www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2025.4.3

УДК 004.056.5
ББК 32.972.53

ЗАЩИТА КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ: ОСНОВА БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ

Олеся Александровна Какорина

Кандидат физико-математических наук,
Заведующий кафедрой информационной безопасности,
Волгоградский государственный университет
kakorina@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Надежда Ильинична Хлыбова

Студент, кафедра педагогики, психологии и социальной работы,
Волгоградский государственный университет
povb-251_342398@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Статья посвящена проблеме конфиденциальности данных. Подробно разбирается понятие защиты данных в разных сферах, от персональных данных до государственной тайны. Рассмотрены ключевые методы краж, такие как фишинг и вредоносное программное обеспечение. Особое внимание уделяется новым трендам в защите: использованию искусственного интеллекта, автоматизации и блокчейна. В заключении автор подчеркивает, что, несмотря на развитие технологий безопасности, основными вызовами остаются растущая сложность атак, нехватка специалистов и жесткие требования законодательства. Цель статьи: рассмотреть понятие конфиденциальности данных в различных контекстах, проанализировать мотивы и методы злоумышленников, а также определить ключевые тенденции и вызовы в области защиты информации в настоящее время.

Ключевые слова: конфиденциальность данных, кибербезопасность, защита информации, персональные данные, коммерческая тайна, кибератаки, фишинг, искусственный интеллект, цифровая безопасность.

© Какорина О.А., Хлыбова Н.И., 2025

В общем понятии конфиденциальность – это необходимость предотвращения разглашения, утечки какой-либо информации. Конфиденциальность данных подразумевает под собой необходимость защиты от утечки информации, которая является ограниченной к доступу и представляет ценность для правообладателя [2]. Такая информация защищена от несанкционированного доступа, использования, раскрытия или модификации.

Отличия и роли конфиденциальности данных в различных отраслях

Конфиденциальность данных в зависимости от вида информации, которую нужно защищать может отличаться в различных отраслях.

Конфиденциальность персональных данных – это защита информации, которая косвенно или напрямую относится к определенному человеку. Такие данные, как правило, могут содержать имя, фамилию, отчество, дату рождения, адрес проживания или прописки, сведения об образовании и семейной жизни [4].

Конфиденциальность коммерческой тайны – это защита данных, имеющих коммерческую ценность благодаря тому, что третьи лица, например, в виде компаний-конкурентов, не имеют о них сведений [10]. Разглашение коммерческой тайны может повлечь за собой юридическую ответственность, включая штрафы и судебные иски.

Конфиденциальность медицинской информации – это защита личных данных пациентов, которые могут быть получены при оказании медицинской помощи врачами или другими медицинскими работниками. Такие данные могут включать в себя: диагнозы и результаты медицинских обследований, данные о состоянии здоровья пациента и его медицинской истории, рецепты на лекарства и информация о применении лекарств и так далее [7]. За разглашение медицинской информации предусмотрена гражданская и уголовная ответственность.

Конфиденциальность государственной тайны – это защита сведений, защищаемых государством, распространение которых может повлечь за собой угрозу безопасности. К государственной тайне относятся сведения из военной области, науки, техники, политики, экономики, разведывательной, контрразведывательной, оперативно-розыскной деятельности и противодействия терроризму [6].

Существует три степени секретности для носителей сведений: «особой важности», «совершенно секретно» и «секретно».

Цели мошенников при взломе персональных данных

Злоумышленники стремятся взламывать конфиденциальные данные в различных целях, которые зависят от типа информации и отрасли. В каждой отрасли информация имеет свою определенную ценность и возможность извлечение из нее максимальной выгоды.

Цели мошенников в краже персональных данных: злоумышленники используют личные данные жертвы для создания банковского счета или оформления микрозайма на имя жертвы [8]. Также мошенники могут получить данные банковского приложения, войдя в доверие жертвы.

Цели мошенников в краже коммерческих данных: киберпреступления в области коммерческих данных могут совершаться с целью их продажи конкурентам компании, это могут быть, как и бизнес-планы, так и доступ к клиентам. Также злоумышленники могут угрожать разглашением конфиденциальной информации, с целью получения денежных средств от пострадавшей компании.

Цели мошенников в краже медицинских данных: злоумышленники могут использовать личные медицинские данные пациентов, чтобы получить доступ к медицинским услугам от имени жертвы, тем самым получая бесплатное лечение за счет страховых компаний. Проанализировав украденные личные медицинские данные, мошенники получают доступ к личной информации пациентов о состоянии здоровья, истории болезней, эта информация может быть использована в целях шантажа и манипуляций.

Цели мошенников в краже государственных данных: хакеры или разведывательные службы, работающие на другие государства, могут получить доступ к конфиденциальной информации, которая может угрожать национальной безопасности страны [1]. Кроме того, если важные данные попадут к иностранным государствам, это может повлечь за собой террористическую деятельность и подрыву экономики.

Защита данных является важной задачей для обеспечения безопасности в цифровом мире, вне зависимости от отрасли. Каждая отрасль имеет свои угрозы в области конфиденциальных данных, и мошенники используют различные данные для достижения своих целей.

Методы мошенников кражи конфиденциальной информации

Фишинг остается самым распространенным методом среди киберпреступников, этот

метод позволяет узнавать конфиденциальные данные жертвы с помощью мошеннической ссылки [3].

Социальная инженерия подразумевает собой обман жертвы для получение конфиденциальной информации через создание доверительных отношений с ним.

Вредоносное ПО. Программы, которые устанавливают на компьютере жертвы для кражи его данных. Есть несколько видов вредоносного ПО:

1. Вирусы – это программы которые вставляют свои копии в приложения. Они активируются при запуске зараженного приложения. Когда вирус активируется он может повредить, уничтожить или распространить данные на другие устройства;

2. Программы-шифровальщики. Такие программы киберпреступники используют для шифрования файлов на устройстве жертвы и требуют выкуп за восстановления к ним;

3. Ключевые логгеры записывают каждое нажатия клавиш пользователя, таким образом можно получить логины и пароли, данные кредитных карт и другую информацию.

Тенденции в области защиты данных

С каждым годом, по мере развития цифровых технологий, безопасность конфиденциальность данных становится все более востребованной. С каждым годом появляется все больше угроз, что требует адаптации методов защиты.

Увеличивающееся внимание к приватности: пользователи начинают больше задумываться о важности защиты данных, происходит увеличение требований к различным организациям по соблюдению стандартов конфиденциальности [5].

Интеграция искусственного интеллекта (далее – ИИ): для активного повышения уровня безопасности в работу включаются ИИ и машинное обучение. Данные технологии могут выявлять угрозу за счет их способности проводить анализ и выявлять потенциальные угрозы в реальном времени [9].

Автоматизация процессов безопасности: включение в работу автоматизированных систем позволяет снизить вероятные ошибки, связанные с человеком, а также ускорить реакцию на инциденты.

Технологии блокчейн: блокчейн может стать основой для создания защищенных реестов, где каждая транзакция будет записываться в защищенной системе, что повысит уровень прозрачности и снизит риски мошенничества.

Развитие законодательных инициатив: более строгие нормы для защиты данных, такие как GDPR, способствуют улучшению методик соблюдения конфиденциальности компании, что планирует продолжаться в будущем с учетом расширения законодательства.

Проблемы увеличения числа киберугроз:

1. Продолжается рост разнообразных кибератак. Мошенники начинают использовать методики все сложнее, что позволяет им добраться к защищенным данным. Это приводит к тому, что организация нужно постоянно менять свои стратегически методы безопасности.

2. Недостаток квалифицированных специалистов: нехватка специалистов в области кибербезопасности ведет за собой трудности во внедрении эффективных мер защиты и реагирования на инциденты.

3. Сложность соблюдения стандартов: компании сталкиваются с трудностями в обеспечении соблюдения многочисленных стандартов и норм.

Заключение

Как показывает статья, несмотря на растущую изощренность методов атак, таких как фишинг, социальная инженерия и сложное вредоносное ПО, параллельно развиваются и средства защиты. Ключевые тенденции – интеграция искусственного интеллекта, автоматизация, внедрение блокчейн-технологий и ужесточение законодательства – задают вектор для построения более устойчивых систем безопасности. Они позволяют не только реагировать на инциденты, но и прогнозировать угрозы. Тем не менее вызовы остаются значительными. Растущее число кибератак, нехватка квалифицированных кадров и сложность соответствия множеству регуляторных требований создают напряженную среду для организаций любого уровня. Успех в защите конфиденциальности данных в конечном итоге зависит от комплексного подхода, со-

четающего технологические инновации, грамотную регуляторную политику и постоянное повышение осведомленности пользователей.

СПИСОК ЛИТЕРАТУРЫ

1. Вестов, Ф. А. Возможности цифровых технологий по противодействию мошенничеству / Ф. А. Вестов, А. Р. Абдрашитов // Базис. – 2024. – № 2 (16). – С. 25–29.

2. Гатиятуллина, Э. М. Защита персональных данных в условиях цифровизации: эволюция и современное состояние / Э. М. Гатиятуллина // Закон и власть. – 2023. – № 3. – С. 33–37.

3. Завьялов, А. Н. Интернет-мошенничество (фишинг): Проблемы противодействия и предупреждения / А. Н. Завьялов // Baikal Research Journal. – 2022. – Т. 13, № 2. – С. 36.

4. Зайнутдинова, Е. В. Конфиденциальность персональных данных в ситуации киберугроз / Е. В. Зайнутдинова // Юридическая наука и практика. – 2023. – Т. 19, № 3. – С. 38–46.

5. Йазгелдиев, Ш. Интернет-безопасность и защита персональных данных: тенденции и вызовы в цифровой эпохе / Ш. Йазгелдиев, А. Керимов, Б. Бабанйазов // in situ. – 2023. – № 7. – С. 11–13.

6. Камалова, Г. Г. Уголовная ответственность за нарушение режима конфиденциальности в российском и зарубежном законодательстве / Г. Г. Камалова // Вестник Томского государственного университета. Право. – 2021. – № 40. – С. 32–48.

7. Макушкин, Е. В. Обеспечение конфиденциальности персональной информации и защиты врачебной тайны при размещении в медицинских информационных системах медицинской информации о лицах с психическими и наркологическими расстройствами / Е. В. Макушкин, Т. В. Клименко // Российский психиатрический журнал. – 2021. – № 4. – С. 29–35.

8. Никифоров, А. О. Проблема защиты приватности в цифровом обществе / А. О. Никифоров // Вопросы медиабизнеса. – 2024. – Т. 3, № 1. – С. 69–74.

9. Прогрессивные тенденции применения искусственного интеллекта в области информационной безопасности / А. К. Бекматов [и др.] // Экономика и социум. – 2023. – № 6-1 (109). – С. 1264–1270.

10. Федоров, П. Г. Защита коммерческой тайны в отношениях с контрагентами на основе использования процессного подхода к управлению организацией / П. Г. Федоров // Имущественные отношения в Российской Федерации. – 2024. – № 7 (274). – С. 32–45.

REFERENCES

1. Vestov F.A., Abdrashitov A.R. Vozmozhnosti tsifrovyh tekhnologiy po protivodeystviyu moshennichestvu [Possibilities of Digital Technologies to Counter Fraud]. *Bazis* [Basis], 2024, no. 2 (16), pp. 25-29.

2. Gatiyatullina E.M. Zashchita personalnyh dannyh v usloviyah tsifrovizatsii: evolyutsiya i sovremennoye sostoyaniye [Personal Data Protection in the Context of Digitalization: Evolution and Current State]. *Zakon i vlast* [Law and Power], 2023, no. 3, pp. 33-37.

3. Zavyalov A.N. Internet-moshennichestvo (fishing): Problemy protivodeystviya i preduprezhdeniya [Internet Fraud (Phishing): Problems of Counteraction and Prevention]. *Baikal Research Journal*, 2022, vol. 13, no. 2, p. 36.

4. Zaynutdinova E.V. Konfidentsialnost personalnyh dannyh v situatsii kiberugroz [Confidentiality of Personal Data in the Situation of Cyber Threats]. *Yuridicheskaya nauka i praktika* [Juridical Science and Practice], 2023, vol. 19, no. 3, pp. 38-46.

5. Yazgeldiev Sh., Kerimov A., Babanyazov B. Internet-bezopasnost i zashchita personalnyh dannyh: tendentsii i vyzovy v tsifrovuoy epohe [Internet Security and Personal Data Protection: Trends and Challenges in the Digital Age]. *in situ*, 2023, no. 7, pp. 11-13.

6. Kamalova G.G. Ugolovnaya otvetstvennost za narusheniye rezhima konfidentsialnosti v rossiyskom i zarubezhnom zakonodatelstve [Criminal Liability for Violation of Confidentiality Regime in Russian and Foreign Legislation]. *Vestnik Tomskogo gosudarstvennogo universiteta. Pravo* [Bulletin of Tomsk State University. Law], 2021, no. 40, pp. 32-48.

7. Makushkin E.V., Klimenko T.V. Obespecheniye konfidentsialnosti personalnoy informatsii i zashchity vrachebnoy tayny pri razmeshchenii v meditsinskih informatsionnyh sistemah meditsinskoy informatsii o litsah s psihicheskimi i narkologicheskimi rasstroystvami [Ensuring Confidentiality of Personal Information and Protection of Medical Secrecy When Placing Medical Information About Persons with Mental and Drug Addiction Disorders in Medical Information Systems]. *Rossiyskiy psihiatricheskiy zhurnal* [Russian Psychiatric Journal], 2021, no. 4, pp. 29-35.

8. Nikiforov A.O. Problema zashchity privatnosti v tsifrovom obshchestve [The Problem of Privacy Protection in Digital Society]. *Voprosy mediabiznesa* [Issues of Media Business], 2024, vol. 3, no. 1, pp. 69-74.

9. Bekmatov A.K., Kutdusova E.R., Mukimov Sh.I., Davlatova N.N. Progressivnye tendentsii primeneniya iskusstvennogo intellekta v

oblasti informatsionnoy bezopasnosti [Progressive Trends in the Application of Artificial Intelligence in the Field of Information Security]. *Ekonomika i sotsium* [Economy and Society], 2023, no. 6-1 (109), pp. 1264-1270.

10. Fedorov P.G. Zashchita kommercheskoy tayny v otnosheniyah s kontragentami na osnove ispolzovaniya protsessnogo podhoda k upravleniyu organizatsiey [Protection of Trade Secrets in Relations with Counterparties Based on the Use of a Process Approach to Organization Management]. *Imushchestvennye otnosheniya v Rossiyskoy Federatsii* [Property Relations in the Russian Federation], 2024, no. 7 (274), pp. 32-45.

DATA PRIVACY PROTECTION: THE FOUNDATION OF SECURITY IN THE DIGITAL WORLD

Olesya A. Kakorina

Candidate of Sciences (Physics and Mathematics),
Head of the Department of Information Security,
Volgograd State University
kakorina@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Nadezhda I. Khlybova

Student, Department of Pedagogy, Psychology and Social Work,
Volgograd State University
povb-251_342398@volsu.ru
Prosp. Universitetsky, 100, 400062, Volgograd, Russian Federation

Abstract. This article examines the critical issue of data privacy as the foundation of security in the digital world. It delves into the concept of data protection across various domains, including personal data, commercial secrets, medical information, and state secrets, highlighting their distinct roles and vulnerabilities. The analysis covers the primary motives and methods employed by malicious actors to steal confidential information, such as phishing, social engineering, and various forms of malware, including viruses, ransomware, and keyloggers. Concurrently, the article identifies and discusses key emerging trends in data protection. These include the growing emphasis on user privacy, the integration of artificial intelligence (AI) and machine learning for real-time threat detection, the automation of security processes, the potential application of blockchain technology for secure record-keeping, and the development of stricter legislative frameworks like GDPR. However, significant challenges persist. The conclusion underscores that despite technological advancements, the increasing sophistication of cyberattacks, a shortage of skilled cybersecurity professionals, and the complexity of complying with evolving regulations remain major obstacles. Therefore, ensuring robust data privacy ultimately requires a comprehensive approach that synergistically combines technological innovation, sound regulatory policies, and continuous user awareness efforts.

Key words: data privacy, cybersecurity, information protection, personal data, trade secret, cyber-attacks, phishing, artificial intelligence, digital security.