УДК 930.25: 616.98:578

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ДАННЫХ И УСИЛЕНИЯ ЗАЩИТЫ СЕТЕЙ В СОВРЕМЕННЫХ ОРГАНИЗАЦИЯХ

Садег Зарей Кариани

аспирант, Высшая школа производственного менеджмента, Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Россия, zarej.ks@edu.spbstu.ru

Вопросы кибербезопасности играют для организаций ключевую роль в защите конфиденциальных данных и обеспечении безопасности. Поскольку сложность киберугроз возрастает, важно постоянно укреплять и защищать сети, чтобы предотвратить действия потенциальных злоумышленников. Цель данной статьи – обсудить стратегии и технологии защиты данных, а также дать предложения для повышения кибербезопасности в современных организациях. Безопасность данных включает использование надежных протоколов шифрования для защиты конфиденциальной информации и предотвращения несанкционированного доступа к системам. Шифрование делает невозможным перехват информации неавторизованными лицами, а реализация средств контроля, включая многофакторную аутентификацию, разграничивает доступ к данным и действия уполномоченного персонала. Совершенствование технологии защиты данных также строится на развертывании систем обнаружения и предотвращения вторжений (IDPS) для выявления и нейтрализации потенциальных угроз в режиме реального времени.

Ключевые слова: цифровая эпоха; информационная безопасность; защита данных организации; организационная информация.

FEATURES OF ENSURING CYBERSECURITY OF DATA AND STRENGTHENING NETWORKS PROTECTION IN MODERN ORGANIZATIONS

Sadegh Zarei Karyani

postgraduate student of the Graduate School of Industrial Management, Peter the Great Saint Petersburg Polytechnic University, Saint Petersburg, Russia, zarej.ks@edu.spbstu.ru

Cybersecurity issues play a key role for organizations in protecting confidential data and ensuring safety. As the sophistication of cyber threats increases, it is important to continuously harden and protect networks to prevent potential attackers. The purpose of this article is to discuss data security strategies and technologies and improve cybersecurity networks in modern organizations. Data security involves the use of strong encryption protocols to protect sensitive information and prevent unauthorized access to the system. Data encryption makes it impossible for unauthorized persons to intercept the information.

These access controls must be implemented to limit access to data and access by authorized personnel, and multi-factor authentication is an important component. The improvement of data protection technology is also based on the deployment of intrusion detection and prevention systems (IDPS) to identify and neutralize potential threats in real time.

Keywords: digital era; information security; organizational data protection; organizational information.

Введение

Достижения цифровой индустрии в современную эпоху повлекли за собой существенные изменения, в частности, процессов цифровизации и автоматизации финансовых и организационных структур. Несмотря на преимущества, обеспечиваемые цифровизацией, проблемы и риски в сфере защиты финансовой информации компаний остаются актуальными. По мере значительного увеличения объема данных в организациях вопросы кибербезопасности становятся все более важными. В последние годы кибератаки и кибердиверсии выявили уязвимости и недостаточную защиту данных в различных организационных структурах. Например, утечка данных из крупнейшего кредитного бюро Equifax в 2017 году привела к компрометации конфиденциальной финансовой информации миллионов людей [1; 2]. Подобные случаи подчеркивают необходимость совершенствования знаний и навыков специалистов в области кибербезопасности для защиты финансовых данных своих клиентов.

Утечки корпоративных данных и их раскрытие могут иметь необратимые последствия, включая значительные финансовые санкции со стороны законодателей и регулирующих органов, а также снижение доверия клиентов [3; 4]. В то же время хакерские атаки программными средствами (разнообразные вирусы, трояны, DDoS-атаки, фишинг и др.) могут существенно нарушить деятельность информационных и коммерческих систем, что приводит к срыву оказания услуг и нанесению репутационных и финансовых потерь [5]. Внутренние угрозы, такие как преднамеренное и непреднамеренное раскрытие информации и данных сотрудниками компаний, хотя и менее обсуждаются, но также несут существенные риски. Организациям следует рекомендовать внедрять системную иммунизацию, чтобы минимизировать данные риски, что потребует применения единого комплексного подхода, включающего анализ стратегий и разграничение прав доступа, который может улучшить защиту данных. Необходимость внедрения таких мер, как контроль доступа, разнообразные методы шифрования и систем сетевого мониторинга для предотвращения несанкционированного доступа, обоснована многочисленными практическими примерами [6–8].

Кроме того, следует учитывать важность информирования сотрудников и реализации программ повышения культуры безопасности в компаниях, предоставляющих финансовые и другие информационные услуги

(рисунок). Профессионалы в области кибербезопасности и менеджмент организаций могут принять соответствующие меры по обеспечению защиты данных и уменьшению вероятности кибератак в информационных системах.

Анализ и рекомендации

Обеспечение безопасности финансовой и организационной информации при постоянно растущих киберугрозах требует значительных затрат, что обусловливает значимость выстраивания сильной и надежной стратегии защиты. При реализации мер киберзащиты следует учитывать особенности и специфику организаций [9; 10].

Пример реализации программы повышения культуры безопасности в организации

Среди совокупности предлагаемых действий можно выделить следующие:

- Детальный контроль доступа. Внедрение точных и действенных механизмов контроля доступа для авторизованных пользователей повышает безопасность систем защиты финансовых данных, что включает использование паролей, основанных на многофакторной аутентификации, доступе на основе ролей, а также регулярную проверку и отзыв прав доступа пользователей.

- Регулярное обновление программных модулей: поддержание актуальности ПО, а также финансовых и информационных систем организаций за счет регулярных обновлений и внедрения новых модулей безопасности, что устраняет уязвимости и предотвращает их использование киберпреступниками.

- Шифрование данных: для защиты данных и финансовой информации рекомендуется использовать методы шифрования как при хранении,

так и при передаче информации, что предотвращает несанкционированный доступ и обеспечивает то, что перехваченные данные остаются нечитабельными для посторонних.

- Повышение осведомленности и обучение сотрудников. Для укрепления культуры кибербезопасности в организации очень важно проводить занятия по повышению киберосведомленности, используя комплекс из теории и практики, держать сотрудников в курсе событий. Эти программы и регулярные тренинги включают в себя идентификацию вредоносных файлов, электронных писем с зараженными ссылками, управление паролями, выявление различных методов социальной инженерии.

- Резервное копирование данных. Финансовые данные следует регулярно резервировать ежедневно или еженедельно и хранить в отдельном месте, что обеспечивает доступность данных после кибератак, сбоя системы или потери данных.

- Разделение сети: в целях безопасности рекомендуется разделить сеть на отдельные сегменты, что включает отделение финансовых систем от остальной сети. Эта стратегия приводит к предотвращению проникновения и уменьшает возможности злоумышленников перемещаться внутри сети.

- Системы обнаружения и предотвращения вторжений (IDPS): внедрение данных систем защиты может значительно повысить безопасность сети. Системы IDPS выявляют подозрительные действия путем мониторинга сетевого трафика и принимают необходимые меры для блокировки потенциальных киберугроз, с их помощью можно вовремя защитить учетные системы и минимизировать последствия атак.

- Регулярная оценка рисков: организация оценивает возможные риски, уязвимости и возможные угрозы для финансовой информации посредством регулярного анализа и принимает соответствующие решения. Проведение тщательной оценки рисков позволяет организациям выявить специфические уязвимости и установить приоритеты безопасности для каждой угрозы, что улучшает целевые меры безопасности.

- Укрепление культуры кибербезопасности. Повышает превентивную осведомленность сотрудников о важности защиты деловой информации, их активного поведения в выявлении потенциальных угроз и обеспечении безопасности.

- Безопасное управление конфигурацией. Следует убедиться, что системы правильно настроены и разделены, ненужные службы отключены и работают только необходимые функции, программы регулярно обновляются для устранения уязвимостей и обеспечения безопасности.

- План реагирования на инциденты. Должен быть четко определен комплексный план реагирования на возможные инциденты, позволяющий противостоять кибератакам, влияющим на учетные записи. План должен

включать действия, которые необходимо предпринять в случае инцидента, включая делегирование ответственности ключевому персоналу, безопасные протоколы связи и процедуры восстановления данных. План следует регулярно обновлять для обеспечения кибербезопасности.

- Непрерывный мониторинг. Его необходимо осуществлять для своевременного реагирования на потенциальные угрозы. Инструменты мониторинга включают системы обнаружения вторжений и решения для управления информацией о безопасности и событиях (SIEM), их следует развертывать для мониторинга подозрительной сетевой активности, что позволяет обнаруживать и быстро реагировать на инциденты безопасности, а также минимизировать ущерб.

- Управление рисками поставщиков: следует уделить внимание сторонним поставщикам услуг, имеющими доступ к финансовой информации организации. Надежные меры управления рисками поставщиков, включающие рассмотрение требований безопасности в контрактах и регулярный мониторинг их соблюдения, помогут обеспечить безопасность данных, передаваемых по всей цепочке поставок.

- Обучение кибербезопасности: комплексное обучение и тренинги сотрудников являются обязательными и регулярными. Человеческий фактор представляет собой главный риск киберинцидентов, поэтому постоянное обучение новейшим угрозам, осведомленности как распознать фишинг, методам уведомления об инцидентах имеет решающее значение. Компании создают надежный «человеческий брандмауэр», расширяя знания и навыки своих сотрудников в области кибербезопасности.

- Соблюдение стандартов: несмотря на существование многочисленных нормативных положений, следует придерживаться действующих стандартов, регулирующих вопросы защиты информации в организациях. Соблюдение применимых нормативных рамок, таких как GDPR или PCI DSS, следует сделать обязательным в зависимости от отрасли и географического местоположения компании.

Заключение

Расширение процессов цифровизации современных финансовых структур и организаций привело к росту киберугроз и уязвимостей. Значимость обеспечения кибербезопасности особенно возросла в разгар злонамеренных атак и утечек данных, включая многочисленные инциденты в компаниях, что подчеркивает необходимость повышения безопасности и совершенствования осведомленности сотрудников. Угрозы, с которыми сталкиваются компании как со стороны хакеров, так и со стороны собственных сотрудников, требуют внедрения комплексных системных мер безопасности, которые ограничивают доступ к данным, используют шифрование и мониторинг сети. Этому также способствует обучение сотруд-

ников в области киберугроз и развитие культуры информационной безопасности. Для повышения кибербезопасности рекомендуется использовать контроль доступа для авторизованных пользователей, регулярное обновление ПО и информационных систем, шифрование данных, резервное копирование и сетевую изоляцию. Ключевую роль также играют внедрение систем наблюдения и обнаружения вторжений, регулярная оценка возможных рисков и мониторинг сетевой активности. Компании должны разработать планы реагирования на инциденты и сосредоточиться на безопасности поставщиков, а также соблюдать законодательные требования, такие как GDPR или PCI DSS, чтобы минимизировать риски и защитить финансовые и конфиденциальные данные.

Библиографические ссылки

1. *Kuipers S., Schonheit M.* Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises // Corporate Reputation Review. 2022.
2. *Wang P., D'Cruze H., Wood D.* Economic Costs and Impacts of Business Data Breaches // Issues in Information Systems. 2019.
3. *Kafi M. A., Akter N.* Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data Protection // American Journal of Trade and Policy. 2023.
4. *Omotunde H., Ahmed M.* A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond // Mesopotamian Journal of Cyber Security. 2023.
5. *Coppola A., Fernholz F., Glenday G.* Estimating the economic opportunity cost of capital for public investment projects: an empirical analysis of the Mexican case // World Bank Policy Res. Work. 2014.
6. *Pee L. G., Kankanhalli A.* Interactions among factors influencing knowledge management in public-sector organizations: A resource-based view // Gov. Inf. Q. 2016.
7. *Masunka W. Sailan, Kinyua G., Muchemi A.* Organizational Culture as an Antecedent of Organizational Performance: Review of Literature // Int. J. Manag. Stud. Res. 2022.
8. *Hartnell C. A., Ou A. Y., Kinicki A.* Organizational Culture and Organizational Effectiveness: A Meta-Analytic Investigation of the Competing Values Framework's Theoretical Suppositions // J. Appl. Psychol. 2011.
9. *Nejati M. H.* The Role of Liberalism in International Relations of Nations // J. Archaeol. Egypt/Egyptology. 2021.
10. *Karimifard H.* Iran's Foreign Policy Approaches toward International Organizations // World Sociopolitical Stud. 2018.