Политика безопасности сервиса «Брейндок»

Редакция от «25» февраля 2025 г.

1. Общие положения

1.1. Политика безопасности содержит информацию о том, как Брейндок обеспечивает безопасность данных, полученных от Пользователей.

1.2. Все термины, используемые в Политике безопасности, имеют значение, определенное в документе «Термины и определения» (https://storage.yandexcloud.net/braindoc/Braindoc_terms_and_definitions.pdf), которое является приложением к Политике безопасности и её неотъемлемой частью, если иное не следует из Политики безопасности.

1.3. Политика безопасности действует в отношении всех данных, которые Брейндок может получить от Пользователей при использовании ими Сервиса.

1.4. Брейндок обеспечивает защиту данных, финансовых операций и учетных записей Пользователей, применяя комплексные меры безопасности на всех уровнях системы.

1.5. Основные принципы безопасности Сервиса включают:

— Конфиденциальность – защита персональных данных Пользователей и бизнес-информации от несанкционированного доступа любых третьих лиц;

— Целостность – предотвращение изменений, повреждений или уничтожения данных в результате сбоев, атак и иных действий злоумышленников;

— Доступность – обеспечение бесперебойного функционирования Сервиса, минимизация простоев и гарантия доступности Сервиса для Пользователей.

2. Архитектура безопасности

2.1. Брейндок строит систему защиты на основе современных технологий и методов:

2.1.1. Сегментация сети – разделение сервисов и баз данных для предотвращения несанкционированного доступа третьих лиц к любым данным Пользователей.

2.1.2. Изоляция сред – использование отдельных окружений для разработки, тестирования и продакшена.

2.1.3. Шифрование данных – применение передовых алгоритмов защиты информации как в хранилищах, так и при передаче.

2.1.4. Механизмы обнаружения угроз – постоянный мониторинг событий безопасности и автоматическая блокировка подозрительной активности.

2.1.5. Минимизация прав доступа – Пользователи, партнеры получают доступ только к необходимым данным.

2.2. Подход к управлению рисками

2.2.1. Брейндок использует проактивные меры для выявления и устранения угроз:

— Регулярный анализ рисков – выявление потенциальных уязвимостей системы и принятие упреждающих мер;

— Стресс-тестирование и моделирование атак – проверка устойчивости Сервиса к возможным угрозам;

— Политика обновлений и исправлений – оперативное устранение уязвимостей путем своевременного обновления системных компонентов;

— Программы обучения сотрудников – повышение уровня осведомленности о киберугрозах и соблюдении стандартов безопасности;

— Встроенные механизмы самопроверки – автоматизированные системы выявления уязвимостей и проверка целостности инфраструктуры.

3. Верификация пользователей

3.1. Для обеспечения безопасности учетных записей Пользователей и соответствия требованиям законодательства Брейндок использует сервис МТС ID KYC (https://developers.mts.ru/id-kyc-api) на основании лицензионного договора с ПАО «Мобильные ТелеСистемы» (ПАО «МТС») – единое решение для аутентификации и идентификации (далее- «МТС KYC»).

3.2. МТС KYC объединяет две ключевые функции:

— Аутентификация через МТС ID – безопасный вход с привязкой к номеру телефона и проверкой личности через доверенного оператора связи;

— KYC-проверку (Know Your Customer) – обязательную верификацию личности перед предоставлением доступа к финансовым и конфиденциальным операциям.

3.3. Процедура KYC включает:

— Подтверждение личности – загрузка и верификация паспорта, загранпаспорта или водительского удостоверения.

— Подтверждение места жительства – предоставление документов (выписки из банка, договора аренды, квитанции ЖКХ).

— Биометрическая проверка – сравнение фотографии из документа с селфи Пользователя.

— Проверка по базам рисков – сверка с санкционными списками, антирейтинговыми базами и проверка на соответствие ПОД/ФТ.

3.4. Использование МТС KYC обеспечивает высокий уровень безопасности, автоматизированную проверку и исключает возможность использования поддельных или недействительных документов.

4. Безопасность хранения данных

4.1. Брейндок использует сертифицированную облачную инфраструктуру YandexCloud (https://yandex.cloud/ru/docs/security/conform?utm_referrer=about%3Ablank), которая отвечает самым высоким требованиям безопасности и сертифицирована по стандарту PCI DSS v3.2.1.

4.2. Основные меры защиты инфраструктуры

— Соответствие PCI DSS – выполнение всех требований стандарта безопасности данных платежных систем;

— Изолированные серверные окружения – разделение данных по различным сегментам для предотвращения утечек;

— Многоуровневая защита данных – шифрование, контроль доступа и мониторинг активности в реальном времени;

— Антивирусная защита и мониторинг – постоянный анализ потенциальных угроз и автоматическое реагирование на подозрительную активность;

— Автоматизированное устранение аномалий – системы машинного обучения, анализирующие подозрительное поведение и блокирующие потенциальные угрозы.

4.3. Шифрование данных

— TLS 1.2+ – защита передачи данных между Пользователями и серверами;

— AES-256 – шифрование хранимых данных, исключающее их компрометацию даже при физическом доступе к носителям.

4.4. Резервное копирование и восстановление данных

— Автоматическое резервное копирование – данные регулярно копируются для защиты от потерь.

— Политика восстановления – возможность быстрого восстановления сервисов в случае сбоев или атак.

— Использование инфраструктуры YandexCloud гарантирует соответствие строгим требованиям по защите данных, обеспечивая безопасность хранения информации пользователей.

5. Защита платежных данных

5.1. Для целей осуществления выплат с использованием функционала Сервиса Брейндо сотрудничает с банками, имеющими лицензию Центрального банка Российской Федерации и сертификат соответствия стандарту PCI DSS.

5.2. Брейндок и банками-партнерами применяются следующие меры для защиты платежных данных:

— Шифрование данных – передача информации о картах напрямую провайдерам через защищённый канал.

— Мониторинг транзакций – анализ подозрительных операций.

— Система контроля аномалий – автоматическое выявление необычных действий в финансовых операциях с уведомлением службы безопасности.

5.3. Брейндок не хранит данные банковских карт Пользователей.

6. Защита от кибератак

6.1. Брейндок применяет следующие меры для защиты от кибератак:

— OWASP – защита от SQL-инъекций, XSS, CSRF.

— IDS/IPS – обнаружение атак в реальном времени.

— Регулярное сканирование уязвимостей.

— Периодические пентесты – независимые тесты на проникновение.

— Автоматизированные обновления безопасности – постоянное внедрение новых мер защиты.

7. Соответствие законодательству

7.1. Брейндок и /или его партнеры соблюдают требования:

— Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ. Обработка Персональных данных Пользователей осуществляется на основании согласия на обработку персональных данных в соответствии с Политикой конфиденциальности Брейндок - https://storage.yandexcloud.net/braindoc/Braindoc_privacy_policy.pdf.

— Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 07.08.2001 № 115-ФЗ;

— Федерального закона «Об электронной подписи» от 06.04.2011 N 63-ФЗ;

— Требований ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»;

— Требований ISO/IEC 27001 — международного стандарта по информационной безопасности, разработанного совместно Международной организацией по стандартизации и Международной электротехнической комиссией

8. Реквизиты Брейндок:

Общество с ограниченной ответственностью «Брейндок»

Генеральный директор: Ромашенко Роман Александрович

ИНН: 7801733651

ОГРН: 1247800047065

Юридический адрес: г. Санкт-Петербург вн. тер. г. Муниципальный округ Васильевский, 17-я линия Васильевского острова, д. 66, литера В, помещение 1, офис 4-20-14

Почтовый адрес: а/я 101 в ОПС 191025

Тел.: +7 911 973 55 42

Email: ceo@braindoc.ru