ПРОБЛЕМЫ КИБЕРЗАЩИТЫ ОБЪЕКТОВ ИНФРАСТРУКТУРЫ ГОСУДАРСТВА

В.Н. Корделюк

Тенденции цифровой трансформации общества (в том числе в Республике Беларусь) показывают все большее внедрение автоматизированных, автоматических систем, реализующих сетевые информационные технологии по управлению технологическими процессами. Интернет был и остается основным каналом возможного воздействия на указанные системы в связи с все большим сопряжением технологических сетей и корпоративных информационных сетей.

Повсеместное функционирование объектов вооруженных сил, промышленности, транспорта, энергетики, электросвязи, здравоохранения и систем жизнеобеспечения с автоматизированными системами управления ставит в прямую зависимость национальную безопасность в различных сферах жизнедеятельности от их надежности и защищенности. При этом вскрывается пропорциональная зависимость – чем глубже интеграция автоматизированных систем управления в киберпространство, тем критичнее для данных объектов результаты активного воздействия извне на их информационные ресурсы [1].

В отличие от информационных сетей, где последствия реализации угроз (утечка информации, блокирование информации, ее несанкционированное уничтожение) имеют больше нематериальный характер, ущерб в сфере управления технологическими процессами в большинстве своем имеет непосредственную физическую форму (отключение электроэнергии, прекращение подачи воды, срыв работы телекоммуникационных сетей, аварии на железнодорожном, авиационном транспорте и т.д.).

Действия в киберпространстве позволяют наносить ущерб дистанционно (анонимно), не нарушая физических границ его государства. Возрастает важность кибербезопасности критически важных объектов инфраструктуры государства.

Список литературы

1. Концепция информационной безопасности Республики Беларусь: утв. Постановлением Совета Безопасности Республики Беларусь 18.03.2019 № 1.

ЗАЩИТА УДАЛЕННОЙ ПОЛЬЗОВАТЕЛЬСКОЙ СТАТИСТИКИ С ПОМОЩЬЮ МЕХАНИЗМОВ ДИФФЕРЕНЦИАЛЬНОЙ ПРИВАТНОСТИ

Е.А. Криштопова

Автоматический сбор данных с пользовательских устройств (персональных компьютеров, смартфонов, фитнес-браслетов и т.п.) дает возможность сборщикам собрать информацию о конкретном пользователе – его предпочтениях, привычках, состоянии здоровья, режиме дня и т.д.

Например, для «анонимизированного» статистики просмотров пользователями фильмов компании Netflix, исследователи показали, что информацию о конкретных пользователях можно восстановить и предсказать их политические взгляды [1].

Вышесказанное делает важным задачу анонимизации пользовательской статистики. Технически это решается использованием механизмов дифференциальной приватности.

Дифференциальная приватность (Differential privacy - DP) – это совокупность методов, которые обеспечивают максимально точные запросы в статистическую базу данных при одновременной минимизации возможности идентификации отдельных записей в ней. Дифференциальная приватность дает математическое определение потери конфиденциальных данных отдельных лиц, путем внесения случайности, описываемой переменной ε, когда их личная информация используется для создания продукта.

Наиболее известны практические реализации локальных дифференциально-приватных алгоритмов: RAPPOR от Google, решения Apple для iOS 10, Microsoft’s PINQ, Uber’s FLEX.