



Руководство по эксплуатации
программного обеспечения Антивирус нового
поколения НейроФортресс

ООО «Сивизй Технолоджиес»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Антивирус нового поколения НейроФортресс

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

На 20 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 «Сивизь Технолоджиес».

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

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	5
1. Общие сведения. Назначение	6
2. Системные требования	7
3. Запуск НейроФортресс	8
4. Главный экран НейроФортресс	9
4.1 Описание главного НейроФортресс	9
4.1.1 Настройка защиты.....	11
4.1.2 Текущее состояние защиты (индикация).....	11
4.1.3 Информация о лицензии.....	11
4.1.4 Управление угрозами.....	11
4.1.5 Текущие анализируемые процессы	12
4.1.6 Потребление ресурсов	12
5. Экран угроз НейроФортресс	12
5.1 Все действия угрозы	13
5.2 Управление угрозой.....	14
6. Экран статистики НейроФортресс	15
7. Экран приложения НейроФортресс	17
8. Настройка НейроФортресс.....	18
8.1 Общие настройки	19
8.2 Настройка защиты.....	19
8.3 Лицензия	20
9. Техническая поддержка.....	20

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращения, которые используются в настоящем документе, приведены в таблице 1.

Таблица 1 – Сокращения и расшифровки

Сокращение	Расшифровка
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
НейроФортресс	Антивирус нового поколения НейроФортресс

1. Общие сведения. Назначение

Из-за остро необходимого процесса цифровизации предприятий торговли, промышленности, строительства и услуг, позволяющей расширяться и оптимизировать процессы и расходы компаний, они все чаще сталкиваются с угрозами киберпреступлений.

В последние годы в связи с экспоненциальным ростом возможных каналов утечки информации — из-за увеличения количества программных продуктов и широкого использования социальных взаимодействий посредством новейших средств личной и корпоративной связи, используемых в современном производстве и деятельности компаний — классические подходы к защите информации не дают полной изоляции информации.

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.

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

В настоящее время для противостояния более сложным угрозам, целенаправленным атакам - организациям необходимо уделять особое внимание не только уровню конечных точек, но и другим потенциальным точкам проникновения злоумышленника в инфраструктуру и, самое главное, на взаимосвязи между ними. Профессиональные киберпреступники сегодня предпочитают многовекторный подход к проникновению в корпоративную сеть, атакуют как можно больше элементов инфраструктуры и часто объединяют множество различных методов в одну запланированную атаку. Организации должны обладать пониманием того, что происходит у них в рамках всей инфраструктуры, контролировать ключевые точки проникновения и получать полную картину атаки, иметь возможность быстро анализировать

первопричины, проводить глубокие расследование сложных инцидентов и реагирования на них в рамках всей инфраструктуры, а не отдельных элементов.

Архитектура системы базируется на интеллектуальном обнаружении и предотвращении. Реагирование на сложные угрозы проводятся путем охвата большого количества источников данных, подсистем предотвращения в рамках конечных точек и сетевой шине обмена статистическими обезличенными данными. На конечных точках используем программное обеспечение НейроФортресс для операционных систем, серверов и персональных компьютеров. Сделаем важное уточнение – система не собирает и не передает персональные сведения, однако защита информации в системе начинает работать с момента рождения таких данных, и подсистема предотвращения утечек прозрачно на уровне ядра операционных систем контролирует весь жизненный цикл защищенных контейнеров, не раскрывая внутреннего содержимого.

2. Системные требования

Операционная система Widows

Операционная система	Windows 10, 11
Процессор	В соответствии с требованиями ОС, установленной на компьютер
Оперативная память	Минимально – 4 ГБ Рекомендуется – 8 ГБ
Жесткий диск (свободное пространство)	10 ГБ

3. Запуск НейроФортресс

Выполните установку программного продукта НейроФортресс согласно документу «Руководство по установке НейроФортресс». При успешно завершении установки программного продукта НейроФортресс автоматически откроется интерфейс ввода ключа лицензии - Рисунок 1.

Введите ключ лицензии, полученный при регистрации личного кабинета НейроФортресс.

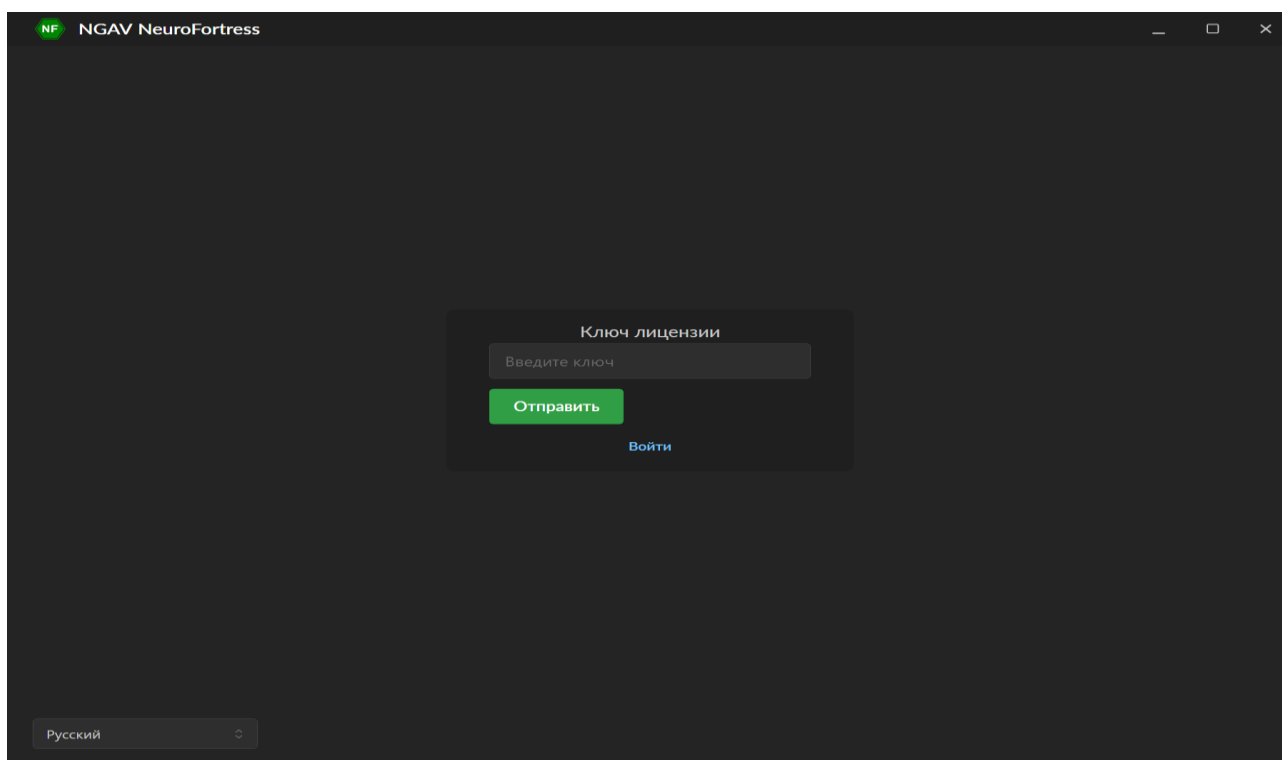


Рисунок 1 – Интерфейс ввода ключа лицензии

После ввода ключа лицензии перед пользователем откроется главный экран программного продукта НейроФортресс.

4. Главный экран НейроФортресс

4.1 Описание главного НейроФортресс

Главный экран состоит из следующих блоков:

- Настройка защиты.
- Текущее состояние защиты (индикация).
- Информация о лицензии.
- Управление угрозами.
- Текущие анализируемые процессы
- Потребление ресурсов

Вид главного экрана представлен на Рисунке 2 и Рисунок 3.

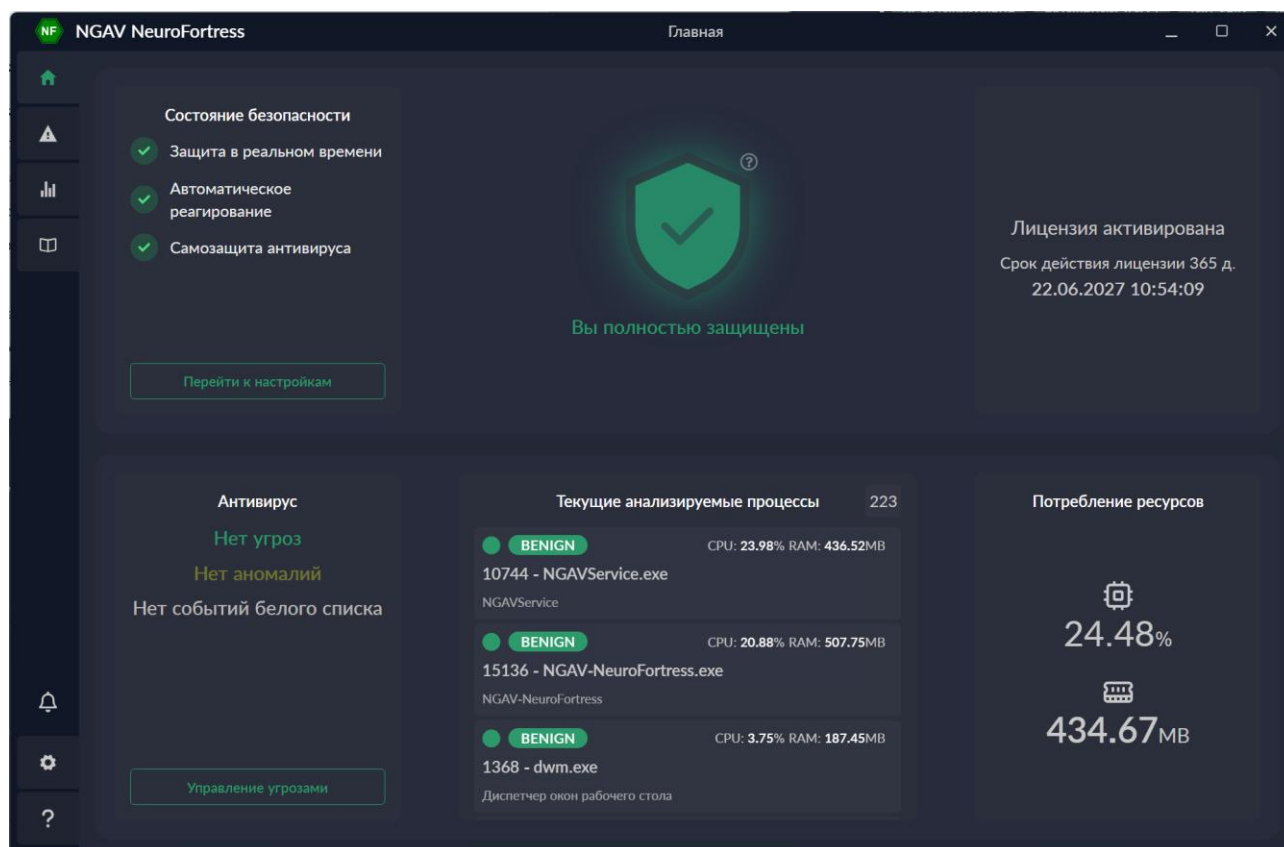


Рисунок 2 – Интерфейс главного экрана НейроФортресс (Полная защита)

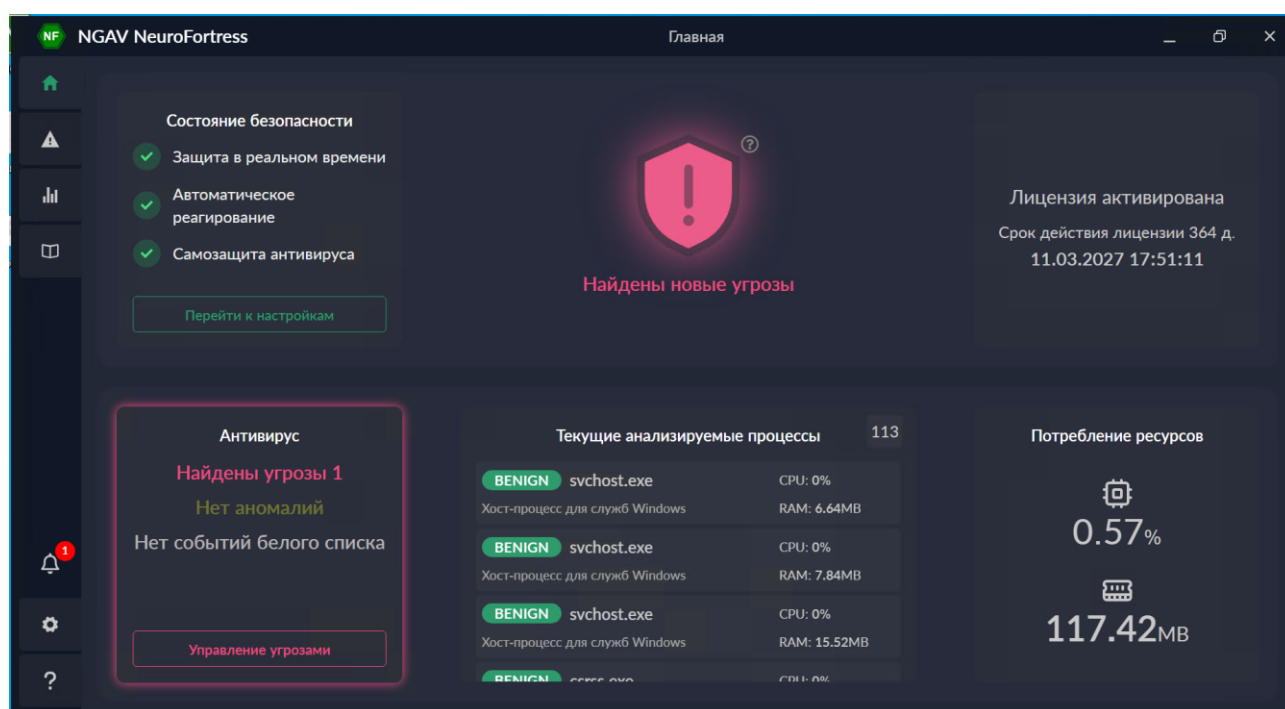


Рисунок 3 – Интерфейс главного экрана НейроФортресс (Найденные новые угрозы)

4.1.1 Настройка защиты

Блок **«Настройка защиты»** имеет три уровня настройки и индикации **«Блокировать процессы»**, **«Система защиты антивируса»**, **«Самозащита антивируса»**.

- вкладка **«Самозащита антивируса»**: - активирует систему самозащиты, предотвращающей несанкционированное удаление антивируса или внесение изменений в его компоненты.

- настройка **«Система защиты антивируса»**: - включает модули безопасности, отвечающие за мониторинг поведения процессов, контроль сетевой и файловой активности, обнаружение, анализ и предотвращение запуска вредоносных процессов;

- настройка **«Блокировать процессы»**: - авто реагирование на вредоносное ПО, включает авто реагирование на обнаруженное вредоносное поведение и блокировку вредоносных процессов без запроса подтверждения пользователя;

4.1.2 Текущее состояние защиты (индикация).

Блок индикации состояния защиты имеет три цвета индикации:

- Зеленый: - включена полная защита, вредоносного воздействия не обнаружено.
- Желтый: - защита включена, но необходимо включить компонент автоблокировки процессов и компонент самозащиты антивируса
- Красный: - найдены новые угрозы, необходимо устранить все угрозы на экране угроз.

4.1.3 Информация о лицензии.

При активации пробного бесплатного периода в блоке **«Лицензия»** указана дата окончания пробного периода использования. Для покупки рабочей лицензии нажмите **«Купить»**.

Если пользователь произвел покупку рабочей лицензии и ввел полученный ключ, то на главном экране будет выведена информация о сроке действия лицензии и дате ее окончания.

4.1.4 Управление угрозами.

Блок **«Управление угрозами»** отображает информацию об обнаруженных угрозах и

аномалиях. При нажатии на кнопку «Управление угрозами» будет осуществлен переход на Экран угроз. Более подробная информация об экране угроз приведена в пункте 5 настоящей инструкции.

4.1.5 Текущие анализируемые процессы

В блоке «Текущие анализируемые процессы» выведены все анализируемые процессы с информацией о типе его классификации, имени процесса, потребляемым ресурсам.

4.1.6 Потребление ресурсов

В блоке «Потребление ресурсов» выводится информация о ресурсах, которые задействует программный продукт НейроФортресс.

5. Экран угроз НейроФортресс

При обнаружении вредоносных или аномальных процессов система НейроФортресс формирует карточки угроз на экране «Угрозы» - Рисунок 4.

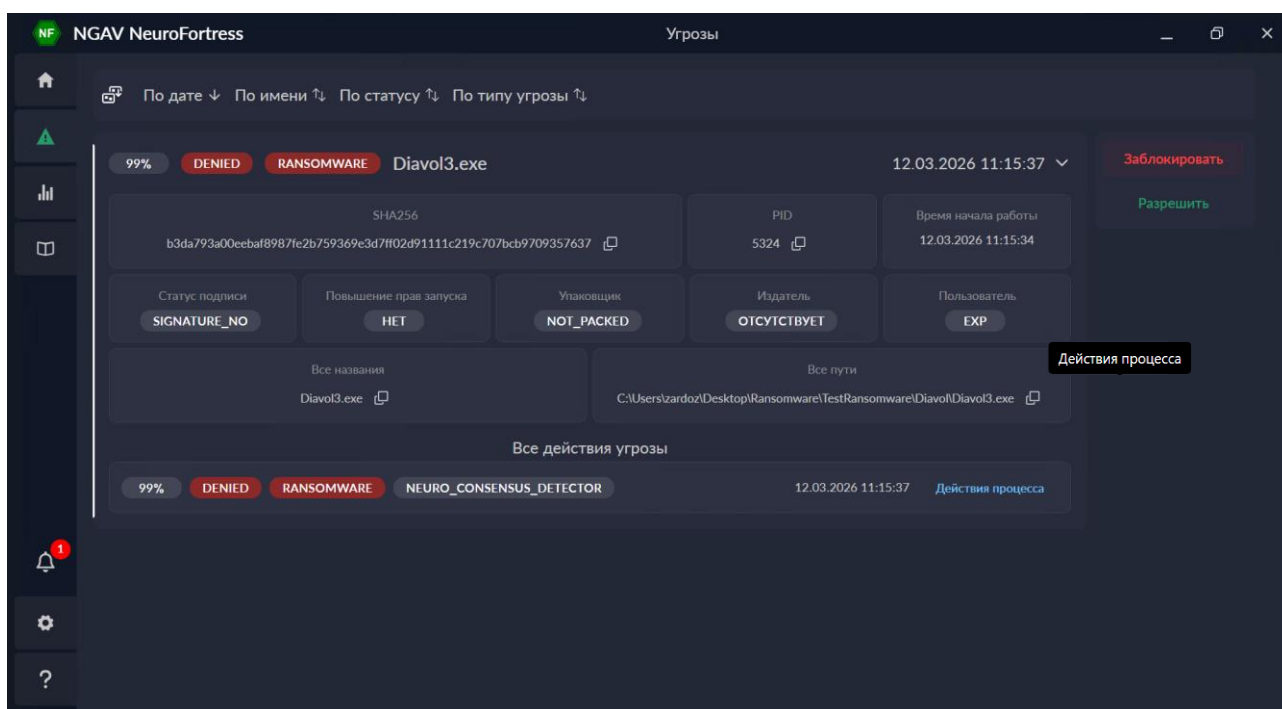


Рисунок 4 – Интерфейс экрана «Угрозы» НейроФортресс

При включенной настройке «Авто реагирование на вредоносное ПО» система автоматически блокирует все выявленные угрозы и аномалии.

Карточка угрозы содержит следующую информацию:

- процент уверенности классификатора;
- название и версию файла.exe;
- криптографический алгоритм хеширования SHA256;
- идентификатор процесса - PID;
- имя пользователя, который запустил процесс;
- путь к файлу.exe;
- все действия, сгенерированные угрозой (подробная информация о событиях приведена в подпункте 5.1 настоящей инструкции);
- кнопки управления угрозой: «Заблокировать», «Добавить в разрешенные процессы», «Последние действия процесса» (подробная информация о кнопках управления угрозами приведена в подпункте 5.2 настоящей инструкции).

5.1 Все действия угрозы

При открытии карточки угрозы в интерфейсе отображаются действия угрозы (пять последних действий) с информацией о классе угрозы, классификаторе, который распознал угрозу и времени выполненного действия.

Пользователь имеет возможность проанализировать все действия угрозы, для этого нажмите на кнопку действия процесса.

Действия процесса (Граф процесса) выводят подробную информацию о том, как и от чьего имени был запущен процесс, результаты классификации процесса, все действия процесса - Рисунок 5.

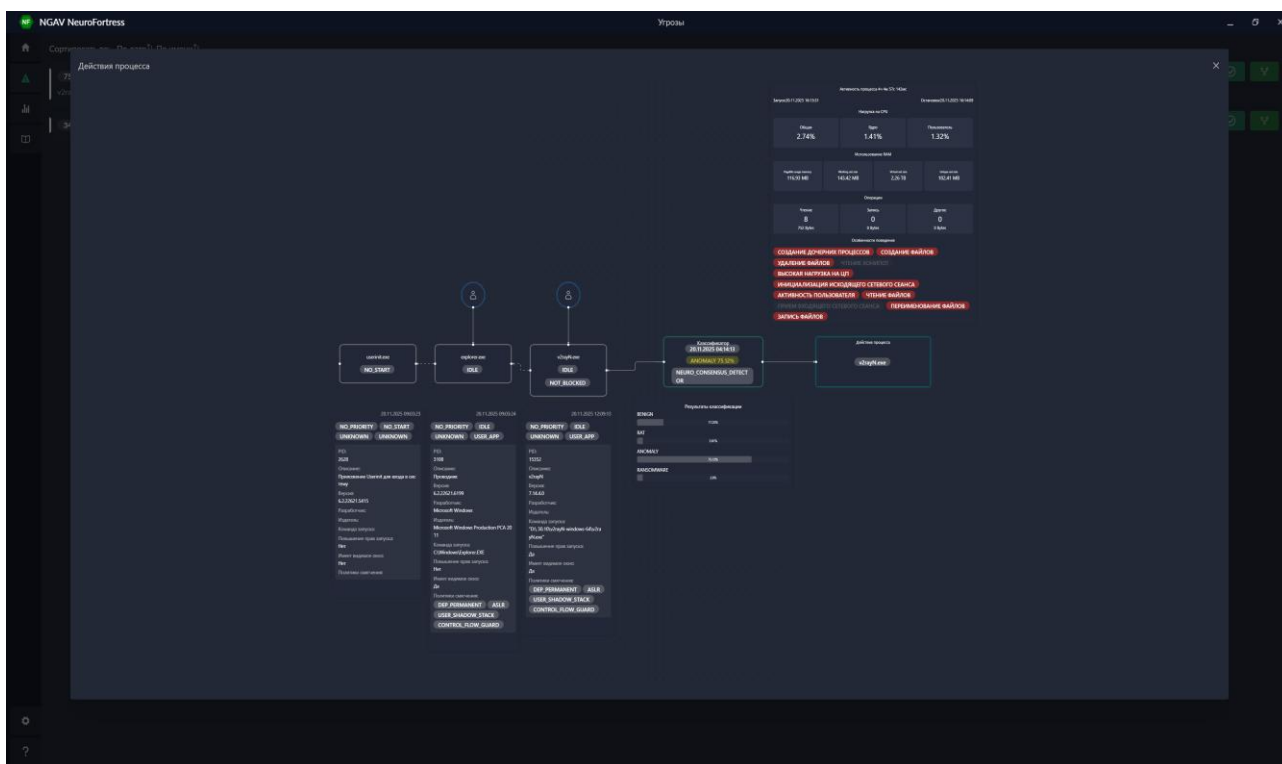


Рисунок 5 – Действия процесса (Граф процесса) НейроФортресс

5.2 Управление угрозами

На экране «Угрозы» расположены кнопки управления «Заблокировать», «Добавить в разрешенные процессы», «Последние действия процесса» Рисунок 6.

Назначение кнопок управления:

- кнопка «Заблокировать» позволяет заблокировать выявленную угрозу со стороны пользователя и добавить ее в «Заблокированные» процессы. Это необходимо для того, чтобы пользователь мог решить доверять данному процессу или нет, при ручной блокировке процесса дальнейшая его классификация не происходит.

- кнопка «Разрешить» позволяет пользователю добавить процесс в «белый список» и не блокировать его при дальнейшем анализе нейросети. Данное действие предусмотрено для стабильной работы программ необходимых пользователю. После добавления процесса в «белый список» его действия будет отслеживаться системой в автоматическом режиме и при подозрительной активности процесс может быть заблокирован повторно.

- кнопка «Действия процесса» - выводят подробную информацию о том, как и от чьего имени был запущен процесс, результаты классификации процесса, все действия процесса - Рисунок 5.

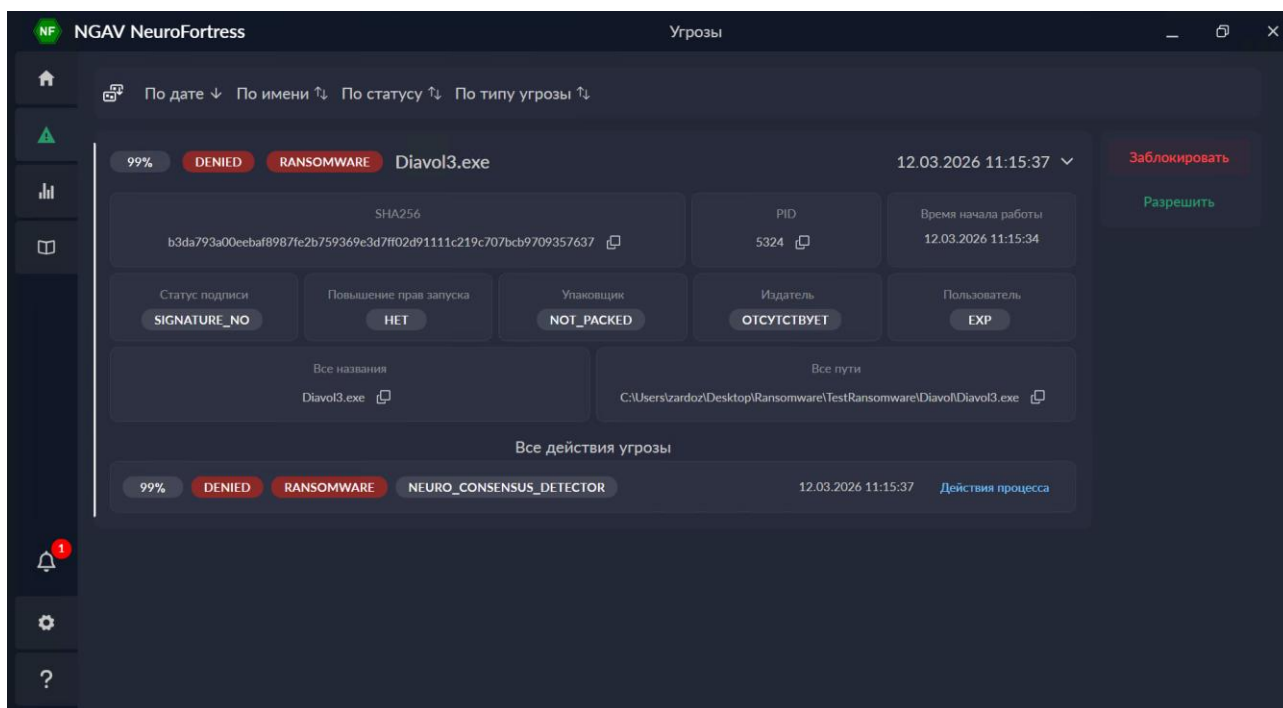


Рисунок 6 – управление угрозами в НейроФортресс

6. Экран статистики НейроФортресс

На экране статистики отображаются два графика - Рисунок 7:

- заблокированные процессы;
- обнаруженные процессы.

График «Заблокированные процессы» выводит информацию о количестве заблокированных процессов и об обнаруженных аномальных процессах, которые требуют принятия решения со стороны пользователя.

График «Обнаруженные процессы» выводит информацию о количестве заблокированных процессов и об обнаруженных аномальных процессах по дням недели.

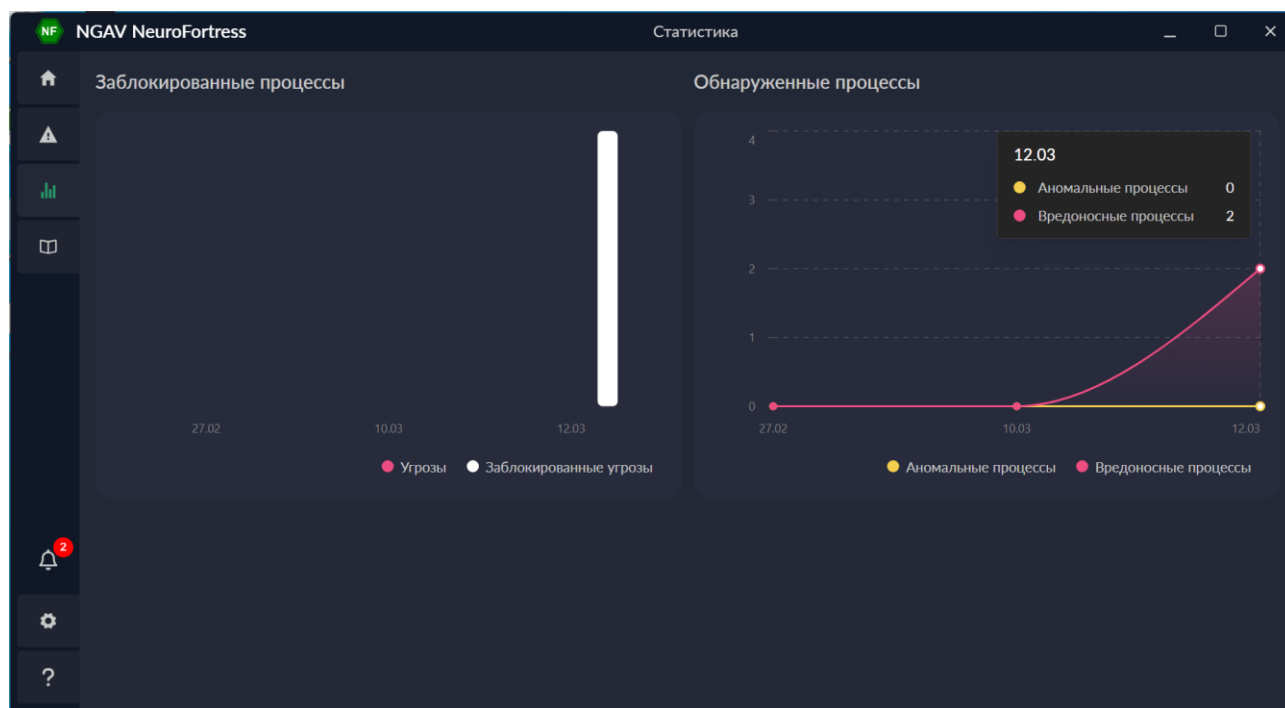


Рисунок 7 – Экран статистики НейроФортресс

7. Экран приложения НейроФортресс

Экран процессов имеет три вкладки «Все», «Разрешенные», «Заблокированные» - Рисунок 8.

Вкладка «Все» содержит информацию о всех обнаруженных и исследуемых процессах на ПК пользователя.

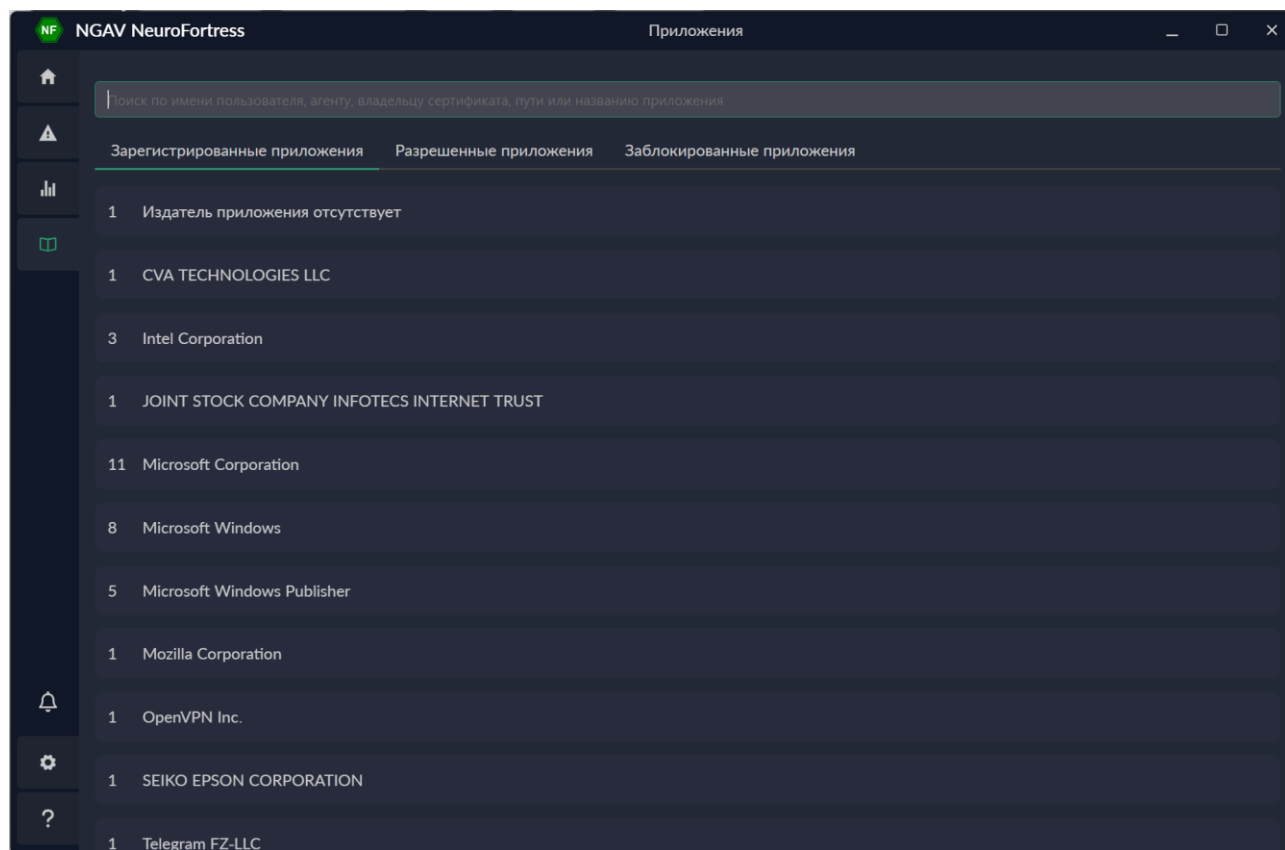


Рисунок 8 – Интерфейс экрана «Приложения» НейроФортресс

Карточка процесса группируется по названию компании издателя сертификата и самому сертификату. Карточка имеет следующую информацию:

- название компании издателя;
- сертификат издателя (срок действия сертификата);
- имя процесса, его версию и время обнаружения;

При выборе определенного процесса отображается следующая информация:

- тип процесса;
- статус упаковщика;

- сигнатура;
- описание;
- имя пользователя;
- имя процесса;
- путь к файлу
- сигнатуры процесса.

Пользователь имеет возможность вручную разрешить все процессы (добавить в Разрешенные), либо заблокировать все процессы (добавить в Заблокированные).

Вкладки «Разрешенные» и «Заблокированные» содержит информацию о процессах, которые разрешены или заблокированы решением пользователя.

8. Настройка НейроФортресс

Настройки НейроФортресс состоят из трех вкладок - Рисунок 9:

- Общие.
- Защита.
- Лицензия.

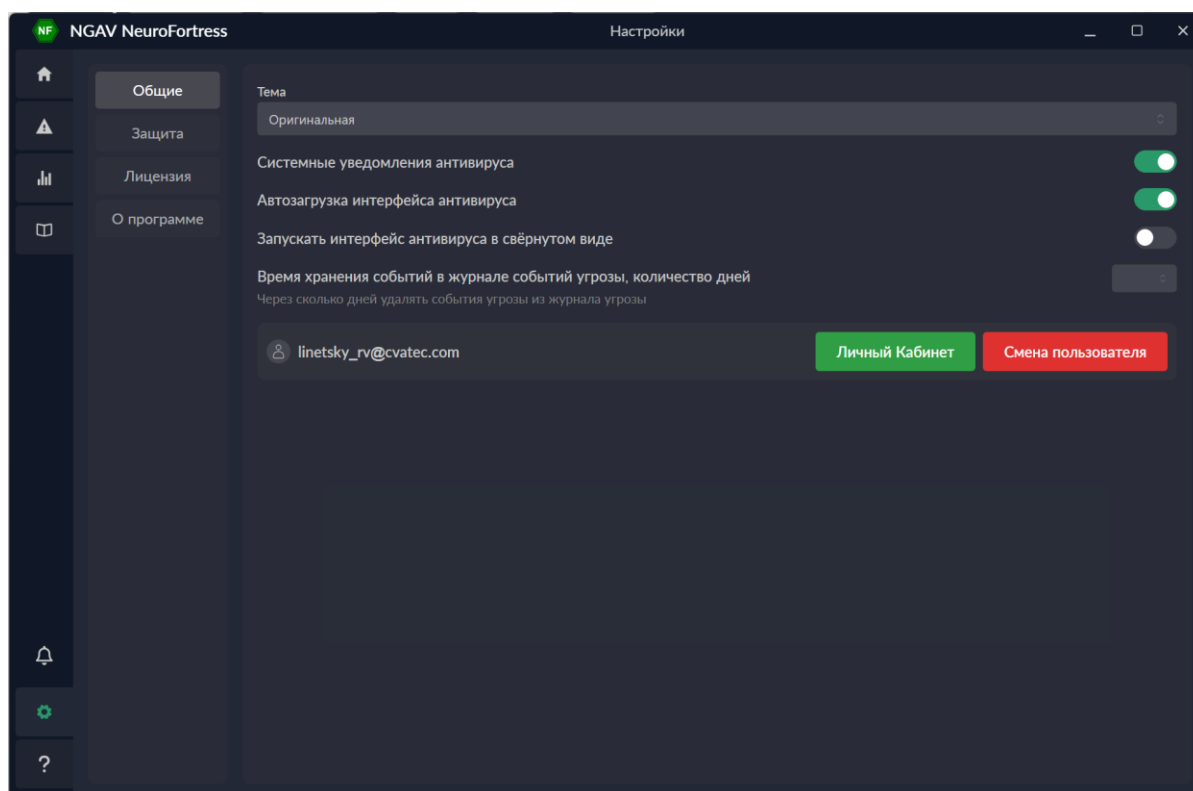


Рисунок 9 – Экран «Настройки» НейроФортресс

8.1 Общие настройки

Вкладка настроек «Общие» содержит три блока. Блок «Язык интерфейса» позволяет выбрать язык интерфейса НейроФортресс.

Блок «Тема» дает пользователю возможность сменить тему оформления интерфейса антивируса.

Третий блок позволяет управлять уведомлениями, поступающими от антивируса и его запуском.

8.2 Настройка защиты

Вкладка настроек «Защита» позволяет выполнить детальную настройку работы НейроФортресс:

- настройка **«Система защиты антивируса»**: - включает модули безопасности, отвечающие за мониторинг поведения процессов, контроль сетевой и файловой активности, обнаружение, анализ и предотвращение запуска вредоносных процессов;

- настройка **«Авто реагирование на вредоносное ПО»**: - включает автоматическое реагирование на обнаруженное вредоносное поведение и блокировку вредоносных процессов без запроса подтверждения пользователя;

- настройка **«Авто реагирование на аномальное ПО»**: - включает автоматическое реагирование на обнаруженное аномальное поведение процессов. Процесс будет заблокирован, если он ведёт себя аномально на протяжении продолжительного интервала времени.

- настройка **«Доверять подписанным процессам»**: - включает автоматическое признание исполняемых файлов, подписанных цифровой подписью издателя, как безопасные. Снижает нагрузку на анализ и уменьшает вероятность ложных срабатываний.

- настройка **«Мониторить поведение только новых процессов»**: - включает наблюдения, при котором система отслеживает поведение исключительно процессов, недавно появившихся в системе, игнорируя уже известные и проверенные программы.

- настройка **«Ограничить мониторинг доверенных процессов»**: - включает параметр, уменьшающий глубину или частоту анализа для программ, признанных безопасными по результатам предыдущего наблюдения. Это повышает производительность без снижения уровня защиты для подозрительных объектов.

- настройка **«Включить систему HoneyPot для выявления вредоносного поведения»**: - активирует скрытые ловушки и приманки в системе, имитирующие уязвимые ресурсы. Их взаимодействие с процессами помогает выявлять вредоносные действия, даже если они маскируются под нормальное поведение.

- вкладка **«Самозащита антивируса»**: - активирует систему самозащиты, предотвращающей несанкционированное удаление антивируса или внесение изменений в его компоненты.

8.3 Лицензия

Вкладка лицензия отображает актуальную информацию о лицензии и ее окончании.

Кнопка «Купить ключ» переводит пользователя на веб-страницу покупки лицензии. После покупки лицензии пользователь может ввести ее в поле для ввода ключа активации лицензии.

9. Техническая поддержка

Контактная информация службы технической поддержки ООО «Сивизй Технолоджиес»:

- Адрес электронной почты: support@neurofortress.ru.