Pedaqoji Universitetin Xəbərləri. Riyaziyyat və təbiət elmləri seriyası – 2022, C. 70, №4, s. 23-28
Transactions of Pedagogical University. Series of mathematics and natural sciences – 2022, V. 70, №4, pp. 23-28

UOT 004

S.Ə.Şabanova
Azərbaycan Dövlət Pedaqoji Universiteti
sevinc65@mail.ru

İNFORMASİYA TƏHLÜKƏSİZLİYİ MƏSƏLƏLƏRİ HAQQINDA

Açar sözlər: *kibercinəyatkarlıq, kibermәkan, informasiya təhlükəsizliyi, internet, kiberhücum, haker, şifrələmə, vayper, bitkoin, kriptoqraf*

Kibermәkanda cinayətkarlıq informasiya-kommunikasiya texnologiyalarının inkişafı ilə əlaqədar son illər beynəlxalq ictimaiyyətin üzləşdiyi ən çətin problemlərdən biridir. Məqalədə qlobal informasiya şəbəkələrində baş vermış məhşur kibercinayətlər araşdırılır, bu cinayətlərin fenomenoloji aspektləri təhlil edilir, kibercinayətkarlıqla mübarizədə beynəlxalq əməkdaşlığın perspektiv istiqamətləri müəyyən edilir.

С.А.Шабанова

ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ключевые слова: *киберпреступность, киберпространство, информационная безопасность, интернет, кибератака, хакер, шифрование, шифрование, биткойн, криптограф*

Преступность в киберпространстве является одной из самых сложных проблем, с которыми сталкивается международное сообщество в последние годы в связи с развитием информационных и коммуникационных технологий. В статье рассматриваются известные киберпреступления, произошедшие в глобальных информационных сетях, анализируются феноменологические аспекты этих преступлений, определяются перспективные направления международного сотрудничества в борьбе с киберпреступностью.

S.A.Shabanova

ABOUT INFORMATION SECURITY ISSUES

Keywords: *cybercrime, cyberspace, Information security, internet, cyber attack, hacker, encryption, wiper, bitcoin, cryptographer*

Crime in cyberspace is one of the most complex problems faced by the international community in recent years due to the development of information and communication technologies. The article examines well-known cybercrimes that occurred in global information networks, analyzes the phenomenological aspects of these crimes, and identifies promising areas of international cooperation in the fight against cybercrime.

İnformasiya müasir dünyada cəmiyyətin inkişafının ən mühüm komponentidir. Postindustrial cəmiyyətin informasiya cəmiyyətinə çevrilməsi o deməkdir ki, informasiya qloballaşır, həm şəxsən bir insan üçün əhəmiyyətli olur, həm də dövlət və bütövlükdə cəmiyyət üçün. Hər kəs qanuni yollarla məlumat axtara, qəbul edə, ötürə, istehsal edə və yaya bilər. İnformasiya axınına heç bir sərhəd yoxdur. Hazırda informasiya ən mühüm dəyərlərdən biri kimi qəbul edilir. Müvafiq olaraq, onun müdafiəsi, onu qəbul etmək və ötürməkdən daha az vacib olmayan fəaliyyət növüdür.

Qloballaşma tendensiyaları gücləndikcə onun əmələ gətirdiyi problemlər daha aydın görünür. Qloballaşma proseslərinin yaratdığı mənfi təzahürlərə, o cümlədən transmilli kibercinayətlərə qarşı mübarizədə dünya miqyasında bütün hüquqi sistemlərin aktivləşməsi mühüm məsələlərdən biridir.

Kibercinayətkarlıq probleminin qlobal mahiyyətini başa düşmək çox vacibdir. Belə ki, kiberhücumlar artıq təkcə özəl şirkətlərin deyil, həm də həm də dövlət orqanlarının işini iflic edir. Dünyada elə bir dövlət yoxdur ki, bu cür hücumlara məruz qalmasın. Kibertəhlükələrin mümkün mənbələri təkcə hakerlər və ya onların qrupları deyil, həm də ayrı-ayrı dövlətlər, terrorçu, cinayətkar qruplar hesab olunur.

Məqaləmizdə dünyada baş verən ən məhşur kiberhücumlar və onların törətdiyi fəsadlardan nümunə gətirmişik.

1. İlk kibersilah: nüvə hücumu STUXNET (2009)

Stuxnet əvvəlcə İranın nüvə obyektlərinə hücum üçün nəzərdə tutulmuşdu. Özündə nüvə obyekti üçün layihə məlumatlarını və uranın zənginləşdirilməsi prosesi haqqında məlumatları cəmləyir. **Stuxnet** iki cür məhv edir:

1) uranın zənginləşdirilməsi sentrifuqalarında təzyiqi artırır və bu da olduqca ciddi ziyan vura bilər.

2) rotorun fırlanma sürətini idarə edir. Bu cür manipulyasiyaların dağıdıcı təsiri daha az olur. Lakin düşmən dövlətin nüvə proqramının inkişafını daim ləngitmək və eyni zamanda özünün mövcudluğunu aşkara çıxartmamaq üçün bu varianta daha üstünlük verilir.

ABŞ-İsrail tərəfindən yaradılmış **Stuxnet** bu variantdan istifadə edir. Mütəxəssislərin fikrincə, virus proqramın işlənməsini təxminən 2 il gecikdirib. **Stuxnet** bütün sentrifuqları bir anda məhv edərdisə, onu bərpa etmək də təxminən eyni vaxt aparacaqdı.

Beləliklə, **Stuxnet** düşmən nüvə obyektlərini məhv etmək üçün nəzərdə tutulmuş **ilk kiber silah** sayıla bilər.

2. Ən əyani hücum «Sındırılmış» cip (2015)

Endi Qrinberq Jeep Cherokee-ni təxminən 110 km/saat sürətlə idarə edərkən avtomobildə nəsə nasazlıq yaranır. Kondisioner sistemi birdən-birə tam gücü ilə soyuq hava üfürməyə başlayır, radio özünü işə salıb hip-hop çalır,

şüşəsilənlər var gücü ilə şüşənin üzərində hərəkət edir, kapotun ucluqlarından su fışqırır və multimedia sisteminin ekranında Endinin yaxşı tanıdığı iki hakerin - Çarli Miller və Kris Valasekin şəkli peyda olur. (https://www.youtube.com/watch?v=MK0SrxBC1xs). Miller və Valasek Cherokee-ni sındıra bildilər və o İnternet vasitəsilə uzaqdan idarə olundu. Bu prosesi əvvəlcədən razılaşma ilə maşının sahibinə mümkün qədər aydın şəkildə nümayiş etdirdilər.

Uzaqdan idarəetmə təkcə musiqini dəyişmək deyil, həm də əyləcləri söndürmək, sükanı çevirmək və qaza basmaq deməkdir: Endi də bütün bunları yaşadı. Hakerlər jurnalisti öldürmək istəsəydilər, bunu asanlıqla həyata keçirə bilərdilər. Bu hadisə 1,4 milyon avtomobilin geri çağrılmasına səbəb oldu.

3. Ən iri miqyaslı kiberhücum: Yahoo (2013-16)

İnternet nəhəngi Yahoo sındırılır və 3 milyard hesab oğurlanır. Sanki Yer kürəsinin demək olar ki, hər ikinci sakininin hesabı oğurlanıb. Əslində, bu, bir yox, iki hücum idi: 2016-cı ilin sentyabrında Yahoo etiraf etdi ki, hələ 2014-cü ildə hakerlər 500 milyon hesaba giriş əldə ediblər, daha sonra, dekabrda boynuna alır ki, 2013-cü ildə daha bir milyard istifadəçinin hesabı sındırılmışdı. Bir az sonra, 2017-ci ildə o, bunun bir milyard deyil, bir az daha çox olduğunu etiraf etdi: cəmi 3 milyard.

2013-cü ildə Yahoo-nu kimin sındırdığı müəyyən edilməmişdir. Lakin 2014-cü ildəki haker hücumuna görə ABŞ Ədliyyə Nazirliyi iki FSB zabitini və Rusiya və Kanadadan olan iki hakeri günahlandırdı. Dörd nəfərdən yalnız kanadalı haker Kərim Baratov günahını boynuna alıb və hazırda hakerliyə görə 5 il həbs cəzası çəkir. (https://finans.az/xeber/yahoo-hesablarini-ogurlayan-xakere-hebs-cezasi-verildi.html)

Bu hücumdan ən çox müxtəlif hesablar üçün eyni paroldan istifadə edənlər zərər çəkib – onların bir çoxunun təkcə poçtu deyil, digər hesabları da əllərindən alınıb. Hər yerə eyni parolu qoymamaq üçün bir səbəb lazım idisə, bu ən yaxşı səbəbdir.

4. Ən qəfil hücum: Dyn-ə qarşı DDOS

21 oktyabr 2016-cı il səhəri dünya "İnterneti sındırmağın" nə demək olduğu ilə tanış oldu: Twitter və Netflix-dən Amazon və Reddit-ə qədər çoxlu xidmətlər artıq mövcud deyildi. ABŞ-ın yarısı internetin artıq olmadığını bildi. Bəziləri üçün hər şey olduqca yavaş işləyirdi, bəziləri üçün, o cümlədən Avropa və Rusiyada ümumiyyətlə işləmədi. İnternet bir neçə saat "yatır" - və bunun səbəbi tarixdə ən böyüklərdən biri olan DynDNS (Dynamic DNS) provayderinə bir sıra DDOS (distributed denial-of-service − paylanmış xidmətdən imtina) hücumları idi.

5. İnsanların həyatını itirdiyi hücum: Ashley Madisson

Tanışlıq saytları evli kişilər və evli qadınlarla doludur. Vaxtilə belə insanlar üçün xüsusi sayt yaradılmışdı - Ashley Madison. 2015-ci ildə bu sayt

sındırıldı. O vaxta qədər saytda 40 milyona yaxın insan qeydiyyatdan keçmişdi. Yahoo və ya LinkedIn standartlarına görə rəqəm çox azdır, lakin hücumun təsiri dəhşətli idi. Əvvəlcə verilənlər bazasına giriş əldə edən hakerlər ondan özləri şantaj üçün istifadə edib, sonra ictimailəşdirib - elektron poçt ünvanları ilə axtarış imkanı veriblər. Bir çox istifadəçi "həyat yoldaşınızı kimlə və harada aldatdığınız barədə hər şeyi bilirəm və mənə 1000 dollar ödəməsəniz hər şeyi dərc edəcəm" kimi məzmunlu e-məktublar alır. Tanınmış yüksək rütbəli məmurlar və iş adamları məsələsində - bələləri də var idi - təbii ki, məbləğ artır. Bu sızma səbəbiylə boşanan evliliklərin sayını heç kim saymadı, amma onların çox olduğu aydındır. Mütləq onlarla, hətta yüzlərlə, bəlkə də minlərlə. Ola bilsin ki, bu cütlüklər onsuz da boşanacaqdılar, lakin sızma insanları hərəkətə keçməyə sövq edir. Daha da pisi, bu, bir neçə insanın həyatına son qoydu: utancın öhdəsindən gələ bilməyən və öz canlarını almaq qərarına gələnlər də var idi. Ashley Madison bu günə qədər fəaliyyətini davam etdirir.

6. **Ən qaranlıq hücum: Black Energy elektrikə qarşı**

23 dekabr 2015-ci il soyuq qış günü saat 15:30-da Ukraynanın İvano-Frankovsk şəhərində işıqlar qəfil sönür. Sovet adamları bu işə öyrəşiblər, amma burada hər şey bir az qeyri-adi idi: 30 yarımstansiya eyni vaxtda sıradan çıxır, 230 minə yaxın insan bir anda işıqsız qalır. Yarımstansiya operatorları tamamilə mistik hadisələri müşahidə edirlər: mausun kursoru birdən ekranda sürüşərək releni idarə edən proqramı işə salır və yarımstansiyanı söndürərək dövrəni açır. "Prikarpatyeoblenergo" şirkətinin operatoru onu dayandırmağa çalışdıqda, o, sadəcə olaraq sistemdən atılır.

Oxşar hadisələr, lakin daha kiçik miqyasda, elektrik təchizatı üçün məsul olan daha iki şirkətdə - Kiyevoblenergo və Chernovtsioblenergoda baş verdi. İvano-Frankovsk vilayətinin bəzi yerlərində elektrik enerjisinin verilməsi yalnız 6 saatdan sonra bərpa edilir.

Mütəxəssislər hesab edir ki, hücumu Black Energy və Sandworm kimi tanınan hakerlər qrupu həyata keçirib. Bəziləri isə bunun bədnam rus hakerlərinin işi olduğuna əmindirlər.

7. **Ən səs-küylü hücum: WannaCry epidemiyası**

Bir çox ekspertlər razılaşırlar ki, WannaCry qurdunun yaradıcısı onu sınaq mühitində saxlaya bilməyib və nəticədə tamamlanmamış şifrələmə qurdu İnternetə daxil olub, bütün kompüterləri fərq etmədən vuraraq, Windows-dakı boşluq vasitəsilə onlara nüfuz edib və şifrələyib. Daha sonra domino effekti kimi bütün kompüterlərə yayılıb. Adi kriptoqraflar həmişə seçim təklif edirlər: pul ödəyin - məlumatı qaytara bilməniz üçün sizə şifrələmə kodu göndəriləcək. WannaCry də bu seçimi təklif etdi. Yalnız faylların şifrəsini açmaq mümkün olmadı. Ya bu koddakı səhv idi, ya da WannaCry internetə qoşulmuş bütün kompüterlər üçün dağıdıcı silah kimi planlaşdırılmışdı.

Epidemiya ən heyrətamiz şəkildə dayandırıldı. Malwaretechblog kimi

tanınan gənc tədqiqatçı Marcus Hutchins, dünyanın bir çox digər tədqiqatçıları kimi WannaCry-dən necə qorunmalı, onun necə yayıldığını, faylların şifrəsini açmaq mümkün olub-olmadığını və s. anlamaq üçün onu təhlil etməyə tələsdi. O aşkar etdi ki, diski şifrələməzdən əvvəl zərərli proqram nədənsə İnternetdə mövcud olmayan hansısa domenə müraciət edir. "Bu domeni qeydiyyatdan keçirsəm nə olacaq?" – deyə Hutchins düşünür. Və qeydiyyatdan keçirir. Bundan sonra zərərli proqram artıq heç nə etmir: yayılması dayandırılmasa da, artıq diskləri şifrələmir.

8. **Ən bahalı hücum: NotPetya/ExPetr Epidemiyası**

Əslində, WannaCry hekayəsi təkrarlandı, amma yenə də tədqiqatçılar bu hücumu birincisindən çox fərqli hesab edirlər. WannaCry daha çox təbii fəlakət hesab edilirsə, NotPetya hədəflənmiş hücumdur. Bunun Ukraynaya yönəldiyinə dair bir fikir var - kimsə Ukrayna şirkətlərinin əhəmiyyətli bir hissəsinin sənəd idarəetməsi və vergi hesabatları üçün istifadə etdiyi M.E.Doc proqramı üçün yeniləmə paketini yoluxdurur. Bir çox Ukrayna təşkilatlarındakı proqram yeniləməni avtomatik olaraq yükləyir - və bu da bütün Windows istifadəçilərinin kompüterlərinin şifrələnməsinə gətirib çıxarır. Lakin məsələ bununla bitmir. NotPetya epidemiyası Rusiyaya, Avropaya və onun hüdudlarından kənara, nəticədə bütün dünyaya yayılır. Bir çox iri şirkətlərə, o cümlədən ən böyük dəniz daşıyıcılarından biri olan Maersk-ə çox ciddi zərbə vurur.

Bir-birinin ardınca kompüter monitorları qaralır və tipik bir mesaj nümayiş etdirilir: "bitcoin ekvivalentində 300 dollar ödə, biz məlumatlarınızı deşifrə edək". Ancaq WannaCry vəziyyətində olduğu kimi ödəniş etmək faydasız olur: NotPetya məlumatları geridönməz şəkildə şifrələyir, yəni antivirus mütəxəssislərinin təsnifatında o, artıq şantajçı deyil, vayper (gürzə) idi. Əsas fərq ondan ibarətdir ki, şifrələyicilər kiçik cinayətkarlar tərəfindən mənfəət əldə etmək üçün istifadə edilən silahdır, vayperlər isə daha çox ziyan vurmaq üçün daha böyük balıqların, hökumətlərin və ya korporasiyaların silahlarıdır.

NotPetya böyük miqdarda ziyan vurdu. Maersk öz itkilərini 370 milyon dollar, FedEx 400 milyon dollar, əczaçılıq nəhəngi Merck & Co 600 milyon dollar qiymətləndirir.

Ümumilikdə 10 milyard dollardan çox ziyan vuran NotPetya ən bahalı maddi ziyanverici kimi tarixə düşür.

Kibercinayətlərin bütün mürəkkəbliyini və təhlükəsini nəzərə alaraq qanunvericilərin, hüquqşünasların və əlbəttə ki, kibercinayətlərə qarşı mübarizəyə yönəlmiş kompüter informasiya texnologiyaları sahəsi üzrə mütəxəssislərin birgə fəaliyyətini inkişaf etdirmək lazımdır.

Həm milli, həm də beynəlxalq normativ aktların tətbiqi ilə mübarizə problemin həlli istiqamətində atılan addım olaraq bəs etmir. İnformasiya texnologiyaları və proqram təminatı sahəsində xüsusi biliyə malik olan mütəxəssislər yetirmək lazımdır.

Bunun üçün universitetlərdə bu sahə üzrə olan proqramlar yenilənməli, lazım gələrsə yeni fənlər tədris olunmalıdır. Yaxşı olardı ki, orta məktəb kursundan başlayaraq şagirdlərdə informasiya təhlükəsizliyi problemlərinə maraq və onların bu sahə üzrə minimum bilik əldə etmələrinə şərait yaradılsın.

ƏDƏBİYYAT

1. *Schjolberg Stein.* A cyberspace treaty — A United Nations convention or protocol on cybersecurity and cybercrime. Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Salvador, Brazil, 12–19 April 2010. Available at: http://cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf.
2. *Sachkov D.I., Smirnova I. G.* Obespechenie informatsionnoi bezopasnosti v organakh vlasti [Ensuring Information Security in the Bodies of Power]. Irkutsk, Baikal State University of Economics and Law Publ., 2015.

Redaksiyaya daxil olub 17.05.2022