DOI: 10.18372/2410-7840.20.12452
УДК 681.3.093:044.3

DATA CENTER AUTHORITY DISTRIBUTION AND CYBER-DEFENSE MODELING

Artemii Kropachev, Denis Zuev

Data Center authority distribution and cyber-defense measures development was analyzed. It was shown that paradigm of openness and information sharing as a cultural norm significantly enlarges number data loss vectors. Analysis demonstrated that on physical level main trend of irresponsible information sharing is exponential growth of the information recording density which was caused by reduction in data storage price. It led to network channel capacity growth and decentralization of information systems in order to organize effective communication infrastructure. It was proposed to divide data loss vectors into groups of people-based vulnerabilities, process-based vulnerabilities and technology-based vulnerabilities. Data loss prevention strategies should be based on data classification methodology. In this work there were used two classification schemes: one of them divides confidential data into categories of customer data, employees' data, transaction data, corporate data. Other one analyzes data loss threat in concordance to the states in the data lifecycle as data at rest, data in motion and data in use. It was mentioned that use of Data Center services significantly increases efficiency of IT infrastructure and data loss prevention strategy implies that for stored confidential data has to be used virtual server that provides a guaranteed part of the Data Center server resources. It was considered that data loss prevention strategy includes stages of data governance, data loss prevention management and information security support. After development of Data Center infrastructure authority distribution, security policies and cyber-defense measures cyber-attack probability could be calculated as sum of bandwidth exhaustion, filtering depletion and memory depletion probabilities.

Keywords: *Data Center, authority distribution, data loss vectors, channel capacity, cyber-attack, bandwidth exhaustion.*

1. Introduction

Confidential data is one of organization's most valuable resources so its protection is a task of great importance. In order to accomplish this task, a number of data loss prevention (DLP) methods which combine strategic and operational measures were implemented. First stage of DLP control development is analysis of sensitive data types, storing methods and transfer protocols. Technological development has caused data volumes and communication channels rapid growth which significantly increased risk of unauthorized parties gain access to confidential data. The current trends of global networks development show growth of the capabilities and connectivity of users, and, thereby, IT risk spectrum will widen.

Ensuring effective Data Center protection is a complex task which includes analysis of the reasons that affect the efficiency of the Data Center work, construction of a mathematical model for the emergence of cyber-threats, as a stochastic process; Data Center management network, load balancing for servers; organization of protection of vulnerable network nodes from cyber-attacks; providing real-time protection system operation; proactive protection of information sources outside the perimeter; development of a strategy for preventing internal information losses; automation of means of protection and proper training of personnel; integration of monitoring systems and cyber-security of Data Center infrastructure. It is important to note that modern Data Centers infrastructure must be scalable and flexible, they combine physical and virtual resources, so security systems must be dynamically scaled and provide permanent protection. Organizing of the internal network should include development of automatic application of the security policies in order to be used in new systems, so that their deployment time could be significantly reduced without losing the efficiency of the protection systems.

2. Data loss vectors

Exponential growth of the density of information recording (Fig. 1a) caused by reduction in price of data storage led to necessity network channel capacity growth (Fig. 1b) and decentralization of information systems in order to organize effective communication by sharing of colossal volumes of data [1, 2].

New paradigm of Open World was born and for most recent generation has grown up with openness and information sharing as a cultural norm (Fig. 2). It was noticed that employees of Data Centers do not always understand that information has value in the real world and its sharing is not always legitimate process. There are a lot data loss vectors and it's often hard to predict how sensitive information could leave an organization [3].

Additionally, regulatory risks for Data Centers and cloud services are also tend to increase. Amount and impact of incidents has resulted in growth of attention from regulators. Data protection requirements are becoming stricter and penalties tend to rise. Thereby reduction of data loss risks will not only prevent of sensitive data and intellectual property loss but also will significantly reduce regulatory risks.

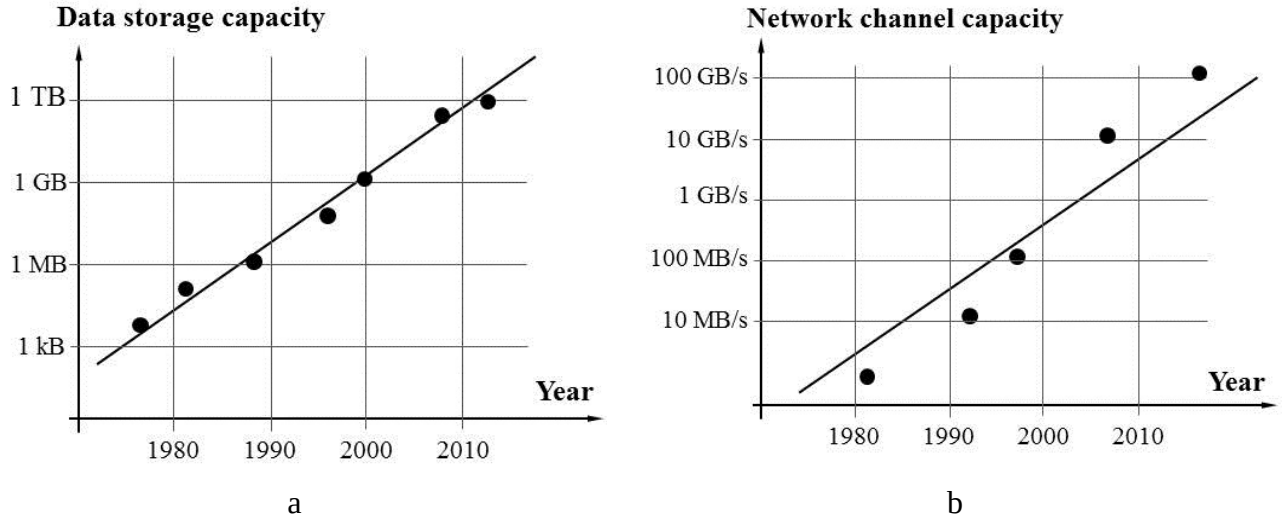

Fig. 1. Tendency of exponential growth of data storage (a) and network channel capacity (b)

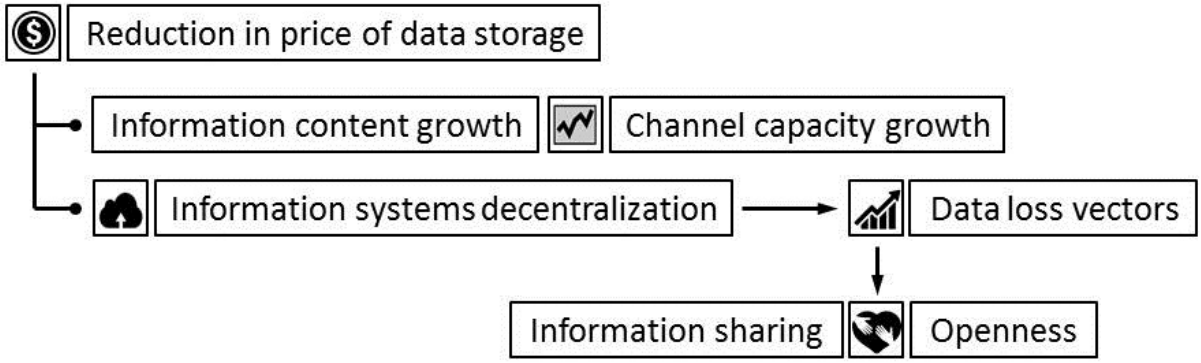

Fig. 2. Trends of Open Worlds Paradigm which increase cyber-threat risks

Data loss vectors are usually forms further groups [3, 4]:

- people-based vulnerabilities;
- process-based vulnerabilities;
- technology-based vulnerabilities.

People-based vulnerabilities group should be starting point of data loss prevention analysis which has to include:

- Data Center employees' awareness analysis;
- Data Center employees' responsibility;
- Data Center accountability policies analysis.

People-based vulnerabilities are mostly based on lack of Data Center users and personal authority distribution. They naturally lead to further process-based vulnerabilities:

- lack of data use policies;
- insecure data transmission procedures;
- insufficient data usage monitoring.

Being ignored process-based vulnerabilities and people-based vulnerabilities become systematical one. Thereby they form group of technology-based vulnerabilities:

- lack of flexibility in Data Center remote connectivity;
- lack of content-aware data loss prevention (DLP) tools;
- no secure communication platforms.

Figure 3 shows links between groups and subgroups of data loss vectors that were mentioned above.

It was shown that Data Canters' employees often do not feel accountable for the protection of sensitive data. Training programs should be focused appropriate use of network technologies and security tools. Each employee's personal responsibility for data protection policies and appropriable penalties should be clearly defined. As for process-based vulnerabilities data classification and data use policies have to be clearly articulated. It includes protocols of sending sensitive data to third party, sharing of data storage and sensitive data protection controls. Ongoing DLP monitoring program, policy violations identification, policy communications organizing and awareness programs implementation effectively prevent. It's also important to provide flexible remote access tools of Data Center infrastructure to prevent alternative unmonitored communication channels.

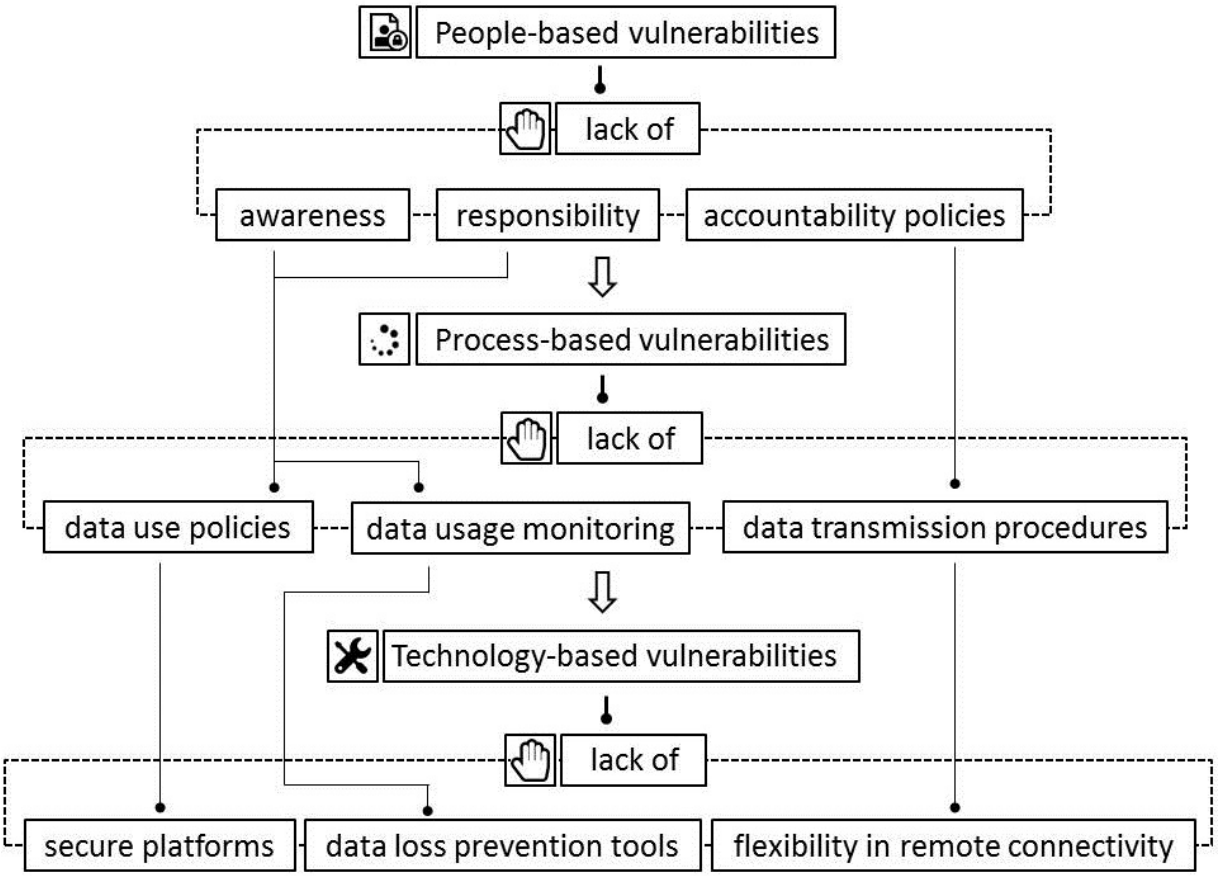

Fig. 3. Data loss vectors groups correlation diagram

3. Data losses classifications

Data Center DLP-strategies are usually based on data classification methodology. Sensitive and confidential data could be divided into further categories (Fig. 4):

- customer data;
- employees data;
- transaction data;
- corporate data.

Customer data losses are associated with inappropriate access of the Data Center employees to the shared storage with sensitive data. Untrained and irresponsible staff member often use insecure data export procedures and copy it on private data storage. Employees personal data losses are also could be associated with staff unawareness but they are often caused due to exploitation of Data Center environment weaknesses. A database administrator is able to use reverse engineering procedure which is could be easily sanitized by referencing hidden tables.

Transaction data losses are usually caused by its reconstruction by developers who knows Data Center access policies and restrictions. In other hand corporate data losses are associated with unsupervised front office work which provides data and screenshots of internal systems to fraudsters, employee discontent and employee insider trading of important data to an external analyst.

It is also important to analyze data loss threat classification related to the states in the data lifecycle (Fig. 5):

- data at rest;
- data in motion;
- data in use.

Data at rest should be stored within Data Center infrastructure which includes servers, databases, open access storage, intranet sites, workstations, portable computers HDD and backup storage, and removable media. Data at rest can also be stored externally at cloud storage. Data in motion is data that is in transit through global networks. Data in use is data with open access for employees which includes data in temporary memory, open reports on workstations, email data and data being transferred between documents [3, 5].

The use of Data Center services significantly increases efficiency of IT infrastructure. DLP strategy implies that for stored data after clarifying the requirements for storage configuration should be used virtual server that provides a guaranteed part of the Data Center server resources. For data used and data in motion, a colocation service is provided, which includes

application and monitoring a client's server. This allows to save on the organization of the communication channel from the provider to the client, so collocation is used for servers intended to support web sites and other global network services that are characterized by a large volume of traffic where has to be used equipment that requires secure access from many points (VPN hubs, IP telephony gateways, etc.). The most effective and flexible solution in this case is the use of dedicated area, i.e., the allocation of a part of the technological area of the Data Center for clients with internal security standards, which can be considered as the creation by the customer of its own virtual Data Center structure based on the original Data Center hardware and software resources.

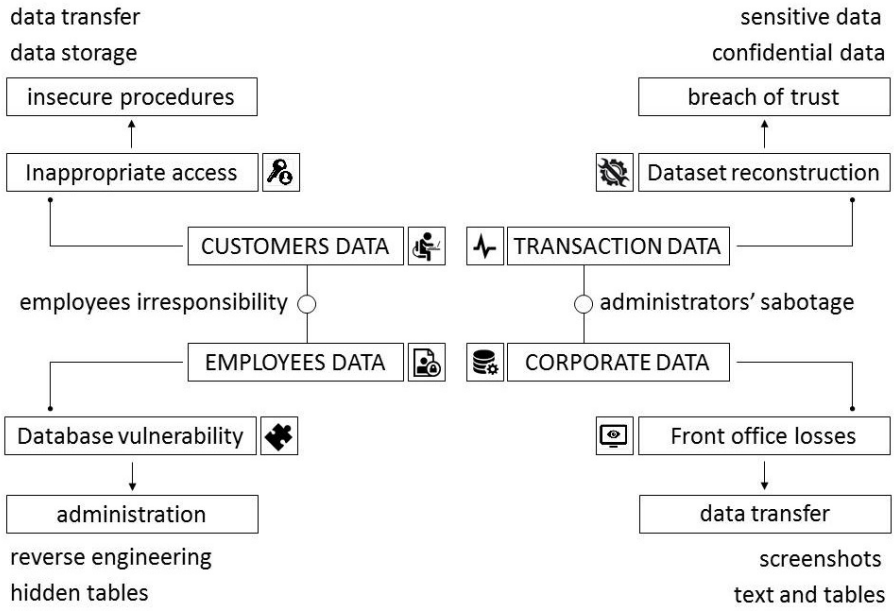

Fig. 4. Sensitive and confidential data categories

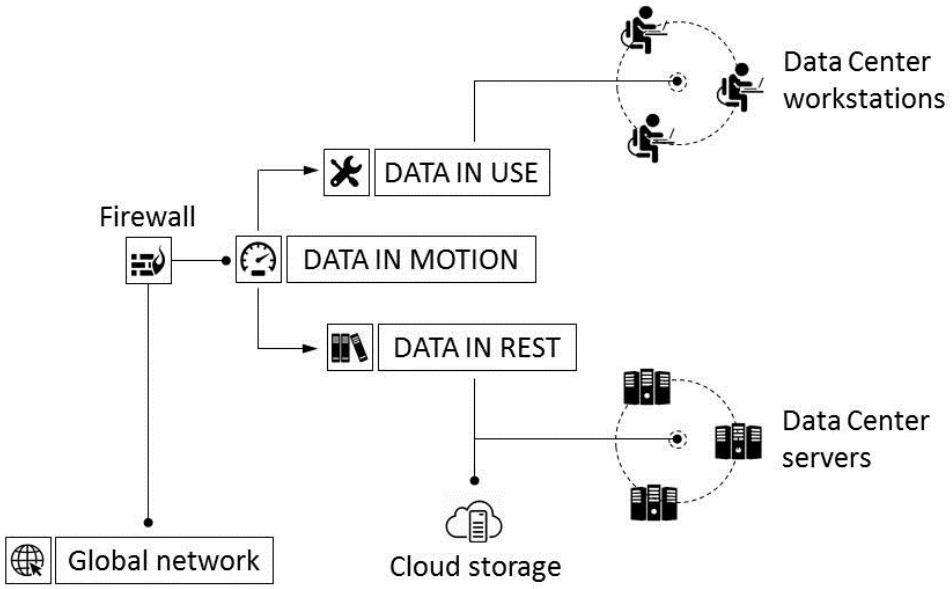

Fig. 5. Data categories classification based on data lifecycle

3. Data losses prevention strategy

The DLP strategy model includes the following phases (Fig. 6):

- data governance;
- DLP management;
- information security support.

The data governance phase consists of developing standards and data center policies, identification models, risk assessments, classification development, architecture's design and quality assessment methodology. DLP controls should be chosen in accordance with functional areas. Information security support in-

cludes access management, event management, configuration management, incident response, physical security, awareness training programs, asset management, data privacy management, employees' screening, system development lifecycle (SDLC), processing continuity, disaster recovery system and compliance management [3, 5, 6].

After defining the types of data to be protected, it is necessary to analyze the place that this information takes in the IT infrastructure of the organization, dividing the data into blocks to be stored in structured repositories and ones to be stored in unstructured repositories which should be shared with end-users on network resources and workstations.

The last phase is analysis in the terms of probability of cyber-attack (CA) which includes analysis of DDoS attack aftermath, filtering properties of DLP-system, bandwidth and memory depletion. It should be mentioned that incoming CA traffic can be blocked in case of insufficient bandwidth and data left after filtering can be also blocked in case of insufficient place in buffer memory. For bandwidth exhaustion probability of P_B, probability of regular traffic filtering of P_R and memory depletion probability of P_M it can be calculated probability of successful CA P_A as sum of bandwidth exhaustion, filtering depletion and memory depletion probabilities [3, 7]:

$$P_A = \sum\left(1 - (1 - P_B) \cdot (1 - P_R) \cdot (1 - P_M)\right). \quad (1)$$

For estimating bandwidth exhaustion probability can be used stochastic model which includes analysis of open channels number, normal traffic, channel bandwidth, average query size of CA and average query size of legitimate users.

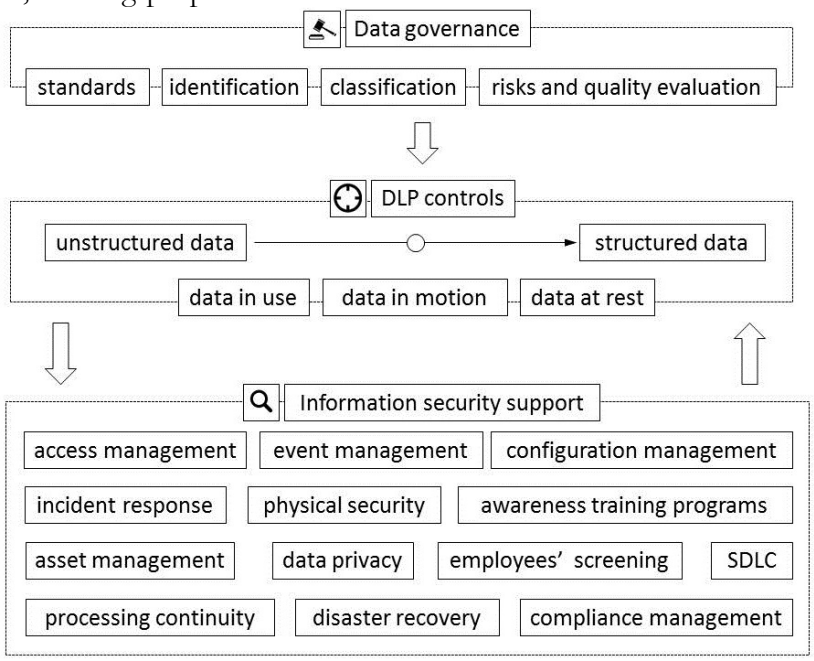

Fig. 6. Basic model of the DLP-strategy for Data Center

4. Conclusions

Paradigm of Open World significantly enlarges number data loss vectors. Data loss vectors could be divided into groups of people-based vulnerabilities, process-based vulnerabilities and technology-based vulnerabilities. Data loss prevention strategies should be based on data classification methodology which include schemes of data categories and data lifecycle. Data Center services significantly increases efficiency of IT infrastructure and data loss prevention strategy implies that for stored confidential data has to be used virtual server that provides a guaranteed part of the Data Center server resources. DLP-strategy has to include stages of data governance, DLP-management and information security support. After development of Data Center infrastructure authority distribution, security policies and cyber-defense measures cyber-attack probability could be easily calculated as a sum of bandwidth exhaustion, filtering depletion and memory depletion probabilities.

REFERENCES

[1]. Z. Sojaat, K. Skalaa, "The dawn of Dew: Dew Computing for advanced living environment", *40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2017, doi:10.23919/mipro.2017.7973447.

[2]. M. Vermaat, S. L. Sebok, S. M. Freund, J. T. Campbell, M. Frydenberg, *Discovering computers 2018: Digital technology, data, and devices*, Boston, MA: Cengage Learning, 2017.

[3]. S. Pulickal, *Data Center: An emerging real estate asset class,* 2013.

[4]. M. T. Raggo, "Understanding Mobile Data Loss Threats", *Mobile Data Loss*, pp. 7-16, 2016, doi:10. 1016/b978-0-12-802864-3.00002-7.

[5]. M. Harris, "Data Center Infrastructure Management", *Data Center Handbook*, pp. 601-618, 2014, doi:10.1002/9781118937563.ch33.
[6]. V. Mulay, "Environmental Control of Data Centers", *Data Center Handbook*, pp. 343-357, 2014, doi:10.1002/9781118937563.ch18.
[7]. Ch. O. Kennedy, *Security Operations Center Guidebook*, 2017, Iv. doi:10.1016/b978-0-12-803657-0.00022-2.

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ РАСПРЕДЕЛЕНИЯ ПОЛНОМОЧИЙ И ОБЕСПЕЧЕНИЯ КИБЕРЗАЩИТЫ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Проанализировано распределение полномочий для центра обработки данных и разработка мер по обеспечению его кибербезопасности. Было показано, что парадигма открытости и обмена информацией как культурной нормы значительно увеличивает вероятность потери данных. Анализ показал, что на физическом уровне основной тенденцией безконтрольного обмена информацией является экспоненциальный рост плотности записи информации, который был вызвана снижением цен на носители информации. Это, в свою очередь вызвало рост пропускной способности сетевых каналов и децентрализацию информационных систем для организации эффективной коммуникационной инфраструктуры. Было предложено разделить векторы потери данных на такие группы уязвимостей как «персонал», «процессы» и «технологии». Стратегии предотвращения потерь данных должны основываться на методологии классификации данных. В этой работе использовались две схемы классификации: одна из них группирует конфиденциальные данные на категории данных клиентов, данные сотрудников, данные транзакций и корпоративные данные. Другая анализирует угрозу потери данных в соответствии с состояниями жизненного цикла данных: данные на хранении, данные в движении и используемые данные. Было отмечено, что использование услуг ЦОД значительно повышает эффективность ИТ-инфраструктуры, а стратегия предотвращения потери данных предполагает, что для сохраненных конфиденциальных данных должен использоваться виртуальный сервер, который обеспечивает гарантированную часть ресурсов сервера центра обработки данных. Было указано, что стратегия предотвращения потери данных включает следующие этапы: управление данными, предотвращением потери данных и поддержка информационной безопасности. После разработки распределения полномочий инфраструктуры ЦОД, политики безопасности и мер кибербезопасности вероятность успешной кибер-атаки может быть рассчитана как сумма вероятностей исчерпания пропускной способности канала, фильтра и памяти вследствие атаки.

Ключевые слова: центр обработки данных, распределение полномочий, векторы потери данных, пропускная способность канала, кибер-атака, пропускная способность канала.

МОДЕЛЮВАННЯ ПРОЦЕСІВ РОЗПОДІЛУ ПОВНОВАЖЕНЬ І ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ЦЕНТРІВ ОБРОБКИ ДАНИХ

Проаналізовано розподіл повноважень для центра обробки даних і розробка заходів щодо забезпечення його кібербезпеки. Було показано, що парадигма відкритості та обміну інформацією як культурної норми значно збільшує ймовірність втрати даних. Аналіз показав, що на фізичному рівні основною тенденцією безконтрольного обміну інформацією є експоненціальне зростання щільності запису інформації, який був викликаний зниженням цін на носії інформації. Це, в свою чергу викликало зростання пропускної здатності мережних каналів і децентралізацію інформаційних систем для організації ефективної комунікаційної інфраструктури. Було запропановано розділити вектори втрати даних на такі групи вразливостей як «персонал», «процеси» і «технології». Стратегії запобігання втрат даних повинні грунтуватися на методології класифікації даних. У цій роботі використовувалися дві схеми класифікації: одна з них групує конфіденційні дані на категорії даних клієнтів, дані співробітників, дані транзакцій і корпоративні дані. Інша аналізує загрозу втрати даних відповідно до станів життєвого циклу даних: дані на зберіганні, дані в русі-ванні і використовуються дані. Було відзначено, що використання послуг ЦОД значно підвищує ефективність IT-інфраструктури, а стратегія запобігання втрати даних передбачає, що для збережених конфіденційних даних повинен користуватися віртуальний сервер, який забезпечує гарантовану частину ресурсів сервера центру обробки даних. Було зазначено, що стратегія запобігання втрати даних включає наступні етапи: управління даними, запобіганням втрати даних і підтримка інформаційної безпеки. Після розробки розподілу повноважень інфраструктури ЦОД, політики безпеки і заходів кібер-безпеки ймовірність успішної кібератаки може бути розрахована як сума ймовірностей вичерпання пропускної спроможності каналу, фільтра і пам'яті внаслідок атаки.

Ключові слова: центр обробки даних, розподіл повноважень, вектори втрати даних, пропускна здатність каналу, кібератака, пропускна здатність каналу.

Kropachev Artemii, Bell Integrator USA Automation Solution Department Manager (USA, Colorado).
E-mail: beckett@protonmail.ch.
Кропачев Артемий Васильевич, менеджер отдела автоматизации Bell Integrator USA (США, Колорадо).
Кропачев Артемій Васильович, менеджер відділу автоматизації Bell Integrator USA (США, Колорадо).

Zuev Denis, Independent Consultant Lead Arcitect, Network and Cloud (USA, Colorado).
E-mail: root@dzuev.pro
Зуев Денис Олегович, независимый консультант, ведущий архитектор Network and Cloud (США, Колорадо).
Зуєв Денис Олегович, незалежний консультант, провідний архітектор Network and Cloud (США, Колорадо).