Azərbaycan Milli Elmlər Akademiyası M. Füzuli adına Əlyazmalar İnstitutu, *ISSN 2224-9257*
Filologiya məsələləri № 6, 2024
Səh. 33-39
https://doi.org/10.62837/2024.6.33

BAĞIRZADƏ NİGAR SƏXAVƏT QIZI
OdlarYurdu Universiteti,
Koroğlu Rəhimov küçəsi
odlaryurdu.magistratura@mail.ru

İNFORMASİYA SİSTEMLƏRİNİN QORUNMASI MƏSƏLƏLƏRİ

Xülasə:

İnformasiya sistemlərinin qorunması, bir şirkətin və ya təşkilatın səlahiyyətli məlumatlarını və informasiya infrastrukturunu qorumaq üçün görülən tədbirləri əhatə edir. Bu, məlumatların qanunsuz giriş və dəyişikliklərdən, sızıntılardan, viruslardan, hücumlardan və digər təhlükələrdən müdafiə olunmasını təmin edir. İnformasiya sistemlərinin qorunması, bir şirkətin səmərəliliyini, etibarlılığını və rekordlarının müdafiəsini təmin edir. Bu məsələlər, müxtəlif təhlükələrin və risklərin idarə edilməsi, məlumatların şifrələnməsi, daxili və xarici hücumların qarşısının alınması və istifadəçilərin məlumatların təhlükəsiz istifadəsini təmin etməklə bağlı müxtəlif strategiyaları əhatə edir. İnformasiya sistemlərinin qorunması məsələləri, təhlükələrə qarşı müdafiə, təhlükəsizlik stratəgiyasının təyin edilməsi, məlumatların şifrələnməsi, məlumatların yedəklənməsi, məlumatlarla işləmək üçün giriş nəzarəti, istifadəçilərin təlimi və informasiya təhlükəsizliyinin bütünən idarə edilməsi kimi məsələləri əhatə edir. İnformasiya təhlükəsizliyi bir aktiv kimi informasiyanı təhdid və ya təhlükələrdən qorumaq üçün lazımi texnologiyadan, düzgün məqsədlə və düzgün şəkildə istifadə etməklə istənilən mühitdə arzuolunmaz şəxslər tərəfindən məlumatın mövcudluğunun qarşısını almaq cəhdidir. İnformasiya təhlükəsizliyi: Təqdim olunan xidmətlərin, sistemlərin və məlumatların qorunmasını təmin edir. İstifadəçilər informasiya təhlükəsizliyini öz rakursundan qiymətləndirdikdə, sadə tərif kimidir. Gündəlik həyatda istifadə olunan kompüter və smartfonlara və istifadə olunan sistemlərə girişin təhlükəsizliyinin təmin edilməsi kimi də düşünülə bilər. Başqa sözlə, məlumatın icazəsiz istifadədən, icazəsiz açıqlanmasından, icazəsiz məhv edilməsindən, icazəsiz dəyişdirilməsindən, məlumatın zədələnməsindən və ya icazəsiz məlumat əldə edilməsinin qarşısının alınması prosesidir. İnformasiya təhlükəsizliyi, kompüter təhlükəsizliyi və informasiya sığortası terminləri tez-tez bir-birini əvəz edən mənada istifadə olunur. Məlumatların paylaşılması və davamlı olaraq əldə oluna bilməsi ilə əlaqədar olaraq, məlumatın məxfi şəkildə, korlanmadan, məhv edilmədən, dəyişdirilmədən və başqaları tərəfindən tutulmadan, bütövlüyü təmin edilməklə, göndərən mənbədən qəbulediciyə ötürülməsi əsasdır informasiya təhlükəsizliyinin təmin edilməsi meyarları.

Açar sözlər: Təhlükəsizlik, Şifrələnmə, Hücumların qarşısının alınması, İdarəetmə və nəzarət, Təlim, Yedəklənmə, Təhlükəsizlik strategiyası, Məxfilik.

Azərbaycan Milli Elmlər Akademiyasi M. Füzuli adına Əlyazmalar Institutu, *ISSN 2224-9257*
Filologiya məsələləri № 6, 2024
Səh. 33-39

Bagyrzade Nigar Sakhavat

ISSUES OF PROTECTION OF INFORMATION SYSTEMS

Abstract:

Information systems protection includes measures taken to protect a company's or organization's authorized data and information infrastructure. This ensures that data is protected from illegal access and changes, leaks, viruses, attacks and other threats. Protecting information systems ensures the efficiency, reliability and protection of a company's records. These issues include various strategies for managing various threats and risks, encrypting data, preventing internal and external attacks, and ensuring users have secure access to data. Information systems protection issues include threat protection, security strategy determination, data encryption, data backup, access control for working with data, user training, and overall information security management. Information security as an asset is the attempt to prevent information from being made available by unwanted persons in any environment by using the right technology, for the right purpose and in the right way, to protect information from threats or threats. Information security: Ensures the protection of services, systems and data provided. When users evaluate information security from their perspective, it is like a simple definition. It can also be thought of as securing access to computers and smartphones and systems used in everyday life. In other words, it is the process of preventing unauthorized use, unauthorized disclosure, unauthorized destruction, unauthorized modification, damage to information, or unauthorized access to information. The terms information security, computer security, and information insurance are often used interchangeably. With regard to the sharing and continuous availability of information, the transfer of information from the sending source to the receiver in a confidential manner, without being corrupted, destroyed, altered or intercepted by others, ensuring its integrity, is the main criteria for ensuring information security.

Keywords: Security, Encryption, Attack prevention, Administration and control, Training, Backup, Security strategy, Privacy.

БАГЫРЗАДЕ НИГЯР САХАВАТ

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Резюме:

Защита информационных систем охватывает меры, принимаемые для защиты авторизованных данных и информационной инфраструктуры компании или организации. Это гарантирует защиту данных от несанкционированного доступа и изменения, утечек, вирусов, атак и других угроз. Защита информационных систем обеспечивает эффективность, надежность и защиту записей компании. Эти проблемы включают в себя различные стратегии управления различными угрозами и рисками, шифрование данных,

предотвращение внутренних и внешних атак и обеспечение безопасного доступа пользователей к данным. Вопросы защиты информационных систем включают защиту от угроз, определение стратегии безопасности, шифрование данных, резервное копирование данных, контроль доступа для работы с данными, обучение пользователей и общее управление информационной безопасностью. Информационная безопасность как актив — это попытка предотвратить доступ к информации нежелательным лицам в любой среде, используя правильную технологию, для правильной цели и правильным способом, чтобы защитить информацию от угроз или угроз. Информационная безопасность: Обеспечивает защиту предоставляемых услуг, систем и данных. Когда пользователи оценивают информационную безопасность со своей точки зрения, это похоже на простое определение. Его также можно рассматривать как обеспечение доступа к компьютерам, смартфонам и системам, используемым в повседневной жизни. Другими словами, это процесс предотвращения несанкционированного использования, несанкционированного раскрытия, несанкционированного уничтожения, несанкционированного изменения, повреждения информации или несанкционированного доступа к информации. Термины информационная безопасность, компьютерная безопасность и информационное страхование часто используются как синонимы. В связи с обменом и постоянной доступностью информации, передача информации от отправляющего источника к получателю конфиденциальным образом, без повреждения, уничтожения, изменения или перехвата другими лицами, обеспечение целостности является основным критерием обеспечения информации. безопасность.

Ключевые слова: Безопасность, Шифрование, Предотвращение атак, Администрирование и контроль, Обучение, Резервное копирование, Стратегия безопасности, Конфиденциальность.

İnformasiya sistemlərinin qorunması məsələləri günümüzün digər bənzərsiz məsələləri kimi ciddi vəziyyətdir. Bu məsələlər müxtəlif sahələrdən (siber təhlükəsizlik, rəqabətçi məxfilik, və məhdudiyyətlər) ibarətdir. Bir informasiya sisteminin qorunmasında diqqət yetirilən əsas məsələlərdən bəziləri aşağıda qeyd olunmuşdur:

1. Siber Təhlükəsizlik: Informasiya sistemlərinin ən böyük təhlükələri siber təcavüzkarlıq və hücumlarla bağlıdır. Bu hücumlar nəticəsində informasiya sızması, məlumatın silinməsi, və ya sistemin dayanıqlılığının məhdudlaşması kimi problemlər yaranır.
2. Məxfilik: İnformasiyanın məxfiliyi və gizliliyi daimi olmalıdır. Hassas məlumatların qorunması üçün təhlükəsizlik stratetiyaları və tədbirləri vacibdir.
3. Digər Qorunma Tədbirləri: Bu, zərərli proqramların (viruslar, mürəkkəb programlar, və s.) qarşısını almaq və informasiya sistemlərinin mümkün qədər

təhlükəsiz edilməsi üçün şəbəkə konfiqurasiyası, parol idarəetməsi, və mürəkkəb şifrələmənin tətbiqi kimi tədbirləri daxil edir.

4. Fiziki Təhlükəsizlik: İnformasiya sistemlərinin fiziki mühitləri də qorunmalıdır. Məsələn, serverlərin və verilənlərin fiziki mühitləri təhlükəsiz olmalıdır.

5. Məhdudiyyətlər: İnformasiya sistemlərinin qorunmasında məhdudiyyətlər də hesaba alınmalıdır. Buna, istifadəçilərin sadəcə lazımi məlumatlara girişinə icazə verilməsi, informasiya paylaşımında məhdudiyyətlərin təyin edilməsi və s. daxildir.

Bu məsələlər ətraflı və təfərrüatlı olaraq nəzərdən keçirilməlidir və informasiya sistemlərinin qorunması üçün güclü bir strateji təyin edilməlidir.

İnformasiya sistemlərinin qorunması məsələləri günümüzün digər bənzərsiz məsələləri kimi ciddi vəziyyətdir. Bu məsələlər müxtəlif sahələrdən (siber təhlükəsizlik, rəqabətçi məxfilik, və məhdudiyyətlər) ibarətdir. Bir informasiya sisteminin qorunmasında diqqət yetirilən əsas məsələlərdən bəziləri aşağıda qeyd olunmuşdur:

1. Siber Təhlükəsizlik: Informasiya sistemlərinin ən böyük təhlükələri siber təcavüzkarlıq və hücumlarla bağlıdır. Bu hücumlar nəticəsində informasiya sızması, məlumatın silinməsi, və ya sistemin dayanıqlılığının məhdudlaşması kimi problemlər yaranır.

2. Məxfilik: İnformasiyanın məxfiliyi və gizliliyi daimi olmalıdır. Hassas məlumatların qorunması üçün təhlükəsizlik stratetiyaları və tədbirləri vacibdir.

3. Digər Qorunma Tədbirləri: Bu, zərərli proqramların (viruslar, mürəkkəb programlar, və s.) qarşısını almaq və informasiya sistemlərinin mümkün qədər təhlükəsiz edilməsi üçün şəbəkə konfiqurasiyası, parol idarəetməsi, və mürəkkəb şifrələmənin tətbiqi kimi tədbirləri daxil edir.

4. Fiziki Təhlükəsizlik: Informasiya sistemlərinin fiziki mühitləri də qorunmalıdır. Məsələn, serverlərin və verilənlərin fiziki mühitləri təhlükəsiz olmalıdır.

5. Məhdudiyyətlər: İnformasiya sistemlərinin qorunmasında məhdudiyyətlər də hesaba alınmalıdır. Buna, istifadəçilərin sadəcə lazımi məlumatlara girişinə icazə verilməsi, informasiya paylaşımında məhdudiyyətlərin təyin edilməsi və s. daxildir.

İnformasiya və texnologiya sistemlərinin yayılması ilə məlumatı etibarlı şəkildə qorumaq çətinləşir. Bu səbəbdən informasiya təhlükəsizliyi ön plana çıxır. İnformasiya təhlükəsizliyi ayrı-ayrı şəxslər və ya qurumlar tərəfindən onların icazəsi və icazəsi olmadan saxlanılan məlumatların əldə edilməsi və bu məlumatların istifadəsi, silinməsi, dəyişdirilməsi və açıqlanması təhlükəsinin qarşısını almaq üçün görülən tədbirləri müəyyən edir. Ümumiyyətlə, informasiya təhlükəsizliyi anlayışına informasiyanın mühafizəsi ilə bağlı müxtəlif ehtiyat tədbirləri və tədbirlər daxildir. Elektron mühitlərdə şəxsi və ya korporativ məlumatların mühafizəsi, saxlanması və daşınması proseslərində bu məlumatların istifadə olunduğu məqsədlər var. İnformasiyanın təyinatından başqa məqsədlər üçün istifadə edilməsi və ya

informasiyaya icazəsiz daxil olması və informasiyanın mühafizəsi ilə bağlı görülən tədbirlər informasiya təhlükəsizliyinin tərifidir.

Kibertəhlükəsizlik rəqəmsal dünyada təhlükəsizlik termini kimi təsvir edilə bilər. Bu anlayışı başa düşmək üçün terminologiyada başa düşülməli olan başqa bir anlayış var: verilənlər. Məlumat kibertəhlükəsizlik anlayışı ilə qorunan bir anlayışdır. Məlumatlar bir-birinə bağlanmazdan əvvəl məlum olan vəziyyət haqqında ifadələr və ya rəqəmsal mühitdə daşına bilən siqnallar və ya bitlər kimi müəyyən edilir. Kibertəhlükəsizlik məlumatların, əməliyyatların, təcrübələrin, siyasətlərin, insanların və əlaqəli sistemlərin kiber mühitdən təhlükəsizliyinin təmin edilməsi kimi müəyyən edilir.

İnformasiya təhlükəsizliyinin təmin edilməsi ilə bağlı məlumatların əhatə dairəsi vacibdir. O, informasiya ilə bağlı baş verən və ya baş verə biləcək təhlükə və hücumların inkişaf və inkişaf təhlükəsinə qarşı informasiya təhlükəsizliyi çərçivəsində müxtəlif üsulları vurğulayır. Lakin informasiyanın mühafizəsində informasiyanın fərdi və ya institusional olması informasiya təhlükəsizliyi adı altında fərqli anlayışlar kimi qiymətləndirilir.

Qurumların informasiya təhlükəsizliyi müəssisənin rəqabətə və davamlı böyüməsinə, həmçinin mənfəət və reputasiya kimi amillərə təsir edə bilər. Ümumiyyətlə, korporativ informasiya təhlükəsizliyi qurumun nüfuzunun qorunması, mənfəətinin artırılması, davamlı inkişafının dəstəklənməsi, daxil olduğu bazar, məhsul və texnologiya haqqında məlumatların hər hansı təhlükə və təhdidlərdən qorunması kimi müəyyən edilə bilər.

Qurumların informasiya aktivlərini qorumaq üçün fiziki mühafizə üsulları ilə yanaşı, elektron mühitə icazəsiz və icazəsiz girişin qarşısının alınması, informasiya və texnologiya infrastrukturunun nəzarətdə saxlanılması və şəbəkə strukturunun etibarlı olması kimi tədbirlərlə korporativ informasiya təhlükəsizliyi təmin edilə bilər. Bu səbəbdən qurumlar məlumatı qorumaq üçün korporativ informasiya təhlükəsizliyi şüuruna dair lazımi bilik və avadanlıqlara malik olmalıdırlar. Qurumların informasiya təhlükəsizliyi ilə bağlı həyata keçirə biləcəyi fiziki tədbirlərə əlavə olaraq, informasiyanın fərdi şəkildə qorunması üçün informasiya təhlükəsizliyində fərdi məlumatlılıq yaradılmalıdır. İnformasiyanın qorunması üçün fiziki tədbirlərlə yanaşı, informasiya təhlükəsizliyini qorumaq üçün fərdlərin bilik, münasibət və davranışları fərdi informasiya təhlükəsizliyi vasitəsilə mümkündür.

İnformasiya Sistemlərinin Auditi qəbul edilmiş milli standartlara və ya daxili siyasətlərə uyğun olaraq təşkilatın informasiya sistemləri infrastrukturunun, tətbiqlərinin, məlumatların istifadəsi və idarə edilməsinin, siyasətlərinin, prosedurlarının və əməliyyat proseslərinin yoxlanılması və qiymətləndirilməsidir. İnformasiya sisteminə nəzarətin effektivliyi informasiya sistemlərinin auditi vasitəsilə qiymətləndirilir.

İnformasiya sistemlərinə məlumatın yerləşdirildiyi və ya daşındığı bütün sistemlər daxildir. Bu kontekstdə məlumatın əlçatanlığı, davamlılığı və təhlükəsizliyi

baxımından bütün sistemlərin nəzarət altında olması və yoxlanılması vacibdir. İnformasiya sistemi server və ya məlumat kabeli ola bilər.

Müəssisələrdə informasiya sistemlərinin istifadəsi ilə informasiya təhlükəsizliyi daha çox əhəmiyyət kəsb edir. Kağız daha çox məlumat saxlama vasitəsi kimi istifadə edildikdə, təhlükəsizlik tədbirləri kimi fiziki təhlükəsizlik tədbirlərinə diqqət yetirildi, lakin rəqəmsal mühitlərdə, verilənlər bazalarında, CD-lər və çıxarıla bilən disklər kimi saxlama vasitələrində məlumat saxlamaq üçün inkişaf edən texnologiyalardan istifadə edildikdə İstifadəçinin 24 saat daxil ola biləcəyi ön plana çıxdı , fiziki təhlükəsizlik tədbirləri qeyri-kafi olmağa başladı. Dünyada bir çox təcavüzkarlar informasiya sistemlərinin qoşulma ehtiyacları nəticəsində internetə çıxış təhlükəsi yaratdığından, daxili istifadəçilər isə şüurlu və ya şüursuz şəkildə informasiya təhlükəsizliyində boşluqlar yaratdığından qurumlarda informasiya təhlükəsizliyinə ehtiyac günü-gündən artır. İnformasiya təhlükəsizliyinə ehtiyacla yanaşı, təhlükəsizliyi təmin etmək və təhlükəsizlik prosesini idarə etmək üçün adekvat sənədlər və metodların yaradılması üçün şüurlu kadrların işə götürülməsi zərurətə çevrilmişdir.

Bu siyasətdə informasiya təhlükəsizliyi aşağıdakıların qorunması kimi müəyyən edilir:

Məxfilik: Məlumatın yalnız ona daxil olmaq üçün səlahiyyətli şəxslər üçün əlçatan olmasını təmin etmək;

Bütünlük: Məlumatın və emal üsullarının dəqiq olmasını və icazə olmadan dəyişdirilə bilməyəcəyini təmin etmək;

Əlçatanlıq: Səlahiyyətli istifadəçilərin lazım olduqda məlumat və əlaqəli resurslara mümkün qədər tez daxil ola bilməsini təmin etmək.

İnformasiya təhlükəsizliyi siyasəti sənədi yuxarıda göstərilən mühafizə və tələbləri təmin etmək üçün yaradılmış nəzarət vasitələrinin həyata keçirilməsi zamanı istifadə olunacaq ən yüksək səviyyəli prinsipləri müəyyən edən sənəddir.

Ədəbiyyat siyahısı

1. Konğyuxovski. «Ekonomiçeskaya informatika». Piter, SPb, 2001.
2. «Ekonomiçeskaya informatika». Pod red. V.V.Evdokimova. Piter, SPb, 2007 q.
3. V.V.Şurakov. Nadejnost, proqrammnoe obespeçenie. M., 2016 q.
4. V.A.Zarenin. Nadejnost ASU. Kiev, 2006 q.
5. V.M.Qluşkov Osnovı bezbumajnoy informatiki. M., Nauka, 1982.
6. S.Q.Kərimov İnformasiya sistemləri və verilənlər bazaları. Bakı – «Elm», 1999 q.
7.Gostomski, H. R. Bungay, "Multivariable Control of Continuous Cultures," AIChE Meeting (1999).
8.D .Hasloop, and B. R. Holt, "A Network Neural Structure for System Identifications," Procpect. of American Control Conf., 2460 (1999).
3.Y. Arkun and E.Hernandez, "Neural Network Model and an Extend DMC Algorithm to Control Nonlinear System," American Control Conf., 2454 (1990).

9.H. Mukai, B. Joseph and Jang, S. “Comparison of Two Approach to On-Line Parameters and State Estimation of Noonlinear System,” English. Chem. 25, 809 (1996)
10.Миллер Н.Р. Финансовый анализ в вопросах и ответах. М.: UK Велби, Изд-во Проспект, 2005.

Redaksiyaya daxil olma tarixi: 03.06.2024
Çapa qəbul olunma tarixi: 28.06.2024
Rəyçi- dos.İmamquliyev Rahib Aydın
tərəfindən çapa tövsiyə olunmuşdur