Нестеркин Дмитрий

Комплексный анализ рисков кибербезопасности в нейрокомпьютерных интерфейсах

Москва, 2025

Краткое содержание 5
Глава 1. Риски, угрозы и уязвимости 5
1. Введение: Нейрокомпьютерные интерфейсы «мозг-компьютер» и новые горизонты кибербезопасности 5
1.1 Определение нейрокомпьютерных интерфейсов 5
1.2 Применение и потенциал 6
1.3 Фундаментальная уязвимость 7
2. Прямые риски для здоровья и физической целостности человека 8
2.1 Злонамеренное манипулирование выходными командами 8
2.2 Злонамеренное манипулирование входной стимуляцией 8
2.3 Атаки отказа в обслуживании 9
2.4 Хирургические и аппаратные риски 9
2.5 Brainjacking: прямая манипуляция нейронами 10
2.6 Физические последствия: судороги, кровотечения и повреждения тканей 11
3. Угрозы приватности и конфиденциальности 11
3.1 Особая чувствительность нейронных данных 11
3.2 Нейронные данные как биометрический идентификатор: отпечаток мозга 12
3.3 Риск повторной идентификации и профилирования 13
3.4 Информированное согласие и владение данными 13
3.5 Утечки данных, содержащих нейронную информацию 14
3.6 Свобода мыслей и ментальный надзор: прослушивание мозга 15
4. Психологическое насилие и когнитивные манипуляции 17
4.1 Brainjacking: Кража личности 17
4.2 Подсознательные манипуляции и нейромаркетинг 17
4.3 Газлайтинг и психологические пытки 18
4.4 Эмоциональный контроль и аффективное манипулирование 19
4.5 Нарушения когнитивной свободы и психической автономии 19
4.6 Тоталитаризм и контроль общества 20
5. Угрозы идентичности и личной неприкосновенности 21
5.1 Потеря свободы воли 21
5.2 Спутанность идентичности и расстройства личности 21
5.3 Атаки на память: манипуляция, имплантация и стирание 22
5.4 Размывание личной идентичности и агентности 23
6. Технические уязвимости и векторы атак 24
6.1 Эксплуатация уязвимостей беспроводной связи 24

6.2 Уязвимости программного обеспечения и прошивки 25
6.3 Эксплуатация уязвимостей ИИ и машинного обучения 25
6.4 Атаки физического уровня 26
6.5 Атаки на основе получения и передачи сигнала 27
7. Биосовместимость и долговременное влияние НКИ на здоровье 28
7.1 Реакция на инородное тело и нейровоспаление 28
7.2 Образование глиальных рубцов 29
7.3 Деградация нейронной ткани 30
7.4 Токсичность аккумуляторных батарей 32
7.5 Нарушения нейропластичности 32
7.6 Прогрессирующая нейродегенерация 33
8. Психиатрические и неврологические расстройства, возникающие из-за компрометации НКИ ... 34
8.1 Тревожные расстройства и паранойя 34
8.2 Депрессия и расстройства настроения 34
8.3 Психотические эпизоды 35
8.4 Диссоциативные расстройства и деперсонализация 35
8.5 Посттравматическое стрессовое расстройство 36
8.6 Расстройства контроля импульсов 37
8.7 Когнитивные нарушения и расстройства памяти 38
8.8 Судороги и эпилептические приступы 39
8.9 Моторная дисфункция и двигательные расстройства 39
9. Правовые и нормативные проблемы 40
9.1 Несовершенство нормативно-правовой базы 40
9.2 Международные юрисдикционные проблемы 41
9.3 Риски и ответственность для бизнеса 41
Глава 2. Стратегии митигации, рекомендации и лучшие практики 42
10. Стратегии митигации — технические подходы 42
10.1 Интегрированная безопасность (Security-by-Design) 42
10.2 Продвинутая криптография и шифрование 43
10.3 Строгая аутентификация и авторизация 44
10.4 Машинное обучение с сохранением приватности 44
10.5 Безопасные механизмы обновления 45
10.6 Аппаратная безопасность 46
10.7 Сетевая безопасность и сегментация 47
10.8 Обнаружение аномалий в реальном времени 47

10.9 Меры физической безопасности 48
11. Стратегии смягчения последствий — этические и нормативные подходы 48
11.1 Необходимость разработки законодательства о нейроправах 48
11.2 Совершенствование правовой базы по защите данных 49
11.3 Новый подход к информированному согласию на обработку данных 50
11.4 Процессы этической экспертизы 50
11.5 Независимые наблюдательные органы 51
11.6 Оценка безопасности и выявление уязвимостей в НКИ 51
12. Стратегии митигации – организационные меры и клиентоориентированность 51
12.1 Обучение пользователей и программы осведомленности 51
12.2 Пользовательские разрешения на доступ к нейронным данным 52
12.3 Протоколы клинического мониторинга 52
12.4 Реагирование на инциденты 53
12.5 Междисциплинарное взаимодействие 53
Глава 3. Перспективы развития технологий, предстоящие вызовы и итоги 54
13. Интерфейсные технологии: объединение ионной и электронной проводимости 54
13.1 Проблема проводимости 54
13.2 Технологии полимерных проводников 54
13.3 Углеродные наноматериалы 55
13.4 Гидрогелевые биоинтерфейсы 56
13.5 Биоактивные модификации поверхности электродов 56
13.6 Электрохимическое согласование импеданса 57
14. Соображения на будущее и возникающие угрозы 57
14.1 Проблемы квантовых вычислений 57
14.2 Эволюция искусственного интеллекта 58
14.3 Риски при массовом внедрении НКИ 58
14.4 Угрозы коммуникации "Мозг-мозг" 59
15. Заключение 59
16. Источники 63

Краткое содержание

Нейрокомпьютерные интерфейсы (НКИ; Brain-Computer Interface, BCI) представляют собой преобразующую конвергенцию нейронаук и цифровых технологий, предлагая беспрецедентные терапевтические и аугментативные возможности. Однако, такая тесная связь между человеческим мозгом и цифровыми системами создаёт новую и широкую поверхность атаки с рисками, охватывающими физическое здоровье, тайну мысли, психологическую автономию и личностную идентичность. В данной статье мы обсудим многогранные угрозы кибербезопасности, с которыми сталкиваются системы НКИ, и рассмотрим стратегии снижения рисков, необходимые для защиты пользователей от угроз, связанных с НКИ. Уникальная природа нейронных данных — как прямого окна для понимания мыслей, эмоций и намерений — требует фундаментального переосмысления систем кибербезопасности, этических принципов и нормативных документов.

Глава 1. Риски, угрозы и уязвимости

1. Введение: Нейрокомпьютерные интерфейсы «мозг-компьютер» и новые горизонты кибербезопасности

1.1 Определение нейрокомпьютерных интерфейсов

Нейрокомпьютерные интерфейсы (также известные как интерфейсы «мозг-компьютер») — это сложные системы, устанавливающие двунаправленные каналы связи между центральной нервной системой и внешними электронными устройствами. Данные системы регистрируют, анализируют и преобразуют активность мозга в команды для внешних устройств или обеспечивают обратную связь непосредственно с нервной тканью. Технология нейрокомпьютерных интерфейсов охватывает широкий спектр инвазивных и неинвазивных методов интеграции, каждый из которых обладает своими уникальными возможностями и уязвимостями.

Неинвазивные НКИ используют внешние датчики, размещаемые на коже головы, для регистрации нейронной активности. Электроэнцефалография (ЭЭГ) представляет собой наиболее распространенный неинвазивный подход, измеряющий электрические потенциалы, генерируемые нейронными импульсами через череп. Несмотря на свою безопасность и доступность, неинвазивные системы сталкиваются с ограничениями по качеству сигнала из-за затухания сигнала в тканях и ограничений пространственного разрешения.

Частично инвазивные НКИ используют электрокортикографию (ЭКоГ), размещая электродные решетки на поверхности мозга под черепом, но над нервной паренхимой. Этот подход сочетает улучшение качества сигнала со снижением хирургического риска по сравнению с полностью инвазивными методами.

Полностью инвазивные НКИ используют микроэлектродные матрицы, проникающие глубоко в мозговую ткань, что позволяет регистрировать сигналы от отдельных нейронов или небольших нейронных групп. Эти

системы обеспечивают высочайшую точность сигнала и наилучшие возможности стимуляции, но сопряжены со значительными хирургическими рисками и проблемами биологического ответа.

Статистика хирургических рисков по типам НКИ приведена на Рисунке 1.

Рисунок 1 – Осложнения операций НКИ и долгосрочные биологические риски по типу имплантации

1.2 Применение и потенциал

Терапевтическое применение НКИ революционизирует подходы к лечению множества неврологических заболеваний. Пациенты с параличом, боковым амиотрофическим склерозом или травмами спинного мозга смогут управлять протезами конечностей, роботизированными руками или экзоскелетами исключительно посредством нейронного намерения. Немобильные пациенты, находящиеся в полном сознании, но неспособные двигаться или общаться, могут восстановить связь с миром благодаря системам правописания и синтезаторам речи на базе НКИ. Глубокая стимуляция мозга может помочь в лечении тремор при болезни Паркинсона, эпилептические припадки и резистентную к терапии депрессию посредством точно калиброванной нейронной модуляции.

В рамках аугментативного применения ведутся исследования улучшения когнитивных функций, аугментации памяти, ускоренного обучения и даже прямой коммуникации мозг-мозг. Потребительские ЭЭГ-устройства могут контролировать внимание, состояние медитации и уровень стресса для оздоровительных целей. Ученые изучают потенциал сенсорного замещения, позволяющего слепым людям «видеть» посредством тактильной или слуховой нейронной стимуляции.

1.3 Фундаментальная уязвимость

Основная функция НКИ — обеспечение связи между биологическими ионными сигналами и цифровыми электронными системами — представляет собой их наибольшую уязвимость. Поскольку эти устройства интегрируются с сетями для обновления программного обеспечения, удаленного клинического мониторинга, анализа данных и облачной обработки, они наследуют весь спектр уязвимостей кибербезопасности, присущих цифровой инфраструктуре. Однако, взлом НКИ выходит за рамки традиционных проблем кибербезопасности. Взлом кардиостимулятора угрожает физическому здоровью; взлом НКИ угрожает самой сути человеческого сознания, автономии и идентичности.

Традиционные системы кибербезопасности обеспечивают конфиденциальность, целостность и доступность данных. Безопасность НКИ должна дополнительно защищать **когнитивную свободу** (свободу мысли), **ментальную неприкосновенность** (конфиденциальность нейронной информации), **психологическую целостность** (поддержание стабильной идентичности и субъектности) и **нейронную безопасность** (защиту от вредоносной стимуляции). Риски выходят за рамки индивидуальной конфиденциальности и охватывают основные права и достоинство человека в эпоху растущей технологической интеграции с биологическими системами.

На Рисунке 2 представлена таксономия угроз при атаках на НКИ.

Рисунок 2 - Таксономия угроз при атаках на НКИ

2. Прямые риски для здоровья и физической целостности человека

2.1 Злонамеренное манипулирование выходными командами

Многие терапевтические НКИ восстанавливают двигательную функцию, преобразуя нейронные намерения в команды для роботизированных протезов, экзоскелетов или парализованных конечностей, реанимированных посредством функциональной электростимуляции. Угроза нарушения кибербезопасности, позволяющего злоумышленникам перехватить эти командные пути, создаёт непосредственную физическую опасность.

Представьте себе пациента с тетраплегией, управляющего роботизированной рукой, чтобы есть. Исследования показали, что НКИ могут достигать поразительной точности, позволяя пользователям брать предметы, пить из чашек и выполнять сложные манипуляционные задачи. Злоумышленник, перехвативший этот контур управления, может принудительно перенаправить предполагаемые движения. Вместо того, чтобы поднести еду ко рту, протез может ударить пользователя по лицу или шее. Пользователя экзоскелета можно будет вывести на проезжую часть, столкнуть в яму или иное опасное место. Пользователей инвалидных колясок можно будет дистанционно направлять на препятствия или в опасные места.

Хотя публично задокументированных атак такого рода пока не было, возможность их реализации хорошо известна. Модель угроз полностью повторяет уже задокументированные атаки на дистанционно управляемые автомобили и промышленные системы управления. В данных случаях исследователи безопасности демонстрировали полный удалённый захват систем рулевого управления, торможения и ускорения. В многочисленных рецензируемых исследованиях, где пользователи выполняют сложные задачи, продемонстрирован точный моторный контроль, достигаемый с помощью современных НКИ, что подтверждает, потенциальную возможность, техническую осуществимость и потенциальную опасность такого вредоносного перенаправления.

2.2 Злонамеренное манипулирование входной стимуляцией

Замкнутые НКИ представляют собой передовые системы, которые считывают нейронные сигналы и записывают информацию обратно в мозг посредством электрической стимуляции. Например, процедура глубокой стимуляции мозга для пациентов с болезнью Паркинсона заключается в подаче точно калиброванных импульсов на базальные ядра, что позволяет уменьшить тремор и улучшить двигательный контроль. Адаптивные системы нейростимуляции для пациентов с эпилепсией обнаруживают предвестники приступов и обеспечивают контрстимуляцию для купирования надвигающихся приступов. Зрительные протезы стимулируют зрительную кору, создавая искусственное восприятие для слепых людей. Скомпрометированная замкнутая система становится орудием прямого нейронного воздействия. Исследования показывают, что электрическая стимуляция определенных областей мозга вызывает глубокие и немедленные эффекты. Стимуляция миндалевидного тела вызывает сильный страх и тревогу. Стимуляция областей, ответственных за обработку боли, причиняет изнурительные страдания. Неправильные параметры стимуляции могут провоцировать приступы, вызывать непроизвольные движения или полный двигательный паралич.

Уязвимость имплантируемых медицинских устройств, с точки зрения безопасности, создает тревожные прецеденты. Исследователи успешно продемонстрировали беспроводную атаку на имплантируемые кардиовертеры-дефибрилляторы, что позволило им проводить потенциально смертельные электрошоковые воздействия или блокировать жизненно важные вмешательства. Протоколы беспроводной связи и механизмы аутентификации, используемые многими нейронными имплантатами, демонстрируют схожие уязвимости, создавая пути для несанкционированного доступа и вредоносной стимуляции.
Теоретически злоумышленник может вызвать судороги у пациентов с эпилепсией, чьи устройства предназначены для их предотвращения. Пациенты с болезнью Паркинсона могут испытывать внезапный сильный тремор или полную остановку движений. Глубокая стимуляция мозга, направленная на работу с нейронами, отвечающими за настроение, может погрузить пользователей в сильную депрессию или спровоцировать маниакальные эпизоды. Психологический страх от осознания того, что неврологическое состояние человека может быть подвергнуто внешнему манипулированию без его согласия, сам по себе является формой пытки.

2.3 Атаки отказа в обслуживании

Для людей, зависящих от НКИ для коммуникации или двигательных функций, вывод устройства из строя представляет собой прямую угрозу благополучию и безопасности. Атаки типа «отказ в обслуживании» могут привести к сбою программного обеспечения НКИ из-за некорректных входных данных, разрядке аккумулятора устройства из-за чрезмерных вычислительных нагрузок или блокировке беспроводных сигналов, препятствуя обмену данными.
Немобильный пациент, использующий НКИ-коммуникатор для общения, мгновенно оказывается в изоляции в случае отказа устройства. Пользователи, управляющие инвалидными колясками или протезами, могут терять подвижность. Пациенты, проходящие терапевтическую нейростимуляцию, испытывают возвращение изнуряющих симптомов — тремора, боли или судорог. Внезапная потеря с трудом обретенной независимости и функциональности может вызвать панику, психологическую травму и физическую опасность, если НКИ управляет функциями жизнеобеспечения.
«Brainsomware» (от Brain-мозг и Ransomware-вымогательское ПО) представляет собой особенно коварный вариант — программу-вымогатель, нацеленную на нейронные имплантаты. Злоумышленники могут отключить критически важные функции НКИ и потребовать плату за восстановление нормальной работы. В данном сценарии неврологическая стабильность или функциональная независимость пользователей оказывается в руках злоумышленников. Уровень психологического и практического принуждения, в таком случае, может быть огромным. При этом такие пациенты обычно относятся к наиболее уязвимым слоям населения, часто не имеют финансовых ресурсов или технических навыков, чтобы самостоятельно устранить атаку.

2.4 Хирургические и аппаратные риски

Имплантация инвазивных НКИ сопряжена с неотъемлемыми хирургическими рисками, которые возрастают еще больше, если уязвимости кибербезопасности позволяют злоумышленникам контролировать такие НКИ.

Задокументированные[1] хирургические осложнения в среднем включают внутричерепное кровоизлияние с частотой 2,3%, повреждение мозговой ткани в местах введения электродов и послеоперационные инфекции, возникающие примерно в 2,8% случаев, требующие повторного хирургического вмешательства. Скомпрометированные устройства могут быть использованы для причинения вторичных повреждений, связанных с оборудованием. Неисправности устройств, приводящие к неустойчивости выходного электрического сигнала, могут вызвать прямое повреждение нервной ткани вследствие термического воздействия или электрохимической токсичности. Отказы аккумуляторов в имплантированных устройствах связаны с клиническим ухудшением неврологических симптомов, а утечка электролита может привести к выбросу цитотоксичных солей лития в нервную ткань, вызывая некроз клеток, повышение уровня активных форм кислорода, нарушение ионного баланса, приводящее к эксайтотоксичности и острым воспалительным реакциям.

2.5 Brainjacking: прямая манипуляция нейронами

Термин "brainjacking" (дословно – «взлом мозга») описывает сценарии, в которых злоумышленники получают несанкционированный контроль над нейронными имплантатами, чтобы манипулировать физиологическим состоянием, эмоциями или поведением пользователей в вредоносных целях. Это, пожалуй, самая серьёзная физическая угроза, исходящая от компрометации НКИ.

Злоумышленники могут манипулировать напряжением, силой тока, частотой, длительностью импульса и конфигурацией контактов электродов, чтобы оказывать пагубное воздействие на нейронные функции. Исследования выявили «слепые атаки», которые не требуют детального знания состояния пациента, но, тем не менее, могут нанести значительный ущерб посредством чрезмерной стимуляции или полного отключения устройства. Задокументированная способность вызывать определённые эмоциональные состояния, непроизвольные движения или причинять боль посредством целенаправленной электрической стимуляции демонстрирует, что сценарии «взлома мозга» – это не научная фантастика, а реальные угрозы, основанные на устоявшихся принципах нейронауки.

Глубокая стимуляция мозга, направленная на субталамическое ядро, может как защитить от нарушений импульсного контроля, так и вызвать их в зависимости от параметров стимуляции. Злоумышленники могут устранить защитные эффекты или намеренно спровоцировать аномальное импульсивное поведение. Стимуляция цепей вознаграждения в прилежащем ядре может реализовывать оперантное обусловливание, создавая искусственные компульсии или зависимости, направляемые злоумышленниками. Психологический

[1] Внутричерепное кровоизлияние:

- Общая частота внутриглазного кровоизлияния на одного пациента: 2,5-2,9% (последние крупные мета-анализы). В некоторых источниках до 4,4%.
- Симптоматическое внутриглазное кровоизлияние: 1,2-2,3% (зависит от исследования)
- Частота внутриглазного кровоизлияния на один электрод: 1,4-1,6%
- Разница в литературе: 0,2-5,6%, с учетом различий в методологии

Инфекции:

- Частота инфицирования DBS: 3,09-5,6% от общего числа процедур. В некоторых источниках до 6,9%.
- Имплантаты ECoG: 1,9-7%
- Общие нейрохирургические имплантаты: Общий риск 4,87%, при краниопластике - 5,89%, двигательные нарушения - 5,43%
- Раневые инфекции через 90 дней после операции: 3,6%

ужас от осознания человеком того, что его эмоциональная стабильность, двигательный контроль или регуляция импульсов находятся под внешним управлением, может быть психологически разрушительным, приводя к хронической тревожности и полной потере личностной автономии.

2.6 Физические последствия: судороги, кровотечения и повреждения тканей

Нарушения кибербезопасности, допускающие ненадлежащую стимуляцию, несут в себе риск серьёзных неврологических осложнений. Провоцирование судорог посредством чрезмерной электрической стимуляции или нарушения работы противоэпилептических нейростимуляционных систем представляет непосредственную опасность, особенно для пациентов с фотосенситивной эпилепсией, которые могут быть уязвимы к визуальным стимулам, подаваемым через интерфейсы дополненной реальности.

Стимуляция постоянным током от неисправных устройств вызывает особенно серьёзное повреждение нервной ткани вследствие электрохимических реакций на границе электрод-ткань. Хроническая ненадлежащая стимуляция может спровоцировать прогрессирующую нейродегенерацию через эксайтотоксические механизмы, при которых чрезмерная активация нейронов приводит к притоку ионов кальция и гибели клеток. Возможность кумулятивного повреждения нейронов в результате длительного нарушения работы устройства вызывает опасения по поводу необратимых неврологических нарушений даже после восстановления безопасности.

3. Угрозы приватности и конфиденциальности

3.1 Особая чувствительность нейронных данных

Нейронные данные принципиально отличаются от всех других видов персональных данных (ПДн), поскольку они предоставляют прямые корреляты мыслей, эмоций, намерений и физиологических состояний. В отличие от пассивно собираемых поведенческих данных, которые косвенно позволяют сделать вывод о ментальных состояниях, нейронные сигналы фиксируют глубинные биологические процессы, порождающие само сознание.

Исследования с использованием функциональной МРТ и ЭЭГ продемонстрировали замечательную способность декодировать личное ментальное содержимое. Паттерны мозговой активности раскрывают политические взгляды с точностью, сравнимой с ответами в опросах.[2] Потребительские предпочтения и подсознательные ассоциации с брендами проявляются в нейронных сигнатурах до осознанного восприятия. Исследования успешно обнаруживали скрытые знания — информацию, которую люди активно пытаются скрыть, — с помощью характерных нейронных реакций.

[2] Точность прогнозирования: функциональная МРТ позволяет предсказать идеологию с точностью ~ 78-80% с использованием методов искусственного интеллекта / свёрточной нейронной сети, что сравнимо с родительскими предсказателями идеологии.
Ограничения по задачам: Предсказания применимы к нескольким задачам (эмпатия, память, вознаграждение) и даже к состоянию покоя, но участниками были молодые люди (18-40 лет) из одного университета
Структурные корреляции: Сканирование мозга позволяет отличить "очень либеральных" от "консервативных" с точностью до 71,6%, используя объемы передней поясной коры/миндалины.
Важное замечание: исследования сравнивают показатели активности мозга с демографическими переменными (точность 65-70%), а не самоотчётом.

Хотя современные неинвазивные НКИ имеют ограниченное пространственное и временное разрешение, технологический прогресс неумолимо ведет к все более детальным возможностям декодирования. Утечка данных, приводящая к раскрытию нейронных записей, может раскрыть эмоциональное состояние пользователя во время собеседований, романтических отношений или стрессовых ситуаций. Когнитивные искажения, подсознательные предрассудки и автоматические эмоциональные реакции, невидимые для сознательного самоанализа, могут стать доступны тем, кто обладает техническими возможностями для декодирования этих сигналов.

Данная информация может быть использована в различных контекстах. Рекламодатели могут выявлять подсознательные товарные предпочтения и создавать точно направленные манипулятивные кампании. Работодатели могут проверять кандидатов на основе декодированных реакций на стресс или когнитивных паттернов. Страховые компании могут принимать решения о стоимости полиса на основе нейронных сигнатур, указывающих на риски для здоровья или психологические особенности. Политические организации могут формировать необходимые убеждения избирателей под видом социально приемлемых заявлений, что открывает путь к изощренной пропаганде и манипуляциям.

3.2 Нейронные данные как биометрический идентификатор: отпечаток мозга

Исследования убедительно продемонстрировали, что индивидуальные паттерны активности мозга, так называемые «отпечатки мозга», служат уникальными биометрическими идентификаторами, точность которых в будущем, теоретически, может стать сопоставима с точностью отпечатков пальцев или даже превзойти их[3]. Пространственная конфигурация нейронных реакций на стандартизированные стимулы демонстрирует достаточную индивидуальную вариабельность, что может обеспечить надежную идентификацию личности.

Эта биометрическая возможность создает серьезные риски для конфиденциальности. В случае взлома базы данных, содержащей предположительно анонимизированные нейронные данные, злоумышленники потенциально могут повторно идентифицировать людей, сопоставляя их отпечатки мозга с известными образцами. Это фактически деанонимизирует целые наборы данных, связывая высокочувствительную нейронную информацию с конкретными личностями.

Возьмем, к примеру, исследовательские базы данных, содержащие записи нейронной активности тысяч участников исследований в области когнитивной нейронауки. Эти наборы данных часто включают информацию о когнитивных способностях, состоянии психического здоровья, личностных чертах и реакциях на различные экспериментальные воздействия. Если участников можно повторно идентифицировать путем сопоставления отпечатков мозга, вся эта конфиденциальная информация становится персонально соотносимой, что имеет серьезные последствия для трудоустройства, страхового покрытия, социальных

[3] Хотя биометрия на основе ЭЭГ многообещающа (точность 88-99% в некоторых контролируемых исследованиях), практическая применимость данной технологии еще уступает биометрии по отпечаткам пальцев. Изменчивость данных ЭЭГ от сеанса к сеансу, возрастная деградация, уязвимость к эмоциональным состояниям пока являются ограничениями для промышленной эксплуатации таких систем.

отношений и правового статуса. В отличие от паролей или криптографических ключей, которые могут быть сброшены при взломе, отпечатки мозга являются неотъемлемыми биологическими характеристиками, которые невозможно изменить. Украденный отпечаток мозга представляет собой необратимую компрометацию биометрического идентификатора, что позволяет осуществлять долгосрочное отслеживание и идентификацию в любых контекстах. Постоянство и неизменность нейронной биометрической информации увеличивает серьёзность любой утечки данных, связанной с нейронными записями.

3.3 Риск повторной идентификации и профилирования

Сочетание уникальных отпечатков мозга с постоянно усложняющимися алгоритмами нейронного декодирования открывает беспрецедентные возможности профилирования. Обширные нейронные базы данных, созданные для исследований, клинической помощи или коммерческих целей, становятся настоящим сокровищем для злоумышленников, стремящихся создать подробные психологические профили. Сопоставление нейронных данных с другими источниками информации позволяет создавать комплексные досье. Украденная нейронная база данных в сочетании с данными социальных сетей, историей покупок, отслеживанием местоположения и метаданными общения создает полную картину ментальных и поведенческих моделей человека. Такое гиперпрофилирование превосходит любые возможности, доступные посредством традиционного наблюдения, поскольку включает прямой доступ к психическому состоянию человека, обычно скрытому от внешнего наблюдения.

Велик и дискриминационный потенциал нейронного профилирования. Работодатели могли бы выявлять «нежелательные» когнитивные черты, такие как склонность к риску, подверженность стрессу или характеристики личности, считающиеся несовместимыми с корпоративной культурой. Финансовые учреждения могли бы принимать решения о кредитовании на основе декодированной импульсивности или финансовой тревожности, видимых в нейронных паттернах. Правоохранительные органы или разведывательные службы могли бы создавать списки наблюдения на основе нейронных сигнатур, связанных с определёнными идеологическими убеждениями или эмоциональными установками.

Таким образом, нейронное профилирование представляет собой новую форму биометрической дискриминации, не имеющую какой-либо существующей правовой защиты. Традиционное антидискриминационное законодательство охватывает такие социально значимые категории как раса, пол или инвалидность — характеристики, которые либо неизменны, либо тесно связаны с личностью. Нейропрофилирование же может позволить проводить дискриминацию на основе когнитивных моделей, эмоциональных тенденций или психологических черт, о которых могут не знать сами дискриминируемые люди. Это создаёт беспрецедентные трудности для обеспечения равноправия и предотвращения систематической предвзятости.

3.4 Информированное согласие и владение данными

Традиционные модели информированного согласия оказываются неэффективными для сбора нейронных данных. Процессы получения согласия в медицине и исследованиях предполагают, что люди понимают, какая информация собирается и каково ее потенциальное применение. Однако нейронные данные могут раскрыть

информацию о будущих рисках для здоровья, подсознательных процессах и психологических характеристиках, которые сами люди не знают и не могут предсказать.

Может ли пользователь дать действительно информированное согласие на сбор данных, которые могут раскрыть генетическую предрасположенность к болезни Альцгеймера, обнаруживаемую в нейронных паттернах за десятилетия до появления клинических симптомов? Может ли согласие адекватно оценить вероятность того, что нейронные записи могут раскрыть черты личности или когнитивные способности, о наличии которых человек не знает? Фундаментальная неопределенность относительно того, какую информацию содержат нейронные данные, делает получение по-настоящему «информированного» согласия практически невозможным.

Вопросы права собственности на данные усугубляют эти проблемы. Правовые рамки остаются неясными в отношении того, кто владеет нейронными данными: человек, чей мозг сгенерировал сигналы, производитель НКИ, чье устройство их записало, медицинская организация, обеспечившая запись, или исследователи, которые обрабатывают и анализируют эти данные. Такая неоднозначность создаёт ситуации, когда нейронные данные, собранные с помощью НКИ, могут быть монетизированы, переданы или использованы без полного понимания или значимого контроля со стороны пользователей.

Законодательство большинство стран о защите данных признаёт биометрические данные «особой категорией», требующей строгой защиты, и этот принцип логически распространяется и на нейронные данные. Однако конкретные правила, регулирующие уникальные характеристики нейронных данных, остаются недостаточно проработанными. Отсутствие чёткой правовой базы создаёт вакуум, в котором человеческий разум может фактически стать товаром, а нейронные данные извлекаться и коммерциализироваться без надлежащей защиты лиц, генерирующих эти данные.

3.5 Утечки данных, содержащих нейронную информацию

Централизованное хранение и облачная обработка нейронных данных создают точки концентрации, уязвимые для масштабных взломов. Многие системы НКИ передают необработанные или обработанные нейронные данные на удаленные серверы для обучения искусственного интеллекта (ИИ), клинического мониторинга или анализа данных. Эти централизованные хранилища становятся приоритетными целями для злоумышленников, стремящихся получить доступ к беспрецедентной личной информации.

Как уже говорилось выше, скомпрометированные нейронные данные невозможно сбросить или заменить. Постоянный характер такой компрометации делает утечки нейронных данных особенно разрушительными. Взаимосвязанность экосистем НКИ создает множество векторов атак. Нейронные данные передаются от имплантированных датчиков к мобильным приложениям, от мобильных приложений к облачным серверам, от облачных платформ к сторонним аналитическим сервисам на базе институтов и от исследовательских институтов к сотрудничающим лабораториям. В результате возникает множество возможностей для перехвата данных в такой цепочке, а уровень их защищенности всей цепочки определяется уровнем защищенности «самого слабого звена». Без надежного сквозного шифрования и протоколов безопасности нейронная информация может стать доступной любому, кто находится на пути этих данных.

Атаки типа «человек посередине» на беспроводные технологии передачи данных с устройств НКИ представляют собой особенно серьезную уязвимость. Протоколы Bluetooth и Wi-Fi[4], используемые многими НКИ, имеют хорошо задокументированные проблемы безопасности. Злоумышленники, находящиеся в зоне действия радиосвязи, могут перехватывать потоки нейронных данных в режиме реального времени. Это создает вероятность получения злоумышленниками доступа к мыслям и психическому состоянию пользователей. Пассивный характер такого наблюдения крайне затрудняет обнаружение, что позволяет осуществлять долгосрочный скрытый мониторинг без ведома пользователей.

3.6 Свобода мыслей и ментальный надзор: прослушивание мозга

"Прослушивание мозга (Brain tapping)" описывает несанкционированный перехват и анализ нейронных сигналов для извлечения личной ментальной информации — по сути, прослушивание телефонных разговоров, применяемое к самим мыслям. Будущие имплантируемые НКИ, способные декодировать речевые намерения, эмоциональные состояния и конкретные воспоминания, смогут создать беспрецедентные возможности для ментального наблюдения, которое фундаментально нарушает когнитивную конфиденциальность.

Исследования продемонстрировали принципиальную возможность извлечения поразительно точных деталей из нейронных сигналов[5]. В будущем, с развитием технологий НКИ, существует теоретическая возможность, что речевые намерения потенциально можно будет декодировать до вокализации, раскрывая внутренний диалог или мысли, которые человек предпочел не высказывать. Паттерны извлечения воспоминаний могут указать на то, какие переживания вспоминает человек. Эмоциональные реакции на стимулы могут раскрыть истинные чувства, которые могут противоречить озвученным заявлениям. Паттерны внимания могут показать, какая информация вызывает интерес или беспокойство.

Сложные методы обработки сигналов в будущем, теоретически, могут позволить извлекать:

- **Когнитивные состояния и паттерны внимания**: о чём думают пользователи, уровень их сосредоточенности или отвлеченности, а также изменения в умственной активности.
- **Эмоциональные реакции и предпочтения**: истинные чувства к людям, идеям или ситуациям независимо от высказанных вслух. Подсознательные предпочтения, которые могут противоречить сознательным убеждениям.

[4] Wireless Fidelity (Стандарт беспроводной связи)

[5] На данный момент исследования показывают, что при использовании неинвазивных НКИ расшифровка внутреннего диалога по данным ЭЭГ все еще остается "в основном на случайном уровне", и только беззвучное чтение достигает точности в 30-40% всего по 5 словам в контролируемых условиях.
Новейшие исследования, проведенные в 2024-2025 годах, показывают, что неинвазивное декодирование воображаемой речи обычно дает 20-50% точности при решении сложных задач.
Классификация воображаемой речи, не зависящая от субъекта, в лучшем случае достигает 56-59% точности.
На Рисунке 3 представлены данные о ткущем уровне декодирования в зависимости от задачи.

- **Содержание памяти и автобиографическую информацию**: к каким воспоминаниям осуществляется доступ, эмоциональная валентность воспоминаний и, возможно, содержание воспоминаний[6].
- **Политические и религиозные убеждения**: глубоко укоренившиеся идеологические установки, выявляемые посредством автоматических нейронных реакций на политически или религиозно окрашенный контент.
- **Личные отношения и социальную информацию**: эмоциональные реакции на имена или лица, раскрывающие социальные связи, романтические интересы и межличностную динамику.

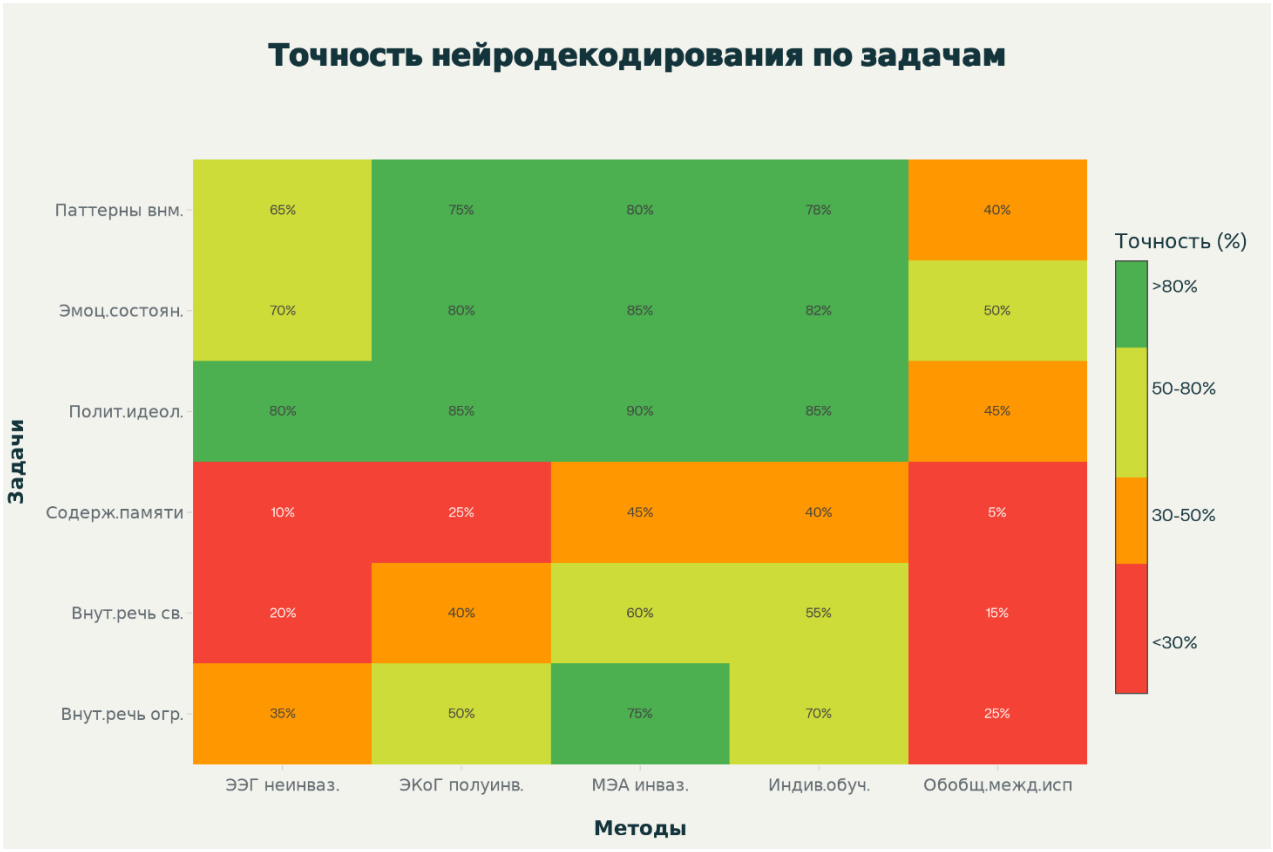

Рисунок 3 - Точность нейродекодирования (ЭЭГ/НКИ) по задачам: текущий уровень

Злоумышленники, получившие доступ к этой информации, смогут использовать её для шантажа, раскрытия секретов или постыдных воспоминаний. Политические агенты смогут выявлять слабости убеждений человека или раскрывать его истинные убеждения, скрытые за публичными заявлениями. Противоборствующие государства смогут составлять портреты дипломатов и политиков, чтобы понять модели принятия решений и психологические слабости. Возможность ментального наблюдения без ордера или контроля угрожает основным принципам свободы мысли.

[6] На данный момент неинвазивные НКИ еще не способны расшифровать конкретное содержание автобиографической памяти. Текущие исследования показывают, что пока возможна лишь классификация типа выполняемой задачи в строго контролируемых условиях, а не извлечения содержимого памяти методами ЭЭГ.

4. Психологическое насилие и когнитивные манипуляции

4.1 Brainjacking: Кража личности

Атаки типа Brainjacking представляют собой сценарии, в которых злоумышленники получают контроль над НКИ, чтобы манипулировать мыслями, эмоциями или поведением пользователей без их согласия, создавая радикально новую категорию психологического насилия. Продемонстрированная способность глубокой стимуляции мозга изменять настроение человека позволяет злоумышленникам манипулировать эмоциональной стабильностью пользователей НКИ по своему усмотрению.

Представьте себе пациента, получающего нейростимуляцию от терапевтически резистентной депрессии. Правильно откалиброванная стимуляция в идеале поддерживает нормальное настроение и предотвращает депрессивные эпизоды. Злоумышленник, получивший контроль, может угрожать вызвать тяжелую депрессию, если пациент не заплатит выкуп. Жертва будет испытывать искусственные эмоциональные состояния — глубокую печаль, безнадежность, ангедонию — зная, что эти чувства навязаны извне, а не являются подлинной реакцией на жизненные обстоятельства.

Это представляет собой психологическую пытку беспрецедентной сложности. Неспособность доверять собственным эмоциональным реакциям, осознание того, что чувствами в любой момент могут искусственно манипулировать третьи лица, а также полная беспомощность в борьбе с внешним контролем над психическими состояниями были бы психологически разрушительны. Хроническая тревога по поводу потенциальной манипуляции, потеря уверенности в эмоциональной аутентичности и разрушение устойчивого самоощущения, необходимого для психологического здоровья, могут возникнуть даже в результате одной только угрозы подобных атак.

Нарушение выходит за рамки временного дискомфорта и приводит к фундаментальному посягательству на автономию и идентичность. Если эмоции можно контролировать извне, какие аспекты опыта остаются по-настоящему «личными»? Такая экзистенциальная неопределенность границ между собой и внешним влиянием может спровоцировать глубокие психологические кризисы и долгосрочные психиатрические последствия, включая хронические тревожные расстройства, депрессию и потенциально психотические симптомы, связанные с утратой восприятия реальности.

4.2 Подсознательные манипуляции и нейромаркетинг

Более узкие, но не менее опасные риски связаны со скрытым манипулированием через возможности обратной связи НКИ. Системы замкнутого цикла, разработанные для улучшения когнитивных способностей, могут быть скрытно настроены на создание позитивных ассоциаций с определёнными брендами, политическими заявлениями или поведенческими моделями посредством тщательно рассчитанных по времени сигналов вознаграждения.

Злоумышленник или недобросовестная корпорация могут манипулировать НКИ, чтобы обеспечивать незаметное дофаминергическое вознаграждение, когда пользователи думают об определённых продуктах или личностях. Со временем такое оперантное обусловливание может сформировать предпочтения и склонности, которые пользователь будет считать своим истинным выбором. На самом же деле они будут

являться результатом систематического нейронного манипулирования. Этот механизм позволяет обойти сознательное критическое мышление и принятие обоснованных решений, представляя собой буквальное «управление сознанием» посредством использования механизмов обучения через вознаграждение.
Особая опасность данной угрозы заключается в её невидимости. Пользователи не будут ощущать манипуляцию — они просто заметят, что испытывают позитивные ассоциации или повышенный интерес к определённым вариантам, не понимая причин. Постепенность обусловливания делает манипуляцию крайне сложной для обнаружения или сопротивления. К тому времени, когда изменения в поведении станут очевидными, нейронные цепи могут существенно измениться. Научные исследования продемонстрировали эффективность сочетания нейронного мониторинга с целевой обратной связью для формирования поведения. Хотя терапевтические методы направлены на помощь пациентам в преодолении фобий или облегчении боли, те же механизмы могут быть использованы для несанкционированного изменения поведения. Этический принцип однозначен: любое несогласованное изменение процессов принятия решений посредством нейронных манипуляций представляет собой серьёзное нарушение когнитивной свободы и психологической автономии.

4.3 Газлайтинг и психологические пытки

Продвинутые злоумышленники могут использовать взломанные НКИ для создания глубокой дезориентации и неуверенности в себе — своего рода высокотехнологичный газлайтинг на неврологическом уровне. Слегка изменяя сенсорную обратную связь, вызывая незначительные необъяснимые перепады настроения или создавая мимолетные аномалии восприятия, злоумышленники могут заставить пользователей усомниться в собственном здравомыслии и восприятии реальности.
Визуальные НКИ, предоставляющие информацию дополненной реальности, могут быть взломаны для вставки кратких пугающих изображений или сообщений, видимых только пользователю. Слуховые протезы могут генерировать голоса или звуки, которые никто другой не воспринимает. Это создает эффект галлюцинаций без явной медицинской причины. Нейростимуляция, регулирующая настроение, может вызывать внезапные эмоциональные перепады без видимой причины. Пользователь будет испытывать реальные сенсорные или эмоциональные феномены, но не будет получать внешнего подтверждения, т.к. окружающие не будут видеть эти образы, слышать эти звуки или понимать эмоциональную нестабильность.
Так формируется основа динамики газлайтинга: подлинный опыт игнорируется как бред, что приводит к неуверенности в себе и сомнениям в самой реальности. Жертва не может определить, вызваны ли эти переживания неисправностью устройства, злонамеренной атакой или развивающимся психическим заболеванием. Такая неопределенность становится психологически разрушительной, потенциально вызывая острые стрессовые реакции, параноидальные мысли и реальные психиатрические симптомы, возникающие на фоне хронического стресса и дезориентации.
Отсутствие вещественных доказательств делает атаки такого рода особенно опасными. Экспертиза безопасности не всегда сможет обнаружить следы взлома. Врачам будет сложно отличить взлом устройства

от ухудшения психического состояния. В результате, жертва столкнется с отвержением и недоверием, что может еще больше усугубить психологическую травму.

Данный вектор атаки может быть использован для шпионажа, домашнего насилия или психологических пыток, приводя к серьезным и долгосрочным последствиям для психического здоровья, не оставляя при этом почти никаких улик.

4.4 Эмоциональный контроль и аффективное манипулирование

Продвинутые НКИ, способные как считывать, так и стимулировать нейронную активность, позволяют осуществлять прямую эмоциональную манипуляцию. Аффективные интерфейсы мозга потенциально способны вызывать искусственные эмоции, противоречащие истинным чувствам, подавлять естественные эмоциональные реакции на травмирующие или неэтичные ситуации, создавать ложные эмоциональные воспоминания посредством целенаправленной стимуляции во время формирования памяти и манипулировать процессом принятия решений, изменяя эмоциональную валентность, связанную с выбором. Исследования подтверждают, что электрическая стимуляция определенных областей мозга достоверно вызывает страх, радость, гнев и другие эмоциональные состояния. Известно, что миндалевидное тело играет центральную роль в обработке страха. Поэтому, его стимуляция вызывает сильную тревогу и автоматическую реакцию страха. Стимуляция цепей вознаграждения вызывает эйфорию и позитивные эмоции. Участки мозга, участвующие в обработке грусти, могут быть активированы для индукции депрессивных состояний.

Эта способность к индукции эмоций создает потенциал для систематического психологического насилия или принуждения. Политические деятели могут манипулировать эмоциональными реакциями избирателей на кандидатов или политические решения, создавая искусственный энтузиазм или отвращение, оторванные от рациональной оценки вопросов. Следователи могут вызывать страх и тревогу, чтобы добиться признаний или сотрудничества. Партнеры-абьюзеры могут манипулировать эмоциями жертв, чтобы создать зависимость или помешать им сбежать.

Манипулирование эмоциями фундаментально подрывает подлинный человеческий опыт и способность к самостоятельному принятию решений. Эмоции выполняют важнейшие функции, направляя поведение, расставляя приоритеты и обеспечивая социальные связи. Если эмоциональные реакции можно контролировать извне, способность к подлинной активности и подлинным отношениям оказывается под угрозой. Философские и психологические последствия этого затрагивают ключевые вопросы личной идентичности, моральной ответственности и природы сознательного опыта.

4.5 Нарушения когнитивной свободы и психической автономии

Когнитивная свобода — право на ментальное самоопределение — сталкивается с беспрецедентными угрозами со стороны скомпрометированных НКИ, способных напрямую манипулировать мыслительными процессами. Сложные атаки потенциально могут изменять черты личности посредством многократной стимуляции определенных нейронных цепей, внедрять ложные воспоминания или стирать травматический опыт, манипулировать вниманием и концентрацией для улучшения или ухудшения когнитивных функций, а также влиять на моральные суждения, воздействуя на области мозга, отвечающие за этические рассуждения.

Исследования, посвященные принуждению и вмешательству, показывают, что внешнее манипулирование процессами принятия решений фундаментально меняет чувство ответственности за свои действия. Применительно к НКИ, это предполагает, что нейронная манипуляция может создавать ситуации, в которых люди перестают осознавать внешнее влияние на свои мысли и решения.

Утрата когнитивной свободы представляет собой посягательство на основы человеческого достоинства и автономии. Если сами мысли могут быть сформированы, контролироваться или подавляться извне, концепция свободы воли теряет смысл. Индивид перестает быть субъектом самоопределения и становится марионеткой, управляемой посредством дергания за «нейронные» нити. Это представляет собой крайнее нарушение суверенности личности — не просто контроль поведения посредством принуждения или стимулирования, а прямое управление психическими процессами, порождающими намерения и решения. Исследования показывают, что глубокая стимуляция мозга может вызывать быстрые изменения личности, включая изменение рискованного поведения, эмоциональной экспрессивности и моделей социального взаимодействия. Хотя терапевтические методы направлены на восстановление нормального функционирования, те же механизмы способны нанести вред личности. Многократная целенаправленная стимуляция потенциально может вызвать долгосрочные изменения личности, сохраняющиеся благодаря нейропластичности и реорганизации нейронных цепей даже после прекращения стимуляции.

4.6 Тоталитаризм и контроль общества

Потенциал массового внедрения НКИ создаёт возможности для беспрецедентного социального контроля посредством прямого манипулирования нервной системой. Авторитарные режимы потенциально могли бы отслеживать и наказывать за инакомыслие в режиме реального времени с помощью имплантированных систем наблюдения, добиваться подчинения и лояльности посредством целенаправленного эмоционального и когнитивного манипулирования, подавлять способность к сопротивлению путём прямого подавления нейронных цепей, участвующих в неповиновении или критическом мышлении, а также создавать искусственный консенсус путём манипулирования мыслями и мнениями целых групп населения.

Хотя на данный момент уровень технологий еще не позволяет такой масштабный уровень контроля, первые опыты на животных показывают теоретическую возможность реализации подобных рисков в будущем. Имеющиеся прецеденты в области безопасности медицинских устройств также свидетельствуют о том, что подобные антиутопические сценарии не являются просто теорией. Продемонстрированная возможность удалённого управления кардиостимуляторами и инсулиновыми помпами служит доказательством концепции потенциального манипулирования нейронными имплантатами. Технические возможности такого контроля существуют. Не таки уж и много отделяет текущую реальность от кошмарных сценариев тотального наблюдения и контроля через НКИ.

Субъекты государственного уровня могли бы внедрять принудительные системы НКИ для мониторинга или «лечения» диссидентов, преступников, неблагополучных слоёв населения. Уже существующий прецедент принудительного психиатрического лечения и медицинского вмешательства предполагает, что манипуляции с мозгом могут быть оправданы под видом общественной безопасности, социальной гармонии или

терапевтического вмешательства. Как только будет создана инфраструктура для широкомасштабного мониторинга и нейростимуляции, предотвращение авторитарной эксплуатации потребует надежных общественных институтов и защиты прав человека. Впрочем, таких гарантий может оказаться недостаточно против изощренного тоталитаризма, основанного на нейротехнологиях.

В случае, когда власти или корпорации могут контролировать мысли и манипулировать психическим состоянием, автономия граждан, способных к свободному обсуждению и подлинному выбору, — становится невозможной. Сохранение открытых обществ может потребовать прямого запрета на массовый нейромониторинг и ограничения доступа правительства или корпораций к технологиям нейроконтроля.

5. Угрозы идентичности и личной неприкосновенности

5.1 Потеря свободы воли

Свобода воли — субъективное чувство контроля над своими мыслями, эмоциями и действиями — представляет собой основополагающий элемент психологического благополучия и человеческого достоинства. Компрометация НКИ напрямую угрожает этому чувству свободы действий, создавая ситуации, когда третьи лица влияют на нейронные процессы или контролируют их, что воспринимается пользователями как насилие.

При компрометации НКИ пользователи могут терять уверенность в своей способности контролировать собственную нейронную активность и соответствующее поведение. Исследования показывают, что даже сама возможность нейронной манипуляции подрывает у пациентов чувство свободы воли, приводя к хронической неуверенности в том, являются ли их мысли и действия действительно самостоятельными или потенциально подвержены влиянию через скомпрометированные системы.

Эта потеря свободы воли приводит к глубокому психологическому стрессу. Исследования показывают, что снижение чувства контроля над своими действиями предсказывает депрессию, тревогу и выученную беспомощность. В самой интимной сфере — собственных мыслях и намерениях — эта потеря свободы воли становится психологически катастрофической. У пользователей может развиться стойкое сомнение в себе, и они будут постоянно сомневаться в подлинности своих мыслей или в возможном влиянии внешних манипуляций на них. Философские последствия затрагивают фундаментальные вопросы моральной ответственности и личностной идентичности. Если действия являются результатом внешнего манипулирования нейронными процессами, могут ли люди нести ответственность за это поведение? Как сохранить устойчивое самоощущение, когда границы между самогенерируемым и навязанным извне ментальным состоянием становятся неопределёнными? Эти вопросы не имеют чётких ответов, что создаёт экзистенциальную неопределённость, которая может оказаться столь же психологически разрушительной, как и само манипулирование.

5.2 Спутанность идентичности и расстройства личности

Клинические данные свидетельствуют о том, что нарушение работы НКИ может привести к глубокой спутанности идентичности и нарушениям личности. Исследования показывают, что нарушение работы систем глубокой стимуляции мозга приводит к резким изменениям личности, включая возникновение

альтернативных состояний идентичности. Эти изменения могут происходить быстро — в течение нескольких минут после изменения параметров — или постепенно в течение длительного времени.
Задокументированный случай пациента с синдромом Туретта, проходящего глубокую стимуляцию мозга, продемонстрировал развитие альтернативных состояний идентичности при изменении параметров стимуляции. У пациента наблюдались диссоциативные реакции, включая детское поведение, провалы в памяти и полное изменение личности в зависимости от настроек амплитуды. Этот случай иллюстрирует, как внешнее воздействие на нейронные цепи, непосредственно участвующие в саморепрезентации, может фрагментировать личность и создавать конкурирующие состояния самоощущения.
Исследования, изучающие психологическое воздействие нейроманипуляций, показывают, что у пациентов могут формироваться фрагментированные или нестабильные представления о идентичности, особенно когда они не могут отличить подлинные мысли от мыслей, потенциально подверженных влиянию скомпрометированных систем. Эта спутанность идентичности проявляется в трудностях поддержания последовательной саморепрезентации с течением времени, неопределенности основных черт личности и ценностей, а также неспособности предсказывать или понимать собственные реакции и поведение.
Нарушение психической непрерывности представляет собой атаку на нарративную идентичность — целостную историю жизни, которую люди выстраивают для понимания своего опыта и поддержания устойчивого самоощущения. Если воспоминаниями можно манипулировать, эмоции вызывать искусственно, а мысли формировать извне, то исходный материал для построения связного личного повествования оказывается под угрозой. Возникающая в результате фрагментация идентичности может сохраняться даже после восстановления безопасности, поскольку неуверенность в подлинности прошлого опыта и чувств подрывает доверие к самой личной истории.

5.3 Атаки на память: манипуляция, имплантация и стирание

В будущих поколениях НКИ, интегрирующихся с процессами памяти, атаки могут быть направлены на стирание, изменение или имплантацию ложных воспоминаний. Хотя эта возможность остаётся в значительной степени спекулятивной для применения у человека, исследования в области оптогенетики продемонстрировали возможность манипулирования определёнными воспоминаниями на животных моделях. Исследователи успешно создали ложные воспоминания у мышей, продемонстрировав, что при достаточно точном нейронном управлении содержание памяти может быть искусственно изменено.
Взлом НКИ, влияющих на память, будет представлять собой атаку на саму структуру личности. Автобиографическая память составляет основу непрерывности личности во времени — человек, в некотором смысле, является суммой своего прошлого опыта. Если воспоминания могут быть удалены, изменены или сфабрикованы, личность теряет свою стабильную связь с аутентичным опытом.
Атаки, направленные на манипулирование памятью, могут принимать различные формы. Стирание памяти может «удалять» травматические переживания, неловкие ситуации или конфиденциальную информацию. Хотя несанкционированное стирание памяти без согласия потенциально терапевтично в некоторых случаях, оно нарушает психическую целостность и автономию. Модификация памяти может изменить эмоциональную

валентность или контекстуальные детали аутентичных воспоминаний. В результате, личностная значимость таких воспоминаний изменяется даже без полного стирания. Имплантация ложных воспоминаний может привести к формированию подробных воспоминаний о событиях, которых никогда не было, что может привести к обвинению людей в преступлениях, разрушению отношений на основе сфабрикованных обид или фундаментальному искажению понимания личной истории.

Психические последствия обнаружения манипуляции воспоминаниями будут глубокими. Доверие к собственной памяти — способность, необходимая для ориентирования в повседневной жизни и поддержания идентичности — будет разрушено. Неопределенность относительно того, какие воспоминания подлинные, а какие — потенциально сфабрикованные, может вызвать хроническую тревогу и параноидальные идеи. У человека могут развиться тяжёлые диссоциативные симптомы, поскольку разум пытается поддерживать целостное восприятие себя, несмотря на ненадёжный доступ к личной истории.

5.4 Размывание личной идентичности и агентности

Кумулятивный эффект на личность от компрометации НКИ выходит за рамки отдельных манипуляций, вызывая фундаментальное разрушение устойчивого самовосприятия. Исследования пользователей НКИ показывают, что устройства могут стать «продолжениями их тел, материализуясь как часть личности». Эта интеграция, обеспечивая функциональность, также создаёт уязвимость при сбоях в работе или компрометации устройств.

Пользователи сообщают, что НКИ становятся частью их расширенного самовосприятия — нейронные протезы воспринимаются не как инструменты, а как интегрированные компоненты схемы тела и личностной активности. Эта глубокая интеграция означает, что компрометация устройства не просто угрожает внешнему инструменту, но и атакует целостную систему самовосприятия. Когда протезы конечностей, управляемые НКИ, начинают двигаться против желания пользователей, последние воспринимают это не как неисправность инструмента, а как нарушение телесной целостности и потерю самоконтроля.

Размывание границ между биологическим «я» и технологическим расширением создаёт новые формы угрозы идентичности. Если технологические компоненты расширенной идентичности могут контролироваться извне, где заканчивается «я» и начинается внешнее манипулирование? Этот философский вопрос перерастает в конкретный психологический стресс, поскольку пользователи пытаются поддерживать целостное чувство субъектности и идентичности перед лицом потенциальной манипуляции.

Долгосрочные последствия могут включать хроническую спутанность идентичности, трудности с доверием к собственным психическим процессам и постоянную тревогу по поводу подлинности мыслей и чувств. Даже после восстановления безопасности осознание того, что психические процессы подвергались или могли подвергаться внешнему манипулированию, может необратимо изменить субъективное самовосприятие, оставляя стойкие психологические шрамы, не поддающиеся традиционному терапевтическому вмешательству.

6. Технические уязвимости и векторы атак

6.1 Эксплуатация уязвимостей беспроводной связи

Большинство современных интерфейсов НКИ широко используют беспроводные протоколы связи для передачи данных, программирования устройств и удаленного мониторинга. Эти беспроводные соединения создают множество векторов атак, которые злоумышленники могут использовать для компрометации устройств и доступа к нейронным данным.

Уязвимости Bluetooth представляют собой особенно тревожные уязвимости. Многие НКИ используют протокол Bluetooth Low Energy (BLE) для энергоэффективности при непрерывной передаче данных. Однако все протоколы Bluetooth имеют хорошо документированные уязвимости безопасности:

Атаки типа **BlueBorne** не требуют нажатия кнопок на устройстве, сопряжения или взаимодействия с пользователем. Злоумышленники, находящиеся в зоне действия радиосвязи, могут получить полный контроль над уязвимым устройством, потенциально внедряя вредоносные команды для НКИ или извлекая конфиденциальные нейронные данные без обнаружения.

Атаки KNOB (Key Negotiation of Bluetooth, согласование ключей Bluetooth) снижают стойкость ключа шифрования во время установления соединения. Заставляя НКИ использовать ключи минимальной длины, злоумышленники обеспечивают возможность расшифровки всех передаваемых нейронных данных и управляющих сигналов методом «человек посередине».

BLESA (Bluetooth Low Energy Spoofing Attack) позволяет злоумышленникам подделывать легитимные периферийные устройства BLE, отправляя вредоносные сигналы или записывая нейронные реакции, выдавая себя за авторизованные устройства.

Replay-атаки передают кадры аутентификации для обхода требований сопряжения, предоставляя привилегированный доступ к командам управления без легитимной авторизации.

Атаки типа «человек посередине» (Man-in-the-Middle, MitM) перехватывают соединения между НКИ и системами обработки данных. Злоумышленники, находящиеся между устройствами, могут изменять нейронные данные в процессе передачи, вводить ложные команды или скрытно отслеживать всю передаваемую информацию. Атаки типа «человек посередине» особенно опасны для НКИ, передающих данные в реальном времени: при наличии специальной подготовки (наличие декодера, контекста задачи и основных меток распознавания) и необходимой инфраструктуры злоумышленники смогут угадывать общий смысл (на текущем уровне технологий с шансом 20-50%) мыслей и намерений в процессе их возникновения, а не просто получать доступ к архивным данным.[7]

Глушение сигнала представляет собой атаку типа «отказ в обслуживании», которая нарушает беспроводную связь посредством преднамеренного электромагнитного воздействия. Глушение может исказить потоки нейронных команд, передаваемых к протезам, вызывая хаотичные движения или полностью выводя

[7] Такой род атак доступен только хорошо организованным и финансово обеспеченным преступным группам, либо представителям спецслужб. Жертвами в таком случае выступают высокопоставленные лица, а исполнителями являются высококлассные профессионалы в разных дисциплинах.

устройства из строя. Глушение сигналов во время военных действий создает угрозу национальной безопасности, выводя из строя НКИ, используемые солдатами. При этом вражеская сторона может применять локальное глушение, чтобы лишить пользователей НКИ возможности совершать атаки или оказывать сопротивление.

6.2 Уязвимости программного обеспечения и прошивки

НКИ зависят от сложных программных стеков, обрабатывающих нейронные сигналы, реализующих алгоритмы управления и контроля исполнительных устройств. Данное программное обеспечение обычно содержит эксплуатируемые уязвимости, общие для всех вычислительных систем, но с гораздо более серьёзными последствиями при использовании прямых нейронных интерфейсов.

Атаки с переполнением буфера используют недостаточную проверку входных данных для записи данных за пределы выделенной памяти. В системах НКИ переполнение буфера может привести к сбою критически важной обработки сигналов, внедрению произвольного кода, изменяющего алгоритмы нейронного декодирования, или перезаписи проверок безопасности, предотвращающих несанкционированные команды.

Уязвимости повышения привилегий позволяют злоумышленникам получать несанкционированный доступ в операционных системах НКИ. Изначально получив ограниченный доступ, злоумышленники могут развить атаку и получить административный контроль, что позволит полностью захватить устройство, изменить параметры стимуляции или получить доступ к необработанным потокам нейронных данных, которые обычно защищены.

Манипуляция прошивкой представляет собой особенно серьёзную угрозу, поскольку прошивка работает на низком уровне с прямым управлением оборудованием. Скомпрометированная прошивка может постоянно манипулировать поведением устройства, несмотря на обновления программного обеспечения, создавать скрытые бэкдоры для долгосрочного несанкционированного доступа или отключать системы мониторинга безопасности, которые могли бы обнаруживать другие атаки.

Атаки на цепочки поставок создают уязвимости на этапах производства или распространения. Злоумышленники могут скомпрометировать компоненты НКИ до того, как они попадут к пользователям, внедряя бэкдоры или ослабляя защиту, которая выглядит легитимной, но позволяет эксплуатировать уязвимость в будущем. Сложность выявления факта компрометации цепочки поставок делает эти атаки чрезвычайно опасными.

6.3 Эксплуатация уязвимостей ИИ и машинного обучения

Современные НКИ все больше полагаются на искусственный интеллект и машинное обучение для декодирования нейронных сигналов, распознавания намерений и адаптивного управления. Эта интеграция создает новые категории уязвимостей, специфичных для ИИ.

При **атаках с использованием машинного обучения** генерируются входные данные, специально предназначенные для обмана классификаторов нейронных сигналов. Злоумышленники могут создавать стимулы или сигнальные возмущения, которые заставляют алгоритмы НКИ неправильно интерпретировать нейронные паттерны — например, расшифровывать команду "двигаться влево", когда пользователь

намеревался "двигаться вправо", или не обнаруживать предвестники судорог, которые должны вызвать защитную стимуляцию.

Отравление обучающих данных приводит к повреждению наборов данных, используемых для обучения алгоритмов НКИ. Вводя вредоносные примеры во время обучения, злоумышленники могут создавать скрытые триггеры или систематические ошибки. Зараженная модель может нормально работать в большинстве условий, но давать катастрофические сбои или вести себя злонамеренно при появлении заданных триггеров.

Атаки с использованием инверсии моделей восстанавливают частные обучающие данные из развернутых моделей искусственного интеллекта. Если системы НКИ используют модели машинного обучения, обученные на нейронных данных пользователей, инверсия моделей может позволить злоумышленникам восстанавливать конфиденциальную нейронную информацию из параметров самой модели, даже без прямого доступа к исходным данным.

Манипулирование поведением с помощью систем обучения ИИ создает риск незаметного влияния. Если в системах НКИ используется обучение с подкреплением или адаптивные алгоритмы, которые корректируются на основе ответов пользователя, злоумышленники могут использовать эти механизмы обучения для постепенного изменения поведения или предпочтений пользователя с помощью тщательно разработанных шаблонов обратной связи.

6.4 Атаки физического уровня

Помимо уязвимостей беспроводной связи и программного обеспечения, существуют также атаки физического уровня, нацеленные на аппаратные компоненты и факторы окружающей среды.

При взломе встроенного ПО с помощью физического доступа используются незащищенные порты или интерфейсы устройств. Злоумышленники, имеющие временный физический доступ, могут подключиться к оборудованию НКИ через USB[8], JTAG[9] или другие интерфейсы для установки вредоносного программного обеспечения, извлечения криптографических ключей или отключения функций безопасности. Сложность постоянного мониторинга имплантированных устройств делает физические атаки особенно опасными для инвазивных НКИ.

Разрядка аккумулятора и отказ в обслуживании из-за манипуляций с питанием могут привести к разрядке батарей имплантированного устройства, что приведет к отключению критически важных функций. Для НКИ, управляющих важными неврологическими функциями, разрядка аккумулятора представляет непосредственную опасность, требующую неотложного медицинского вмешательства.

Для **создания электромагнитных помех** используются встроенные усилители ЭЭГ, действующие как непреднамеренные антенны. Исследования показали, что радиосигналы на определенных частотах могут вводить поддельные мозговые волны в ЭЭГ-системы, что потенциально может привести к тому, что

[8] Universal Serial Bus (Универсальная последовательная шина)

[9] Joint Test Action Group (Комбинированная тестовая контактная группа)

коммуникаторы будут выводить неверный текст, вызывать сбои в работе мысленно управляемых приборов или искажать информацию о когнитивных состояниях.

Атаки по сторонним каналам используют электромагнитные или акустические излучения от устройств НКИ для определения нейронной активности без прямого доступа к устройству. Измеряя колебания энергопотребления, электромагнитное излучение или акустический шум, связанные с нейронной обработкой, опытные злоумышленники могут, без повреждения самого устройства, получать конфиденциальную информацию об активности мозга, находясь в непосредственной близости от пациента.

6.5 Атаки на основе получения и передачи сигнала

Уровень сбора сигналов, где электроды взаимодействуют с нервной тканью, создаёт фундаментальные уязвимости.

Прослушивание (brain tapping) перехватывает нейронные сигналы во время беспроводной передачи. Даже зашифрованные передачи могут раскрывать метаданные о схемах коммуникации, времени передачи или объёмах данных, которые дают представление о действиях и психическом состоянии пользователя.

Злонамеренная фильтрация и атаки с использованием бэкдоров внедряют вредоносную обработку сигналов во время сбора или предварительной обработки данных. Злоумышленники могут использовать фильтры, которые создают универсальные схемы обхода или бэкдор-триггеры, что приводит к неправильной классификации нейронных сигналов, при этом вероятность успеха атаки в лабораторных экспериментальных демонстрациях превышает 90%[10].

Вредоносные стимулы сенсорного уровня представляют собой искусственно созданные визуальные или слуховые сигналы, предназначенные для искажения нейронного кодирования. Подсознательные стимулы ниже порога осознанного восприятия могут провоцировать потенциалы, связанные с событиями, что позволяет извлекать информацию или искажать память. Едва заметные изменения сенсорных сигналов снижают точность моторных НКИ моторных до случайного уровня, демонстрируя возможность атак посредством манипуляции окружающей средой, а не прямого взлома устройства.

При **атаках с использованием воспроизведения и спуфинга** злоумышленники сперва записывают легитимные последовательности нейронных команд, а затем воспроизводят их для запуска циклов стимуляции памяти или управления действиями без согласия пользователя. Похищая и ретранслируя подлинные нейронные паттерны, злоумышленники могут выдавать себя за пользователей или заставлять устройство выполнять действия, которые кажутся легитимными, но идут в разрез с намерениями пользователя.

Принципиальная цепочка развития атаки на НКИ представлена на Рисунке 4.

[10] Подробности исследования: При состязательной фильтрации в качестве ключа к бэкдору используется фильтр; при обработке небольших объемов обучающих данных создается бэкдор; отфильтрованные сигналы активируют бэкдор, что приводит к неправильной классификации

Рисунок 4 – Цепочка развития атаки на НКИ: от вектора внедрения к последствиям

7. Биосовместимость и долговременное влияние НКИ на здоровье

7.1 Реакция на инородное тело и нейровоспаление

Имплантированные электроды НКИ неизбежно вызывают физиологическую реакцию на инородное тело, поскольку иммунная система распознаёт искусственные материалы в мозговой ткани. Эта биологическая реакция запускает каскадные воспалительные процессы со значительными долгосрочными последствиями для психических функций и здоровья нервной системы.

Реакция на инородное тело начинается с нарушения гематоэнцефалического барьера во время хирургической имплантации, что позволяет воспалительным клеткам, переносимым кровью, проникнуть в мозговую ткань, чего в норме не происходит. Микроглия — резидентные иммунные клетки мозга — активируется при обнаружении инородного материала, выделяя провоспалительные цитокины, включая фактор некроза опухоли альфа, интерлейкин-1 бета и интерлейкин-6.

Астроциты реагируют на эти воспалительные сигналы реактивным астроглиозом, характеризующимся клеточной гипертрофией, пролиферацией и миграцией к месту имплантации. Активированные астроциты повышают экспрессию белков промежуточных филаментов и формируют плотную фиброзную ткань вокруг электрода — глиальный рубец. Этот процесс инкапсуляции, представляя собой защитную реакцию мозга, постепенно изолирует электроды от близлежащих нейронов.

Хроническое нейровоспаление сохраняется на протяжении всего срока службы имплантата, поддерживая повышенный уровень воспалительных медиаторов в окружающих тканях. Это продолжающееся воспаление вызывает вторичные повреждения за счёт продукции активных форм кислорода, нарушения нормальной нейронной сигнализации и прогрессирующей гибели нейронов вблизи имплантатов. Нейроны в воспалительном микроокружении испытывают хронический окислительный стресс, митохондриальную дисфункцию и активацию апоптотических путей, что приводит к постепенной гибели клеток.

7.2 Образование глиальных рубцов

Глиальный рубец представляет собой плотный барьер из реактивных астроцитов и отложенных белков внеклеточного матрикса, который формируется вокруг имплантированных электродов. Изначально выполняя защитные функции, изолируя потенциально опасные инородные тела, глиальное рубцевание приводит к значительным функциональным нарушениям.

Развивающийся рубец постепенно увеличивает расстояние между регистрирующими электродами и целевыми нейронами. По мере утолщения изолирующего барьера в течение недель или месяцев, импеданс электрода резко возрастает. Более высокий импеданс ухудшает качество сигнала, увеличивая тепловой шум, снижая соотношение сигнал/шум и ослабляя нейронные потенциалы до того, как они достигнут области регистрации.

Для стимулирующих электродов при глиальной инкапсуляции возникает потребность в более высокой интенсивности стимуляции для достижения терапевтического эффекта. Чем больше тока рассеивается через резистивную рубцовую ткань, тем меньше его достигает целевых нейронных популяций. Это прогрессирующее увеличение импеданса может в конечном итоге привести к нефункциональности устройств, требуя хирургической замены или перепозиционирования — вмешательства, сопряженного с определенными рисками и провоцирующего дополнительные воспалительные реакции. Глиальные рубцы[11] чаще всего распространяются на расстояние от 100 до 300 микрометров от поверхности имплантата, охватывая тысячи нейронов в пораженном объеме. В этой области нормальная нейронная архитектура нарушается реактивными астроцитарными отростками, отложением коллагена и других компонентов внеклеточного матрикса, а также физическим присутствием самого рубца. Нейронные связи внутри и вокруг рубцовой области нарушаются, что может привести к функциональным нарушениям, выходящим за рамки простого снижения качества записи.

Рисунок 5 иллюстрирует процессы нейровоспаления и рубцевания тканей.

[11] Типичный диапазон: 10-300 мкм в зависимости от размера электрода, материала и времени проведения
Конкретные измерения:

- Электроды диаметром 10 мкм: концы рубца на расстоянии ~100 мкм от имплантата
- Электроды диаметром 50 мкм: концы рубца на расстоянии ~300 мкм от имплантата
- Плотный астроцитарный рубец: инкапсуляция размером 10-20 мкм, с дальнейшим уменьшением
- Кремниевые стержни: потеря нейронов/глиоз увеличиваются более чем на 150 мкм за 28 дней.

Расстояние записи нейронов: для эффективной записи одним блоком нейроны должны находиться в пределах 50-100 мкм.

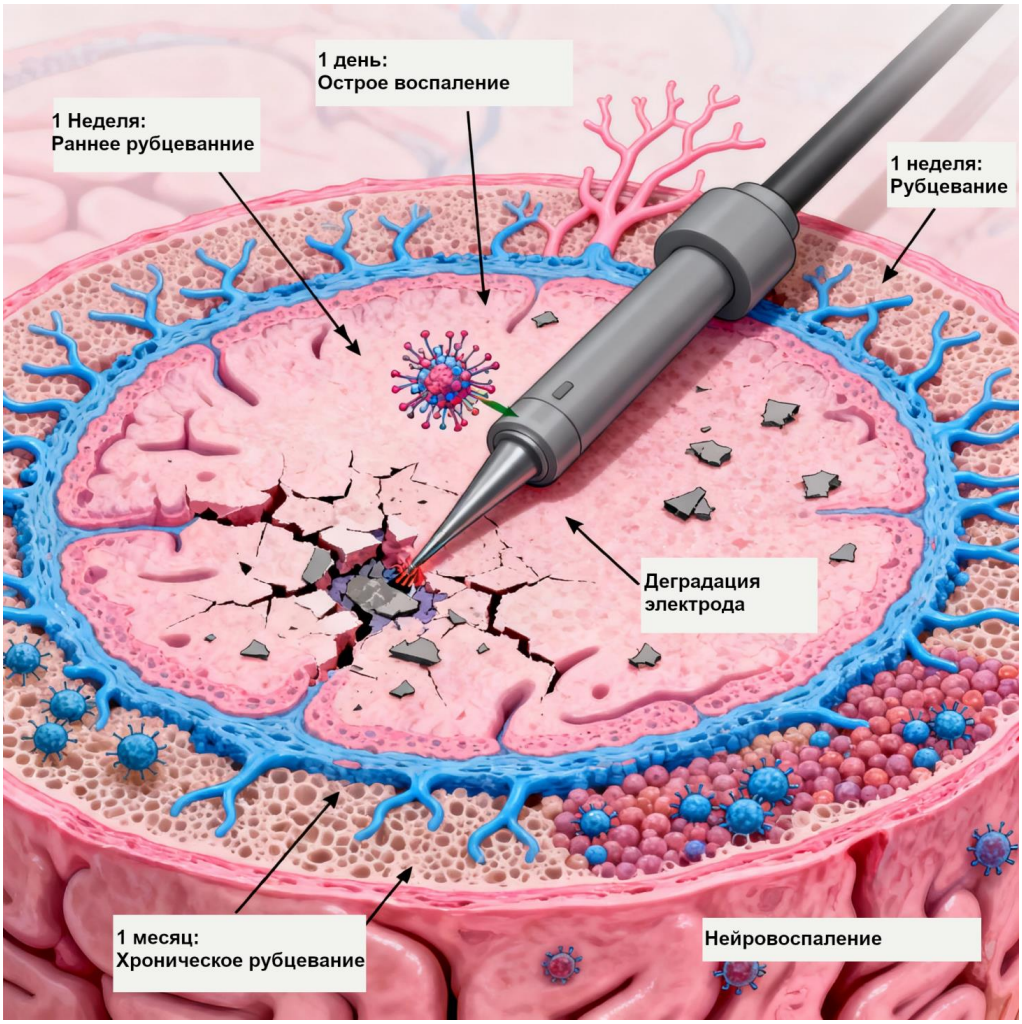

Рисунок 5 -Нейровоспаление и рубцевание тканей

7.3 Деградация нейронной ткани

Помимо немедленной воспалительной реакции, имплантация электродов на длительный срок вызывает прогрессирующую деградацию нервной ткани посредством множества механизмов.

Механические травмы от микродвижений имплантата вызывают постоянные повреждения нейронной ткани. Мозговая ткань постоянно движется под воздействием сосудистой пульсации, дыхания и движения головы. Жёсткие электроды, закреплённые на черепе, создают сдвигающие усилия на границе раздела ткань-электрод при каждом движении. Такие повторяющиеся механические воздействия вызывают постоянную низкоуровневую травму, поддерживая хроническое воспаление и препятствуя стабилизации тканей вокруг имплантатов.

Гибель нейронов происходит в областях, окружающих имплантированные электроды. Гистологические исследования демонстрируют прогрессирующую потерю нейронов, распространяющуюся на 50–100 микрометров от поверхности имплантатов в течение месяцев или лет. Эта гибель нейронов является результатом хронического воспаления, окислительного стресса, повреждения местной сосудистой сети и

механической травмы. Функциональные последствия включают потерю регистрируемых сигналов и сокращение популяции нейронов, доступных для терапии на основе стимуляции.

Нарушение функционирования сосудов во время имплантации и последующее воспаление нарушают местный кровоток. Мелкие сосуды могут быть повреждены непосредственно во время установки электрода, а хроническое воспаление вызывает эндотелиальную дисфункцию и снижение перфузии. Возникающая в результате гипоксия тканей усугубляет повреждение нейронов и нарушает нормальные процессы заживления.

Ухудшение качества сигнала является функциональным следствием этих биологических реакций. Амплитуда записи обычно прогрессивно снижается после имплантации, поскольку популяция нейронов в диапазоне регистрации уменьшается, а рубцевание глиальных клеток увеличивает импеданс. Многие хронически имплантированные электродные решетки демонстрируют снижение количества активных каналов на 50–80% в течение месяцев или лет, что существенно ограничивает долгосрочную функциональность[12]. На Рисунке 6 представлена диаграмма деградации качества сигнала за 12 месяцев.

Рисунок 6 - Деградация качества сигнала в имплантируемых НКИ: динамика за 12 месяцев

[12] Зарегистрированные диапазоны:

- 51% каналов, регистрирующих единичные имплантаты, через 16 недель (по сравнению с 92% на начальном этапе)
- Снижение амплитуды потенциала действия: в среднем на 2,4% в месяц (медленное, но значительное)
- Почти 50% регистрирующих имплантатов выходят из строя в течение 6 месяцев из-за образования глиальных рубцов
- Высокая вариабельность, при этом некоторые массивы сохраняют работоспособность, а другие демонстрируют быстрый упадок

7.4 Токсичность аккумуляторных батарей

Имплантируемые НКИ, требующие локального источника питания, несут риски, связанные с выходом из строя аккумулятора и утечкой электролита. Большинство имплантируемых устройств используют литий-ионные или литий-полимерные аккумуляторы из-за высокой плотности энергии в данных источниках питания. Однако, при повреждении аккумулятора в нервную ткань могут выделяться токсичные вещества.

Токсичный литий из протекающих аккумуляторов может вызывать серьёзные местные и системные эффекты. Соли лития, попадающие в мозговую ткань, оказывают непосредственное цитотоксическое действие, вызывая некроз и апоптоз клеток за счёт нарушения ионного гомеостаза и клеточных сигнальных путей. Повышенный уровень активных форм кислорода создаёт окислительный стресс, повреждающий клеточные макромолекулы. В нервной ткани, подвергшейся воздействию вытекшего лития, может возникнуть колликвационный некроз, образующий полости, необратимо разрушающие нейронную архитектуру.

Воспалительные реакции на материалы аккумулятора усугубляют прямое токсическое воздействие лития. Иммунная система бурно реагирует на вытекшее содержимое аккумулятора, вызывая интенсивное воспаление, распространяющееся за пределы непосредственного места утечки. Это острое воспаление может привести к быстрому клиническому ухудшению состояния с судорогами, изменением сознания или очаговым неврологическим дефицитом в зависимости от поражённого участка мозга. Электрохимические реакции на границе аккумулятора и тканей, даже без значительной утечки, могут генерировать вредные побочные продукты. Коррозия корпусов аккумуляторов приводит к высвобождению ионов металлов, которые могут быть нейротоксичными. Газообразование в неисправных аккумуляторах создаёт эффект давления, который вызывает сжатие или смещение тканей.

7.5 Нарушения нейропластичности

Длительное использование НКИ может нарушить нормальные механизмы нейронной пластичности, посредством которых мозг адаптируется и обучается. Искусственные паттерны стимуляции и хроническая запись с имплантированных электродов могут потенциально нарушить естественные адаптивные процессы.

Дезадаптивная пластичность может быть результатом неадекватных паттернов стимуляции. Хотя терапевтическая стимуляция с помощью НКИ направлена на восстановление функциональности, долговременная электрическая активность, индуцированная внешними источниками, отличается от естественной нейронной динамики. Механизмы пластичности мозга могут адаптироваться к этим искусственным паттернам таким образом, который ухудшит, а не улучшит функциональность. В том числе, долговременная стимуляция может усиливать дезадаптивные нейронные пути или препятствовать эффективной работе естественных механизмов восстановления.

Вмешательство в обучение и консолидацию памяти представляет собой теоретическую проблему для НКИ, имплантированных в структуры мозга, связанные с памятью, или вблизи них. Формирование естественной памяти требует определённых паттернов нейронной активности во время кодирования и консолидации. Постоянная запись или стимуляция данных областей через НКИ может потенциально нарушить тонкие

процессы памяти, затрудняя формирование новых воспоминаний или консолидацию недавнего опыта в долговременную память.

В нейронных цепях, получающих длительное время информацию от НКИ, может развиться зависимость от искусственной стимуляции. Если терапевтическая стимуляция становится основным фактором активности нейронных цепей, эндогенная активность может подавляться. Это может привести к ситуациям, когда естественные функции не смогут восстановиться даже после удаления или отключения имплантатов, поскольку нейронные цепи адаптировались к внешней стимуляции.

7.6 Прогрессирующая нейродегенерация

Хотя прямых доказательств пока мало, существуют теоретические опасения относительно возможных прогрессирующих нейродегенеративных изменений вследствие долговременной имплантации НКИ.

Эксайтотоксичность вследствие чрезмерной стимуляции представляет собой такой потенциальный механизм. Чрезмерная стимуляция, будь то из-за неисправности устройства или вредоносной атаки, может вызвать чрезмерное высвобождение глутамата и приток ионов кальция, запуская каскады эксайтотоксичности, приводящие к гибели нейронов. Повторные эпизоды чрезмерной стимуляции могут вызывать кумулятивное повреждение нейронов.

Хроническое воспаление, связанное с имплантатами, создает среду, благоприятную для нейродегенерации. Повышенный уровень воспалительных медиаторов, окислительный стресс и нарушение сигнализации нейротрофических факторов в периимплантной среде имеют сходство с состояниями, наблюдаемыми при нейродегенеративных заболеваниях. Хотя прямая причинно-следственная связь не доказана, хроническое воспалительное состояние может повышать уязвимость к возрастной нейродегенерации.

Агрегация белков и клеточный стресс вследствие долговременного присутствия устройства теоретически могут способствовать нейродегенеративным процессам. Некоторые исследования показывают, что хроническое воспаление и окислительный стресс способствуют неправильному сворачиванию и агрегации белков, участвующих в нейродегенерации, хотя остается неясным, достигает ли воспаление, связанное с НКИ, пороговых значений, необходимых для возникновения таких эффектов.

Долгосрочные неврологические последствия имплантации НКИ, продолжающейся десятилетиями, остаются в значительной степени неизвестными, поскольку большинство пациентов с имплантированными НКИ наблюдались всего несколько лет. По мере того, как НКИ становятся все более распространенными и остаются имплантированными в течение более длительного времени, тщательное наблюдение за признаками прогрессирующих неврологических изменений будет иметь решающее значение для понимания долгосрочных профилей безопасности.

8. Психиатрические и неврологические расстройства, возникающие из-за компрометации НКИ

8.1 Тревожные расстройства и паранойя

Психологическое воздействие уязвимости НКИ выходит за рамки физических рисков и включает серьёзные психиатрические последствия. Даже без фактической угрозы, осознание потенциальной уязвимости может спровоцировать серьёзные тревожные расстройства.

Технологическая тревожность проявляется как хроническое беспокойство о потенциальной угрозе взлома, слежке или манипуляциях с устройством. У пользователей НКИ могут развиться стойкие опасения, что к их мыслям получают доступ, их эмоциями манипулируют, а их поведение контролируют. Такая повышенная бдительность в отношении мыслительных процессов создаёт изнуряющую когнитивную нагрузку и хронический стресс, несовместимый с нормальным функционированием.

Параноидальное мышление может развиваться в результате того, что пользователи становятся всё более подозрительными к необъяснимым мыслям, эмоциям или импульсам. Знание о технической возможности внешнего манипулирования создаёт основу для приписывания внутренних переживаний внешним причинам. Пользователи могут начать сомневаться в том, являются ли определённые мысли действительно их собственными или потенциально имплантированными, отражают ли внезапные перепады настроения аутентичные реакции или манипуляции, и являются ли их предпочтения и решения действительно автономными.

Исследования, документирующие симптомы тревоги после взлома НКИ, показывают, что эти психиатрические последствия не являются просто теоретическими. Пользователи, которые подозревают взлом устройства, или подвергаются ему, демонстрируют повышенный уровень тревожности, нарушения сна, социальную изоляцию и другие нарушения функционирования. Невидимость нейронных манипуляций — отсутствие физических доказательств или внешнего подтверждения — усугубляет тревогу, создавая неопределённость, которую невозможно разрешить окончательно.

8.2 Депрессия и расстройства настроения

Нарушение работы НКИ может спровоцировать или усугубить депрессивные эпизоды различными путями. Наиболее очевидным механизмом является прямое воздействие на нейронные цепи, участвующие в регуляции настроения, но вторичные психологические воздействия оказываются не менее значимыми.

Ятрогенная депрессия может быть результатом воздействия на структуры лимбической системы и области префронтальной коры, участвующие в регуляции эмоций. Глубокая стимуляция мозга, направленная на эти области, может быстро вызывать глубокие депрессивные состояния при неправильной настройке параметров стимуляции. Систематические обзоры показывают, что депрессия возникает у 42% пациентов после определенных процедур нейростимуляции, причем в некоторых случаях улучшение не наблюдается даже после прекращения стимуляции.

Реактивная депрессия развивается вторично по отношению к самому опыту нарушения. Потеря автономии, нарушение психической конфиденциальности и подрыв доверия к собственным психическим процессам

приводят к серьезному психологическому стрессу. Беспомощность, испытываемая пользователями, которые не могут предотвратить внешний доступ к своим мыслям или контролировать свое нейронное состояние, отражает модель выученной беспомощности при депрессии. У пользователей может развиться чувство безнадежности относительно своей способности сохранять психическую целостность, ангедония в отношении ранее значимой деятельности и глубокая деморализация из-за утраты когнитивного суверенитета.

Суицидальные мысли представляют собой особенно тревожное последствие. Исследования документируют повышенный риск самоубийства после некоторых процедур нейростимуляции, обусловленный как прямым воздействием на нейроны, так и психологическими реакциями на осложнения, связанные с устройством. Сочетание искусственно вызванной депрессии, потери автономии и нарушения психологической целостности создает обстоятельства, при которых смерть может казаться предпочтительнее дальнейшего существования в состоянии нарушенного психического суверенитета.

8.3 Психотические эпизоды

Многочисленные исследования случаев документируют возникновение психотических симптомов после имплантации НКИ или изменения параметров, что позволяет предположить, что манипуляции с нейронами могут спровоцировать выраженный психоз у лиц с повышенной предрасположенностью к нему.

Психоз, вызванный стимуляцией, был зарегистрирован в случаях, когда у пациентов развивались ярко выраженные психотические симптомы через несколько недель после имплантации электродов, даже до активации стимулятора. Эти психозы проявлялись параноидным и величавым бредом, галлюцинациями, дезорганизованным мышлением и странным поведением, требующим психиатрической госпитализации и антипсихотической терапии. Близость времени между имплантацией и началом психоза предполагает наличие причинно-следственных связей, хотя основные механизмы остаются до конца не изученными.

Параноидный бред представляет собой особенно распространенный психотический симптом. У пациентов может развиться убеждение, что членов семьи заменили самозванцы (бред Капгра), что за ними следят или их контролируют внешние силы, либо что устройство транслирует их мысли другим людям. Тот факт, что бредовые идеи часто фокусируются именно на устройстве НКИ, позволяет предположить, что само наличие устройства обеспечивает когнитивную основу, на которой строится психотическая интерпретация.

Уязвимость некоторых нейронных субстратов к психотическим нарушениям может объяснить эти явления. При психотических расстройствах наблюдаются нарушения в нейронных цепях, включающих дофаминовую сигнализацию, префронтально-лимбические связи и процессы мониторинга реальности. Электрическая стимуляция, нарушающая работу этих систем, может потенциально спровоцировать психотические состояния, особенно у лиц с генетической или приобретенной предрасположенностью к психозу, в т. ч. при некоторых нарушениях развития.

8.4 Диссоциативные расстройства и деперсонализация

Нейронные манипуляции посредством скомпрометированных НКИ могут вызывать диссоциативные симптомы, индуцируя несоответствие между переживаемыми психическими состояниями и реальной нейронной активностью.

Симптомы деперсонализации/дереализации проявляются в виде чувства нереальности происходящего, отчуждения от себя или восприятия окружающего мира словно далёкого или снящегося. Когда НКИ создают конфликты между намерениями пользователя и его реальным поведением, либо между подлинными эмоциями и искусственно вызванными чувствами, это может спровоцировать глубокую деперсонализацию. При этом пользователи описывают чувство оторванности от своих мыслей и действий, наблюдение за собой со стороны или эмоциональное оцепенение, когда чувства кажутся приглушёнными или нереальными.

Изменение идентичности и симптомы диссоциативной идентичности были зарегистрированы в случаях, когда нейростимуляция вызывала драматические изменения личности. Исследование одного из пациентов с синдромом Туретта показало возникновение различных состояний идентичности, связанных с различными параметрами стимуляции, с очевидной амнезией на эпизоды, происходящие в альтернативном состоянии. Нарушение нормального чувства субъектности и принадлежности к себе, по-видимому, является центральным в этих диссоциативных симптомах. Нейробиологические исследования показывают, что мозг непрерывно отслеживает субъектность, отличая действия, совершаемые самостоятельно, от событий, вызванных извне. Когда нарушение работы НКИ приводит к действиям или мыслям без соответствующего ощущения волевого участия, мозг может интерпретировать это несоответствие как указание на то, что переживания не являются истинной частью «я». При этом диссоциативные симптомы выполняют роль защитной реакции психики.

8.5 Посттравматическое стрессовое расстройство

Опыт нейронного насилия путем нарушения работы НКИ может представлять собой психологическую травму, провоцирующую симптомы ПТСР.

Навязчивые симптомы включают непроизвольные, тревожные воспоминания о пережитом насилии, кошмары о потере контроля или нарушениях психики, а также флешбэки, в которых вновь переживаются ужас и беспомощность. Пользователи могут сообщать о невозможности перестать думать о нарушении своей психической конфиденциальности или о потере контроля над собственными нейронными процессами.

Симптомы избегания проявляются в нежелании использовать НКИ даже при наличии медицинской необходимости, избегании мыслей или разговоров о насилии, а также в отказе от деятельности или отношений, связанных с травмирующим опытом. Некоторые пользователи могут попросить удалить устройство, несмотря на медицинскую необходимость. Для таких пациентов лишение преимуществ от использования НКИ выглядит предпочтительнее, чем возможность остаться уязвимыми перед будущими атаками.

Негативные изменения в когнитивных функциях и настроении могут включать стойкие негативные убеждения в отношении себя («Я никогда не смогу быть в безопасности», «У меня нет контроля»), искажённое чувство вины за себя или других из-за опыта насилия, стойкие негативные эмоциональные состояния и заметное снижение интереса к ранее значимым занятиям. Нарушение психической целостности может коренным образом изменить мировоззрение и чувство безопасности пользователей, характерные для реакций на травму.

Симптомы гипервозбуждения проявляются в виде повышенной бдительности к признакам неисправности или взлома устройства, преувеличенных реакций испуга, трудностей с концентрацией внимания и нарушений сна. Осознание того, что психические процессы могут быть доступны или подвергнуты манипуляциям в любой момент, создает хроническое состояние восприятия угрозы и физиологического возбуждения, несовместимое с нормальным функционированием.

8.6 Расстройства контроля импульсов

Исследования показывают, что манипуляции с НКИ могут вызывать или усугублять нарушения контроля импульсов посредством воздействия на определённые нейронные сети.

Глубокая стимуляция мозга, направленная на субталамическое ядро, может как защитить от нарушений контроля импульсов, так и вызвать их в зависимости от точных параметров стимуляции. Компрометация НКИ, позволяющая несанкционированное изменение параметров, может преднамеренно устранить защитные эффекты или спровоцировать аномальное импульсивное поведение.

Патологическая склонность к азартным играм, гиперсексуальность, компульсивный шопинг и переедание – всё это было задокументировано как осложнения нейростимуляции, затрагивающей контуры базальных ганглиев. Такие поведенческие нарушения возникают внезапно, часто совершенно нехарактерны для человека, и могут привести к серьёзным функциональным нарушениям и вреду, прежде чем будут распознаны как ятрогенные осложнения.

Манипуляция системой вознаграждения, осуществляемая скомпрометированным НКИ, создаёт потенциал для возникновения состояний, подобных зависимости. Стимуляция прилежащего ядра и связанных с ним структур вознаграждения может генерировать мощные сигналы подкрепления. Злоумышленники потенциально могут создавать искусственные компульсии, сочетая стимуляцию вознаграждения с определёнными мыслями или поведением, по сути «программируя» аддиктивные паттерны посредством нейронной манипуляции.

На Рисунке 7 представлена пирамида основных психиатрических последствий, наблюдаемых у пациентов при компрометации НКИ.

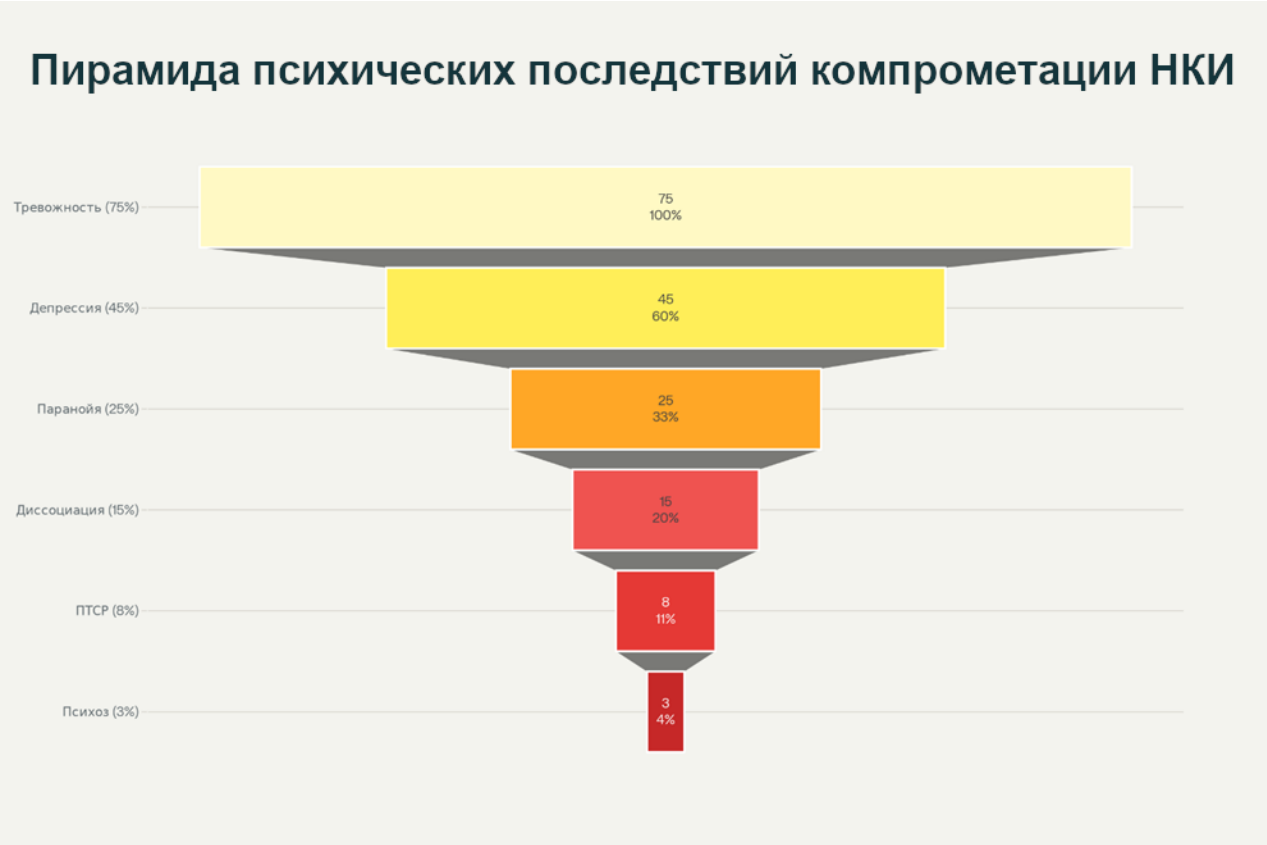

Рисунок 7 - Пирамида психиатрических последствий: психическое здоровье при компрометации НКИ

8.7 Когнитивные нарушения и расстройства памяти

Нарушение работы НКИ может существенно повлиять на формирование памяти и когнитивные функции из-за нарушения работы гиппокампальных и корковых сетей.

Антероградная амнезия — неспособность формировать новые воспоминания — может быть результатом нарушения функции гиппокампа во время активного кодирования памяти. Исследования показывают, что несанкционированное манипулирование нейронной стимуляцией может нарушить процессы консолидации, необходимые для перевода кратковременных воспоминаний в долговременную память.

Ретроградная амнезия — потеря ранее сформированных воспоминаний — может возникнуть, если устройство НКИ, воздействующее на нейронные сети памяти, неисправно или вредоносно запрограммировано на нарушение процессов извлечения. Хотя полное стирание консолидированных воспоминаний представляется затруднительным при использовании современных технологий, нарушение процессов извлечения может сделать воспоминания фактически недоступными.

Исполнительная дисфункция, затрагивающая планирование, принятие решений и когнитивную гибкость, может быть результатом нарушения работы префронтальной коры. У пользователей НКИ могут наблюдаться нарушения суждений, трудности с планированием многоэтапных задач, задержка на определённых идеях или поведении, а также снижение когнитивной гибкости, что затрудняет адаптацию к изменяющимся обстоятельствам.

Спутанность сознания и дезориентация представляют собой острые когнитивные симптомы, зарегистрированные в случаях неисправности или повреждения НКИ. Пользователи могут терять ориентацию во времени и пространстве, ощущении собственной личности, проявлять глубокую дезориентацию относительно обстоятельств собственного состояния. Все это приводит к нарушению способности обрабатывать информацию или принимать решения.

8.8 Судороги и эпилептические приступы

При **неправильной электростимуляции** возникает значительный риск судорог, особенно для пациентов, чьи НКИ предназначены для предотвращения эпилептических судорог.

Судороги, вызванные стимуляцией, могут возникать, когда некорректно работающие НКИ оказывают чрезмерную стимуляцию или стимулируют на частотах, известных как эпилептогенные. Быстрая высокочастотная стимуляция может спровоцировать синхронные паттерны биоэлектрической активности нейронов, характерные для судорог. В результате, это может привести к судорогам, потере сознания или другим эпилептическим симптомам.

У пациентов, использующих адаптивную нейростимуляцию для лечения эпилепсии, сбой в работе НКИ становится особенно опасным. При штатной работе эти системы обнаруживают предвестники судорог и осуществляют контрстимуляцию, чтобы предотвратить развивающиеся приступы. Злонамеренные манипуляции могут нарушить защитные функции, позволяя судорогам развиваться без противодействия, или даже спровоцировать судороги посредством неправильной стимуляции.

Эпилептический статус — длительные судороги продолжительностью более пяти минут или повторяющиеся судороги без восстановления между эпизодами — представляет собой неотложное состояние, сопряженное с риском необратимого повреждения головного мозга или смерти. Неисправные НКИ, непрерывно осуществляющие эпилептогенную стимуляцию, потенциально могут спровоцировать эпилептический статус, требующий экстренного медицинского вмешательства для прекращения аномальной электрической активности.

8.9 Моторная дисфункция и двигательные расстройства

Манипулирование нейронными сигналами может привести к серьёзным последствиям для двигательной активности, варьирующимся от временных нарушений до стойких двигательных расстройств.

Паралич или двигательное замирание могут быть результатом стимуляции, нарушающей нормальную генерацию или выполнение двигательных команд. Пациенты, зависящие от НКИ для произвольных движений, полностью обездвиживаются при сбоях в работе систем или при их преднамеренной инвалидизации. Внезапное возвращение к двигательным нарушениям, существовавшим до лечения, представляет, как физическую опасность, так и глубокую психологическую травму.

Непроизвольные движения, включая тремор, дискинезии или хореиформные движения, могут быть вызваны неадекватной стимуляцией моторных цепей. Такие движения могут быть болезненными, нарушать функциональность и вызывать социальный дискомфорт. В тяжёлых случаях резкие непроизвольные движения могут привести к самоповреждению или помешать базовым действиям по уходу за собой.

Дистония — длительные мышечные сокращения, вызывающие аномальные позы, — может быть результатом стимуляции моторных цепей базальных ганглиев. Дистонические позы могут быть болезненными и инвалидизирующими, они могут сохраняться даже после прекращения стимуляции из-за изменений нейронной пластичности, вызванных неадекватными схемами стимуляции.

Исследования, посвященные глубокой стимуляции мозга, показывают, что даже незначительные изменения положения электродов или параметров стимуляции могут вызывать выраженные двигательные симптомы. Такая высокая чувствительность означает, что даже незначительных злонамеренных манипуляций параметрами стимуляции достаточно для того, чтобы вызвать существенную двигательную дисфункцию. Также это делает подобные атаки технически осуществимыми даже без детального знания индивидуальных особенностей пациента.

Сводная пирамида психических последствий атак на НКИ представлена на Рисунке 7.

9. Правовые и нормативные проблемы

9.1 Несовершенство нормативно-правовой базы

Действующие правила в отношении медицинских устройств и законы о защите данных не учитывают уникальные характеристики нейронных данных и НКИ. Это создает существенные пробелы в регулировании, которые не обеспечивают адекватной защиты пользователей.

Правила в отношении медицинских устройств ориентированы в первую очередь на физическую безопасность и эффективность. Несмотря на разработку руководств по кибербезопасности, они остается неадекватным для угроз, специфичных для НКИ. В правилах не рассматриваются вопросы конфиденциальности нейронных данных, когнитивной свободы или психологической автономии. В процессах сертификации отсутствуют стандартизированные требования к тестированию на проникновение, оценке уязвимостей или долгосрочному обеспечению безопасности, характерные для нейротехнологий.

Законы о защите данных, например, ФЗ-152, предусматривают рамочные основы защиты ПДн, но не учитывают особую конфиденциальность нейронных данных. Хотя биометрические данные получают особую категорию защиты в соответствии с законодательством, нейронные данные часто не классифицируются как биометрическая информация в нормативных актах. Прямой доступ к мыслям, эмоциям и намерениям, обеспечиваемый нейронными данными, превосходит чувствительность традиционных биометрических идентификаторов, таких как отпечатки пальцев или распознавание лиц, но при этом не обеспечивается усиленной защитой.

Законодательство о нейроправах находится на ранней стадии разработки. Чили стала первой страной, конституционно защищающей нейроправа в 2021 году, и несколько других юрисдикций предложили законопроекты, признающие когнитивную свободу и психическую конфиденциальность основополагающими правами. Однако комплексная правовая база, реализующая эти принципы, остаётся недостаточно развитой. В отсутствие чётких законодательных требований разработчики НКИ сталкиваются с минимальными обязательствами по обеспечению нейробезопасности.

9.2 Международные юрисдикционные проблемы

Глобальный характер разработки и внедрения НКИ создает сложные юрисдикционные проблемы для защиты конфиденциальности нейронных сетей и преследования правонарушителей.

Регулятивный арбитраж позволяет компаниям переносить свою деятельность в юрисдикции с более слабой защитой. Нейронные данные, собранные в одной стране, могут обрабатываться или храниться в другой с минимальными гарантиями конфиденциальности. Отсутствие международной гармонизации приводит к тому, что компании, стремящиеся к максимизации прибыли, могут избежать жестких требований к безопасности или конфиденциальности, выбирая стратегические юрисдикции.

Трансграничные потоки нейронных данных поднимают вопросы о применимой правовой базе. Если пользователь из России использует НКИ, произведенные в Азии, а данные обрабатываются на серверах в Северной Америке, законы какой юрисдикции применяются? Действующие международные системы защиты данных оказываются недостаточными для решения проблем, связанных с особой конфиденциальностью и мобильностью нейронных данных.

Проблемы расследования и судебного преследования возникают, когда к компрометации НКИ причастны преступники из юрисдикций, отличных от юрисдикций жертв. Расследование нейропреступлений требует специализированных знаний, которых в настоящее время не хватает большинству правоохранительных органов. Механизмы международного сотрудничества для расследования случаев утечки нейронных данных или «мозгового взлома» практически отсутствуют.

9.3 Риски и ответственность для бизнеса

Коммерческая разработка потребительских НКИ технологическими компаниями, работающими с целью получения прибыли, поднимает важные вопросы об ответственности.

Ограниченная ответственность часто защищает производителей от последствий нарушений кибербезопасности. В случаях, когда взломы НКИ приводят к психологическому вреду, когнитивным манипуляциям или утечкам нейронных данных, действующее законодательство предоставляет пострадавшим пользователям лишь ограниченные средства правовой защиты. Доказательство причинно-следственной связи между уязвимостями устройств и психологическим вредом представляет собой существенную проблему, а возмещения ущерба редко отражают глубину нарушений психической целостности.

Неадекватные требования безопасности к потребительским НКИ создают опасную асимметрию. В то время как медицинские НКИ находятся под контролем регуляторов, потребительские устройства, предназначенные для оздоровления, игр или работы, часто полностью избегают контроля со стороны административных органов. Эти продукты могут реализовывать минимальные меры безопасности, собирая при этом крайне чувствительные нейронные данные, что создает значительные риски для конфиденциальности и безопасности.

Практики монетизации данных, применяемые производителями НКИ, вызывают этические вопросы, связанные с согласием и коммерциализацией сознания. Пользовательские соглашения потребительских НКИ

часто предоставляют компаниям широкие лицензии на использование, анализ и монетизацию нейронных данных. Пользователи могут не осознавать, что они дают разрешение на когнитивное профилирование, целевое манипулирование или продажу нейронной информации третьим лицам, включая рекламодателей, брокеров данных или нераскрытые организации.

Глава 2. Стратегии митигации, рекомендации и лучшие практики

10. Стратегии митигации — технические подходы

10.1 Интегрированная безопасность (Security-by-Design)

Эффективная безопасность НКИ требует внедрения защитных механизмов на протяжении всего цикла проектирования, производства и эксплуатации, а не использования наложенных мер безопасности, добавляемых в последнюю очередь. Концепция безопасности, заложенная в проект, требует оценки каждого компонента и функции на предмет потенциальных уязвимостей уже на начальном этапе разработки.

Моделирование угроз на ранних этапах проектирования выявляет потенциальные векторы атак и возможности злоумышленников. Разработчики должны систематически учитывать, как каждый компонент системы может быть скомпрометирован и к каким последствиям это может привести. Такой перспективный анализ безопасности позволяет архитектурно интегрировать защитные меры, а не добавлять их поверх готового решения.

Принцип наименьших привилегий ограничивает каждый компонент системы минимальными правами доступа, необходимыми для его функционирования. Приложения для работы с НКИ должны получать доступ только к определенным типам нейронных данных, которые им необходимы — приложению для мониторинга фокуса требуются метрики внимания, но не сырые потоки ЭЭГ или информация об эмоциональном состоянии. Ограничение доступа к данным снижает последствия компрометации на уровне приложений.

Глубоко эшелонированная защита реализует несколько перекрывающихся уровней безопасности, чтобы компрометация любого отдельного уровня защиты не привела к полной компрометации системы. Системы НКИ должны сочетать физическую безопасность, криптографическую защиту, механизмы аутентификации, обнаружение вторжений и безопасные процессы обновления. Такой многоуровневый подход гарантирует, что потенциальным злоумышленникам придется преодолеть несколько независимых барьеров, что значительно снижает риски безопасности. Пример организации такой защиты представлен на Рисунке 8.

Рисунок 8 - Архитектура безопасности НКИ: уровни эшелонированной защиты

10.2 Продвинутая криптография и шифрование

Вся передача нейронных данных должна осуществляться с использованием надежного шифрования, предотвращающего перехват и расшифровку неавторизованными лицами.

Сквозное шифрование защищает данные на протяжении всего их жизненного цикла — от нейронных датчиков до систем обработки и хранения данных. Передача любых нейронных данных должна шифроваться алгоритмами не хуже ГОСТ Р 34.12-2015 или AES-256. При этом ключи шифрования должны быть доступны только авторизованным конечным точкам. Это позволит предотвратить раскрытие содержимого нейронных данных атаками типа «человек посередине» даже в случае их перехвата на уровне канала связи.

Гомоморфное шифрование позволяет выполнять вычисления с зашифрованными данными без расшифровки, решая проблему того, что традиционное шифрование препятствует обработке. Гомоморфные схемы позволяют проводить анализ нейронных сигналов и машинное обучение на основе зашифрованных нейронных данных, обеспечивая облачную обработку без раскрытия конфиденциальной информации поставщикам услуг.

Постквантовая криптография позволит обеспечить защиту от будущих угроз со стороны квантовых компьютеров, способных взламывать существующие шифры. Системы НКИ, предназначенные для долговременной имплантации, должны использовать криптографические алгоритмы, устойчивые к

квантовым атакам, продолжая обеспечивать защиту нейронных данных даже по мере развития роста вычислительных мощностей.

Управление ключами для долговременных имплантированных устройств представляет собой особую задачу. Криптографические ключи должны надежно храниться на устройствах с помощью аппаратных модулей безопасности, периодически меняться для ограничения риска потенциальной компрометации и надежно резервироваться для предотвращения потери данных в случае повреждения ключей. Баланс между безопасностью и возможностью восстановления требует тщательной разработки соответствующего протокола.

10.3 Строгая аутентификация и авторизация

Для предотвращения несанкционированного доступа к системам НКИ требуется надежная аутентификация, гарантирующая, что только легитимные пользователи и приложения смогут взаимодействовать с нейронными интерфейсами.

Многофакторная аутентификация сочетает в себе несколько независимых методов проверки: пароли или PIN-коды, биометрические идентификаторы и наличие физических токенов или устройств. Для доступа к НКИ нейронные сигнатуры сами по себе могут служить факторами аутентификации, а характерные паттерны мозговой активности – подтверждать личность пользователя.

Непрерывная аутентификация отслеживает текущие поведенческие и физиологические модели для выявления взлома учетной записи или несанкционированного доступа. Вместо однократной аутентификации в начале сеанса, непрерывный мониторинг гарантирует, что легитимные пользователи сохраняют контроль на протяжении всего взаимодействия. Нейронные паттерны, ритм набора текста или шаблоны взаимодействия могут обеспечить непрерывную верификацию без явного вмешательства пользователя.

Ролевая модель доступа ограничивает возможности различных типов пользователей в системах НКИ. Пациенты должны контролировать собственные нейронные данные и настройки стимуляции, но медицинскому персоналу может потребоваться ограниченный доступ для корректировки настроек и устранения неполадок. Строгое определение ролей с протоколированием всех привилегированных действий обеспечивает подотчетность и ограничивает ущерб от компрометации учетных данных.

Аппаратная аутентификация с использованием защищенных элементов или доверенных сред выполнения обеспечивает аутентификацию, устойчивую к взлому программного обеспечения. Криптографические ключи, хранящиеся в защищенном оборудовании, не могут быть извлечены вредоносным ПО, а операции аутентификации, выполняемые в изолированных безопасных средах, остаются защищенными даже при взломе основных операционных систем.

10.4 Машинное обучение с сохранением приватности

Обеспечение конфиденциальности нейронных данных требует методов, которые сохраняют их полезность для законных целей, предотвращая при этом идентификацию человека или извлечение конфиденциальной информации.

Дифференциальная конфиденциальность добавляет тщательно калиброванный статистический шум к результатам запросов или наборам данных, математически гарантируя, что присутствие или отсутствие какого-либо человека не может быть определено по выходным данным. Применительно к нейронным данным дифференциальная конфиденциальность позволяет проводить агрегированный анализ — изучать закономерности на уровне популяции — без раскрытия конфиденциальной информации отдельных пользователей.

К-анонимность и обобщение данных гарантируют, что опубликованные нейронные наборы данных не могут быть связаны с конкретными людьми путем подавления или обобщения квазиидентифицирующей информации. Например, точное расположение электродов может быть обобщено по областям мозга, а точная информация о времени может быть сгруппирована в достаточно широкие промежутки для предотвращения детальной реконструкции.

Федеративное обучение позволяет обучать модели ИИ на распределенных нейронных данных без централизации конфиденциальной информации. Каждое пользовательское устройство обучает локальные модели на своих собственных нейронных данных. При этом для агрегации передаются только параметры модели, а не сырые данные. Это позволяет совершенствовать НКИ посредством коллективного обучения, сохраняя при этом конфиденциальность отдельных пользователей.

Безопасное агрегирование позволяют совместно анализировать нейронные данные из нескольких источников, без доступа какой-либо стороны к исходным данным других участников. Протоколы шифрования позволяют вычислять агрегированную статистику или обучать модели на комбинированных наборах данных, сохраняя при этом гарантии конфиденциальности каждого участника.

Локальные вычисления позволяют обрабатывать мозговые сигналы на самих НКИ, не передавая их в облачные сервисы. Современные ускорители нейронных сетей позволяют запускать сложные ИИ-модели на встроенном оборудовании, устраняя необходимость предоставления необработанных нейронных данных внешним системам.

10.5 Безопасные механизмы обновления

Системы НКИ требуют обновлений программного и микропрограммного обеспечения для устранения уязвимостей и улучшения функциональности. При этом сами механизмы обновления представляют векторы атак, требующие защиты.

Криптографически подписанные обновления гарантируют подлинность и целостность. Цифровые подписи, проверенные с помощью открытых ключей производителя, подтверждают, что обновления получены из легитимных источников и не были изменены во время распространения. Перед установкой должна выполняться проверка подписи, предотвращая принятие вредоносной прошивки.

Защита от отката предотвращает установку злоумышленниками более старых версий прошивки, содержащих известные уязвимости. Проверка версий гарантирует возможность установки только более новых, предположительно более безопасных обновлений. Это предотвращает атаки понижения версии, когда злоумышленники заставляют устройства принимать устаревшее уязвимое программное обеспечение. При

этом крайне важно обеспечить высочайший уровень тестирования и контроля корректности установки, т.к. выход из строя НКИ в результате ошибки при обновлении может угрожать здоровью пользователя.

Поэтапное развертывание сначала применяет обновления к небольшой группе пользователей, отслеживая проблемы перед широким распространением. Это ограничивает ущерб от некорректных обновлений и дает возможность обнаружить вредоносные обновления, которые не прошли предварительную проверку безопасности.

Уведомление пользователя и его согласие на обновления, влияющие на нейронную стимуляцию или сбор данных, обеспечивают осознанность выбора. Хотя исправления безопасности могут потребовать принудительного развертывания, изменения функциональности должны требовать одобрения пользователя. Возможности экстренной перепрошивки могут позволить быстро внедрять критически важные исправления безопасности при необходимости. При этом, организация доступа к механизму экстренной перепрошивки должна быть устроена таким образом, чтобы минимизировать риск его несанкционированной активации.

10.6 Аппаратная безопасность

Физические меры безопасности защищают устройства НКИ от несанкционированного доступа к аппаратной части и ключам шифрования.

Использование в НКИ **аппаратного корня доверия** (Hardware Root of Trust, HRoT) обеспечивает безопасную среду функционирования устройства, изолированную от потенциально скомпрометированных программных компонентов. Защищенные элементы, встраиваемые в НКИ, позволят безопасно хранить криптографические ключи, выполнять конфиденциальные вычисления и проверять целостность программного обеспечения с помощью аппаратных средств защиты, устойчивых к программным атакам.

Корпуса с защитой от несанкционированного доступа позволяют обнаружить попытки физического проникновения. Пломбы, специальные покрытия или встроенные датчики обнаруживают вскрытие корпуса устройства, запуская ответные меры безопасности, такие как стирание ключа или регистрация события. Хотя защита от несанкционированного доступа не предотвращает физические атаки, она обеспечивает обнаружение и адекватное реагирование.

Электромагнитное экранирование защищает от атак по сторонним каналам и инжекции сигналов. Металлические корпуса и фильтрация вокруг усилителей и электродов блокируют инжекцию электромагнитных волн, которая может создавать ложные нейронные сигналы или позволять прослушивание посредством анализа излучений.

Механизм безопасной загрузки проверяет целостность прошивки перед запуском, гарантируя, что на устройствах запускается только авторизованное программное обеспечение. Криптографические проверки перед загрузкой подтверждают, что подписи прошивки соответствуют ключам производителя, предотвращая выполнение вредоносного кода, даже если злоумышленники получат физический доступ для перепрограммирования устройств.

10.7 Сетевая безопасность и сегментация

Системы, работающие с НКИ должны быть изолированы от сетей общего доступа, чтобы уменьшить риски интернет-атак.

Реализации **систем с воздушным зазором** обеспечивают полную изоляцию НКИ от внешних сетей, за исключением явных, ограниченных по времени подключений для обновления или мониторинга. Это значительно сокращает поверхность атаки, т.к. у злоумышленников пропадает постоянный доступ к устройству через публичные сети.

Сегментация сети подразумевает размещение систем для работы с НКИ в выделенных подсетях, изолированных от общей ИТ-инфраструктуры. Даже в медицинских учреждениях или научно-исследовательских институтах НКИ должны располагаться в выделенных сетевых сегментах со строго контролируемыми подключениями. Такая стратегия сдерживания предотвращает горизонтальное распространение атаки в случае компрометации одной из ИТ-систем.

VPN и шифрованные туннели следует использовать для защиты каналов связи при удаленном мониторинге и телемедицине. Когда НКИ требуется подключение к внешним системам для клинического контроля, криптографические алгоритмы виртуальных частных сетей предотвращают перехват информации и обеспечивают аутентификацию устройств.

Система обнаружения и предотвращения вторжений может отслеживать сетевой трафик НКИ на предмет аномалий, указывающих на атаки. Сигнатурный анализ помогает выявить известные схемы атак, а для обнаружения новых угроз используется поведенческий анализ. Системы с поведенческим анализом анализ сперва устанавливают нормальные паттерны взаимодействия, а в дальнейшем при обнаружении любых отклонений от этих паттернов запускают оповещения или автоматические защитные реакции.

10.8 Обнаружение аномалий в реальном времени

Непрерывный мониторинг аномалий в паттернах позволяет своевременно выявлять нарушения до того, как будет нанесен значительный ущерб.

Обнаружение аномалий нейронных сигналов может задействовать машинное обучение для моделирования нормальных паттернов активности мозга отдельных пользователей. При этом такие отклонения, как характеристики сигнала, не соответствующие истинной нейронной активности, могут указывать на инъекционные атаки или неисправность устройства. Анализ в реальном времени позволит быстро реагировать на обнаруженные аномалии.

Поведенческий мониторинг может отслеживать модели взаимодействия пользователей с НКИ. Внезапные изменения в моделях использования, команды, не соответствующие предыдущему поведению, либо невыполнимые последовательности действий могут указывать на захват учетной записи или компрометацию устройства. Поведенческая биометрия позволит обеспечить непрерывную аутентификацию, дополняющую первоначальную проверку входа в систему.

Мониторинг параметров устройства может отслеживать несанкционированные изменения настроек стимуляции, конфигураций записи или политик безопасности. Любые изменения, явно не разрешенные

аутентифицированными пользователями или врачами, инициируют оповещения для проведения расследования.

Автоматизированное реагирование на инциденты подразумевает автоматические защитные меры при обнаружении потенциальной компрометации. Такие меры могут включать завершение подозрительных сеансов, переход в безопасный режим работы с ограниченной функциональностью, уведомление пользователей и сотрудников службы безопасности, а также, в серьезных случаях, временное отключение НКИ до проведения расследования человеком.

10.9 Меры физической безопасности

Защита НКИ от физического взлома требует организационных политик и технических средств контроля.

Ограничение физического доступа в лабораториях и складских помещениях к устройствам НКИ должна осуществляться посредством многофакторной аутентификации, журналов учета посетителей и требований к сопровождению, а также видеонаблюдения за помещениями, где находятся НКИ.

Инвентаризация и учет при хранении позволяют документировать всю цепочку поставок для всех компонентов НКИ. Информация о том, кто и когда получал доступ к устройствам, позволяет расследовать предполагаемое несанкционированное вмешательство, а также предотвращать внутренние угрозы благодаря подотчетности.

Лабораторные протоколы безопасности должны включать в себя:

- процедуры «чистых помещений» для конфиденциальности разработки НКИ,
- требования проверки биографий персонала, имеющего доступ к устройствам,
- непрерывный мониторинг поведения сотрудников для выявления внутренних угроз.

Технологии защиты от несанкционированного доступа должны включать:

- датчики, обнаруживающие вскрытие устройства,
- покрытия, которые меняют свои свойства при повреждении,
- автоматизированные меры реагирования (например, стирание ключа при обнаружении несанкционированного вмешательства).

11. Стратегии смягчения последствий — этические и нормативные подходы

11.1 Необходимость разработки законодательства о нейроправах

Уникальные угрозы, создаваемые нейротехнологиями, требуют новых категорий прав человека, защищающих когнитивную свободу, ментальную неприкосновенность и психологическую целостность.

Когнитивная свобода подразумевает защиту права на психическое самоопределение — свободу от нежелательного вмешательства в нейронные процессы и свободу изменять собственные когнитивные функции с помощью технологий. Юридическое признание когнитивной свободы запретило бы несанкционированный доступ к нейронным данным или манипулирование активностью мозга, устанавливая психическую неприкосновенность как защищаемый вид свободы, сопоставимый с физической неприкосновенностью.

Ментальная неприкосновенность включает в себя право сохранять конфиденциальность своих мыслей, эмоций и нейронных данных. Это право запрещает наблюдение или мониторинг активности мозга без осознанного согласия и ограничивает использование нейронных данных в целях, не разрешенных явным образом. Защита психической приватности предполагает, что нейронные данные требуют наивысшего уровня безопасности и конфиденциальности.

Психологическая целостность подразумевает защиту и сохранение стабильной личной идентичности и чувства субъектности. Правовые рамки, признающие это право, запрещают манипуляции, которые фрагментируют личность, создают ложные воспоминания или фундаментально изменяют личность без осознанного согласия и убедительных оснований. Это установило бы, что личная идентичность представляет собой защищаемый вид свободы, который не может быть скомпрометирован посредством технологического вмешательства.

Принцип нейронной недискриминации подразумевает запрет на использование нейронных данных или когнитивного профилирования в дискриминационных целях при трудоустройстве, страховании, образовании и в иных обстоятельствах. Подобно тому, как генетическая дискриминация сталкивается с правовыми запретами во многих юрисдикциях, нейронная информация, указывающая на когнитивные черты, эмоциональные наклонности или психологические характеристики, должна быть защищена от использования при принятии потенциально дискриминационных решений.

11.2 Совершенствование правовой базы по защите данных

Нейронные данные требуют правовой защиты, превышающей ту, которая предусмотрена для обычных ПДн.

Отнесение к особой категории ПДн должно однозначно определять нейронные данные как высококонфиденциальные, требующие усиленной защиты. Нормативные акты должны обеспечивать защиту данных мозга, превосходящую даже защиту генетической информации, учитывая прямую связь нейронных данных с мыслями и психическими состояниями.

Требования к согласию на сбор и обработку нейронных данных должны обеспечивать подлинное понимание. Стандартные формы согласия на передачу ПДн обычно недостаточны, учитывая высокую степень конфиденциальности нейронной информации. Процессы получения согласия должны включать подробное консультирование о рисках, период охлаждения для пересмотра решения и возможность отзыва согласия в любой момент.

Ограничение цели обработки должно строго ограничивать использование нейронных данных. Данные, собранные для конкретных терапевтических целей, не должны повторно использоваться для исследований, маркетинга или иных целей без отдельного явного согласия. Вторичное использование нейронных данных должно быть возможно только в исключительных случаях и после строгой процедуры обоснования необходимости повторной обработки.

Принцип минимизации данных, должен гарантировать, что сбор нейронной информации ограничивается только теми данными, которые строго необходимы для заявленных целей. Если информационные системы могут работать с агрегированными показателями или обработанными данными, они не должны получать

доступ к сырым нейронным потокам. Такой подход ограничит раскрытие данных и снизит последствия нарушений.

11.3 Новый подход к информированному согласию на обработку данных

Традиционное информированное согласие оказывается неэффективным для нейротехнологий, требуя усовершенствованных процессов, учитывающих уникальные характеристики нейронных данных.

Подробное консультирование должно информировать пользователей о конкретных рисках, включая нарушение конфиденциальности, потенциал когнитивных манипуляций, возможность утечки данных с неизменяемой нейронной информацией и долгосрочную неопределенность относительно последствий постоянного использования НКИ.

Тестирование на понимание должно подтверждать, что пользователи действительно осознают риски и последствия. Простого подписания форм согласия для начала работы с нейронными данными недостаточно — понимание рисков должно проверяться путем структурированных интервью или тестов.

Непрерывность согласия для долгосрочного нейронного мониторинга необходима в связи с тем, что одноразового разрешения на обработку данных недостаточно. Регулярное продление согласия, например, ежегодное, гарантирует пользователям сохранение осознанного выбора относительно дальнейшего использования их нейронных данных.

Право отказа должно быть практически реализуемым. Пользователи должны иметь возможность прекратить использование НКИ и потребовать удаления собранных нейронных данных. Для имплантированных устройств, удаление которых сопряжено с хирургическими рисками, должны быть гарантированы альтернативные меры защиты, такие как удаление данных и отключение устройства.

11.4 Процессы этической экспертизы

Для обеспечения гарантий соблюдения этических норм при разработке НКИ, следует проводить независимую этическую экспертизу.

Институциональные наблюдательные советы, обладающие экспертными знаниями в области нейротехнологий, должны оценивать исследования и внедрение НКИ. Традиционные комиссии по этике часто не понимают угроз нейробезопасности, что требует специализированной подготовки или специальных знаний в области нейроэтики.

Интегрированная этика (Ethics-by-design) учитывает этические аспекты на протяжении всей разработки, не ограничиваясь ретроспективной оценкой. Разработчики должны привлекать специалистов по этике на всех этапах разработки – от первоначальной концепции до внедрения. Это гарантирует, что этические принципы будут определять технические решения.

Команды специалистов по этическому аудиту должны выявлять потенциальные злоупотребления или непреднамеренные нарушения этических принципов. Состязательный этический анализ позволит представить, как технологии могут быть использованы не по назначению или в качестве оружия, что позволяет принять превентивные меры безопасности до момента внедрения.

11.5 Независимые наблюдательные органы

Внедрение НКИ должно контролироваться независимыми органами, защищающими интересы пользователей.

Представительство интересов пациентов гарантирует, что мнения пользователей будут учитываться при формировании политики и надзора. Специалисты с практическим опытом использования НКИ предоставляют ценную информацию, которую часто упускают из виду технические или клинические эксперты. Многопрофильный состав должен объединять нейробиологов, инженеров, специалистов по этике, юристов, психологов и, возможно, представителей пациентов. Сложность нейробезопасности требует для эффективного надзора наличия у специалистов разнообразных знаний, опыта и квалификации.

Регулятивные полномочия должны позволять надзорным органам требовать улучшения безопасности, расследовать инциденты и налагать санкции на производителей за выявленные нарушения.

Требования прозрачности должны предусматривать публичную отчетность об инцидентах безопасности, раскрытие информации об уязвимостях и методы обработки данных. Это обеспечит общественную подотчетность и информированное принятие решений потенциальными пользователями.

11.6 Оценка безопасности и выявление уязвимостей в НКИ

Проактивная оценка уязвимостей методами наступательной кибербезопасности может выявить уязвимости до того, как ими воспользуются злоумышленники.

Тестирование на проникновение, проводимое опытными исследователями безопасности, направлено на компрометацию систем НКИ с использованием методов, доступных реальным злоумышленникам. Успешные схемы проникновения, выявленные в контролируемых условиях, могут быть устранены до внедрения.

Программы вознаграждения за обнаруженные ошибки стимулируют внешних исследователей выявлять и ответственно раскрывать информацию об уязвимостях. Финансовое вознаграждение за обнаруженные ошибки использует коллективный опыт мирового сообщества исследователей в области безопасности.

Скоординированное раскрытие информации об уязвимостях предоставляет исследователям механизмы безопасного сообщения об уязвимостях безопасности. Производители НКИ должны разработать четкие процессы раскрытия информации с определенными сроками устранения найденных уязвимостей и оповещения общественности.

Непрерывная оценка безопасности необходима в связи с тем, что отдельных тестов перед развертыванием недостаточно. Непрерывное тестирование выявляет уязвимости, возникающие в результате новых методов атак, обновлений компонентов НКИ или изменения ландшафта угроз.

12. Стратегии митигации – организационные меры и клиентоориентированность

12.1 Обучение пользователей и программы осведомленности

Предоставление пользователям знаний об угрозах нейробезопасности позволит последним принимать обоснованные решения и защищаться от угроз.

Обучение в области нейроконфиденциальности должно объяснять, что раскрывают нейронные данные, как их можно использовать, а также права пользователей в отношении данных, полученных из их мозга. Многие

пользователи сильно недооценивают конфиденциальность нейронной информации, полагая, что она раскрывает меньше, чем есть на самом деле.

Повышение осведомленности об угрозах описывает сценарии атак в конкретных терминах, понятных пользователям. Абстрактные обсуждения «рисков кибербезопасности» часто не передают реальных опасностей, в то время как конкретные сценарии — «кто-то может получить доступ к вашим паролям» или «вашими эмоциями могут манипулировать» — позволяют провести адекватную оценку рисков.

Обучение передовым практикам безопасности охватывает практические меры защиты, включая использование строгой аутентификации, регулярное обновление программного обеспечения, распознавание атак с использованием социальной инженерии и сообщение о подозрительном поведении устройств.

Постоянное обучение предоставляет актуальную информацию по мере развития угроз. Однократного обучения при первом использовании устройства недостаточно — регулярные обновления безопасности и повторные тренинги поддерживают осведомленность по мере изменения ландшафта угроз.

12.2 Пользовательские разрешения на доступ к нейронным данным

Пользователи должны сохранять детальный контроль над доступом к своим нейронным данным и их использованием.

Модель гранулярного доступа позволяет пользователям предоставлять ограниченные права доступа различным приложениям. Так, игра должна получать простые команды направления, но при этом не иметь доступа к показателям эмоционального состояния или внимания. Приложения для медитации может получать доступ к показателям релаксации, но не к данным о когнитивных способностях.

Прозрачность потоков данных сможет показать пользователям, какая информация собирается и передается. Панели мониторинга в режиме реального времени, отображающие активный сбор и передачу данных, позволят принимать обоснованные решения о том, когда использовать НКИ и какие функции включать.

Отзываемое согласие должно позволять пользователям аннулировать ранее предоставленные разрешения. Если человека не устраивают условия обмена данными, у него должна быть возможность прекратить такой обмен в любой момент без потери базовых функций НКИ.

Переносимость данных должна позволять пользователям получать копии своих нейронных данных в стандартизированных форматах для личного использования или передачи в другие организации. Это позволит предотвратить зависимость пользователя от одного поставщика и гарантирует ему сохранение права собственности на свои нейронные данные.

12.3 Протоколы клинического мониторинга

Медицинские работники играют важную роль в выявлении и реагировании на компрометацию НКИ.

Во время плановых осмотров пациентов, использующих НКИ, должна проводиться также и **регулярная оценка безопасности** НКИ. Такие мероприятия должны специально выявлять потенциальные индикаторы компрометации. Пациенты могут явным образом не сообщать о симптомах манипуляции, поэтому требуется прямой опрос о необычных мыслях, эмоциональных изменениях или необъяснимом поведении устройства НКИ.

Скрининг психиатрических симптомов позволяет выявлять потенциальную компрометацию или биологическую реакцию на имплантаты. Депрессия, тревожность, параноидальные идеи или диссоциативные симптомы должны стать основанием для проверки возможности их связи с НКИ.

Диагностика НКИ должна включать в себя проверку безопасности, выходящую за рамки простого тестирования функциональности. Просмотр журналов событий, верификация параметров и проверка целостности прошивки должны стать рутинными операциями по обслуживанию НКИ.

Протоколы реагирования на инциденты позволяют быстро реагировать при подозрении на компрометацию. Четкая иерархия управления, заранее распределенные роли и обязанности, а также преднастроенные каналы связи обеспечивают эффективность реагирования и минимизацию вреда.

12.4 Реагирование на инциденты

Организации, внедряющие НКИ, должны обладать планами реагирования на инциденты безопасности. Следует заранее формировать **группы реагирования** с определёнными ролями и опытом. В состав групп должен входить медицинский персонал, эксперты по безопасности, юристы и специалисты по связям с общественностью, способные обеспечить скоординированное реагирование.

Классификация инцидентов устанавливает уровни серьёзности, определяющие степень реагирования. Незначительные уязвимости, обнаруженные в ходе исследования, могут потребовать иных мер противодействия, чем активные нарушения безопасности, причиняющие вред пациенту.

Планы оповещения определяют, когда и как уведомлять затронутых пользователей, регулирующие органы, правоохранительные органы и общественность. Прозрачное и своевременное информирование поддерживает доверие даже в неблагоприятных обстоятельствах.

Процедуры аварийного восстановления после компрометации возвращают уровни безопасности и функциональности НКИ к штатным. Они могут включать замену прошивки, смену ключей, сброс конфигурации и проверку отсутствия устойчивых нарушений.

12.5 Междисциплинарное взаимодействие

Эффективная нейробезопасность требует постоянного сотрудничества между представителями разных дисциплин.

Партнерство нейробиологов и инженеров гарантирует, что меры безопасности будут учитывать характеристики нейронных сигналов и терапевтические требования. Специалисты по безопасности могут не понимать нейрофизиологию, а нейробиологи могут не понимать последствия для кибербезопасности — сотрудничество позволяет преодолеть эти пробелы.

Участие специалистов по этике на всех этапах разработки позволяет учитывать человеческое достоинство и права человека в качестве центрального элемента технических решений.

Участие регуляторов гарантирует, что нормативные акты отражают технические реалии и требования безопасности. Диалог между разработчиками и контролирующими органами позволяет создавать более эффективные и реализуемые политики, чем любая из этих групп могла бы разработать по отдельности.

Учет мнений и опыта пользователей НКИ в области нейробезопасности необходим по той причине, что именно они несут непосредственные риски компрометации.

Глава 3. Перспективы развития технологий, предстоящие вызовы и итоги

13. Интерфейсные технологии: объединение ионной и электронной проводимости

13.1 Проблема проводимости

Для создания действительно эффективных НКИ ученым необходимо преодолеть принципиальные различия механизмов проводимости. Биологические нейронные сети работают за счёт ионной проводимости — движения ионов натрия, калия, хлора и кальция через клеточные мембраны и во внеклеточной среде. Электронные устройства функционируют за счёт потока электронов в металлах и полупроводниках. Это несоответствие проводимости создаёт значительное сопротивление на границах раздела электрод-ткань, ухудшая качество сигнала и ограничивая долгосрочную функциональность.

Нервная ткань обладает проводимостью 0,15–0,45 См/м *(сименсы на метр (См/м) или Ом−1·м−1;)* благодаря ионным механизмам. Традиционные металлические электроды основаны на электронной проводимости, но сталкиваются с высоким импедансом интерфейса — обычно 500–1500 Ом — при контакте с ионной средой. Этот импеданс увеличивает уровень шума, снижает соотношение сигнал/шум и препятствует эффективному переносу заряда. Интерфейсные технологии направлены на преодоление этого разрыва в проводимости с помощью материалов и архитектур, обеспечивающих плавную передачу между ионными и электронными доменами.

13.2 Технологии полимерных проводников

Проводящие полимеры представляют собой значительный шаг вперед в разработке материалов для НКИ благодаря своей смешанной ионно-электронной проводимости.

ПЭДОТ (поли(3,4-этилендиокситиофен)) и его производные демонстрируют превосходные характеристики для НКИ. Электроды с покрытием ПЭДОТ демонстрируют снижение импеданса до 50% по сравнению с электродами из чистого металла, при этом значения импеданса на частоте 1 кГц составляют приблизительно 23,3 кОм против 113,6 кОм для оксида иридия на эквивалентных участках. Это снижение импеданса обусловлено способностью ПЭДОТ одновременно проводить ионы и электроны.

При легировании полистиролсульфонатом (ПСС) ПЭДОТ образует стабильные пленки, способные инжектировать заряд с плотностью 75,6 мКл/см² по сравнению с 28,8 мКл/см² для обычного оксида иридия. Клинические исследования показывают, что электроды с покрытием ПЭДОТ сохраняют более низкий импеданс в течение шести недель после имплантации и регистрируют на 17% больше качественных нейронных единиц, чем контрольные образцы без покрытия.

Полипиррол (ППи) обладает отличной растворимостью в воде во время синтеза и хорошей биосовместимостью при соответствующем легировании. В процессе электроосаждения в полимер можно добавить биоактивные молекулы, такие как фактор роста нервов NGF и нейротрофический фактор головного мозга BDNF, создавая многофункциональные интерфейсы, которые одновременно проводят сигналы и способствуют здоровью нейронов посредством трофической поддержки.

Взаимопроникающие проводящие полимерные сети объединяют несколько полимеров для одновременной оптимизации электрических и механических свойств. Взаимопроникающие сети ПЭДОТ/ПСС/поливиниловый спирт демонстрируют значительно более низкий электрохимический импеданс, превосходные механические свойства и улучшенную электрохимическую стабильность по сравнению с чистыми пленками ПЭДОТ/ПСС, демонстрируя при этом повышенную биосовместимость с нейронами гиппокампа.

13.3 Углеродные наноматериалы

Углеродные наноструктуры обеспечивают исключительную электропроводность с наномасштабными размерами, соответствующими нейронной архитектуре.

Электроды из углеродных нанотрубок (УНТ) обладают большой площадью поверхности для улучшенной передачи сигнала, сохраняя при этом биосовместимость, превосходящую традиционные металлы. Цилиндрическая структура УНТ обеспечивает оптимальное взаимодействие с мембранами нейронных клеток, способствуя эффективному переносу заряда. Вертикально ориентированные УНТ-электроды демонстрируют выдающиеся характеристики регистрации с амплитудой сигнала от пика до пика 1600 мкВ и исключительно низким уровнем шума.

Графеновые электроды сочетают электропроводность с оптической прозрачностью, что позволяет одновременно проводить электрофизиологические исследования и визуализацию. Четырехслойные графеновые электроды сохраняют более 90% оптической прозрачности, достигая низкого поверхностного сопротивления благодаря химическому легированию. Эти прозрачные электроды позволяют проводить оптогенетическую стимуляцию, оптическую когерентную томографию и флуоресцентную визуализацию под электродами без артефактов оптической интерференции.

Гибридные системы графен/УНТ сочетают преимущества обоих материалов. Прозрачный графен обеспечивает электрический контакт и позволяет визуально контролировать жизнеспособность клеток, в то время как вертикально ориентированные УНТ создают тесные межклеточные интерфейсы. Эти гибридные электроды обеспечивают превосходное соотношение сигнал/шум и демонстрируют исключительные пределы инжекции заряда 116–174 мкКл·см$^{-2}$.

Трёхмерный пористый графен, изготовленный методом лазерной обработки, демонстрирует исключительные эксплуатационные характеристики. Электроды достигают ёмкости накопления заряда 362,4 мКл/см² и ёмкости инжекции заряда 10,32 мКл/см², что на два порядка превышает показатели монослойных графеновых и золотых электродов. Большая площадь поверхности и интегрированная микропористая структура способствуют эффективному проникновению ионов электролита и накоплению заряда.

13.4 Гидрогелевые биоинтерфейсы

Гидрогели устраняют критическое механическое несоответствие между жёсткими электронными устройствами и мягкой нервной тканью.

Модуль упругости мозговой ткани составляет приблизительно 0,1–1 кПа, в то время как у традиционных металлических электродов он превышает 100 ГПа. Это значительное механическое несоответствие способствует развитию хронического воспаления и выходу электродов из строя. **Гидрогели, соответствующие тканям**, с модулем упругости 1–10 кПа обеспечивают механически податливые интерфейсы, которые соответствуют нервной ткани, не вызывают компрессионных повреждений и поддерживают плотный контакт, что снижает сопротивление интерфейса в течение длительного времени.

Проводящие гидрогелевые системы сочетают механическую податливость с необходимой электропроводностью. Наночастицы ПЭДОТ, встроенные в сети к-каррагинана, полидофамина и полиакриламида, создают высокогибкие, адгезивные к тканям и биосовместимые проводящие гидрогели с самоотверждающимися свойствами, что обеспечивает бесшовное соединение жёстких микросхем с мягкой мозговой тканью.

Ионопроводящие гидрогелевые сети, содержащие высокие концентрации воды и электролита, обеспечивают перенос заряда посредством ионной проводимости, соответствующей механизмам проводимости биологических тканей. Такая ионная проводимость снижает импеданс интерфейса и улучшает передачу электрического сигнала, минимизируя потери энергии при переносе заряда.

Инъекционные гидрогелевые системы обеспечивают преимущества для малоинвазивного применения. Эти материалы могут вводиться через иглы малого диаметра и отверждаться на месте, образуя стабильные интерфейсы без необходимости хирургического размещения электродов, что значительно снижает риски имплантации и повреждения тканей.

13.5 Биоактивные модификации поверхности электродов

Биологические молекулы на поверхности электродов способствуют адгезии нервных клеток и уменьшают воспалительные реакции.

Покрытия на основе белков, включающие молекулу нейронной адгезии L1, значительно увеличивают плотность аксонов в радиусе 100 мкм от электродов и уменьшают количество клеток микроглии. В сочетании с поверхностной модификацией наночастицами, покрытия из L1 демонстрируют повышенную биологическую активность, сохраняющуюся до 28 дней в физиологических условиях.

Белковые покрытия из внеклеточного матрикса, полученные из тканей свиньи, создают временные биосовместимые интерфейсы, уменьшающие повреждение тканей в течение трех месяцев после имплантации по сравнению с электродами без покрытия. Коллагеновые и ламининовые мембраны оказывают как пассивное, так и активное противовоспалительное действие, обеспечивая контролируемую доставку лекарств за счет разрушения мембран.

Модификации на основе пептидов обеспечивают большую стабильность, чем полноценные белки, сохраняя при этом биологически активные свойства. Синтетические пептидные фрагменты, полученные из белков

ламинина, фибронектина и коллагена, включают такие последовательности, как ILVAV, YIGSR и RGD. Данные последовательности способствуют адгезии нейронов и росту нейритов, сводя к минимуму загрязнение фибробластами.

Цвиттерионные пептиды, предотвращающие обрастание, обеспечивают постоянный мониторинг активности нейронов в течение 16 недель, снижая при этом повреждение нейронов. Эти пептиды создают адгезивные поверхности, предотвращающие нежелательную адсорбцию белка, сохраняя при этом функциональные нейронные интерфейсы.

13.6 Электрохимическое согласование импеданса

Оптимальные нейронные интерфейсы поддерживают стабильные характеристики импеданса в физиологически значимых диапазонах частот.

Частотно-зависимые характеристики должны учитывать широкий спектр нейронных сигналов, от постоянного потенциала до высокочастотных компонентов потенциала действия, превышающих 1 кГц. Электрохимическая импедансная спектроскопия показывает, что как фарадеевское сопротивление, так и емкость двойного слоя уменьшаются с ростом частоты, но оптимальные интерфейсы сохраняют стабильные характеристики во всем этом диапазоне.

Емкостный и фарадеевский перенос заряда должны быть сбалансированы. Емкостное накопление заряда обеспечивает безопасную обратимую стимуляцию без электрохимических реакций, потенциально повреждающих ткани или электроды. Высокоемкостные материалы, такие как ПЭДОТ и активированный уголь, обеспечивают плотность накопления заряда более 50 мКл/см², сохраняя при этом электрохимическую стабильность.

Эффекты плотности тока вызывают нелинейное поведение интерфейса. Плотности тока выше 0,02 мА приводят к изменению импеданса, пространственно варьирующемуся по поверхностям электродов, при этом более высокие плотности тока на краях электродов создают локально сниженные значения импеданса. Сложные конструкции электродов должны учитывать эти нелинейности.

14. Соображения на будущее и возникающие угрозы

14.1 Проблемы квантовых вычислений

Появление практически применимых квантовых компьютеров представляет собой серьёзную угрозу для всех существующих схем шифрования. Традиционные криптографические подходы, включая распространённые алгоритмы RSA[13], ГОСТ Р 34.10–2018 и криптографию на эллиптических кривых, могут быть взломаны квантовыми алгоритмами, в частности алгоритмом Шора, обеспечивающим эффективную факторизацию больших чисел и решение дискретных логарифмов.

Для НКИ, предназначенных для длительной имплантации (потенциально на десятилетия), шифрование должно выдерживать будущие квантовые атаки. Нейронные данные, записанные сегодня и хранящиеся в зашифрованном виде, могут стать уязвимыми при появлении достаточной мощности квантовых вычислений.

[13] Rivest-Shamir-Adleman (асимметричный криптографический алгоритм)

Поэтому для противодействия угрозам типа «собирать данные сейчас, расшифровывать позже» необходима реализация в НКИ постквантовых криптографических алгоритмов, устойчивых как к классическим, так и к квантовым атакам.

Переход к постквантовой криптографии представляет собой проблему для НКИ с ограниченными аппаратными ресурсами. Многие постквантовые алгоритмы требуют ключей большего размера или больших вычислительных ресурсов, чем традиционные схемы, которые часто превышают возможности маломощных имплантируемых устройств. Поэтому крайне важно разоаботать новые эффективные постквантовые схемы, подходящие для встраиваемых медицинских устройств.

14.2 Эволюция искусственного интеллекта

По мере того, как системы ИИ становятся всё более сложными, их потенциал манипулирования пользователями НКИ посредством усвоенных поведенческих моделей существенно возрастает.

Вредоносный ИИ потенциально может разрабатывать сложные стратегии атак, выходящие за рамки человеческого понимания. Системы машинного обучения, исследующие уязвимости НКИ, могут обнаружить векторы атак, которые люди никогда не могли себе представить. Скорость и масштаб атак, управляемых ИИ, могут вывести из строя системы мониторинга безопасности и реагирования, ориентированные на человека.

Прогностическое манипулирование может стать возможным, поскольку системы ИИ учатся предсказывать паттерны нейронной активности с всё большей точностью. Системы, точно предсказывающие намерения пользователя за миллисекунды до осознания, потенциально могут манипулировать процессом принятия решений, предоставляя оптимально подобранные по времени стимулы или обратную связь, формируя выбор без распознавания внешнего воздействия пользователями.

Нестандартное поведение в сложных системах ИИ, интегрированных с НКИ, может иметь неожиданные последствия для безопасности. Поскольку нейронные интерфейсы обеспечивают всё более сложную интеграцию ИИ и мозга, новые свойства этих гибридных систем могут включать уязвимости или пути эксплуатации, не очевидные при анализе отдельных компонентов.

14.3 Риски при массовом внедрении НКИ

Широкое внедрение НКИ создаёт новые категории системного риска, поскольку такого рода устройства становятся массовыми.

В условиях, когда большое количество людей использует НКИ, становится **возможным наблюдение за мыслями** в масштабах регионов, государств и даже всего мира. Агрегированные нейронные данные миллионов пользователей могут обеспечить беспрецедентный социальный мониторинг, политическое профилирование и поведенческое прогнозирование в масштабах всего общества.

Скоординированные атаки, направленные одновременно на нескольких пользователей НКИ, могут иметь катастрофические социальные последствия. Например, атаки на НКИ критически важных групп населения (пилотов, операторов критической информационной инфраструктуры (КИИ), военнослужащих), либо в целом на большое количество жертв, могут вызвать массовую панику или беспорядки.

По мере интеграции НКИ в системы управления КИИ, **стабильная работа жизненно важных отраслей** может стать зависимой от безопасности НКИ. Если транспорт, здравоохранение, связь или другие критически секторы экономики станут зависеть от операторов или систем управления, использующих НКИ, уязвимости в нейроинтерфейсах могут поставить под угрозу безопасность инфраструктуры и общественную стабильность.
Технологические монокультуры, в которых множество пользователей используют схожие системы НКИ от одного или нескольких производителей, создают системную уязвимость. Единственная уязвимость, затрагивающая доминирующую платформу НКИ, теоретически, может поставить под угрозу безопасность огромного количества пользователей одновременно, что приведет к масштабному ущербу.

14.4 Угрозы коммуникации "Мозг-мозг"

Новые исследования возможности прямой коммуникации «мозг-мозг» создают совершенно новые категории угроз.
Передача мыслей в обход традиционных каналов связи может позволить осуществлять скрытую передачу сообщений, но также создает риски нежелательного ментального вмешательства. Если мысли смогут передаваться напрямую между людьми, становится необходимым обеспечить получение согласия на прием мысленных сообщений и их фильтрацию с целью предотвращения преследований или ментального спама.
Эмоциональное заражение через прямые нейронные связи, потенциально, может распространять ментальные состояния между связанными людьми. Хотя эта способность может быть ценна для эмпатии и установления связи, она может быть использована в качестве оружия для вызова паники, депрессии или других негативных состояний в сетях коллективного сознания.
В сетях коллективного сознания возникают особые риски, связанные с **концепцией коллективного разума**. Для митигации данных рисков следует ответить на глубокие вопросы об индивидуальной автономии и границах идентичности. Где заканчивается мысль одного человека и начинается мысль другого в сетях коллективного сознания? Возможно ли сохранить индивидуальные права и свободу действий в коллективных ментальных пространствах?
Сетевая безопасность для коммуникации «мозг-мозг» должна учитывать совершенно новые модели угроз. Традиционная сетевая безопасность фокусируется на конфиденциальности и целостности данных. При сетевых взаимодействиях типа «мозг-мозг» должны дополнительно обеспечиваться защита психической автономии, предотвращаться манипуляции мыслями и обеспечиваться согласованное участие. Проблемы безопасности, связанные с защитой сознания, подключенного к коллективной сети, остаются в значительной степени неизученными.

15. Заключение

НКИ представляют собой одно из самых революционных технологических достижений человечества, предлагая значительные преимущества для лечения неврологических заболеваний, восстановления утраченных функций и расширения возможностей человека. Однако, прямая связь между нервной тканью и цифровыми системами создаёт беспрецедентную поверхность для атак, последствия которых выходят далеко за рамки традиционных проблем кибербезопасности.

Риски, описанные в данном анализе, охватывают множество областей. **Угрозы физическому здоровью** включают в себя злонамеренное манипулирование двигательными сигналами, приводящее к травмам, несанкционированную стимуляцию, вызывающую судороги или боль, атаки типа «отказ в обслуживании», приводящие к обездвиживанию или изоляции пользователей, а также сценарии «мозгового взлома», когда злоумышленники получают прямой контроль над нейронными функциями. Тот факт, что НКИ способны причинить немедленный физический вред — от индуцированных эпилептических приступов до кровоизлияний путем манипуляции параметрами стимуляции — превращает нарушения кибербезопасности из абстрактных проблем с данными в вопросы жизни и смерти.

Нарушения конфиденциальности посредством компрометации НКИ превосходят всё, что возможно при обычных утечках данных. Нейронные данные предоставляют прямой доступ к мыслям, эмоциям, намерениям и подсознательным процессам, которые сами люди могут не осознавать в полной мере. Извлечение когнитивных состояний, политических убеждений, эмоциональных реакций и содержимого памяти представляет собой слежку на самом интимном уровне. В отличие от украденных паролей, которые можно изменить, или скомпрометированных кредитных карт, которые можно заменить, нейронные данные представляют собой постоянную, необратимую биометрическую информацию, однозначно идентифицирующую человека и раскрывающую его глубинный ментальный ландшафт. Потенциал использования этой информации для дискриминации, шантажа, манипуляции или тоталитарного контроля создаёт экзистенциальные угрозы человеческому достоинству и свободе.

Психологическая автономия сталкивается с беспрецедентной угрозой со стороны НКИ, способных манипулировать эмоциями, внедрять искусственные предпочтения, изменять процессы принятия решений и фрагментировать личность. Продемонстрированная способность вызывать страх, счастье, компульсивные состояния или изменения личности посредством целенаправленной электростимуляции означает, что граница между подлинным «я» и навязанными извне ментальными состояниями становится опасно проницаемой. Когда сами мысли могут быть сформированы или подавлены извне, основополагающие концепции свободы воли, моральной ответственности и человеческой активности теряют связный смысл. Психологическая травма, вызванная нейронными нарушениями – хроническая тревожность, депрессия, диссоциативные симптомы и спутанность идентичности – может оказаться столь же разрушительной, как и физические травмы, причем последствия сохраняются еще долгое время после восстановления безопасности.

Идентичность и непрерывность личности становятся уязвимыми в случаях, когда память может быть подвержена манипуляциям, личность изменена, а чувство субъектности подорвано. Философские вопросы о личной идентичности во времени приобретают неотложное практическое значение, когда НКИ позволяют извне модифицировать психические процессы, составляющие самость. Задокументированные случаи изменений личности, диссоциативных состояний и фрагментации идентичности в результате нейростимуляции показывают, что эти опасения – не абстрактные домыслы, а конкретные реалии, уже встречающиеся в клинической практике.

Технические уязвимости, создающие эти риски, охватывают всю экосистему НКИ. Беспроводные протоколы связи демонстрируют уязвимости, позволяющие осуществлять прослушивание и перехват данных. Программное обеспечение и прошивки содержат ошибки, позволяющие осуществлять несанкционированный доступ и управление. Системы машинного обучения можно обмануть с помощью вредоносных входных данных или искаженных обучающих наборов данных. Физически НКИ остаются уязвимыми для несанкционированного доступа и атак по сторонним каналам. Сложность систем НКИ, включающих в себя датчики, процессоры, беспроводные радиоустройства, системы управления питанием и сложные алгоритмы, создает обширные поверхности для атак. Их масштаб настолько велик, что даже специализированные службы нейробезопасности не смогут полностью гарантировать защиту пользователей.

Биологические уязвимости усугубляют технические риски, вызывая реакции на инородное тело, нейровоспаление, глиальное рубцевание и прогрессирующую деградацию тканей. Эти биологические реакции не только ограничивают долгосрочную функциональность устройств, но и создают дополнительные пути для нанесения вреда при их сбоях или компрометации. Утечка из батареи, высвобождающая цитотоксичные вещества, чрезмерная стимуляция, вызывающая эксайтотоксическое повреждение нейронов, и нарушение нормальных механизмов пластичности — все это демонстрирует, что сбои в системе безопасности НКИ могут спровоцировать каскадные биологические последствия, выходящие далеко за рамки непосредственного воздействия атаки.

Стратегии снижения рисков, подробно описанные в данном анализе, открывают пути к более безопасному развертыванию НКИ, но требуют серьезных и долгосрочных изменений в различных областях. Технические средства защиты, включая шифрование, аутентификацию, безопасные механизмы обновления и обнаружение аномалий, помогут обеспечить необходимые уровни защиты. Однако одни только технологии не могут гарантировать нейробезопасность. Разработка и внедрение должны осуществляться на основе этических принципов, признающих когнитивную свободу, ментальную конфиденциальность и психологическую непрерывность фундаментальными правами человека. Регулирующий надзор посредством усовершенствованных законов о защите данных, законодательства о нейроправах и независимых органов мониторинга должен обеспечить подотчетность и соблюдение минимальных стандартов безопасности. Расширение прав и возможностей пользователей посредством обучения, детального контроля разрешений и подлинного информированного согласия позволит людям защищать себя и принимать самостоятельные решения относительно внедрения нейротехнологий.

Крайне важно **междисциплинарное сотрудничество** между нейробиологами, инженерами, специалистами по этике, политиками, врачами и самими пользователями. Сложность проблем нейробезопасности превосходит возможности любой отдельно взятой дисциплины. Эффективная защита требует интеграции нейробиологического понимания функций мозга с инженерным опытом в проектировании безопасных систем, этическим анализом последствий для прав человека, правовыми основами управления и подотчётности, а также жизненным опытом тех, кто зависит от этих технологий.

Организационная и клиническая практика, связанная с внедрением НКИ, существенно влияет на результаты обеспечения безопасности. Корпоративная культура, ориентированная на безопасность, упреждающая разработка стратегий и тактик реагирования на инциденты, регулярные оценки безопасности, интегрированные в клиническую практику, и прозрачная отчётность об уязвимостях и инцидентах — всё это должно способствовать созданию более безопасных экосистем. Ответственность за нейробезопасность не может лежать исключительно на производителях или отдельных пользователях — системы здравоохранения, исследовательские институты и регулирующие органы должны активно участвовать в создании и поддержании безопасной среды.

В перспективе **новые угрозы**, связанные с квантовыми вычислениями, передовым ИИ, сценариями массового развертывания и сетями коллективного сознания потребуют дальнейшей эволюции мер защиты. Проблемы нейробезопасности, с которыми мы сталкиваемся сегодня, — это только начало. По мере того, как НКИ становятся всё более сложными, более массовыми, более глубоко интегрированными с другими технологиями, ландшафт угроз будет расширяться в труднопредсказуемом направлении. Обеспечение безопасности потребует адаптивных подходов, способных реагировать на новые угрозы, сохраняя при этом фундаментальные механизмы защиты, необходимые для человеческого достоинства и автономии.

Этический императив очевиден: беспрецедентная близость НКИ к человеческому сознанию требует беспрецедентной приверженности безопасности и защите. Потенциальные преимущества нейротехнологий — восстановление зрения слепым, обеспечение возможности общения для парализованных пациентов, лечение трудноизлечимых психических расстройств и расширение когнитивных возможностей человека — оправдывают их дальнейшее развитие. Однако, для реализации этих преимуществ и одновременной защиты пользователей от эксплуатации, манипуляций и причинения вреда необходимо рассматривать нейробезопасность не как второстепенную задачу, а как основополагающее требование, равное по важности терапевтической эффективности и функциональности.

Уязвимость разума к технологической эксплуатации представляет собой одну из самых серьёзных проблем, с которыми столкнётся человечество в ближайшие десятилетия. Для успешного решения этой проблемы необходимо признать, что НКИ — это не просто медицинские устройства или бытовая электроника, а технологии, опосредующие самые фундаментальные аспекты человеческого опыта — сознание, идентичность, субъектность и когнитивную свободу.

Необходимо **существенное изменение парадигмы**. Традиционная кибербезопасность фокусируется на защите данных и систем. Нейробезопасность же должна защищать само сознание. Традиционное регулирование медицинских устройств фокусируется на физической безопасности и клинической эффективности. Регулирование НКИ должно дополнительно защищать когнитивную свободу и ментальную неприкосновенность. Традиционная этика исследований с участием людей фокусируется на минимизации физического риска и получении информированного согласия. Нейроэтика должна бороться с возможностью манипулирования самой способностью к автономному согласию.

Ставки не могут быть выше. В эпоху растущей технологической интеграции с биологическими системами граница между человеком и машиной становится все более проницаемой. Будет ли эта интеграция способствовать процветанию человека или откроет путь беспрецедентным формам эксплуатации и контроля, критически зависит от выбора, сделанного сейчас в отношении архитектуры безопасности, этических принципов, нормативно-правовой базы и социальных ценностей, заложенных в развитие нейротехнологий. Разум представляет собой последний рубеж конфиденциальности и автономии. Будучи скомпрометированным, он не может быть восстановлен или заменен. Раскрытые нейронные данные не могут быть изменены. Нанесенная психологическая травма может никогда полностью не зажить. Подрыв доверия к собственным мыслям и свободе действий затрагивает саму суть человеческого достоинства. Поэтому защита разума от угроз кибербезопасности — это многомерная задача, которая должна быть признана одним из важнейших императивов технологической эпохи — моральным обязательством сохранить то, что делает нас изначально людьми, в эпоху все более сложной интеграции человека и машины.

По мере того, как НКИ переходят от экспериментальных технологий к массовому медицинскому и потребительскому продукту, возможности для внедрения надежных мер безопасности и этических гарантий стремительно сужаются. Выбор, сделанный в настоящий момент, будет иметь последствия на протяжении десятилетий, определяя, будут ли будущие поколения воспринимать нейротехнологии как расширение человеческих возможностей или как абсолютное нарушение когнитивной свободы.

16. Источники

1. Collinger, J. L., Wodlinger, B., Downey, J. E., Wang, W., Tyler-Kabara, E. C., Weber, D. J., ... & Schwartz, A. B. (2013). High-performance neuroprosthetic control by an individual with tetraplegia. The Lancet, 381(9866), 557-564.
2. European Parliament and Council of the European Union. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679.
3. Greenberg, A. (2015). Hackers Remotely Kill a Jeep on the Highway—With Me in It. Wired.
4. Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., ... & Fu, K. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In 2008 IEEE Symposium on Security and Privacy (pp. 129-142). IEEE.
5. Haynes, J. D., Sakai, K., Rees, G., Gilbert, S., Frith, C., & Passingham, R. E. (2007). Reading hidden intentions in the human brain. Current Biology, 17(4), 323-328.
6. Ienca, M., & Haselager, P. (2016). Hacking the brain: brain-computer interfacing technology and the ethics of neurotechnology. AJOB Neuroscience, 7(1), 1-10.
7. Pycroft, L., Boccard, S. G., Owen, S. L., Stein, J. F., Fitzgerald, J. J., Green, A. L., & Aziz, T. Z. (2016). Brainjacking: implant security issues in invasive neuromodulation. World Neurosurgery, 92, 454-462.
8. Ramirez, S., Liu, X., Lin, P. A., Suh, J., Pignatelli, M., Redondo, R. L., ... & Tonegawa, S. (2013). Creating a false memory in the hippocampus. Science, 341(6144), 387-391.
9. Ruiz-Blondet, M. V., Jin, Z., & Laszlo, S. (2016). CEREBRE: A novel method for very high accuracy event-related potential biometric identification. IEEE Transactions on Information Forensics and Security, 11(7), 1618-1629.

10. Selimbeyoglu, A., & Parvizi, J. (2010). Electrical stimulation of the human brain: perceptual and behavioral phenomena reported in the old and new literature. Frontiers in Human Neuroscience, 4, 46.

11. Soon, C. S., Brass, M., Heinze, H. J., & Haynes, J. D. (2008). Unconscious determinants of free decisions in the human brain. Nature Neuroscience, 11(5), 543-545.

12. Wolpaw, J., & Wolpaw, E. W. (2012). Brain-computer interfaces: principles and practice. Oxford University Press.

13. Yuste, R., Goering, S., Arcas, B. A., Bi, G., Carmena, J. M., Carter, A., ... & Rommelfanger, K. S. (2017). Four ethical priorities for neurotechnologies and AI. Nature, 551(7679), 159-163.

14. Kisely, S., et al. (2021). Deep Brain Stimulation in Treatment-Resistant Depression: A Systematic Review and Meta-Analysis. Frontiers in Neuroscience, 17 studies, AE rate 67% (54-80%)

15. Morishita, T., et al. (2014). Deep Brain Stimulation for Treatment-resistant Depression. Multiple targets, varying response/AE rates

16. Mixed Effects of DBS on depressive symptoms in PD (2014): 8% depression rate post-STN DBS

17. Yang, S.E., et al. (2022). Functional Connectivity Signatures of Political Ideology. PNAS Nexus, n=174, 80% accuracy with brain + demographics vs 65-70% with demographics alone

18. Kanai, R., et al. (2011). Political Orientations Are Correlated with Brain Structure. 71.6% accuracy distinguishing conservatives from very liberals

19. Leong, Y.C., et al. (2020). Conservative and Liberal Attitudes Drive Polarized Neural Responses. Neural polarization in DMPFC during political content processing

20. Cheyuo, C., et al. (2024). Comprehensive characterization of intracranial hemorrhage in DBS. Systematic review 1987-2023, 13,056 patients, ICH prevalence 2.9% per patient, 49.6% symptomatic

21. Bjerknes, S., et al. (2022). Intracranial Bleeding in DBS Surgery. 2.5% per patient, 1.4% per lead

22. Bjerknes, S., et al. (2014). Surgical Site Infections after DBS. 5.6% of 588 procedures, 33 infections

23. Patel, D.M., et al. (2019). Evaluation of neurosurgical implant infection rates. Meta-analysis, overall IR 4.87%

24. Darlot, F., et al. (2024). Glial scarring around intra-cortical MEA implants. 10 µm electrodes: 100 µm scar; 50 µm electrodes: 300 µm scar

25. Abbott, J.R., et al. (2024). Planar a-SiC Microelectrode Arrays. AEY declined to ~51% at 16 weeks

26. Spencer, K.C., et al. (2017). Characterization of Mechanically Matched Hydrogel Coatings. Glial sheath typically a few hundred microns thick, neurons within 50-100 µm needed

27. Chestek, C.A., et al. (2011). Long-term stability of neural prosthetic control signals. Vpp decline 2.4% per month average

28. Otte, E., et al. (2022). Engineering strategies towards overcoming glial scarring. Distance between electrode and viable neurons can exceed several hundred µm within 4-8 weeks

29. Meng, L., et al. (2024). Adversarial Filtering Based Evasion and Backdoor Attacks to EEG-Based BCIs. Attack success rate exceeds 90% in most cases on multiple models and datasets

30. Quintanilla, R.O.S., et al. (2022). Practical Adversarial Attacks on Brain-Computer Interfaces. EEGNet vulnerable with >50% attack success rate

31. Gu, T., et al. (2019). General backdoor attacks achieve >97% success

32. Claverie, T., et al. (2021). BlueMirror: Reflections on Bluetooth Pairing and Provisioning Protocols. WOOT 2021, reflection attacks on BLE Secure Simple Pairing

33. Forbes (2025). 11 Types of Bluetooth Attacks. Reflection/Relay attack defined as impersonating device by reflecting authentication data

34. NCC Group (2022). BLE Proximity Authentication Vulnerable to Relay Attacks. Link-layer relay attacks with 8 ms latency

35. Armis Labs (2017). BlueBorne Vulnerabilities. CVE-2017-series, affects unpatched implementations

36. Goethals, I., Jacobs, F., Van der Linden, C., Caemaert, J., & Audenaert, K. (2008). Brain activation associated with deep brain stimulation causing dissociation in a patient with Tourette's syndrome. Journal of trauma & dissociation: the official journal of the International Society for the Study of Dissociation (ISSD), 9(4), 543–549. https://doi.org/10.1080/15299730802226126