DOI 10.37882/2223-2966.2025.11.40

# ПОТЕНЦИАЛЬНЫЕ ИНЦИДЕНТЫ НАРУШЕНИЯ КИБЕРБЕЗОПАСНОСТИ СКВОЗЬ ПРИЗМУ ЭТИЧЕСКИХ ПРИНЦИПОВ РАБОТЫ С ИНФОРМАЦИЕЙ

## POTENTIAL INCIDENTS OF CYBERSECURITY VIOLATIONS THROUGH THE LENS OF ETHICAL PRINCIPLES OF WORKING WITH INFORMATION

***O.Yakovleva***
***N. Verezubova***
***O. Kishkinova***

*Summary*. Along with the innovation of digital platforms and electronic resources where personal data, confidential information and financial resources of organizations and users are stored, the number of cyber-attacks is increasing every month — cybercrimes are being improved by intruders through the use of digital technologies and artificial intelligence. Data protection rules apply not only to the regulation of technical procedures, but also require compliance with ethical standards, including the principles of privacy, responsibility, transparency in reporting on security measures, non-harm, legality and respect for the rights and freedoms of users. Teaching Russian students, the basics of cybersecurity is relevant due to the growth of information and personal data stored in data centers, electronic versions of documents, including in the Unified Identification and Authentication System (USIA), due to the fact that the promotion and observance of ethical standards in this area helps to prevent incidents of interference by intruders and trained by them. neural networks, minimize the risks of cyber-attacks. The problem of ethics in cybersecurity concerns both employees who provide a set of measures, technologies and practices aimed at data protection, as well as groups responding to violations, and users in the performance of their work and organization of personal digital space.

*Keywords*: cybersecurity, ethics, working with information, cyberattack, potential incidents, violations, data protection, digital systems.

***Яковлева Ольга Анатольевна***
*Кандидат с/х наук, доцент, Московская государственная академия ветеринарной медицины и биотехнологии имени К.И. Скрябина*
*yakovleffo@yandex.ru*
***Верезубова Наталья Афанасьевна***
*Кандидат экономических наук, доцент, Московская государственная академия ветеринарной медицины и биотехнологии имени К.И. Скрябина*
*nverez@mail.ru*
***Кишкинова Ольга Алексеевна***
*Старший преподаватель, Московская государственная академия ветеринарной медицины и биотехнологии имени К.И. Скрябина*
*olga.19672015@yandex.ru*

*Аннотация*. Наравне с инноватизацией цифровых платформ и электронных ресурсов, где хранятся личные данные, конфиденциальная информация и финансовые средства организаций и пользователей, ежемесячно возрастает число кибератак — киберпреступления совершенствуются злоумышленниками за счет использования цифровых технологий и искусственного интеллекта. Правила защиты данных распространяются не только на регламентацию технических процедур, но и требуют соблюдения этических норм, включая принципы приватности, ответственности, прозрачности в освещении предпринимаемых мер безопасности, непричинения вреда, законности и уважения прав и свобод пользователей. Обучение российских студентов основам кибербезопасности актуально в связи с ростом информации и личных данных, которые хранятся в дата-центрах, электронных вариантах документов, в том числе, в Единой системе идентификации и аутентификации (ЕСИА), ввиду того, что продвижение и соблюдение этических стандартов в обозначенной сфере помогает предотвращать инциденты вмешательств злоумышленников и обученных ими нейросетей, минимизировать риски кибератак. Проблема этики в кибербезопасности касается как сотрудников, обеспечивающих комплекс мер, технологий и практик, направленных на защиту данных, а также групп реагирования на нарушения, так и пользователей при выполнении их трудовой деятельности и организации личного цифрового пространства.

*Ключевые слова*: кибербезопасность, этика, работа с информацией, кибератака, потенциальные инциденты, нарушения, защита данных, цифровые системы.

## Введение

Основной целью киберпреступника является атака на пользователя или сотрудника, поскольку это самый простой способ получить доступ к конфиденциальной информации частных лиц и компаний. Согласно исследованиям С.Г. Сепульведа и Ж.Е.В. Мазо *(Sepúlveda, Mazo 2025)*, во многих случаях не человеческий фактор сам по себе, а плохо продуманные процессы делают человеческий фактор и нарушения безопасности неизбежными [9, p. 5].

В современной реальности сформирована строгая этика кибербезопасности — моральные принципы, требующие от специалистов не только корректного и своевременного введения и контроля данных, но и их неразглашения. Тем не менее, существует достаточно много прецедентов, когда сотрудники во время выполнения своих трудовых обязанностей или после собственного увольнения нарушают договор и конфиденциальность — распространяют личные данные пользователей, продают их третьим лицам либо сами используют их в мошеннических целях. Ежегодно действия недобросовестных лиц совершенствуются и видоизменяются, что требует систематического контроля и бдительности пользователей и законодательных органов в сфере защиты информации.

Все чаще кибератаки совершают не люди, а специально обученные хаккерами искусственные интеллекты (ИИ) и программы, а также ИИ-модели, создающие *AI*-усиленные атаки — как подчеркивает Д.Е. Намиот (2024), «кибератаки, основанные на ИИ, меняют ландшафт кибербезопасности» [4, с. 132].

*Материалы и методы* основаны на системном подходе и включают анализ, синтез и структуризацию материала, аналитику и обработку данных, междисциплинарный подход.

## Результаты и обсуждение

Пользователи обладают разным уровнем цифровой грамотности, мотивации и способности действовать безопасно, что влияет на их уязвимость перед кибератаками [10, p. 9]. Так, согласно опросу 3500 россиян старше 18-ти лет, 10 % респондентов не соблюдают правила кибербезопасности и хранения данных на рабочем месте [2] (см. рисунок 1):

Согласно статистическим данным РБК (см. рисунок 1), 42 % россиян из 3500 опрошенных знают правила защиты данных, однако, периодически их игнорируют — данное поведение характерно для мужчин и женщин в одинаковой степени, в то время как «правильное хранение данных и соблюдение принципов кибербезопасности — это вопрос стратегической важности для сотрудников, компаний и всей экономики, … халатное отношение к такого рода вопросам негативно отражается на уровне защиты конфиденциальных данных и чреваты прямыми финансовыми и репутационными потерями» [2]. По мнению специалистов Сбербанка, многие игнорируют правила хранения и защиты данных, а также необходимость придерживаться этических норм вследствие того, что требования кибербезопасности (далее — КБ) влекут за собой разные ограничения для пользователей [1].

Отсутствие превентивных мер в области безопасности, недостаточное внимание к осведомленности пользователей и недостаток надежных решений при потенциальных кибератаках создают серьезные проблемы для этики в кибербезопасности [9, p. 7].

Т.Ф.А. Масаид *(Masaeid 2025)* акцентирует внимание на существовании целостной модели формирования безопасного поведения в сети и при защите данных, принимающей во внимание психологические, социальные и технологические аспекты киберугроз. Однако, как отмечают К. Мерсинас, М. Бада, С. Фернелл *(Mersinas, Bada, Furnell 2024)* в вопросах морали, связанных с поведенческими вмешательствами в сфере кибербезопасности, остаются неизученные области, требующие создания моделей, которые обеспечивали бы баланс между личной свободой и безопасностью [8].

Обнаружение инцидентов нарушения кибербезопасности, по мнению К. Мерсинас, М. Бада, С. Фернелл *(Mersinas, Bada, Furnell 2024)*, в значительной степени зависит от мониторинга поведения пользователей и сетей в режиме реального времени, позволяющего выявлять отклонения от нормы, указывающие, чаще всего, непосредственно на горизонтальное перемещение (горизонтальное распространение) злоумышленников в сети (например, скомпрометированного устройства или аккаунта) после получения ими первоначального доступа к личным данным пользователя или инфраструктуре организации. Подозрительные сеансы входа в систему из неизвестных источников, повторяющиеся попытки доступа к несвязанным системам и нарушение последовательности действий в рабочем процессе являются индикаторами данных инцидентов [8]. Т.Ф.А. Масаид *(Masaeid 2025)* подчеркивает, что наиболее надежную защиту обеспечивает Модель безопасности с нулевым доверием *(ZTSM — Zero Trust Security Model)*, предполагающая непрерывную аутентификацию и строгие ограничения доступа к данным [7, p. 251].

Огромное значение при выявлении кибернарушений имеет поведенческий анализ атак с использованием ИИ, т.к. ИИ может усиливать или ослаблять меры безопасности. Возможности нейросети не ограничиваются выявлением угроз, возникающих из-за вредоносных про-

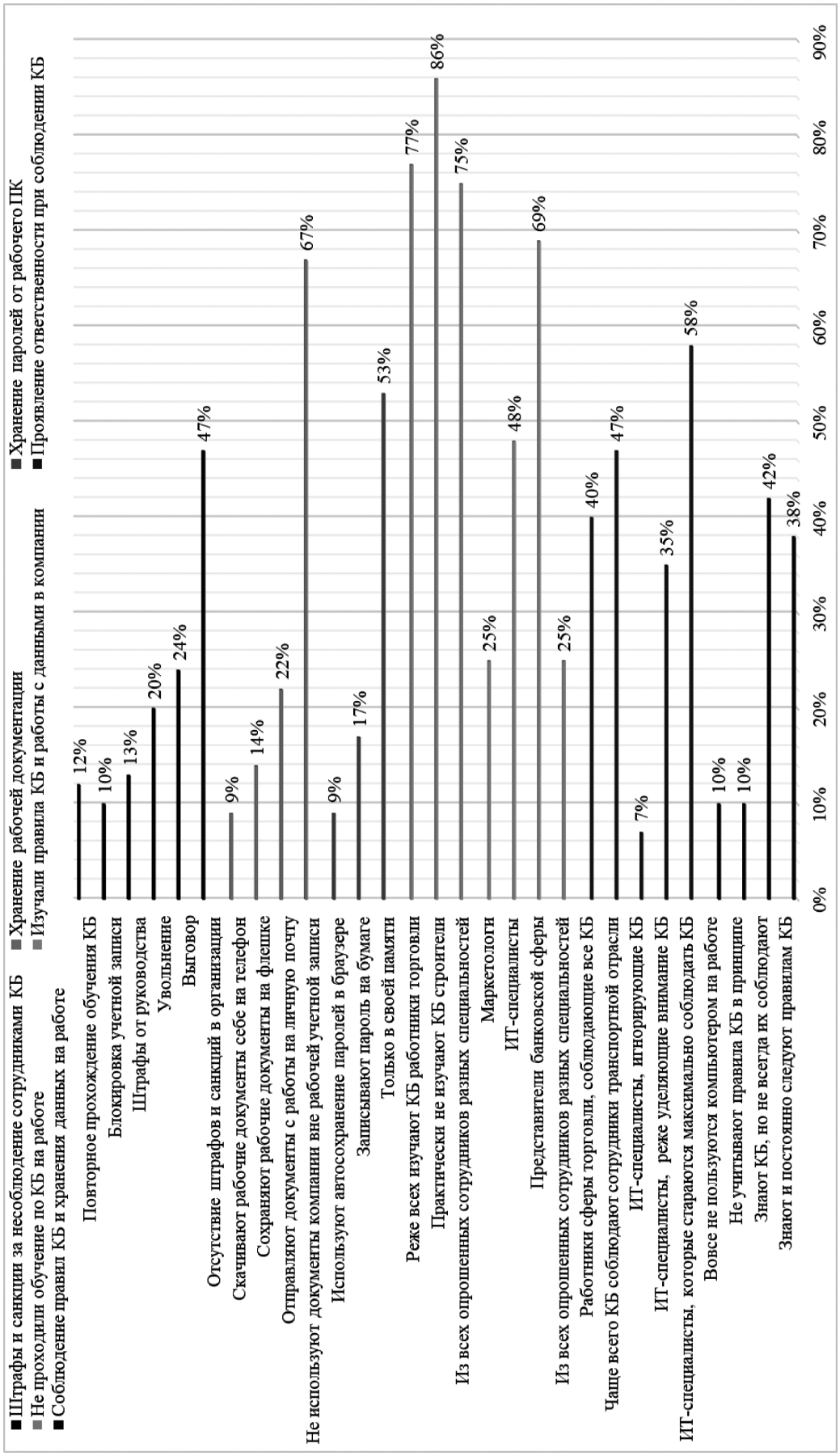


Рис. 1. Соблюдение правил кибербезопасности (КБ) на рабочем месте. Данные РБК (май, 2024 г.; рисунок наш)

грамм — ИИ способен проводить поведенческий анализ даже действий человека [7, p. 251], что является эффективным инструментом обнаружения нарушений этических принципов взаимодействия в интернет-пространстве. Для проведения сложных атак с использованием ИИ применяются передовые технологии машинного обучения, глубокого обучения и обработки естественного языка. Для защиты от атак с использованием ИИ, в свою очередь, используются анализ предсказуемости и обнаружение аномалий [7, p. 251].

По мнению М. Тхакара *(Thakar 2025)*, человеческая ошибка часто является следствием несовершенства процесса, а не халатности отдельного сотрудника. Сосредоточившись на системных факторах и формируя культуру доверия, обучения и подотчетности, можно снизить вероятность повторения ошибок и повысить общий уровень безопасности. Этические соображения являются неотъемлемой частью разработки и внедрения методов поведенческого моделирования в системах безопасности, в т.ч., которые работают на основе ИИ.

В рамках этики ИИ особое внимание важно уделять таким принципам, как прозрачность, ответственность, конфиденциальность и доверие, которые необходимы пользователям для поддержания уверенности в их собственной безопасности, а также важно обеспечение ответственного использования поведенческих данных. Реализация этих принципов помогает решить проблемы, связанные с конфиденциальностью данных [10, p. 15], а соблюдение принципов, представленных на рисунке 2, обеспечивает мягкие превентивные меры, которые важно применять в сфере кибербезопасности:

Нарушение вышеперечисленных принципов влечет за собой уязвимость кибербезопасности в контексте этических норм, о чем важно знать обучающимся, в последующем, сотрудникам всех специальностей. Более того, необходимо проявлять заботу о собственном психоэмоциональном здоровье и здоровье других пользователей; повышать свои технологические, научные, информационные и цифровые компетенции [5, с. 64]; своевременно и адекватно реагировать на инциденты нарушения кибербезопасности; «признавать и уважать границы юрисдикции, законные права, правила и полномочия сторон, участвующих в мероприятиях, связанных с реагированием на инциденты» [3]; руководствоваться только достоверной информацией из авторитетных источников.

Хорошей практикой может быть использование средств аутентификации или постоянный мониторинг сети, но при этом нельзя упускать из виду человеческий фактор, поскольку поведение людей может приводить к формированию привычек, создающих серьезные уязвимости для кибербезопасности [9, p. 7]. Кроме того, А.А.А. Зани, А.А. Норман, Н.А. Гани и Р.С. Сианьтури *(Zani, Norman, Ghani, Sianturi 2025)* описывают этические способности как информацию, мотивацию и возможности для межличностного общения в интернете, которые


Рис. 2. Этические принципы кибербезопасности (КБ) пользователей, нарушение которых ведет к потенциальным инцидентам (рисунок наш)

соответствуют закону и социальным нормам. Соответственно, пользователи должны уметь распознавать приемлемые, правильные, желательные и законные аспекты своих действий, прежде чем они осознают их последствия [11, p. 2]. Помимо этого, принимать во внимание, что злоумышленники часто имитируют поведение обычных пользователей, чтобы их не обнаружили, что снижает уровень бдительности пострадавшей стороны [9, p. 283].

Необходимо выделять достаточные ресурсы для постоянного поддержания и обновления инфраструктуры кибербезопасности, чтобы успешно противостоять возникающим угрозам. Важно отметить, что, уделяя приоритетное внимание кибербезопасности, учебные заведения не только защищают целостность своих данных, но и укрепляют доверие среди обучающихся и заинтересованных сторон [8; 6].

*Выводы:* чтобы успешно противостоять возникающим угрозам кибербезопасности, важно формировать привычки соблюдения этических принципов защиты данных, хранения информации и поведения в сети еще до трудоустройства — во время обучения в общеобразовательных учреждениях. Нарушение этики при работе с информацией чревато различными инцидентами и угрозами.

Среди наиболее важных этических принципов кибербезопасности пользователей необходимо выделить принципы доверия, конфиденциальности, уважительного отношения к другим пользователям и их интеллектуальной собственности, мнению, концептам и идеям, скоординированности действий по противостоянию кибератакам, а также систематического повышения цифровой и информационной компетентностей посредством достоверных источников и авторитетных ресурсов.

ЛИТЕРАТУРА


1. Защитник или надзиратель? Проблема этики в кибербезопасности // Официальный сайт Сбербанка. URL: https://www.sberbank.ru/ru/person/kibrary/articles/zashchitnik-ili-nadziratel-problema-ehtiki-v-kiberbezopasnostii (дата обращения: 14.11.2025).
2. Исследование: 10% россиян не соблюдают правила кибербезопасности в работе // РБК. Статья от 30.05.2024. URL: https://companies.rbc.ru/news/Dm0DGt8xl8/issledovanie-10-rossiyan-ne-soblyudayut-pravila-kiberbezopasnosti-v-rabote/ (дата обращения: 13.11.2025).
3. Кодекс этики // Форуме групп реагирования на инциденты и обеспечения безопасности = EthicsfIRST. Ethics for Incident Response and Security Teams. URL: https://www.first.org/global/sigs/ethics/ethics-first (date: 14.11.2025).
4. Намиот Д.Е. О кибератаках с помощью систем Искусственного интеллекта // International Journal of Open Information Technologies. 2024. №9. С. 132–141.
5. Юсуфзода И.М. Борьба с киберугрозами: важность кибербезопасности в современном мире // Форум молодых ученых. 2024. №4 (92). С. 63–64.
6. Chasokela D., Ncube Ch. (2024) Leveraging Technology for Organizational Efficiency and Effectiveness in Higher Education // In book: Leveraging Technology for Organizational Efficiency and Effectiveness in Higher Education (pp.381–410). Publisher: IGI Global. https://doi.org/10.4018/979-8-3693-6967-8.ch014.
7. Masaeid T.F.A. (2025) AI-Driven Cyber Threats: Behavioral Analysis and Strategic Defenses // In book: Strategic AI Integration in Business Intelligence (pp. 251–284). https://doi.org/10.4018/979-8-3373-6801-6.ch011.
8. Mersinas K., Bada M., Furnell S. (2024) Cybersecurity Behavior Change: A conceptualization of Ethical Principles for Behavioral Interventions // Computers & Security 148(02):104025. https://doi.org/10.1016/j.cose.2024.104025.
9. Sepúlveda S.G., Mazo J.E.V. (2025) Ciberseguridad aplicada a la gestión de datos en empresas de bienes y servicios: una revisión de literature // Cuaderno activa 16(1). 10 p. https://doi.org/10.53995/20278101.1804.
10. Thakar M. (2025) Enhancing Human Resilience to Social Engineering Attacks through Integrated AI Detection and Context-Aware Behavioral Interventions. 76 p. https://doi.org/10.13140/RG.2.2.25474.75200.
11. Zani A.A.A., Norman A.A., Ghani N.A., Sianturi R.S. (2025) Navigating Social Media: How Offline Ethics, Online Etiquette, and Protection Behavior Shape Self-Disclosure // IEEE Access PP. (99):1-1. https://doi.org/10.1109/ACCESS.2025.3555548.


© Яковлева Ольга Анатольевна (yakovleffo@yandex.ru); Верезубова Наталья Афанасьевна (nverez@mail.ru);
Кишкинова Ольга Алексеевна (olga.19672015@yandex.ru)
Журнал «Современная наука: актуальные проблемы теории и практики»