



КИБЕРБЕЗОПАСНОСТЬ

ПРОБЛЕМА БЕЗОПАСНОСТИ

С развитием интернет-технологий наше сообщество: государства, отдельные ячейки инфраструктуры, бизнес и др. сталкиваются с такой проблемой, как **кибертерроризм и киберпреступность**.

Чем быстрее и стремительнее наше сообщество использует информационные технологии, компьютерные системы, автоматизированные системы управления процессами, тем более высока вероятность кибератаки и кибертерроризма.

Отличительной особенностью кибератак является то, что **они нацелены на критически важные узлы инфраструктуры, финансовые узлы экономики, или бизнеса**: нарушить работу трубопровода, нефтеперерабатывающего завода, объектов выработки/транспорта электроэнергии, объектов транспорта.

Кибертерроризм – это преднамеренная, идеологически и политически мотивированная преступная деятельность, осуществляемая в киберпространстве посредством цифровых технологий и направленная против **информации, компьютерных систем, компьютерных программ и баз данных**, а также объектов критической информационной инфраструктуры, которая создаёт угрозу жизни, здоровью людей или наступления других тяжких последствий.

При этом, **кибератаки могут быть направлены на объекты, как виртуальной, так и реальной действительности.**



КАКОЕ РЕШЕНИЕ ПРЕДЛАГАЕТ

RELICTUM PRO BLOKCHAIN?

**ДЛЯ ТОГО ЧТОБЫ ПРЕДОТВРАТИТЬ КИБЕРУГРОЗЫ И ОБОСТРЕНИЕ
ПРОБЛЕМ В КИБЕРПРОСТРАНСТВЕ, МЫ – НАШЕ СООБЩЕСТВО,
ДОЛЖНЫ БЫТЬ НА ШАГ ВПЕРЕДИ!**



РЕШЕНИЕ RELICTUM PRO BLOKCHAIN

RELICTUM PRO BLOKCHAIN ПРЕДЛАГАЕТ НАДЕЖНУЮ И ВЫСОКО ТЕХНОЛОГИЧЕСКУЮ ЗАЩИТУ ДАННЫХ ОТ ВЗЛОМА, ПОХИЩЕНИЯ И УНИЧТОЖЕНИЯ ЦЕННОЙ ИНФОРМАЦИИ.

ПРИНЦИП РАСПРЕДЕЛЁННОЙ СЕТИ МОЖЕТ ПРИМЕНЯТЬСЯ ДЛЯ ЗАЩИТЫ ОТ КИБЕРАТАК И ГАРАНТИРУЕТ БЕЗОПАСНОСТЬ ЗА СЧЁТ УСТОЙЧИВОСТИ КО ВЗЛОМУ

RELICTUM PRO BLOKCHAIN СПОСОБЕН ЗАЩИТИТЬ ПРОЦЕСС ОБМЕНА ИНФОРМАЦИИ – ДЛЯ ЭТОГО РЕАЛИЗОВАН «СЕКРЕТНЫЙ ЧАТ»

ЗАЩИТА ОТ КИБЕРАТАК, ГАРАНТИЯ БЕЗОПАСНОСТИ

Например, если при взломе классической системы хранения данных злоумышленник может получить доступ ко всем десяткам, а то и тысячам объектов, то при взломе децентрализованной блокчейн-системы преступник сможет получить только один фрагмент от общего количества данных, что делает их действия невероятно трудоемкими и невозможными для взлома децентрализованной системы в целом.



ЗАЩИТА ПРОЦЕССА ОБМЕНА ИНФОРМАЦИИ

Всем известны недавние взломы Facebook, Twitter, WhatsApp. Они имеют собственные системы безопасности, но не идут в ногу с новыми технологиями.

А Relictum Pro Blockchain 5.0 идёт на шаг, а в некоторых случаях и на два шага впереди.

Технология Blockchain может децентрализовать сеть, разделить, зашифровать методанные и гарантировать их совокупную безопасность.

РЕШЕНИЯ RELICTUM PRO BLOCKCHAIN



НОВЫЙ ПОДХОД

Системы защиты интернет-серверов баз данных должны не просто успевать развиваться в след за технологиями, а **значительно опережать** их.



ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Применение Relictum Pro Blockchain в сочетании с искусственным интеллектом может использоваться для **фильтрации и идентификации важной информации** и поиска в огромных массивах данных.

БЕЗГРАНИЧНЫЕ ВОЗМОЖНОСТИ

Область применения Relictum Pro Blockchain в кибербезопасности **безгранична** благодаря **надёжности, общедоступности, адаптивности, эффективности и рентабельности**. Использование данной технологии может быть использовано в таких сферах, как финансовые услуги, законодательство, транспортная отрасль или любой другой сферы.



БЕЗОПАСНОСТЬ

Разработка высокотехнологичных механизмов противодействия киберпреступности является первоочередной задачей для крупных предприятий и государства/сообщества в целом.



RELICTUM PRO BLOCKCHAIN ОБЛАДАЕТ ВСЕМИ ВЫШЕПЕРЕЧИСЛЕННЫМИ ХАРАКТЕРИСТИКАМИ, КОТОРЫЕ СМОГУТ ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ ДАННЫХ ЛЮБОЙ СТЕПЕНИ ВАЖНОСТИ НА ВЫСОЧАЙШЕМ УРОВНЕ!