Marketing data

меньше минуты назад

Растущее значение автомобильной кибербезопасности

С развитием интеллектуальных технологий в автомобильной промышленности произошли значительные технологические изменения во всем мире. Эти передовые технологии были интегрированы между собой, что позволило повысить безопасность и удобство, а также обеспечить экономическую эффективность.

Автомобильная промышленность сегодня во многом определяется потребительскими предпочтениями и инновациями. Концепция подключенных транспортных средств подчеркивает разработку транспортных средств с технологиями, которые, среди прочего, обеспечивают связь с другими устройствами, облачным хранилищем и инфраструктурой.

Ожидается, что рост числа подключенных автомобилей увеличит потребность в автомобильной кибербезопасности. Автомобильный рынок кибербезопасность генерироваться доход 1260000000 $ в 2018. Доходы по прогнозам, достигнет 6030000000 $ 2029, растет в среднем на 14,25% в течение прогнозируемого периода, 2019-2029, согласно отчету , рынок разведки Global Automotive Market Кибербезопасность - Анализ и прогноз, 2019-2029 BIS Research.

Факторы, формирующие мировой автомобильный рынок кибербезопасности

Рынок автомобильной кибербезопасности определяется такими факторами, как увеличение числа подключенных транспортных средств, рост киберугроз и увеличение количества электронных компонентов в транспортных средствах.

Все большее число подключенных автомобилей поддерживается растущей проблемы , связанные с безопасностью дорожного движения, увеличивая заторы, и рост спроса на связи транспортных средств , которые привели правительства и производителей автомобилей , чтобы коллективно стимулировать рост подключенных автомобилей. В 2018 году на долю подключенных автомобилей пришлось 44% общего объема производства автомобилей в мире.

Хотя растущие технологические достижения в автомобильной промышленности приводят к ряду инноваций в секторе автономных транспортных средств, они также создают киберугрозу

из-за увеличения данных и подключения транспортных средств. Подключенные транспортные средства считаются частью интегрированной транспортной системы и, как ожидается, будут создавать эффективные, действенные и надежные транспортные системы, использующие данные в реальном времени с пассажирских транспортных средств, коммерческих транспортных средств и транспортной инфраструктуры. Однако вычисленные данные хранятся в транспортном средстве, что всегда сопряжено с риском, связанным с безопасностью и нарушением данных. Это может сделать транспортные средства уязвимыми, так как хакеры могут получить к ним удаленный доступ.

Кроме того, растущее число электронных компонентов в транспортных средствах способствует технологическому прогрессу в автомобильной промышленности, такой как электроника двигателя, трансмиссии и ходовой части, а также помощь водителю, комфорт пассажиров и развлекательные системы. Однако увеличение количества электронных компонентов увеличивает угрозу кибератак, так как многие электронные компоненты связаны друг с другом, что увеличивает сетевое соединение между системами.

Ожидается, что в первые годы прогнозируемого периода увеличение числа подключенных транспортных средств и рост киберугроз окажут большое влияние на отрасль. Тем не менее, ожидается, что влияние со временем уменьшится.

Кроме того, существуют возможности, в том числе расширение масштабов внедрения MaaS и взвода транспортных средств, расширение применения автомобильного облака для хранения и обмена данными и беспроводное обновление программного обеспечения, а также высокий спрос на современные решения в области кибербезопасности с повышенным уровнем автономии, которые могут еще больше повысить рост рынка.

Сегментация мирового рынка автомобильной кибербезопасности

В целях исследования данные, относящиеся к сегментации рынка, включены в отчет. Мировой рынок автомобильной кибербезопасности сегментирован на основе типа продукта, типа транспортного средства и региона.

Сегмент рынка продуктового типа далее сегментируется на систему обнаружения вторжений (IDS) и систему обнаружения и предотвращения вторжений (IDPS). Система IDS отвечает за наблюдение трафика за вредоносными действиями и действиями, нарушающими правила, тогда как система IDPS отвечает за выявление уязвимых мест в потоке сети для предотвращения различных типов возможных атак.

Сегмент IDPS является лидером на мировом рынке автомобильной кибербезопасности, на его долю приходится около 80% всего рынка в 2018 году, и ожидается, что он сохранит свое доминирующее положение в течение прогнозируемого периода. Это в основном связано с преимуществами IDPS по сравнению с IDS, такими как предотвращение уязвимостей, блокирование внешних кодов, обеспечение нулевых ложных срабатываний, отсутствие необходимости подключения, незначительное влияние на производительность и отсутствие необходимости обновления антивирусных программ.

Сегментация типов транспортных средств на рынке кибербезопасности была разделена на пассажирские и коммерческие транспортные средства. Пассажирские транспортные средства включают в себя подключенные и автономные автомобили и робо-такси, а коммерческие транспортные средства включают в себя тяжелые грузовики и тяжелые автобусы. Сегмент пассажирских транспортных средств в настоящее время доминирует на мировом рынке

автомобильной кибербезопасности с долей 74,51% от общего рынка в 2018 году и, по прогнозам, сохранит свое доминирование в течение прогнозируемого периода. Тем не менее, прогнозируется, что сегмент коммерческого транспорта будет расти с более высоким CAGR в течение прогнозируемого периода с 2019 по 2029 год. Некоторые из факторов, влияющих на рост рынка, включают широкомасштабное внедрение взвода транспортных средств, растущий спрос на надежную логистику и увеличение количества подключенных и автономных коммерческих транспортных средств.

В региональном разрезе рынок был сегментирован на Северную Америку, Европу, Азиатско-Тихоокеанский регион и остальные страны мира. Азиатско-Тихоокеанский регион (APAC) в настоящее время доминирует на мировом рынке автомобильной кибербезопасности, предоставляя 44,32% от общей доли рынка в 2018 году. Кроме того, ожидается, что APAC продолжит доминировать на рынке в течение прогнозируемого периода.

Ссылка на статью: Растущее значение автомобильной кибербезопасности