



Функциональные возможности программного обеспечения
Антивируса нового поколения НейроФортресс

ООО «Сивизй Технолоджиес»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
Антивируса нового поколения НейроФортресс

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

На 6 листах

Ростов-на-Дону
2026

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам.

Товарные знаки «НейроФортресс» принадлежат ООО «Сивизй Технолджиес».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем.

Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

СОДЕРЖАНИЕ

1.	Общая информация	6
2.	Функциональные характеристики НейроФортресс	7

1. Общая информация

Для решения задач идентификации вредоносных воздействий и решения вопроса атак «Нулевого дня» — нами разработан искусственный интеллект из нескольких гетерогенных сверхточных слоев, позволяющих получить высокую точность при обнаружении ранее неизвестных атак.

В наших продуктах успешно применяется разработанный нами способ идентификации и блокирования вредоносного программного обеспечения с применением каскадов самообучающихся нейронных сетей.

Патентованная инновационная разработка, не имеющая аналогов в секторе кибербезопасности и систем идентификации и классификации, не опирается на известные открытые решения, не зависит от внешних поставщиков услуг машинного обучения. ИИ обогащается мотивацией и обратной связью систем управления инцидентами.

Реализован на C++, является кроссплатформенным.

Контроль работы ИИ прозрачен для пользователя - оператор имеет возможность выбирать зону контроля.

2. Функциональные характеристики НейроФортресс

Система обеспечивает следующие функциональные возможности:

- Детектирование на основе искусственного интеллекта — выполняется динамический анализ поведения процессов в реальном времени для выявления вредоносной активности.
- Проактивная защита — предотвращает и нейтрализует атаки до момента их реализации.
- Адаптивное самообучение — интеллектуальная модель автоматически совершенствуется за счёт облачной корреляции данных об угрозах.
- Минимизация ложных срабатываний — применяется интеллектуальная фильтрация событий и механизмы белых списков.
- Автономный режим работы — система сохраняет способность к защите при отсутствии подключения к серверу управления.
- Сверхнизкая нагрузка на ресурсы — функционирование системы не влияет на производительность и не вызывает конфликтов с антивирусами сторонних производителей.

Основной функционал системы включает:

- блокировку вирусов, программ-шифровальщиков, RAT-троянов и APT-атак;
- автоматическую изоляцию подозрительных процессов;
- выявление аномального поведения пользователей и сервисных компонентов;
- проверку сертификатов и контроль целостности исполняемого кода;
- ручное управление и оперативный сбор статистики по угрозам;
- интеграцию с системами **NGSIEM**, **EDR** и **SOAR**.