Pedaqoji Universitetin Xəbərləri. Riyaziyyat və təbiət elmləri seriyası – 2021, C. 69, №3, s. 39-47
Transactions of Pedagogical University. Series of mathematics and natural sciences – 2021, V. 69, №3, pp. 39-47

UOT 004.

A.P.Orucəliyev[1], Z.A.Səmədova[2]
DTX-nin H.Əliyev adına Akademiyası[1]
Azərbaycan Dillər Universiteti[2]
zamina68@hotmail.com

İNFORMASİYA TEXNOLOGİYALARINDAN EHTİYATSIZ İSTİFADƏ VƏ YA İNSAN AMİLİ İNFORMASİYA TƏHLÜKƏSİZLİYİ SİSTEMİNİN ƏN ZƏİF BƏNDİ KİMİ

Açar sözlər: *informasiya təhlükəsizliyi, informasiya mühafizəsi, konfidensial məlumatlar, kiber təhlükəsizlik, rəqəmsal təhdidlər*

Məqalədə informasiya texnologiyalarının sürətlə inkişaf etdiyi bir dövrdə bu texnologiyalardan ehtiyatsız istifadə zamanı yarana biləcək təhlükələrdən və bu təhlükədə insan amilindən bəhs olunur. Məlumdur ki, müasir informasiya texnologiyalarından ehtiyatsız istifadə ayrı-ayrı insanların rəqəmsal təhlükəsizliyinin deyil, bütövlükdə informasiya təhlükəsizliyi sisteminin pozulması kimi çox ciddi fəsadlara gətirib çıxara bilər. Bu isə rəqəmsal təhdidlərdən mühafizə probleminin qlobal problemə çevrildiyinin bariz nümunəsidir. Bu problemlərə kompüterlərin, kompüter sistemlərinin və şəbəkələrinin işinə qeyri-qanuni müdaxilə, onların sıradan çıxarılması, kompüter informasiyasının oğurlanması, mənimsənilməsi, ələ keçirilməsi, yayılması, məhv edilməsi və s. kimi təhlükəli yeni sosial təzahürləri aid etmək olar.

İnformasiya təhlükəsizliyi problemlərini araşdıran ekspertlərin qənaətinə görə informasiya təhlükəsizliyində əsas faktorlardan biri, bəlkə də ən əsası insan faktorudur. Belə ki, informasiya təhlükəsizliyi təhdidlərini və konfidensial məlumatların sızdırılmasını araşdıran ekspert-analitik mərkəzlərin gəldiyi nəticələrə görə, əksər hallarda bu təhdidlər istifadəçilərin ya bilərəkdən, ya da ki, səhlənkarlıqları ucbatından baş verir. Hal-hazırda informasiya mühafizəsinin təmini məsələləri artıq birinci dərəcəli məsələyə çevrilmişdir.

А.П.Оруджалиев, З.А.Самедова

НЕОСТОРОЖНОЕ ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ ЧЕЛОВЕЧЕСКИЙ ФАКТОР КАК САМОЕ СЛАБОЕ ЗВЕНО СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ключевые слова: *информационные безопасности, защита информации, конфиденциальная информация, кибербезопасность, цифровые угрозы*

В статье обсуждаются опасности, которые могут возникнуть в результате неосторожного использования этих технологий в период бурного развития информационных технологий, и человеческий фактор в этой опасности. Известно, что неосторожное использование современных информационных

технологий, может привести к очень серьезным последствиям, таким как нарушение системы защиты информации в целом, а не цифровой безопасности отдельных лиц. Это наглядный пример того, что проблема защиты от цифровых угроз превратилась в глобальную проблему. Эти проблемы включают в себе опасные новые социальные проявления, такие как незаконное вмешательство в работу компьютеров, компьютерных систем и сетей, их уничтожение, кражу, незаконное присвоение, конфискацию, распространение, уничтожение компьютерной информации и т.д.

По мнению специалистов, изучающих проблемы информационной безопасности, одним из основных факторов информационной безопасности, пожалуй, самым важным, является человеческий фактор. По данным экспертно-аналитических центров, исследующих угрозы информационной безопасности и утечки конфиденциальной информации, в большинстве случаев эти угрозы возникают либо умышленно, либо по халатности пользователей. В настоящее время вопросы информационной безопасности стали приоритетными.

A.P.Orujaliyev, Z.A.Samadova

INACCURATE USE OF INFORMATION TECHNOLOGY OR A HUMAN FACTOR AS THE WEAKEST ELEMENT OF THE INFORMATION SECURITY SYSTEM

Keywords: *information security, information protection, confidential information, cyber security, digital threats*

The article deals with the dangers that can arise as a result of the careless use of these technologies during the period of rapid development of information technology, and the human factor in this danger. It is known that the careless use of modern information technologies can lead to very serious consequences, such as a violation of the information protection system as a whole, and not the digital security of individuals. This is a clear example of the fact that the problem of protecting against digital threats has become a global problem. These problems include dangerous new social manifestations such as illegal interference with computers, computer systems and networks, their destruction, theft, misappropriation, confiscation, distribution, destruction of computer information, etc.

According to experts studying information security problems, one of the main factors of information security, perhaps the most important, is the human factor. According to data from expert and analytical centers investigating threats to information security and leaks of confidential information, in most cases these threats arise either intentionally or through user negligence. Currently, information security issues have become a priority.

İnsan həyatının ayrılmaz bir hissəsinə çevrilmiş internetdən istifadə ilə bəşəriyyət ardıcıl surətdə rəqəmsal dünyada irəliləməkdədir. Müxtəlif informasiya mənbələrinin verdiyi məlumatlara görə 2020-ci ildə dünya əhalisinin təqribən 60%-

i (4,66 milyard insan) internet istifadəçisidir. Bu əhalinin əksər hissəsini, yəni 4,2 milyardını sosial şəbəkə istifadəçiləri təşkil edir. Dünya əhalisinin informatlaşdırma yolu ilə aktiv irəliləməsi bəşəriyyət qarşısında bir tərəfdən yeni, çox güclü imkanlar açdığı halda, digər tərəfdən, yeni-yeni naməlum risklər doğurur. Belə ki, internet istifadəçilərinin artması səbəbindən istər adi cinayətkarlar tərəfindən, istərsə də mütəşəkkil kiberqruplar tərəfindən edilən rəqəmsal təhdidlərin də miqyası genişlənməkdədir. İndi demək olar elə bir müəssisə və təşkilat və ya ayrıca bir internet istifadəçisi yoxdur ki, onun bədniyyətlilər üçün bu və ya digər səviyyədə maraq kəsb edən müxtəlif xarakterli informasiyası olmasın. Bura hər şeydən əvvəl, kommersiya məlumatları, müəssisənin intellektual mülkiyyəti haqqında informasiya, konfidensial məlumatlar, ayrı-ayrı insanlar haqqında özəl məlumatlar daxildir. Sirr deyildir ki, müasir informasiya texnologiyalarından ehtiyatsız istifadə ayrı-ayrı insanların rəqəmsal təhlükəsizliyinin deyil, bütövlükdə informasiya təhlükəsizliyi sisteminin pozulması kimi çox ciddi fəsadlara gətirib çıxara bilər. Bu isə rəqəmsal təhdidlərdən mühafizə probleminin qlobal problemə çevrildiyinin bariz nümunəsidir.

Məlumdur ki, istənilən müasir şirkətin müvəffəqiyyəti və onun ciddi rəqabət şəraitində inkişafı informasiya texnologiyalarından istifadə səviyyəsindən və deməli, informasiya təhlükəsizliyinin təmini dərəcəsindən asılıdır. Ekspertlərin qənaətinə görə, hazırda informasiya təhlükəsizliyi bazarında dəyərlərin kardinal qiymətləndirilməsi baş verir. Əgər əvvəllər informasiya təhlükəsizliyinin təminatı məsələlərinə axırıncı olmasa da, birinci dərəcədən uzaq bir məsələ kimi baxılırdısa, indi informasiya mühafizəsinin təmini məsələləri artıq birinci dərəcəli məsələyə çevrilmişdir. Belə ki, əgər əvvəllər informasiya mühafizəsi üzrə insidentlərin baş verdiyi zaman tədbirlər görülürdüsə, indi hər bir təşkilat və müəssisə bütün gücü ilə bu insidentlərdən qaçmağa çalışır. Bu zaman bir sıra məsələlərin, o cümlədən informasiya sistemlərinin təhlükəsizliyi üzrə görülən tədbirlərin effektivliyinin qiymətləndirilməsi üçün etibarlı və effektiv monitorinq sistemlərinin qurulması, informasiyanın icazəsiz istifadədən qorunması sahəsində hüquqi təminatın, eləcə də informasiya şəbəkələrinə icazəsiz müdaxilənin qarşısını almaq üçün operativ reaksiya verilməsi mexanizm və vasitələrin hazırlanması kimi həlli o qədər də asan olmayan məsələlərin həlli tələb olunur. Bu məsələlərin lazımı səviyyədə həlli 2019-cu ildən davam edən COVİD-19 pandemiyası şəraitində xüsusilə aktuallaşdı. Belə ki, COVİD-19 nəinki insan sağlamlığı üçün təhlükə yaratdı, eləcə də istər ayrı-ayrı istifadəçi olsun, istərsə də şirkətlər üçün kibertəhlükə sahəsində riskləri də artırdı. Təəssüf ki, bu risklərin aradan qaldırılması istiqamətində görülən tədbirlər heç də həmişə lazımi səviyyədə səmərə vermir. Bunu informasiya təhlükəsizliyi üzrə beynəlxalq şirkət ekspertlərinin gəldiyi qənaətlər də göstərir.

Misal üçün, informasiya təhlükəsizliyi sahəsində beynəlxalq ekspert kimi tanınan **Eset** şirkətinin verdiyi məlumata görə, pandemiya şəraitində özünütəcridə keçən internet istifadəçiləri kibertəhdidlərlə qarşılaşmışlar. Belə ki, şirkətin

apardığı sorğuda iştirak edən respondentlərin 36%-i Beynəlxalq Səhiyyə Təşkilatının adı ilə koronavirusla bağlı ***fişinq*** hücumlarına məruz qaldıqlarını, 22%-i isə ziyankar proqramlarla, o cümlədən ***troyan*** və viruslarla qarşılaşdıqlarını bildirmişlər. Bundan başqa, respondentlərin 11%-i fırıldaqçıların ***sextortion*** tipli hücumlarına da məruz qalmışlar. Belə ki, bədniyyətlilər öz qurbanlarını inandırmağa çalışmışlar ki, onların kompüterlərinə veb-kameralara girişi təmin edən ziyankar proqram quraşdırılmışdır. İnternet istifadəçisinin şəxsi həyatı ilə bağlı özəl videoları, eləcə də veb-kameralarını izlədiklərini və müəyyən zaman ərzində onlara aid əldə etdikləri intim materialları şəbəkədə yaymaqla hədələyən dələduzlar bunun baş verməməsi müqabilində öz qurbanlarından pul tələb etmişlər. Şirkətin məlumatına görə təkcə Rusiya Federasiyası üzrə hər 10 nəfərdən biri özünütəcrid şəraitində şantajdan zərər çəkmişdir. Eset sadalanan kibertəhdidlərin daha çox yayıldığı sahələri də müəyyənləşdirmişdir. Bu zaman öndə gedən sosial şəbəkələr (68%), messencerlər (25%), saxta tibbi saytlar (23%), saxta internet-mağazalar və apteklər (24%) olmuşdur.

Beynəlxalq standartlara uyğun olaraq təhdidlərin aktuallığının qiymətləndirilməsi risklərin identifikasiyası mərhələlərindən biridir. Təhdidin aktuallığı isə, öz növbəsində informasiya sistemlərinin mühafizə səmərəliliyinin göstəricisidir. Mühafizə sistemlərinin səmərəliliyi istifadə olunmuş ehtiyatların – zaman, güc və vasitələrin informasiya mühafizəliliyi səviyyəsinə nisbəti ilə təyin olunur [1]. Kompüter sistemlərinin təhlükəsizliyinin təmini üzrə dünya miqyaslı "**Doktor Veb**" şirkətinin də 2020-ci il üçün internet-təhdidləri analiz edərək antivirus aktivliyi üzrə məlumatına görə, internet istifadəçilərinin kütləvi şəkildə ən çox qarşılaşdıqları təhdid kompüter və smartfonların normal işinə maneə yaradan reklam əlavələrini, müxtəlif ziyanverici proqramları və digər ziyankar elementləri istifadəçi qurğularına quraşdıran **troyan-dropperlər** olmuşdur. Baxmayaraq ki, bu təhdid əsasən **Windows** **ƏS**-nin idarəsi altında işləyən qurğular üçün təhlükə mənbəyi olmuşdur, bununla belə, **macOc** idarəsi altında işləyən kompüterlər də bu risk zonasında olmuşdur. Bu zaman əksər hallarda təhdid altında o istifadəçilər olmuşdur ki, onlar kompüterlərdə quraşdırılmış təhlükəsizlik elementlərinin işini dayandırmış və ya bu sistemlərlə bağlı əlavələri etibarsız mənbələrdən yükləmişlər. Belə istifadəçilər işlərini asanlaşdırmaq naminə, daha dəqiq desək, sistemə daha tez daxil olmaq, öz funksiyalarını daha tez yerinə yetirmək üçün zəruri olan autentifikasiya proseduralarından keçmədən sistemə girdiklərinə görə təhdid altında olmuşlar. "Doktor Veb"in məlumatına görə, Android ƏS bazasında işləyən mobil qurğu istifadəçiləri reklam, casus və bank troyan proqramları, eləcə də ziyankar proqramları əsasən **Google Play** kataloqu vasitəsilə köçürüb istifadəçi qurğularına yükləyən xüsusi yükləmə proqramlarının təhdidi altında olmuşlar. **Check Point** şirkətinin tədqiqatçılarının **Global Threat İndex** hesabatına əsasən məlum olmuşdur ki, 2021-ci ilin yanvar ayı ərzində ən aktiv internet-təhdid **Emotet** ziyankar proqramı olmuşdur. Mövcud olmuş ən bahalı və dağıdıcı ziyankar

proqramlardan biri olan Emotet 2014-cü ildən bəri daim təkmilləşdirilmiş və onun zərərsizləşdirilməsi yalnız hüquq-mühafizə orqanlarının birgə səyi nəticəsində mümkün olmuşdur. Bu zaman o da qeyd edilir ki, bu troya proqramının hər bir versiyasının aradan qaldırılması 1 mln dollara başa gəlmişdir. Mütəxəssislərin rəyinə görə, zərərsizləşdirilən hər bir ziyankar proqramın yerinə yeniləri gəlməkdədir.

İnformasiya təhlükəsizliyi problemlərini araşdıran ekspertlərin qənaətinə görə, informasiya təhlükəsizliyində əsas faktorlardan biri, bəlkə də ən əsası insan faktorudur. Belə ki, informasiya təhlükəsizliyi təhdidlərini və konfidensial məlumatların sızdırılmasını araşdıran ekspert-analitik mərkəzlərin gəldiyi nəticələrə görə, əksər hallarda bu təhdidlər istifadəçilərin ya bilərəkdən, ya da ki, səhlənkarlıqları ucbatından baş verir. Təəssüf ki, belə vəziyyət istifadəçilərin **"rəqəmsal"** mədəniyyətinin aşağı səviyyəli olmasından və informasiya mühafizəsinin texniki vasitələrinə kifayət qədər diqqət etməmələrindən qaynaqlanır. İstisna deyildir ki, internetdə bu və ya digər şəxs haqqında nə qədər çox informasiya tapmaq olarsa, bir o qədər onun üçün müxtəlif təhdidlərlə qarşılaşmaq imkanları da artar, başqa sözlə, dələduzluq və ya fərdi məlumatların oğurlanması baş verər. Belə halların baş verməməsi üçün öz şəxsi məlumatlarını kiminlə və nəyə görə bölüşmək fikrində olan hər bir istifadəçi diqqətli olmalıdır ki, bu məlumatlar sonradan onun özünə qarşı istifadə edilməsin. Bütün bunlar informasiya texnologiyalarından ehtiyatsız istifadə probleminin kəskin bir şəkildə mövcudluğunu göstərir. Məsələ ondadır ki, İnformasiya texnologiyalarının ilkin inkişaf mərhələlərində informasiya təhlükəsizliyinə təhdidlər xaricdən gözlənilirdisə, sonralar artıq təhlükə mənbələrinin əksər hallarda müəssisənin, təşkilatın bilavasitə həssas informasiyasını etibar etdiyi öz əməkdaşlarının olması aşkarlandı. Başqa sözlə desək, nəinki müəssisənin konfidensial informasiyasını, eləcə də özünəməxsus özəl informasiyanın da qorunmasını təmin etməli olan əməkdaş və ya adi internet istifadəçisinin bu məsələyə barmaqarası baxışı sonda informasiya təhlükəsizliyinə edilən təhdidlərin real təhlükələrə çevrilməsinə gətirib çıxarır.

İnformasiya təhlükəsizliyi üzrə ekspertlərə görə informasiya təhlükəsizliyi sferası hələ ki, bütün təşkilat və müəssisələri birləşdirə biləcək **qərarların** olmadığı bir sahədir. Bu, hər şeydən əvvəl, ayrı-ayrı təşkilat və müəssisələrdə bir-birindən fərqli müasir tələblərə cavab verməyən proqramlarla işləyən və deməli, fərqli təhlükəsizlik qərarları da tələb edən avtomatlaşdırılmış sistemlərin olmasından qaynaqlanır. Belə hissə-hissə avtomatlaşdırılmış sferada böyük sayda mahiyyətcə o qədər də sadə olmayan müxtəlif məsələlərin, o cümlədən, müəssisəni sıradan çıxara bilən antivirus təhdidləri ilə bağlı, fərdi verilənlərin emalı zamanı zəruri tələblərə riayət olunması ilə bağlı məsələlərin, eləcə də konfidensial informasiyanın istər daxildən, istərsə də xaricdən mühafizəsi kimi kifayət qədər mürəkkəb məsələlərin praktiki həlli tələb olunur. Bu problemlərin həlli istiqamətində qarşıya

çıxan ən **birinci sualı** belə ifadə etmək olar: ümumiyyətlə, hər bir internet istifadəçisinin, eləcə də şirkətin informasiya təhlükəsizliyini tam şəkildə təmin edə bilən mühafizə sistemi mümkündürmü? Praktik nöqteyi-nəzərdən mühafizə olunan sistem, sistemin təhlükəsizliyini poza bilən, heç bir boşluğa malik olmayan sistemdir. Məlumdur ki, istənilən proqramda səhvlər vardır. Lakin heç də istənilən səhv boşluq deyildir, yəni heç də bütün səhvlər sistemə hücum imkanı yaratmır, xüsusən də bədniyyətliyə sistemə girmək imkanı vermir. Bununla belə, nəzərə alsaq ki, mahiyyətcə heç kimin bilmədiyi, heç bir təhlükəsizlik sisteminin qarşısını ala bilmədiyi "sıfırıncı gün" (ing. *zero day*) boşluğu deyilən bir boşluq da vardır ki, elə bu boşluq məhz bədniyyətlilər tərəfindən istifadə oluna bilər [2]. Bütün bunlar heç də o demək deyildir ki, mühafizə olunan təhlükəsizlik sistemləri yaradılmamalıdır. İT təhlükəsizlik sferasında dünyada məşhur **Check Point Software Technologies** şirkətinin ekspertlərinin mövqeyinə görə qızğın kibersilahlanma əsrində yaşadığımız üçün kiberhücumların sayı və mürəkkəblik səviyyələri də artacaqdır. Bundan başqa, hazırkı dövrdə təşkilatlar ən müasir təhlükəsizlik məhsulları ilə təmin olunsalar da, kompüter və işçi stansiyaların sındırılma riski onsuz da qalacaq və tamam aradan qaldırılan olmayacaqdır. Böyük və ya kiçik olmasından asılı olmayaraq, təşkilatlar tərəfindən kibercinayətkarları qabaqlamaq və potensial hücumların qarşısını almaq üçün qabaqlayıcı tədbirlərin təşkili zəruridir. Məhz edilən hücumların əvvəlcədən aşkarlanması və avtomatik bloklanması zərərdəymənin qarşısını ala bilər. İnformasiya təhlükəsizliyi insidentlərinin tədqiqi ilə məşğul olan bəzi mütəxəssislərin rəyinə görə isə, informasiya təhlükəsizliyi infrastrukturuna təsir edə biləcək bütün təhdidləri əvvəlcədən müəyyənləşdirmək çox mürəkkəbdir. Həmişə müəyyən şərtlər kombinasiyası olacaqdır ki, onları əvvəlcədən infrastrukturda nəzərə almaq mümkün olmayacaq. Belə ki, real informasiya təhlükəsizliyində fəaliyyət çoxşaxəli olduğuna görə, bəzən "başgicəlləndirici" elə hallar mümkündür ki, bu vəziyyətlərdə düzgün cavabın tapılması üçün təhlükəsizlik sistemlərinin reallaşdırdığı tədbirlər kifayət etməsin. Başqa sözlə desək, bütövlükdə tam şəkildə mühafizə olunan informasiya sistemlərinin yaradılması üçün **universal** resept təklifi yoxdur. Bu, hər şeydən əvvəl informasiya təhlükəsizliyi infrastrukturlarının fərdiliyi ilə bağlıdır. Bu zaman informasiya təhlükəsizliyi üzrə, daha dəqiq desək, informasiya təhlükəsizliyinə təhdidlərin aktuallığının qiymətləndirilməsi üçün istər hər bir kompüter istifadəçisinin, istərsə də bütövlükdə şirkətin qarşısında duran sual **dünyəvi trendlərin** nəzərə alınıb-alınmaması sualıdır. Mövcud dünyəvi trendlər isə bunlardır: **Monitorinq, maşın təlimi** və **davranış analizi** (ing.*UEBA-user and entity behavior analitics*) [3]. Yalnız müəssisə daxilində və bütövlükdə şəbəkə daxilində zəruri monitorinqlər aparmaqla, eləcə də süni intellekt elementlərindən istifadə ilə inkişafetdirici maşın təlimi və UEBA-nın köməyilə informasiya təhlükəsizliyi təhdidlərini vaxtında aşkarlamaq və onlara qarşı lazımi tədbirlər görmək olar. Şirkətdə baş vermiş insidentlərin təhqiqat vaxtının və bu təhqiqata

cəlb olunmuş əməkdaşların sayını azaltmaqla keyfiyyətlə araşdırılması, eləcə də gələcəkdə baş verə biləcək insidentlərin proqnozlaşdırılması və ya idarə olunması məqsədini daşıyan **davranış analizi** (UEBA) bir adaptiv alqoritm kimi hazırda müxtəlif informasiya təhlükəsizlik sistemlərində sürətlə tətbiq edilməkdədir. Sadaladığımız bu trendlər elədir ki, onlar inkişaf edən texnologiyalar kimi istəsək də, istəməsək də, tətbiq olunmalıdır. Bütöv müəssisə, şirkət perimetri üzrə aparılan monitorinq, eləcə də situasiyaya adaptasiya oluna bilən maşın təlimi real rejimdə girişlərə nəzarət edir, əməkdaşın iş yerində özünü bilavasitə necə aparmasını analiz edir, pozucunu avtomatik bloka salmağa imkan verir. Bütün şəbəkə üzrə belə analiz bütövlükdə sistemdə istər istifadəçi tərəfindən, istərsə də serverlərdə baş verən mümkün sapmaların vaxtında aşkar edilməsinə imkan verə bilər. Bu zaman süni intellekt sferasına daxil olan kompüter görmə qabiliyyəti əsasında informasiya mühafizəsi vasitələrini də unutmaq olmaz. Belə ki, belə vasitələr real zaman daxilində veb-kamera vasitəsilə obyekti tanımaqla təhlükəsizlik siyasətinin pozulması faktını fiksə edə bilir, misal üçün sistemə giriş icazəsi olmayan şəxsin üzünü, sistem əhatəsində olan smartfonu, ekranın şəklini çəkə bilən qurğunu, İP-kameranı və s. aşkar edə bilir. İnformasiya mühafizə sistemlərinin bütün siniflərində tətbiq olunan bu dünyəvi trendlərə arxayınlaşmaq doğru olmazdı. Unutmaq olmaz ki, bədniyyətlilər də boş dayanmırlar və daim öz hücum alət və texnologiyalarını təkmilləşdirirlər. Ona görə də qarşıya olduqca aktual olan belə bir sual çıxır: **Ayrı-ayrı internet istifadəçisi nöqteyi-nəzərindən öz təhlükəsizliyini necə təmin etməli?** İnkarolunmaz faktdır ki, ən yaxşı mühafizə – ümumiyyətlə, yoluxma imkanına yol verməməkdir. Lakin qeyd etdiyimiz kimi, internet istifadəçilərinin heç də hamısının rəqəmsal savadlılığı tələb olunan səviyyədə olmur. Ona görə də informasiya təhlükəsizliyi sferasında fəaliyyət göstərən ekspertlərin tövsiyələrinə əməl etmək olduqca vacibdir. Belə tövsiyələrdən aşağıdakıları sadalamaq olar:

1. Ev daxilində şəbəkəyə necə birləşdirilməsindən asılı olmayaraq qoşulmuş istənilən kompüteri kifayət qədər təhlükəsiz iş yeri hesab etmək olmaz. Mütəxəssislərin ironiya ilə dedikləri kimi, yeganə ən təhlükəsiz kompüter seyfdə saxlanılan, istənilən informasiya mənbəyindən, o cümlədən elektrik qida mənbəyindən əlaqəsi kəsilmiş kompüter hesab olunur;
2. Müntəzəm olaraq sizə məxsus verilənlərin və xüsusilə ən vacib faylların ehtiyat surətlərini yaratmalı; Əgər mümkündürsə avtomatik ehtiyat surətçıxarmanı qoşmalı;
3. Potensial təhdidləri tanımağa çalışın. Yoluxmanın ən çox yayıldığı üsullar hələ ki, spam və fişinq elektron məktublardır;
4. Məlum proqramları yalnız rəsmi saytlardan yükləməli;
5. Şübhəli internet-resurslara daxil olmamalı;
6. Naməlum mənbələrdən göndərilən məktubları açmamalı, xüsusilə bu məktublarda linklər (adətən ziyankar saytlara aparan) varsa;

7. İlkin kibergigiyena qaydalarına əməl edin və şübhəli məktublar haqqında əlaqədar kibertəhlükəsizlik xidmətinə (CERT) xəbər verin;
8. İstər fərdi, istərsə də korporativ sistem şəraitində iş zamanı fayllara girişə məhdudiyyət qoyun. Korporativ sistemlərdə müvəffəqiyyətli hücumun ziyanını minimallaşdırmaq üçün hər bir istifadəçiyə lazım olan fayllarla işləmək imkanı yaratmalı. Bu, hər şeydən əvvəl hücumun daxili şəbəkəyə yayılmasının qarşısını ala bilər. Belə ki, bir istifadəçi sistemində hücumun nəticələrinin aradan qaldırılması problemli olsa da, şəbəkə hücumunun ziyanı az olar;
9. Müntəzəm surətdə siqnatura əsasında antivirus və digər mühafizə vasitələrini yeniləməli. Yenilənməni mərkəzləşdirilmiş şəkildə, yəni insan amilini istisna etmək üçün istifadəçi olmadan aparılmasını təmin edin;
10. Android ƏS idarəsi altında işləyən qurğularda *Google Play*-dən istifadə zamanı təhlükəsizlik tədbiri olaraq bu proqramın Google Play Protect imkanından istifadə etmək məsləhətdir. Belə ki, bu proqram əlavəsi Play Market vasitəsilə yüklənən bütün əlavələri əvvəlcədən yoxlayır, qurğunu kənar mənbələrdən ola bilən potensial təhlükəli əlavələrin olub-olmadığı üzrə skan edir, mövcud təhdid haqqında istifadəçini xəbərdar edir və məlum təhlükəli əlavəni sistemdən yox edir;
11. İş yerini zərurət olduğu təqdirdə tərk edərkən kompüteri bloklamaq (yaxud da söndürmək) tövsiyə olunur. Bu amilin unudulması verilənlərin sızması üçün müəyyən risk yaradır. Belə hallarda informasiyaya girişi istənilən adam, hətta təsadüfi bir şəxs də əldə edə bilər;
12. Yalnız daim yeniləşən lisenziyalı proqram təminatından istifadə etməli. Qənaət naminə pulsuz şübhəli proqram təminatından istifadə etməməli. Unutmamalı ki, pirat proqram təminatında əksər hallarda heç bir xəbərdarlıq edilməyən və bədniyyətlilərə informasiyanı oğurlamağa imkan verən ziyankar kodlar (viruslar) yerləşdirilir;
13. Zəruri informasiya olan fləş-kart, disk, hətta noutbukların itirilməsi konfidensial informasiyanın sızma mənbəyi olması unudulmamalıdır. Onu da yaddan çıxartmaq olmaz ki, qurğunun özünün itirilməsindən dəyən zərər bu qurğunun içindəki informasiya sızmasından dəyə bilən ziyanın yanında əhəmiyyətsiz ola bilər;
14. Fləş-kartların ziyankar kodların yoluxma mənbəyi olması səbəbindən onlardan istifadə zamanı diqqətli olmalı. Bundan başqa, fləş-kartlardan faylların təhlükəli təmizlənməsinin istifadəçinin qəflətdə saxlanılması olması da yaddan çıxarılmamalıdır. Belə ki, bu fləş-kartları ələ keçirən bədniyyətli hətta sadə bərpa proqramlarının köməyilə "yox edilmiş" faylları əldə edə bilər;
15. Korporativ noutbukun qorunmayan açıq şəbəkəyə və ya kiberhücumlardan kifayət qədər mühafizə sisteminə malik olmayan ev şəbəkəsinə birləşdirilməsi bədniyyətlinin ofis informasiya sisteminə və ya təşkilatın informasiya

təhlükəsizliyi infrastrukturuna nüfuz etməsinə kömək edə bilər. Bu, onunla bağlıdır ki, statistikaya görə açıq və ev routerlərinin 45%-i ziyankar kodlarla yoluxmuş və ya etibardan salınmış qurğulardan ibarətdir;
16. İri həcmli faylların, xüsusilə fayllar arxivinin mübadilə edilməsində ehtiyatlı olmalı. Belə ki, 20-50 Mbayt həcmli informasiyanın e-mail ilə göndərilməsi məhdudiyyət səbəbindən mümkün olmadığı üçün istifadəçilər alternativ yollardan, misal üçün qorunmayan açıq fayl-mübadiləsi serverlərindən istifadə edirlər. Belə mübadilə birbaşa informasiya sızması mənbəyi olduğu kimi əlavə mürəkkəbliklər də yaradır. İnformasiya təhlükəsizliyi xidməti bu mübadiləyə nəzarət imkanına malik ola bilmədiyi üçün bu təhdidin reallaşma ssenarisi onun nəticəsi nöqteyi-nəzərincə olduqca çox ağır, böhranlı ola bilər.

Nəticə olaraq onu demək lazımdır ki, istənilən təhlükəsizlik sistemi yalnız xəbərdarlıq edə və sadə əməliyyatlarda məhdudiyyətlər qoya bilər. Onun nəticəsinin tədqiqini aparmaq isə insan işidir. Elə bir vahid ssenari yoxdur ki, onun köməyilə bir neçə təhlükəsizlik komponentini seçib mühafizə olunan səmərəli şəbəkə qurmaq mümkün olsun. Başqa sözlə desək, artıq köhnə sistemlərlə mühafizə mümkün deyildir. Yalnız informasiya təhlükəsizliyi üzrə dünyəvi trendlərə əsaslanmaqla informasiya təhlükəsizliyi problemində nailiyyətlər əldə etmək olar. İnformasiya təhlükəsizliyi problemlərinin həlli zamanı sosial mühəndisliyi də yaddan çıxartmaq olmaz. Belə ki, ondan şirkəti qorumaq olduqca mürəkkəbdir. Təəssüf ki, sosial mühəndislik istənilən maşın təlimi sistemindən də çox sürətlə inkişaf edir. Sosial mühəndislik bazasında dələduzluq hazırda çox sürətlə yayılmaqdadır. Onun köməyilə istənilən texniki mühafizə olunan şirkəti sındırmaq olar. Daha dəqiq desək, informasiya təhlükəsizliyində onsuz da ən zəif bənd məhz **insan** qalacaqdır.

ƏDƏBİYYAT

1. Проблемы информационной безопасности. // Компьютерные системы, – 2020. № 3, – с.24-31.
2. *Зегжда Д.П., Жуков И.Ю.* Особенности обеспечения информационной безопасности вычислительных систем. // Безопасность информационных технологий, – 2021. Т.28, №1, – с.42-61.
3. Стресс, к которому стоило быть готовым заранее // Информационная безопасность, 2020. № 3, июль, – 60 с.
4. Вестник информационной безопасности, – 2020. № 2(191), февраль.
5. Вестник информационной безопасности, – 2020. № 4(52), апрель
6. Вестник кибербезопасности, – 2020. № 8(56), август
7. Вестник кибербезопасности, – 2021. № 2(62), февраль.

Redaksiyaya daxil olub 14.06.2021