закону потрібно мати статус закритої.

Такі програмні інструменти, як Honeypot існують у формі або частини існуючої системи, або самостійної спеціально створеної системи для того, щоб потенційні зловмисники зміщували свій акцент саме на останній спеціальних системах, а не реальних. Іншими словами використовуючи Honeypot, відбувається умовне "заманювання" потенційних зловмисників, для того, щоб або отримати доступ до такої віртуальної системи, рівень захисту якої значно нижчий ніж в реальній системі, або взагалі відсутній.

З іншої сторони програмні інструменти Honeypot все ж таки є частиною реально існуючої інформаційної системи того, хто задіяв зазначений інструмент захисту, а також хто бажає здійснювати виявлення, моніторингу, захисту та протидії потенційних загроз. В даному випадку Honeypot є частиною реальної інформаційної системи, а тому відсутність елементів захисту в Honeypot, що було зроблено спеціально, означає відсутність захисту реальної інформаційної системи, а тому потенційні зловмисники безперешкодно "увійшовши" до реальної інформаційної системи через спеціально створені відкриті канали Honeypot, не будуть нести відповідальність за такі дій.

Адже, для об'єкта посягання в розумінні чинного законодавства повинен бути елемент закритості інформаційної системи, тобто володілець такої системи повинен здійснити дії із захисту інформації,

яка міститься в такій системі. Про це також вказує ст.21 Закону України “Про інформацію”[4], відповідно до якої конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень, а також інформація, визнана такою на підставі закону. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом.

Висновки

Отже, використання програмних засобів Honeypot покладає додаткову відповідальність за схоронність конфіденційної інформації на осіб, що використовують такі інструменти в рамках своєї інформаційної системи, а також добавляє потенційні ризики стосовно позбавлення можливості захистити свої права у законний спосіб. Тому, потенційні користувачі Honeypot повинні розуміти повний обсяг складності технічної сторони існування сукупності реальної інформаційної системи та Honeypot.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cole, Eric; Northcutt, Stephen. "Honeypots: A Security Manager's Guide to Honeypots".

2. Кодекс України про адміністративні правопорушення: Кодекс України, Кодекс, Закон від 07.12.84 № 8074-10, // Відомості Верховної Ради України (ВВР), 1984, додаток до № 51, ст. 1123. URL: https://zakon.rada.gov.ua/laws/main/80731-10.

3. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III // Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст. 131. URL: https://zakon3.rada.gov.ua/laws/show/2341-14/page9.

4. Закон України “Про інформацію”, Закон, Закон України від 2.10.1992 № 2657-XII // Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

Смоляк Ігор Анатолійович — студент групи 1КІТС-22м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: igor14smolyak@gmail.com

Smolyak Igor A. **–** student of 1CSITS-22m group Department of Management and Information Security, Vinnytsa National Technical University, Vinnytsia**,** e-mail: igor14smolyak@gmail.com