

*Махлин Борис Михайлович, студент 2 курс магистратуры, кафедра
«Железнодорожная автоматика, телемеханика и связь», Российский
университет Транспорта (МИИТ), Россия, г. Москва*

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

Аннотация: Статья посвящена проблеме обеспечения информационной безопасности систем управления технологическими процессами критически важных объектов. Автор раскрывает новые угрозы для государственной безопасности и описывает способы их избежать. На основе анализа исторических событий, сформированных в мировом сообществе решений и их практической результативности, определяется наиболее действенный способ обеспечения информационной безопасности государства.

Ключевые слова: вирусы, информационная безопасность, доверенная платформа, киберпространство.

Abstract: The article is devoted to the problem of ensuring information security of process control systems for critical facilities. The author reveals new threats to state security and describes ways to avoid them. Based on the analysis of historical events formed in the global community of decisions and their practical effectiveness, the most effective way to ensure the information security of the state is determined.

Key words: viruses, information security, trusted platform, cyberspace.

Развитие и использование информационных технологий в современном мире, дало возможность их применения во всех сферах деятельности общества. Способы их интеграции постоянно расширяются, принося не только новые возможности, но и подвергая риску появления новых угроз. За последние годы, во всём мире появилось и получило быстрое распространение кибероружие, обладающее возможностью использования вне зависимости от существующих границ государств.

Во множестве стран ведётся разработка технологии кибернетических атак, отличающихся скрытностью и эффективностью, позволяя нарушать функционирование производственных и технологических процессов предприятий, компаний, вплоть до ответственных систем жизнеобеспечения городов, не оставляя при этом улик. Возможность использовать кибернетические атаки связана с наличием уязвимостей в управляющих и информационно-коммуникационных системах, чем атакующая сторона и пользуется, проникая и захватывая данные системы под свой контроль [2].

Параллельно с техникой атак, развивается промышленный и политический шпионаж. Во всём мире растёт количество операций, использующих киберпространство, направленных на кражу информации либо нарушение и остановку работы объектов инфраструктуры различных стран.

Прародителем таких атак, принято считать компьютерные вирусы, которые также используют программные уязвимости, но эффект от них не настолько деструктивен, и в большинстве случаев отсутствует необходимая избирательность действий. Однако, современная тенденция подключения всё большего количества систем к сети Интернет, позволяет использовать вирусы более качественно, за счёт расширения их возможностей. Например, связав вирус с центром управления, появится возможность проводить атаки и взлом систем «на лету», используя уязвимости в программном обеспечении. Подобное развитие вирусов стало понятно после успешной хакерской атаки с помощью вирусного червя Stuxnet, занесённого в систему управления, который

позволил в 2010 году нарушить работу центрифуг на иранских ядерных объектах.

Это послужило появлению методологии Advanced Persistent Threat (APT), которая включает в себя различные методы проникновения в единую систему и даёт возможность проводить эффективные хакерские атаки самых разных объектов. Таким образом, это означает повышенный риск нарушения работы, вплоть до полной остановки важнейших структур правительства, армии, городских служб, что может вызвать экономический коллапс и панику среди населения.

Для исследования способов обеспечения информационной безопасности, был проведён анализ наиболее крупных АСУ ТП Российских и зарубежных предприятий. Выяснилось, что в большинстве случаев, разработанные частными компаниями программные продукты – проприетарны, а значит имеют закрытый исходный код. Как показывает статистика, в них содержится большее число уязвимостей и недокументированных возможностей, при этом у конечного пользователя отсутствует возможность исследования исходного кода таких продуктов в связи с его закрытостью поставщиком продукции.

Помимо атак на программные продукты, потенциальную угрозу представляет системное и прикладное программное обеспечение, а именно – внутренние функции, к которым у пользователей отсутствует прямой доступ. В качестве примера можно привести процессор, и специализированное ПО, входящее в состав чипов Trusted Platform Module, сервисных управляющих модулей BMC (контроллер управления основной платой) – встроенный в платформу автономный микроконтроллер, а также современных интеллектуальных сетевых адаптеров. Провести полноценный аудит функций данных модулей производителям проприетарных операционных систем и прикладного программного обеспечения крайне сложно, а делать это конечному потребителю на практике не представляется возможным.

Использование операционной системы с закрытым и не исследованным исходным кодом, различных компонентов и модулей, с закрытой

документацией, таких как BIOS и пр., ставит под сомнение обеспечение безопасности информации, как при обработке, так и при хранении данных. В том случае, если информация об исходном коде и документации стала доступна для исследования, это станет решением проблемы. Зачастую современные системы сложны, как с аппаратной, так и в программной части, и только разработчику известен весь функционал. Гарантирование безопасности возможно, если всю систему разрабатывает одна команда разработчиков и каждый этап работ сопровождается тщательным исследованием исходных кодов и документации [1]. Такое решение обеспечивает только доверенная вычислительная платформа и это то, к чему нужно стремиться.

Решение вопросов об обеспечении информационной безопасности, после появления Stuxnet, было также взято на государственный уровень. Информационная безопасность АСУ ТП критически важных объектов (КВО) обозначена в руководящем документе Совета Безопасности РФ «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» [3]. Появление документа показывает, что руководящим органам РФ понятна вся актуальность существующей проблемы.

Данный документ включает в себя меры, направленные на поддержку отечественных разработок в области информационной безопасности и импортозамещение. Практически, это единственный выход, позволяющий гарантировать полностью свободное от уязвимостей, закладок и других средств изменения функционирования системы оборудование. Используя импортное оборудование, таких гарантий дать нельзя.

Россия обладает собственными аппаратными и программными разработками, позволяющими строить и развивать полностью доверенные системы. Сегодня они применяются как в военной, научной и др. «закрытой» отраслях, так и в «открытой» гражданской, и являются тем ключом, обеспечивающим безопасность и надёжность систем АСУ ТП.

Библиографический список:

1. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. – М.: МГТУ им. Н. Э. Баумана, 2016. – 252 с.
2. Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности. – Санкт-Петербург: Питер, 2017. – 256 с.
3. Указ Президента РФ №803 от 03.02.2012. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. – 2012 [Электронный ресурс]. КонсультантПлюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_150730/7c1a2b6c9f1f4bc7a522adfbb02b613651b3e175/ (дата обращения: 03.10.2019).