Distant təhsil sistemlərində kibertəhlükəsizlik riskləri

Rita İlqar qızı Əsədova
Azərbaycan Dövlət Pedaqoji Universiteti
E-mail: rita_asadova_98@list.ru

Rəyçilər: t.ü.f.d., dos. S.B.Mazanova,
t.ü.f.d., Ç.M.Həmzəyev

Açar sözlər: distant təhsil, kibertəhlükə, risk, təhsil, kiber, alqoritm
Ключевые слова: дистанционное обучение, кибербезопасность, риск, образование, кибер, алгоритм
Key words: distance learning, cybersecurity, risk, education, cyber, algorithm

Bu gün təhsil müəssisələri fəaliyyətlərində elektron məlumatlardan, kompüter texnologiyalarından, informasiya sistemlərindən, İnternet resurslarından və distant təhsil sistemlərindən (DTS) geniş istifadə edirlər.

Bu baza sistemləri bir-biri ilə və təhsil prosesinin iştirakçıları ilə qarşılıqlı əlaqə quraraq, virtual sosial-texniki sistem əmələ gətirir. Bu da müəllimin və şagirdin zaman və məkan xaricində qarşılıqlı əlaqəsinin interaktivliyini və davamlılığını təmin edir.

Distant təhsil texnologiyaları təlim mövzuları, verilənlər bazaları və virtual təhsil obyektlərinin qarşılıqlı əlçatanlığını artıraraq tam zamanlı təhsil imkanlarını genişləndirməyə imkan verir. DTS-ləri olaraq həm təhsil müəssisəsindəki avtomatlaşdırılmış işçi stansiyaları, həm də uzaq qurğular ola bilər. Bunun nəticəsində də kibertəhlükə bütün bir sistemdə zəiflik yaradır. Bu da o deməkdir ki, müxtəlif təhdidlərin təsiri nəticəsində DTS təhlükəsizliyinin pozulması bütöv bir təhsil müəssisəsinin seqmentində və ya bütün məlumat sistemində informasiya təhlükəsizliyinin pozulmasına səbəb olur.

DTS üçün kiber təhlükəsizlik təhdidlərinin mənbələri

Tarixi mənbələrin təhlili göstərir ki, informasiya təhlükəsizliyi təhdidlərinin çoxlu təsnifatı mövcuddur. Praktiki olaraq hər təsnifatda meydana gəlmənin təbiəti (antropogen, texnogen, təbii) və təhlükənin mənbəyi kimi əlamətlər vardır. Bu əlamətləri əsas olaraq götürərək, nəticəyə gələ bilərik ki, baş verənlərin təbiətinə görə, idarəçilərin, DTS istifadəçilərinin, daxili və xarici müdaxilələrin və əlaqəli süni mənbələrin DTS xidmətlərinin proqram çatışmazlıqları, avadanlıqların etibarlılığı və rabitə kanalları məlumat infrastrukturu hərəkətləri səbəbindən antropogen mənbələr DTS üçün daha aktual olacaqdır. Təhdid modeli nəzərə alınmaqla, DTS -də İnformasiya sistemlərinin pozucuları aşağıdakı kimi təsnif olunur:

- **Xarici subyektlər (fiziki fərdlər) - bu təhtid xarici təhtid növünə aiddir. Aşağıdakı məqsədlərlə törədilir:**

— maliyyə / nüfuzuna zərər vurmaq
— özünü həyata keçirmək arzusu;
— bir təhsil müəssisəsinin DTS və İS-in sonrakı satışları və maddi fayda əldə etmək məqsədi ilə onların zəifliklərinin müəyyən edilməsi;
— əqli mülkiyyət oğurluğu (müəllif hüquqları ilə bağlı təhsil materialları, kurslar);
— DTS-in mənbələri və xidmətləri üçün ƏDV əldə etmək;

— tədris prosesinə dair tədris materiallarının və məlumatların bütövlüyünün pozulması və ya məhv edilməsi;

— veb saytın və DTS serverinin mövcudluğunun pozulması;

— DTS istifadəçiləri üçün məlumat və təlim kurs materiallarının mövcudluğunun pozulması;

— tələbə və universitet işçilərinin şəxsi məlumatları üçün ƏDV əldə etmək.

- **Rəqabət aparan qurumlar-xarici təhtiddir və aşağıdakı məqsədlə törədilir:**

— rəqabət üstünlükləri əldə etmək

- **Müəllim, təhsilalanlar**
- **Metodistlər**
- **DTS idarəçiləri, inkişaf etdiriciləri və texniki dəstək xidməti, informasiya təhlükəsizliyi mütəxəssisləri**

Hər biri xarici təhtid növüdür və aşağıdakı məqsədlərlə törədilir:

— DTS-in mənbələri və xidmətləri üçün ƏDV əldə etmək;

— imtiyazları aşmaq və DTS üzərində nəzarəti əldə etmək;

— bir təhsil müəssisəsinin daxili İS-ə güzəştli DTS ƏDV vasitəsilə əldə edilməsi;

— elmi materialların və əqli mülkiyyətin oğurlanması: təhsil materialları, qiymətləndirmə materialları və təhsil prosesinin iştirakçıları tərəfindən kollektiv olaraq yaradılan materiallar;

— tələbə və işçilərin şəxsi məlumatları üçün ƏDV əldə etmək;

— ƏDV almaq və təhsil bəyanatlarının məlumat bazasında dəyişikliklər etmək;

— İS-də saxlanılan və işlənən daxili xidmət və digər məxfi məlumatlar üçün ƏDV əldə etmək;

— tədris prosesinə dair tədris materiallarının və məlumatların bütövlüyünün pozulması və / və ya məhv edilməsi;

— veb saytın və DTS serverinin mövcudluğunun pozulması;

— DTS istifadəçiləri üçün məlumat və təlim kurs materiallarının mövcudluğunun pozulması;

— maliyyə / nüfuzuna zərər vurmaq

Zərərvericinin fəaliyyətinin nəticəsi informasiya, əməliyyat, maliyyə, nüfuz xarakterli təhlükəsizlik riskləri ola bilər. Bunlardan bəziləri təhsil müəssisəsi tərəfindən icazə verilən və qəbul edilən sahədə ola bilər, bəziləri isə qəbuledilməz ola bilər. Risk qərar vermə və strategiya seçimi davamlı idarəetmə dövrünün bir hissəsi olaraq həyata keçirilməlidir.

DTS üçün kiber təhlükəsizlik risklərinin idarə edilməsi alqoritmi

DTS-in müəyyən edilmiş kiber təhdidləri, təhdidin qarşısını almaq və nəticələrin potensial risklərini azaltmağa yönəlmiş qoruyucu vasitələrin və mexanizmlərin istifadəsinin uyğunluğu və ehtiyacı üçün araşdırmaya məruz qalır. Bunun üçün təhdidlərin həyata keçirilmə ehtimalı və mümkün zərər kimi xüsusiyyətləri araşdırılır. Qiymətləndirmə təhlükəsizlik hadisələri haqqında işlənmiş statistik məlumatlar, modelləşdirmə və ya ekspert rəyi əsasında edilə bilər.

Ekspert qrupu yaradılarkən təhdidləri və parametrlərini (ehtimal, ziyan) kəmiyyət, keyfiyyət və ya qarışıq miqyasda qiymətləndirən analitiklərdən, informasiya təhlükəsizliyi mütəxəssislərindən, inkişaf etdiricilərdən, istifadəçilərdən və menecerlərdən bir neçə kateqoriyalı mütəxəssis cəlb olunur, sonra onların təhlili əsasında hər bir təhdid parametrinin ayrılmaz qiymətləndirməsini təşkil edir. Zərər, İT təhdidinin həyata keçirilmə ehtimalı (tezliyi) arasındakı əlaqə təhdidlərin təhlükə dərəcəsinə görə sıralanması zamanı nəzərə alınan təhdidin həyata ke-

çirilməsinin risk səviyyəsini müəyyən edir. Təhlükə nə qədər güclü olsa, risk və onun DTS üçün aktuallığı daha yüksəkdir. DTS həyat dövrünün bütün mərhələlərində təhdidlərin aktuallığını vaxtaşırı qiymətləndirmək tövsiyə olunur, çünki bu təhlükəyə qarşı mübarizə vasitələri və mexanizmlərindən nə qədər istifadə olunmasının zəruriliyini göstərir.

Məqalədə DTS-in kibertəhlükəsizlik risklərini qiymətləndirmək üçün kəmiyyət parametrlərinə əsaslanan iki alqoritm təklif olunur.

Birinci alqoritmə görə şəxsi təhdid siyahılarından hər bir TRij təhdid üçün hansı ki burada j, i-ci DTS alt sistemi üçün xüsusi təhdidlər siyahısındakı təhdidin sıra nömrəsidir. Risk ehtimal olunan bir kəmiyyətdir. Bunu hesablamaq üçün, gözlənilən zərərin göstəricisi - U və təhlükənin reallaşma ehtimalı - p olan iki faktorlu qiymətləndirmə modeli istifadə olunur.

$$R(TR_{ij}) = U_p$$

Təhlükənin reallaşma ehtimalı [0; 1] aralığında dəyişir. Kəmiyyətin dəyəri birbaşa bu DTS-in alt sistemində müdafiə tədbirlərinin olmaması və belə bir təhdidin həyata keçirilmə tezliyinə dair statistik məlumatlardan – h parametrin mövcudluğundan təsirlənir. Mühafizə tədbirlərinin DTS-in alt sistemində təhlükə ehtimalına təsirini qiymətləndirmək üçün hər birinə performans faktoru təyin edilmiş 4 səviyyəli qorumadan istifadə etmək təklif olunur:

- qorunma tədbirləri yoxdur (QSMlevel = 1);
- müdafiə tədbirləri təhlükənin həyata keçirilməsinə maneə yaradır və onun həyata keçirilmə ehtimalını azalda bilər (QSMlevel = 0.75);
- müdafiə tədbirləri bir neçə maneə yaradır və təhdidin həyata keçirilmə prosesini əhəmiyyətli dərəcədə çətinləşdirir (QSMlevel = 0.5);
- qoruma tədbirləri təhlükəni tamamilə maneə törədir (QSMlevel = 0).

Yuxarıdakı düstur və qaydalar nəzərə alınmaqla, i-ci DTS-in alt sistemindəki hər bir təhlükədən yaranan risk miqdarı aşağıdakı formula uyğun olaraq hesablanacaq.

$$R(TR_{ij}) = U_j h_j QSMlevel_j$$

DTS-in hər bir alt sistemi üçün ümumi risk aşağıdakı kimi müəyyən ediləcəkdir:

$$R_i = \sum_{j=1}^{m} R(TR_{ij}) = \sum_{j=1}^{m} U_j h_j QSMlevel_j$$

Burada i DTS-in alt sistemləri, j -hər bir i-ci alt sistemdəki təhtid,m- i-ci alt sistemdə təhtidlərin sayı, $QSMlevel_j$- hər bir alt sistemdəki qoruma tədbirlərinin səmərəlilik faktorudur.

Təhlükənin risk səviyyəsinə uyğunluğunu müəyyən etmək üçün əldə edilənləri məqbul risk səviyyəsi ilə müqayisə etmək lazımdır. Qəbul ediləndən aşağı olan bütün dəyərlər qəbul edilməlidir, qalanları sığortalanmalı və ya qoruma vasitələrindən istifadə edərək azaldılmalıdır.

Riskləri hesablamaq üçün təhlükənin tezliyini, zərərini və təhdidlə mübarizə aparmaq üçün əks tədbirlərin effektivlik əmsalını nəzərə alan üç faktorlu bir modelin istifadəsi təklif olunmuşdur. Təklif olunan yanaşma DTS-in dizayn və tətbiq mərhələsində və ya daxili təhlükəsizlik audit prosesində tətbiq oluna bilər.

İkinci alqoritm "İnformasiya texnologiyaları təhlükəsizliyinin idarə edilməsi üsulları" alqoritmi adlanır. Burada risklər aşağıdakı düstura görə hesablanır:

$$R = P(t) \cdot P(v) \cdot S$$

P (t) - informasiya təhlükəsizliyi təhdidinin həyata keçirilmə ehtimalı;
P (v)-sistemin qorunma dərəcəsi;
S - aktivlik dərəcəsidir.

Məqalənin aktuallığı. Məqalənin müasir təhsil sistemində distant təhsil sistemlərinin kibertəhlükəsizliyinin təmin edilməsi mövzuzundan bəhs etdiyini, eyni zamanda burada əsas təhlükəsizlik risk faktorları, təhlükə növləri və mənbələrinin araşdırıldığını nəzərə alsaq, onu aktual saya bilərik.

Məqalənin elmi yeniliyi. Elmi yenilik kimi məqalədə distant təhsil sistemində informasiya təhlükəsizliyinə zərərvericinin modelinin tərtib edilməsi, onların növləri və məqsədlərinin təsvir olunması, eləcə də kibertəhlükəsizlik risklərinin qiymətləndirilməsi üçün bir alqoritmin təklif və riyazi olaraq təsvirini göstərə bilərik. Həmçinin burada riskləri hesablamaq üçün təhlükənin tezliyi, zərəri və təhdidlə mübarizə aparmaq üçün əks tədbirlərin effektivlik əmsalını nəzərə alan üç faktorlu bir modelin istifadəsi verilmişdir.

Məqalənin praktik əhəmiyyəti və tətbiqi. Məqalədən orta ixtisas və orta ümumtəhsil məktəblərinin müəllimləri, tələbə və magistrantlar istifadə edə bilərlər.

Ədəbiyyat

1.Оладько В.С. Функциональная модель исследования безопасности системы дистанционного обучения/ В.С. Оладько// Безопасность информационных технологий. - 2018. - Т. 25. - № 3. - С. 101-111.

2.Петрова Р.Г. Возможности и риски дистанционного образования в высшей школе/ Петрова Р.Г., Петров С.И., Рябова Т.В. //Казанский педагогический журнал. – 2015. - №. - С. 294 – 299.

3.Руденко Л.И. Моделирование оценки рисков информационной безопасности/ И.Л. Руденко, Пушкарева Е.В. // V Всероссийская с международным участием научно-практическая конференция. Крымский федеральный университет имени В.И. Вернадского. - 2019. – С. 163 – 165.

Р.И. Асадова

Риски кибербезопасности в системах дистанционного образования

Резюме

В статье затрагивается проблема обеспечения кибербезопасности систем дистанционного обучения в образовательных учреждениях. Рассмотрены основные факторы риска безопасности, виды и источники опасности. Разработаны модели вредителя информационной безопасности в системе дистанционного обучения, описаны виды и назначение вредителей.

R.I. Asadova

Cybersecurity risks in distance education systems

Summary

The article touches upon the problem of ensuring the cybersecurity of distance learning systems in educational institutions. The main safety risk factors, types and sources of danger are considered. Models of information security pest in the distance learning system have been developed, the types and purpose of pests are described.

Redaksiyaya daxil olub: 22.10.2021