**Кошелев Александр Романович,** магистрант,
Кубанский Государственный университет

# НЕЙРОТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕС-ПРОЦЕССОВ: УГРОЗЫ В ЦИФРОВОЙ СРЕДЕ

**Аннотация.** В статье рассматриваются актуальные угрозы информационной безопасности, связанные с внедрением нейротехнологий в бизнес-процессы. Обращается внимание на повышенную чувствительность собранных нейроданных и риски их утечек в цифровой среде. Анализируются правовые и этические вопросы конфиденциальности нейроданных и существующие подходы к их регулированию. Оцениваются корпоративные риски при использовании нейроинтерфейсов и ИИ-модулей, анализирующих когнитивную активность сотрудников, включая возможные нарушения «ментальной приватности», дискриминацию и утечку коммерческих тайн. Предлагаются задачи дальнейших исследований: систематизация новых видов угроз, разработка норм и стандартов защиты нейроданных, а также методов обеспечения правомерного и безопасного применения нейротехнологий в организациях.

**Ключевые слова:** Нейротехнологии, информационная безопасность, нейроданные, конфиденциальность, правовое регулирование, корпоративные риски, нейроинтерфейсы.

Развитие технологий интерфейсов «мозг – компьютер» и иных нейротехнологий открывает новые возможности для оптимизации бизнес-процессов (например, повышение эффективности работы, мониторинг состояния сотрудников, управление оборудованием силой мысли). Вместе с тем это порождает **уникальные риски безопасности**: данные об активности мозга крайне чувствительны и могут содержать информацию о мыслях, эмоциях и намерениях человека. В современных условиях широкая доступность нейрогаджетов (носимых ЭЭГ-шлемов, нейрочипов, приложений нейрофидбэка и др.) и интеграция их в рабочую среду неизбежно приводят к появлению новых угроз конфиденциальности и возможности кибератак. ЮНЕСКО в 2025 году подчеркнуло важность принципа **неприкосновенности разума** и необходимость обеспечить защиту нейроданных от несанкционированного доступа. В настоящей работе ставится задача всестороннего анализа следующих аспектов:

A. **утечки нейроданных как новая угроза цифровой среде**;
B. **конфиденциальность и правовое регулирование** в сфере нейротехнологий;
C. **корпоративные риски** при внедрении нейроинтерфейсов и ИИ-модулей, анализирующих когнитивную активность сотрудников.

В основе статьи – гипотеза о том, что сочетание нейротехнологий и ИИ в бизнесе создает новые векторы атак и уязвимости, требующие специальных мер защиты и правового оформления. Новизна материала заключается в объединении исследований из разных областей (кибербезопасность, нейронауки, законодательство) с учётом актуальных событий и практик последних лет.

**Утечки нейроданных как новая угроза**

Данные, полученные с помощью нейротехнологий (далее – *нейроданные*), обладают особенностью экстремальной чувствительности. Они могут отражать не только физиологические сигналы (например, электрические потенциалы мозга), но и косвенно содержать информацию о мыслях, воспоминаниях, эмоциональном состоянии или невольных когнитивных реакциях человека. Это делает подобные данные привлекательным «ресурсом» для злоумышленников. Так, при перехвате сигналов нейроинтерфейса возможна

*инфраструктурная атака типа «brain tapping»* – несанкционированное считывание мозговых волн и извлечение личной информации о пользователе. Аналогично подмена или искажение стимулов (атакующий искусственно изменяет обратную связь) может воздействовать на психику и поведение сотрудника (атака «misleading stimuli»).

Например, в СМИ описывался случай, когда потребительские нейрогаджеты (тренажёры концентрации FocusCalm), используемые известными спортсменами, возможно, передавали мозговые данные их производителей в Китае. Если коммерческие или конкурентные структуры получат доступ к подобным данным, это может привести к промышленному шпионажу и нарушению коммерческой тайны. Также промышленные шпионы или даже иностранные спецслужбы при успешной атаке на корпоративные нейросистемы могут получить сведения о стратегических намерениях сотрудников (намерения, планы, скрытые эмоции).

Таким образом, утечка нейроданных - объективно новая угроза: помимо общих рисков кражи данных, она затрагивает «ментальную приватность» человека и может привести к предсказанию или манипуляции поведением сотрудника. С развитием нейроинтерфейсов эти угрозы становятся более практическими: повсеместное внедрение портативных «мозгочитающих» устройств в корпоративную среду существенно расширяет векторы атаки.

**Конфиденциальность и правовое регулирование в нейротехнологиях**

Правовые системы пока не успевают за быстрыми инновациями в нейротехнологиях. На сегодня **неинвазивные** нейросистемы (ЭЭГ-шлемы, гарнитуры для медитации и др.) большей частью попадают в «регуляторную пустоту»: они не требуют медицинской лицензии и работают на потребительском рынке практически без правового контроля. Например, как отмечает исследование, аппаратные платформы фиксируют нейроданные пользователей без достаточного информирования и защиты, а индустрия демонстрирует несоответствие международным нормам конфиденциальности. Во многих компаниях при этом правовыми основаниями остаётся лишь общее соглашение пользователя и стандартная защита персональных данных, что недостаточно для нейросигналов как столь интимной информации.

В нескольких юрисдикциях приняты специальные меры. В США ряд штатов уже расширил законы о конфиденциальности, включив «нейроданные» в число особо защищаемой информации. Например, в 2022 году штат Колорадо дополнил свой Закон о конфиденциальности данных, отнесением «биологических данных», включая нейронную активность, к чувствительной категории. Традиционно и наиболее прогрессивно в законодательном смысле действует Латинская Америка: в 2021 году Чили конституционно закрепила неприкосновенность «мозговой активности и информации, полученной из неё», приравняв эти данные к основополагающим правам. Верховный суд Чили даже обязал компанию удалить собранные нейроданные потребителя, признав их сбор нарушающим право на ментальную приватность. Аналогичные инициативы появляются в других странах Латинской Америки и ряде штатов США.

Международные организации тоже уделяют внимание проблеме. Так, ЮНЕСКО в 2025 г. приняла рекомендации по этике нейротехнологий, подчёркивающие принцип **неприкосновенности человеческого разума** и ограничивающие применение нейросистем в работе (например, запрещается следить за продуктивностью сотрудников без их добровольного согласия). OECD и ОАГ выпустили руководства по нейроэтике (2019-2023), а У.Специальный докладчик ООН по праву на приватность призвал ввести специальные нормы для нейротехнологий. В Европе пока действует преимущественно GDPR, который в целом относится к нейроданным как к «особым персональным» и обеспечивает некоторую защиту. Однако нейротехнологии прямо не упомянуты в тексте GDPR, что остаётся предметом обсуждения. В 2024-2025 гг. также обсуждаются поправки к законам: например, в ЕС принят

AI Act, запрещающий «сильное сублиминальное» нейропроникновение и выводящий проверки эмоций на работе за рамки разрешённых случаев.

В целом можно констатировать, что законодательство в области нейротехнологий находится на стадии формирования: **существующие регламенты часто не учитывают специфику данных мозга**. Необходим переход от простого применения общих норм к созданию специализированных правил, учитывающих права на «ментальную приватность», автономию и запрет нейродискриминации.

**Корпоративные риски внедрения нейроинтерфейсов и ИИ-модулей**

В бизнесе нейротехнологии могут использоваться для повышения эффективности работы: мониторинга концентрации, оценки стресса, адаптивного управления оборудованием и т.д. Однако это сопряжено с новыми корпоративными рисками. Прежде всего, применение нейроинтерфейсов в рабочей среде представляет собой форму интенсивного надзора - *нейросервейлленса*. С одной стороны, руководитель может стремиться оптимизировать производительность, но с другой - контроль за внутренним состоянием сотрудников открывает путь к многочисленным злоупотреблениям. Исследование показало, что обязательное ношение ЭЭГ-устройств может привести к значительным нарушениям прав работников: рисковых для их здоровья (постоянный стресс, «аутичная» гиперконцентрация), дискриминационных практик («нейродискриминация») и даже коммерческих злоупотреблений. Например, если часть сотрудников согласны на такую слежку (согласно анкетам, до 35% работников готовы к использованию подобных инструментов в ближайшие годы), остальные могут лишиться объективной оценки своих результатов наравне с «чипированными» коллегами.

Кроме того, **утечка нейроданных из корпоративной системы** может привести к ущербу бизнесу: мозговые сигналы могут «выдавать» стратегические решения или интеллектуальную собственность. В гипотетическом сценарии описан менеджер, чьи воспоминания и мысли были подменены хакерами, что позволило похитить корпоративные секреты и нанести компании колоссальный ущерб. Практически же, как отмечено экспертами, уже есть примеры использования нейрогаджетов для контроля эмоционального состояния сотрудников: в Китае работодатели массово применяют носимые устройства для отслеживания внимания и настроения персонала. Это говорит о том, что такая практика может стать мировым трендом. Без соответствующей нормативной базы компании рискуют получить серьезные репутационные и юридические издержки (пока отсутствие специальных законов не исключает судебных исков по факту нарушения конфиденциальности).

Наконец, сочетание нейроинтерфейсов с алгоритмами ИИ открывает дополнительные риски безопасности. Любая уязвимость в инфраструктуре сбора или обработки мозговых данных может позволить злоумышленникам внедрять ложные сигналы, манипулировать интеллектуальными системами или дистанционно влиять на когнитивные процессы работников. В ряде отчётов указано, что нейроустройства обычно «снимают» полные массивы данных мозга, передавая их без достаточной фильтрации третьим лицам, что делает потенциальной целью для кибератак такие системы полностью загруженные биометрическими данными. Таким образом, корпоративная информационная безопасность должна учитывать новые атаку типа «нейрофишинг» (социальная инженерия через обновления нейропрограмм) и «нейроботнеты» для удалённого перехвата мозговых сигналов.

Для снижения этих рисков бизнесу необходимо не только технически защищать каналы связи и хранилища нейроданных (шифрование, сегментация доступа), но и разработать внутрикорпоративную политику «нейробезопасности». Это включает «этический аудит» внедрения нейротехнологий, особые требования к информированному согласию сотрудников и прозрачности обработки нейроданных, а также проведение анализа рисков и стресс-тестов

ИТ-инфраструктуры на предмет готовности к нагрузке от «нейростримов». Без таких мер внедрение нейротехнологий в бизнес может обернуться снижением доверия персонала и усилением внутренних конфликтов.

Нейротехнологии стремительно выходят из лабораторий в повседневную и деловую среду, что обостряет проблемы информационной безопасности. **Утечки нейроданных** представляют новую категорию угроз: они пересекают границы личного пространства, раскрывая практически невидимые аспекты мышления и психики. **Недостаточность текущего регулирования** усугубляет уязвимость: существующие законы часто не охватывают данные мозга, а нейротехнологические компании сохраняют полный контроль над собранными данными пользователей. **Корпоративные риски** включают нарушение приватности сотрудников, потенциальную дискриминацию и экономический ущерб от кражи «мысленных» данных.

Необходим системный подход: сначала следует формулировать гипотезы о возможных угрозах и формировать исследовательские задачи (например, моделирование сценариев атак на нейросистемы в организации). Дальнейшие исследования должны установить методы **защиты нейроданных** (технические и организационные), а также **принципы регуляции** (от согласия и неприкосновенности разума до запретов на определённые применения, как рекомендует ЮНЕСКО). Только при сочетании продвинутых правовых норм и надёжных технических средств можно обеспечить баланс между пользой нейротехнологий для бизнеса и сохранением базовых прав сотрудников. Итоговая цель – интегрировать «ментальную приватность» в практики информационной безопасности, что станет новым направлением исследований на стыке нейронаук, права и кибербезопасности.

*Список литературы:*

1. Фарахани Н. А. Будущее нейроправ: свобода и защита человеческого разума в цифровую эпоху. – М.: Издательство НИУ ВШЭ, 2023.
2. Ienca M., Andorno R. «На пути к новым правам человека в эпоху нейротехнологий и искусственного интеллекта» // Life Sciences, Society and Policy. – 2017.
3. UNESCO. Ethics of Neurotechnology: Protecting Human Rights and Freedoms. – Paris: UNESCO Publishing, 2025.
4. Greely H. «Neuroscience, Mind Reading, and Cognitive Liberty» // Harvard Journal of Law & Technology. – 2022.
5. Alkhatib J., Gutala S., Centofanti D. «Risks of Neurowearable Technologies in the Workplace» // Frontiers in Human Dynamics. – 2024.
6. Cocchi C., Arcidiacono C., Cianchetti C. «Neurosurveillance in the Workplace: Ethical and Legal Implications» // Frontiers in Human Dynamics. – 2023.
7. Farahany N. A., Greely H., Wagner A. D. «Mental Privacy: Navigating Risks, Rights, and Regulation» // Journal of Law and the Biosciences. – 2024.
8. World Economic Forum. Brain-Computer Interfaces: Opportunities and Cybersecurity Risks. – Geneva: WEF, 2024.
9. European Union. Artificial Intelligence Act: Regulation of High-Risk AI Systems. – Brussels: Official Journal of the EU, 2024
10. Кокорев А. В., Смирнов И. С. Нейроданные как объект информационной безопасности // Информационное право. – 2022
11. Лапшин В. А., Киселёв А. Н. Цифровые риски и защита персональных данных в корпоративных системах. – М.: Юрайт, 2021
12. Лапшин В. А., Киселёв А. Н. Цифровые риски и защита персональных данных в корпоративных системах. – М.: Юрайт, 2021.