ISSN 2278-3091

Volume 9 No.2, March -April 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse90922020.pdf

https://doi.org/10.30534/ijatcse/2020/90922020

Web Security in "Digital Prison" Management

Vu Anh Tuan
PhD in law,
Deputy Head of the Department of Personnel Management,
People's Police Academy,
Hanoi, Vietnam

ABSTRACT

In the prison system, it's important to organize effective operational management using digital transformations and interdisciplinary relations, taking into account the social, psychological and legal aspects of systemic processes. It's important to preserve and develop the emergent properties of the system and to build evolutionary paths, based on synergistic principles of management. The issue of security, including web resources and access to them, is also relevant for penal institutions and prisons. IT-infrastructure should be formed and modernized, which not only ensures security, but also allows prisoners to increase the potential of subsequent socialization in society, educational potential. The management of such processes is complicated not by the systemicity of approaches, uncertainty or redundancy in the system. There are communication barriers, emotional barriers and deliberate use of malicious new technologies. This study describes the approaches and principles for a systematic analysis of the manageability and security of prison web resources, and the model and procedure for this task.

Key words: security, prison, site, management, infrastructure, tracking, prisoners, training.

1. INTRODUCTION

The IT-infrastructure of the prison system of any state is undergoing digital transformations. Local and global challenges of the fourth industrial revolution are emerging [1]. They also affect the prison system and its digital reform [2]. New technologies and systems are integrated in conditions not only of detention of prisoners, but also of the entire FSIN system. The execution of punishment is also based on modern trends, technologies, socio-psycho-pedagogical aspects, legal management and regulation of activities in the context of digital transformations in the Penal Correction System (PCS) and throughout society [3].

This leads to the need for systematic research into new, digital technologies and approaches in prison management, creating conditions for solving their current and systemic problems. There's increasing interest in creating and maintaining prison sites, but even more in ensuring their safety. The reflection of social differences is also relevant [4].

The problem of infrastructure for tracking prisoner behavior using web resources, the Internet, is also relevant. The tasks of the educational plan for prisoners are also being intensified. For example, a prisoner is enrolled in an online course or undergoes additional education in a second specialty.

In particular, these include the acquisition of additional competences by prisoners in the following forms:

1) distance learning - organization of distributed educational process on the basis of self-education, self-organization;

2) open, mass online training (courses) - support of individual and hybrid (1 and 2) trajectory of training or scientific and educational activities.

Most prison web resources are not adapted for mass safe, use. The management of such resources is complicated by uncertainty and redundancy. The content of such sites isn't relevant to the goals of the prison system, does not stimulate adequate behavior of the prisoner [5].

Some prisoners, even in detention, are ready to wage information war against society, the state, the society[6]. There are unjustified communication barriers, even an emotional stress. Information processing is difficult, users experience difficulties if they try to structure and organize the content themselves. They can fall under the influence of negative information[7].

A separate and important task is the use of web resources in the management and security of prisons. Up to the use of technological innovations by intruders, for example, UAVs [8]. The necessity of innovative methods tested in the practice of PCS is emphasized in the main evolutionary document of the Russian Federation [9].

This work systematically analyzes the problem of ensuring manageability, sustainability and security of web resources of PCS, and proposes an approach and model for solving this and related problems. For example, such an application is of interest to those who investigate corruption in Russia [10].

2. METHODOLOGY

The integration of methods, technologies and targets in the above tasks is feasible in various ways. Let's highlight those that are most significant:

1) interaction of web-technologies in ensuring solution of tasks (the impact of economic policy uncertainties must also be assessed;

2) high-quality digital transformation, development of IT infrastructure, including limited, managed Internet access;

3) modernization and improvement of management, effective use of web resources and web tools.

4) ensuring awareness and motivation (both employees and prisoners) in the use of non-prohibited and non-recommended online platforms, resources[11].

It should be noted that the analysis of the responses of most of the staff and prisoners interviewed anonymously by experts showed that they want to receive more information, but are difficult to find it, do not understand the consequences of the use of web resources not safe for them and society [12]. It's important to address the problem of restricted, filtered access, for example, only for educational purposes and subsequent socialization [13;14].

We also take into account new approaches to solving socio-economic problems based on the transition to individualism [15].

The main methodology of attracting to the web resource used in this work, conditional and meaningful, can be indicated by the principle: "Promotion of writing, education and safety in virtual space". It concerns promotion, which shouldn't weaken comfort, interactivity, security of the site and IT-infrastructure of the institution PCS. It's also protection of content, structure, as well as protection against CMS hacking and access to site management (administration) through possible "loopholes" (vulnerabilities) of the site. We find a "middle ground": we protect the site - we do not make it difficult to work with it, its escort in the future.

We also use formal methods - an approach using likelihood functions. You can also use a multi-agently approach, as in work Kleiner[16]. Prison architectonic is taken into account[17].

3. DISCUSSIONS AND RESULTS

The management of the information resources of the UIS institution raises the following topical questions, which we will give with our answers, as we present them.

What to protect? - Specifications, templates, content, programs, data structures, databases, contacts, code and password information, etc.

What to fear? - Illiterate, unskilled actions (without intent or with malicious intent), failures, unstable, easily hacked passwords, viruses, etc.

How to insure? - Coded access, logging, staff reliability, regular auditing and training, data duplication and backup.

Problems of information product security, management of information-logical resources – many [18]. The following classes of threats, vulnerabilities are common, regardless of "power," topics and location of the site:

1) operation errors;

2) actions of unscrupulous users;

3) maintenance, software (equipment, programs) failures;

4) introduction of viruses (Trojans, worms, etc.);

5) ignoring accepted rules and system access restrictions;

6) design, development errors (they are not mandatory, but probable).

Security activities directly depend on threats to the site, for example, we offer the following effective measures:

1) selection of reliable CMS;

2) coded and priority, controlled access (password system generation);

3) dynamic audit of user activity (profiles);

4) filtration (content, etc.);

5) reliable personnel (careful selection and testing);

6) stimulation of safe work of personnel and training of personnel (improvement of competences and self-education);

7) monitoring, testing and auditing of the site (better performed with the help of outsourcing companies);

8) use of up-to-date antivirus databases and packages (licensed only);

9) backup of databases and data (place in clouds or on the resource of outsourcing company).

To develop an effective security policy is to solve half the case. The second half is activity tracking. Where, when and to what pages the user entered - everything is now available to hackers. Programs are designed to track children's activities at a computer or staff during working hours.

Video tracking is integrated with PCS safety systems - local networks, workplaces of personnel, protected area, GPS and GLANASS navigation.

There are police programs (for example, StaffCop, Russian program) monitoring personnel. Similar wardens should be developed and effective. We also take into account statistics according to which companies lose millions annually because employees "sit" on social networks; engage in insider, although the Law on Insider and Insider Information is quite effective (note, very "strict"), etc.

The virtual supervisor (operator) collects information on:

1) programmes (what, when, how long worked);

2) sites (when, which pages, sites were opened, when they were viewed);

3) computer screens (screenshots, images at the specified interval);

4) USB devices, if enabled (device type, connection/disconnect time), etc.

With the help of such a virtual warden, who manages the PCS system, discipline can be increased and violations prevented.

Although the public expresses concern about the security of information, studies have shown that cases of hidden (unauthorized, unjustified for the purposes of clients) collection of data on users do not disappear. For example, due to the growing popularity of auctions, where advertisers acquire the necessary information on the web activity of users. There's also a growing number of virtual fraud, directly from the prison cell. For example, cases of fraudulent schemes on AVITO, on web payment systems are known.

Although fraud is not regulated fully by law ("Trying to regulate everything by law will rather cause defects" - Spinoza), intolerance against it in society, web communities, media and legal literacy of prisoners should be increased.

The competences of prison staff in introducing innovations and best practices, as well as the flexibility and dynamism of PCS processes, are important here. Competences of system analytics, situational modeling, and general legal culture are necessary, because prisoners often don't think themselves outside of virtual space. They should be provided with access, and law-abiding citizens should be protected from "IT traps", criminals themselves apply IT.

Opportunities to track site visitors, apply neuro-marketing, neural network tracking algorithms, etc., are also growing. There are various facial recognition programs, such as YouTube Faces, which activates more than 3,000 videos across 1,500 individuals, including in different environments and shooting conditions.

It's proposed to use plausible inconsistencies [19] in conditions of small samples of observations.

It maximizes the probability densities of inconsistencies between the current image (input) and the references extracted from the last layers of neuro network convolution (output). As a criterion for assessing likelihood, we take the distribution of Jensen-Shannon inconsistencies [20], see also [21]:

$$F(p,q) = 1 + 0.5\sum_{i=1}^{n}\left(p_i log_2\frac{p_i}{p_i + p_j} + q_i log_2\frac{q_i}{q_i + q_j}\right).$$

Let's note that

$$p = (p_1, p_2, \dots, p_n),\ q = (q_1, q_2, \dots, q_n)$$

Are distributions of probabilities (inconsistencies), and the following conditions are fair:

$$\sum_{i=1}^{n} p_i = 1,$$

$$\sum_{i=1}^{n} q_i = 1.$$

When recognizing, we identify the proximity of the input with all outputs, for each class we estimate the likelihood of identified inconsistencies.

4. CONCLUSION

You can get almost half of the information about users by their web visits, stories. And latently, with the help of data collector programs, which operate after visiting the site where they are installed.

Are legal conflicts with privacy problems possible? - The question is complex, subtle, compromise. Do you want to include "non-tracking feature (DoNotTrack button, DNT)" in your web browser? - Almost a third of Internet users know about it, but only use 4%. At the same time, for example, 45% of respondents in the USA know about the right to privacy on the Internet.

In the Intranet (corporate Internet environment), you can detect an intrusion by using tools to find and analyze the behavior of the user, his deviations from the behavior of the regulated. Based on statistical methods, signature analysis, network segments, and individual security policies for each user.

Reliability is a measure of quality. It's a quantified and qualitatively evaluated indicator that affects processes depending on the peculiarities of conditions, external impacts (interference immunity, for example) and the growth of their importance. Everything is determined by security policy, risk, threat, impact assessments, which can summarize data in real mode, from various sources.

Security policy measures include outsourcing of the following processes:

1) web site development, its support;
2) automation (especially office management);
3) services from Big Data, data centers, etc.;
4) security, including re-engineering;
5) improvement of tools such as CMS;
6) increased and shared responsibility;
7) risk management, etc.

The results of this work show the need to combine both formal-mathematical and information-logical methods (algorithms) and heuristic, web-analytical methods.

In this direction, work can be developed.

REFERENCES

[1] A.V. Scherbakov.Theoretical and legal aspects of security criminal correction system / A.V.Scherbakov // Person: crime and punishment. Vol.26(1-4), № 2.pp.187-192.2018.

[2] Y.I. Duk.Problems of reforming the criminal executive system of the Russian Federation // Criminology: Yesteday, Today, Tomorrow, No 2(45), pp.52-56. 2017.

[3] V.G. Gromov. Implementation of Principles of Penal Enforcement Legislation in Execution // Modern law, №9, p.20.2008.

[4] C. Torres&S.Canon. The neighborhood: social sphere of agreements and disagreements // Revista Amazonia Investiga, vol.4(7), pp.66-73.2015

[5] H.Hartmann. Ego-Psychology and the Problem of Adaptation.–N.-Y.: International University Press.1950.

[6] V.E. Lepsky.Technologies of Management in Information Wars (from Classic to Post-Classical).-M.: Kogito-center, p.160.2016.

[7] D. Li&L.Agha. Big names or big ideas: Do peer-review panels select the best science proposals? // Science, 348(6233), 434–438. DOI: 10.1126/science.aaa0185.2015.

[8] S.M. Kolotushkin. Legal and organizational aspects of prevention of revenues to the territory of institutions of the Federal Penitentiary Service of the forbidden objects with use of unmanned aerial vehicles // The III International penitentiary forum "Crime, Punishment, Correction": collection of theses of reports (Ryazan, November 21-23, 2017, vol.1). -Ryazan: FSIN of the Russian Federation academy, pp.148-152.2017.

[9] Concept of Development of the Penal Correction System of the Russian Federation until 2020, The Government of the Russian Federation of October 14, 2010 №1772-r [Electronic resource] // ATP "Garant" (date of appeal: 17.01.2020).

[10] R.Mukhayev&E. Prokopenko.Corruption as a global threat to sustainable development: a look from Russia. Amazonia Investiga, No 9(25), pp.160-175.Retrieved from: https://www.amazoniainvestiga.info/index.php/amazonia/article/view/1041(date of appeal: 17.01.2020).2019

[11] V.M.Kaziev, B.V. Kazieva&K.V. Kaziev.Basics of legal informatics and informatization of legal systems (2nd ed.), INFRA-M, -Moscow. -336 p.2017.

[12] V.T. Volov. Innovative system of education in extreme conditions // The Bulletin of Volgograd University, vol.4, pp.49–54.2008.

[13] V.T. Volov. Higher education as a factor of social safety of society. Publishing house of the Samara Center of the Russian Academy of Science. -Samara, 393 p. (In Russian).2013

[14] V.T.Volov, N.U. VolovaandV.V. Volov.Theoretical-methodological basic of the prisoner's person socialization control problem / Social pedagogical education institute of the Russian Academy of Education. -Moscow. -175 p. (In Russian). 2017.

[15] I.L. Lyubimov. From universalism to individualism: New approaches to economic growth analysis. VoprosyEkonomiki, No 11, pp.108-126.(In Russ.) DOI: https://doi.org/10.32609/0042-8736-2019-11-108-126.2019.

[16] G.B. Kleiner, M.A. Fishachuk & D.V. Ushakov. Agent-oriented model of professional expertise and decision-making in support of selected socially significant initiatives // Terra Economics, 17(2), pp.23-39. DOI: 10.23683/2073-6606-2019-17-2-23-39. 2019.

[17] M.V. Sorokin & O.E. Sorokina. Prison Architectonics as an Element of Prison Security // Journal of Vladimir State University (series: jurisprudence), No 2(8), pp. 35-43.2016.

[18] Prison Technologies An appraisal of technologies of political control. Luxemburg.2010.

[19] A. V.Savchenko. Image recognition based on the method of maximum likelihood dissimilarities // Russian National Conference MMPR-18. -Russia, Taganrog, October 9–13, p.101.2017.

[20] J. Lin. Divergence measures based on the Shannon entropy // Information Theory, IEEE Transactions on, vol.37, N1, pp.145–151.1991.

[21] V.Dobrynin, N.Rooney &J.Serdyuk.Setting lower bounds on Jensen–Shannon divergence and its application to nearest neighbor document search // The Bulletin of Saint Petersburg University (Applied Mathematics. Computer Science. Control Processes), vol.14, iss.4, pp.334–345. DOI:https://doi.org/10.21638/11702/spbu10.2018.406. 2018.