БЕЗОПАСНОСТЬ И СЛОЖНОСТЬ УПРАВЛЕНИЯ СОВРЕМЕННЫМИ ТЕХНИЧЕСКИМИ СИСТЕМАМИ УПРАВЛЕНИЯ

Гусев С.С.

Институт проблем управления им. В.А. Трапезникова РАН

Аннотация: в докладе рассматривается безопасность современных сложных систем управления и методы управления ими. Приводится один из важных факторов безопасности сложных систем управления, таких как защита конфиденциальной информации в современных системах управления. Так для защиты конфиденциальной информации приводится генератор шумов ГШ-2500, предназначенный для защиты объектов вычислительной техники.

Ключевые слова: сложные системы управления, безопасность сложных систем, вычислительная техника, конфиденциальная информация, теория управления.

Безопасность современных сложных технических систем управления является на сегодняшний день одним из острых вопросов в управлении. Ведь сам процесс управления сложными техническими системами и безопасность его актуальны как никогда и очень важны в современной науке. Безопасность современных сложных технических систем управления – один из важных факторов защиты, будь то защита конфиденциальной информации, охраняемых объектов, находящихся под наблюдением охранно-пожарных систем, систем видеонаблюдения, систем контроля управления и доступом (СКУиД), интеллектуальных систем, автоматизированных систем управления технологических процессов управления (АСУ ТП) и ряда других систем. Все перечисленные выше системы по своей совокупности представляют сложные технические системы управления. В теории управления безопасность сложных технических систем управления представляет собой надежность и наличие защищенности системы управления в целом.

Для каждой современной сложной технической системы управления можно сформировать алгоритм, отвечающий заданным начальным условиям с определенными параметрами или иными словами, отвечающий определенным требованиям в управлении. То есть необходимым и достаточным условием является наличие программного обеспечения (ПО).

Большинство современных сложных технических систем управления на стадии разработки оборудовано определенным ПО, необходимым для решения конкретных задач в управлении современных сложных технических систем управления. Они, как правило, поставляются в комплекте вместе с техническим оборудованием. Однако, встречаются случаи, когда оборудование необходимо оснастить специальными техническими средствами, модулями и программным обеспечением, например, с целью защиты конфиденциальной информации от посторонних людей, с доступом секретно, совершенно секретно или особой важности, в зависимости от важности обеспечения доступа к информации. Тут встает вопрос о хранении и доступе к архивным данным информационных систем (ИС) в управлении современными сложными техническими системами, их безопасности и конфиденциальности. ИС обеспечиваются необходимым ПО для безопасного хранения данных современных сложных технических систем. Сложность управления современными сложными техническими системами определяется сложностью ПО, поставляемого вместе с ИС. Не только доступ к определенной конфиденциальной информации определяет важность самой информации, но и программное обеспечение, которое поставляется вместе с информационными системами, определяет защиту информации и безопасность современных сложных технических систем управления. Следует подчеркнуть, что ИС, как и ПО сложны по своей структуре и архитектуре, что усложняет безопасность современных сложных технических систем управления, а также процесс управления ими.

В промышленности важную роль в управлении технологическим процессом играют промышленные контроллеры, с помощью которых организуется процесс управления, а также безопасность современных сложных технических систем управления. Принцип действия промышленных контроллеров заключается в управлении промышленным производством на предприятии, часто на заводах с помощью ПО, которым они обеспечены. Как правило, промышленные контроллеры используются в станках с ЧПУ, на

конвейерных линиях для обеспечения безопасности управления сложного технического и технологического процессов на предприятии. Безопасности отводится важная роль в управлении, будь то станком с ЧПУ, конвейерной линии или управления предприятием или промышленным производством в целом.

Безопасность современных сложных технических систем управления не нова и методы управления ею заложены еще в XX столетии. Обеспечение безопасности современных сложных технических систем управления, как было сказано ранее, обусловлено наличием информационных систем и программного обеспечения, с помощью которого обеспечена защита персональных данных, данных об объекте управления, сложных технических систем управления. Бурное развитие информационных систем получило свое развитие вначале 80-х годов XX века. Информационные технологии (ИТ) стремительно развиваются и на сегодняшний день они заняли свою определенную нишу в управлении сложными системами. Этот процесс развития ИТ стал необратимым и уже сейчас на их базе создаются автономные системы в управлении, которые позволяют самостоятельно обучаться и управлять физическими процессами сложных систем. Роль ИТ такова, что управление сложными системами без их участия уже невозможна. Предсказание поведения процессов, событий неотъемлемо связано с ключевой ролью участия ИТ [1]. Информационные технологии совершенствуются, как по своим параметрам, так и по своей структуре.

Как было сказано ранее, в докладе рассматривается безопасность современных сложных технических систем управления. Сопоставим безопасность сложных систем управления с доступностью конфиденциальной информации. Чем выше уровень защиты информации, тем более высокая безопасность требуется для таких систем. Однако безопасность систем информации бывают разными – могут рассматриваться от безопасности современных технических простых систем управления [2] до сложных автоматизированных систем управления. А требования к защите

информации могут оставаться одинаковыми. Логично предположить, что чем сложнее система, тем более высокие требования предъявляются к ней для ее же безопасности.

Довольно часто для защиты конфиденциальной информации используют генераторы шумов (ГШ). Так популярным считается использование ГШ-2500, разработанного, производимого и поставляемого ФГУП СКБ ИРЭ РАН. Генератор шума ГШ-2500 предназначен для защиты объектов вычислительной техники первой, второй и третьей категорий секретности от утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН) путем формирования и излучения в окружающее пространство электромагнитного поля шума (ЭМПШ) и путем наведения маскирующего сигнала в отходящие цепи в диапазоне частот от 0,1 до 2000 МГц. Генератор шума формирует маскирующее электромагнитное поле и в диапазоне частот ниже 0,1 МГц (до 10 кГц). Уровни спектральной плотности шума в диапазоне частот от 0,01 до 0,1 МГц не нормируются.

Один ГШ-2500 обеспечивает маскировку (защиту) информации устройств вычислительной техники, размещенной в помещении площадью примерно 40 м^2. Отличительной особенностью ГШ-2500 является использование рамочной антенны для создания пространственного зашумления.

Необходимость применения генераторов шума для создания систем активной защиты конфиденциальной информации, обрабатываемой средствами вычислительной техники, вызвана, как правило, недостаточными размерами контролируемой зоны вокруг указанных средств. Мы рассмотрели вопрос генерации шума для защиты конфиденциальной информации современных сложных технических систем управления. Однако остался нерассмотренный до конца вопрос безопасности современных сложных технических систем управления. Перейдем к нему для завершения написания статьи на данную тему.

Проблема безопасности современных сложных технических систем управления актуальна на сегодняшний день и вопрос как было сказано ранее стоит остро в безопасности таких систем. Прежде всего, безопасность таких систем обусловлена информационной базой для поддержания необходимого уровня доступа к информации. Уровень доступа, как было описано ранее, имеет определенные ограничения к соответствующему классу объектов управления. Класс объекта определяется технической сложностью самого объекта – системы управления. Поэтому необходимым и достаточным условием будет являться информативность оператора, обслуживающего определенный объект управления, как правило, современный сложный технический объект управления.

В заключении стоит отметить, что всегда найдется ряд сдерживающих факторов, которые будут наложены на объект управления, откуда будет ясна проблема безопасности сложного современного технического объекта управления и необходимые и возможные пути решения к ней. Таким образом, будет определяться уровень доступа к данным, степень их защиты и их безопасность, и возможные рычаги управления ими – данными.

Список использованных источников

1. Гусев С.С. *Роль информационных технологий в управлении сложными системами* // «Интерактивная наука». 2016. № 8. С 59-61.

THE SAFETY AND COMPLEXITY OF MODERN COMPLEX TECHNICAL CONTROL SYSTEMS

Gusev S.S.

Russia, V.A. Trapeznikov Institute of control sciences of RAS

Abstract: the report discusses the safety of modern complex control systems and methods of managing them. Is one of the important factors in safety of complex control systems, such as the protection of confidential information in modern control systems. So, for the protection of confidential information is a noise generator GN-2500, designed for protection of objects of computing.

Keywords: complex system control, security, complex systems, computer technology, confidential information, control science.