Вопросы обеспечения защищенности информации при её обработке в автоматизированных системах управления

И.В. Машкина
Факультет информатики и робототехники
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: mashkina.vtzi@gmail.com

И.Р. Гарипов
Факультет информатики и робототехники
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: ildar.garipov.92@mail.ru

Аннотация[1]

В данной статье приведены итоги анализа проблем обеспечения информационной безопасности автоматизированных системах управления технологическими процессами, списки основных уязвимостей современных автоматизированных систем управления технологическими процессами и перечень основных угроз информационной безопасности, отмеченных в реальных инцидентах. Представлен список ряда отраслевых решений, стандартов и рекомендаций как отечественных так и зарубежных, предлагаемых для использования в ходе разработки систем обеспечения информационной безопасности на промышленных предприятиях. Данные, представленные в этой статье, позволяют реально оценить положение дел в области обеспечения информационной безопасности автоматизированных систем управления технологическими процессами.

1. Введение

Современные информационные технологии сегодня активно используются в промышленности, позволяя автоматизировать производство, что в свою очередь дает возможность промышленным предприятиям повысить свою эффективность. Для организации управления производственными мощностями используются автоматизированные системы управления технологическими процессами.

Автоматизированная система управления технологическими процессами (АСУ ТП) – это совокупность программных и технических средств, используемых для автоматизации управления технологическим оборудованием на промышленных предприятиях. Эти системы позволяют сотрудникам промышленных предприятий оперативно и удаленно производить контроль над производственными процессами при помощи систем сбора данных о технологических процессах и систем управления агрегатами, задействованными в этих процессах.

2. Публикация

Материалы конференции публикуются оргкомитетом, как в бумажном варианте, так и в виде электронного издания.

2.1. Текст доклада

В то время, когда АСУ ТП впервые стали внедрятся, они представляли из себя изолированные автоматизированные системы и функционировали на базе узкоспециализированного оборудования. На тот момент задача обеспечения информационной безопасности АСУ ТП на промышленных предприятиях решалась путем использования организационных методов. Со временем подходы к разработке и построению АСУ ТП изменились. Развитие современных технологий привело к тому, что в современных системах управления для сокращения расходов на разработку и внедрение часто стали использоваться широко распространенные операционные системы, сетевое оборудование и сетевые протоколы, которые имеют недостатки в виде уязвимостей.[1]

Наличие уязвимостей в широко распространенных операционных системах и протоколах передачи данных, используемых в современных промышленных системах, привело к тому, что для нынешних АСУ ТП стали актуальны угрозы нарушения информационной безопасности, присущие современным информационным системам. АСУ ТП некоторых современных промышленных предприятиях для обеспечения удобного взаимодействия с бизнес-приложениями, организации быстрого и защищенного обмена данными без использования внешних носителей и налаживания удаленного контроля интегрируются в состав корпоративных информационных систем. Такой подход несет за собой некоторые преимущества, но он так же приводит и к

Труды Шестой всероссийской научной конференции "Информационные технологии интеллектуальной поддержки принятия решений", 28-31 мая, Уфа-Ставрополь, Россия, 2018

повышению рисков нарушения информационной безопасности АСУ ТП, так как в корпоративном сегменте сети могут присутствовать компьютеры, подключенные к внешним сетям, например к интернету. Конечно, в АСУ ТП критически важных объектов (КВО) такой подход является редкостью, так как потеря контроля над этими системами может привести к необратимым последствиям, например выходу из строя критически важных объектов инфраструктуры государства. Сам подход к безопасности АСУ ТП КВО весьма жестко регламентируется различными регулирующими органами государственной власти и нормативно-правовой документацией.

В современном мире АСУ ТП получили широкое распространение и используются на производственных площадках промышленных предприятий, на электростанциях, на водозаборных и очистительных сооружениях, на заводах по переработке и хранению нефти, газа, угля и других энергоносителей, руды, полезных ископаемых и драгоценных металлов, предприятиях пищевой, фармацевтической и химической промышленности, в некоторых городских телекоммуникационных системах, на объектах коммунального хозяйства и во многих других областях. Автоматизация производственных процессов прочно закрепилась на своих позициях в современном мире.

Почему вопрос обеспечения информационной безопасности АСУ ТП на сегодня стоит так остро? Интерес к проблеме безопасности промышленных систем появился после того как стало известно об инцидентах, связанных с компьютерными вирусами Stuxnet, Flame и Duqu, атаковавшими иранские ядерные объекты, государственные учреждения и промышленные объекты Китая, Индии и некоторых других стран.[2] Ранее считалось, что АСУ ТП сами по себе являются сложными для взлома системами в связи с использованием специфичного оборудования и программного обеспечения, однако с приходом современных технологий все изменилось.

Статистика, предоставленная ICS-CERT (Industrial Control Systems Cybersecurity Emergency Response Team) на конец 2016 года, свидетельствует о том, что количество инцидентов информационной безопасности, зафиксированных в период с начала 2014 по конец 2016 года, велико, поэтому проблема обеспечения информационной безопасности промышленных систем является актуальной на сегодняшний день.[3]

Информация, циркулирующая в информационных системах промышленных предприятий, является коммерческой тайной, а если предприятие обслуживает государственные интересы - государственной тайной. Информация может иметь высокую ценность и должная подлежать защите.

Конкуренция между производителями различной продукции зачастую приводит к недобросовестным методам борьбы за рынки сбыта. В целях экономии средств и времени, которые требуется затратить, чтобы догнать конкурента, занимающего лидирующее положение, либо не допустить в будущем отставания от конкурента, если тот разработал или разрабатывает новую перспективную технологию, а также чтобы выйти на новые для предприятия рынки, конкурирующие предприятия могут прибегать к промышленному шпионажу [4], и в этом направлении работают профессионалы высокого уровня.

Киберпреступность не стоит на месте, так как с каждым днем появляются новые средства, используемые для реализаций атак на промышленные объекты. Обнаруженные злоумышленниками уязвимости в информационных системах используются для кражи данных, их модификации, нарушения их целостности, зачастую это приводит к нарушению доступности информации для авторизированных пользователей. Несанкционированный доступ к промышленным системам управления, который зачастую могут получить злоумышленники, а также неправомерные действия, производимые злоумышленниками, направленные на нарушение нормальной работы информационно-управляющей системы предприятия, зачастую приводят к отказу промышленного оборудования, что в свою очередь может привести к необратимым последствиям, например авариям на производстве или техногенным катастрофам.

Существует такой термин как кибервойна. В ряде стран существуют специализированные подразделения - кибервойска, деятельность которых направлена на выведение из строя инфраструктуры, будь то гражданская или военная, на стороне потенциального противника.[2]

К основным уязвимостям современных АСУ ТП эксперты относят [5,6]:

- отсутствие или слабая защита от несанкционированного доступа к системам автоматизированного управления (пароли, персональные идентификаторы);
- недекларированные возможности SCADA - систем (систем диспетчерского управления и сбора данных);
- использование беспроводных коммуникаций (незащищенные беспроводные соединения);
- отсутствие должного контроля управляющих воздействий;
- отсутствие чётких границ между разными сегментами сети (к примеру между корпоративными и промышленными);

- использование дистанционных методов управления (возможно по незащищенным каналам связи);
- несвоевременное или некорректное обновление программного обеспечения;
- отказ от минимальных мер безопасности (так как, нередко ради удобства и производительности компании отказываются от установки не только, например, антивирусной, но и даже парольной защиты критически важных активов);
- распространение Windows в качестве основной операционной системы для рабочих станций и даже для серверов;
- Web-технологии, используемые на верхнем уровне АСУ ТП (если таковые используются, к примеру в HMI).

Утечке информации на промышленных предприятиях также может поспособствовать человеческий фактор. Сотрудники предприятий могут совершать ошибки в ходе профессиональной деятельности непреднамеренно, но также могут целенаправленно производить неправомерные действия, направленные на создание каналов утечки информации, в том случае если были подкуплены. Ошибки персонала могут привести к появлению уязвимостей, которые в дальнейшем могут быть использованы злоумышленниками или нарушителями - самими сотрудниками для реализации атак на промышленные системы.

Ниже представлен перечень основных угроз информационной безопасности АСУ ТП, отмеченных в реальных инцидентах:[2]

- атаки на узлы управления;
- атаки на SCADA - системы;
- атаки на программируемые логические контроллеры (PLC) с использованием уязвимостей самих PLC (пароль по умолчанию, неавторизованный доступ к фирменному программному обеспечению, удалённое изменение пароля и т.д.);
- атаки на инфраструктуру информационно-управляющей системы промышленного предприятия (вирусы, троянские программы, черви, DoS- и DDos-атаки, ARP-спуфинг - перехват трафика после объявления себя маршрутизатором);
- атаки с использованием уязвимостей протоколов, используемых в информационно-управляющей системе предприятия (OPC - переполнение буфера, уязвимости протоколов TCP/IP);
- атаки на базы данных промышленных систем (несанкционированный доступ, SQL инъекции).

Реализация перечисленных выше угроз может привести к необратимым последствиям, таким как:

- отказ промышленного оборудования (неправильная работа оборудования, отказ системы управления и т.д.);
- техногенные катастрофы (аварии на производстве);
- человеческие жертвы (среди сотрудников и гражданского населения);
- экологические катастрофы (загрязнение окружающей среды);
- материальные и финансовые потери для предприятия или государства.

На сегодня, в области защиты информации в системах управления (АСУ ТП ,Control Systems, SCADA) существует целый ряд отраслевых решений, стандартов и рекомендаций как отечественных так и зарубежных, например таких как:[6]

- стандарты NERC для систем управления электрическими сетями;[7]
- стандарты ChemITC для химической индустрии;[8]
- Cisco SAFE for PCN;[9]
- ISA S99 - Комитет общества приборостроения, системотехники и автоматизации (ISA); [10]
- NIST PCSRF Security Capabilities Profile for Industrial Control Systems; [11]
- IEC 61784-4; [12]
- КСИИ ФСТЭК (Приказ №31 от 14.03.2014 г.). [13]

Выше перечисленные зарубежные отраслевые решения и стандарты рекомендуется использовать при разработке и внедрении промышленных систем. Создание систем с учетом лучших мировых практик разработки автоматизированных систем и программных кодов в безопасном исполнении может значительно повысить уровень защищенности корпоративных систем.

Для обеспечения высокого уровня информационной безопасности на промышленных предприятиях необходимо использование организационных и технологических (программных и программно-аппаратных средств защиты информации) мер. Организационные и технические меры защиты информации, реализуемые в автоматизированной системе управления в рамках ее системы защиты, в зависимости от класса защищенности, угроз безопасности информации, используемых технологий и структурно-функциональных характеристик автоматизированной системы управления и особенностей ее функционирования, должны обеспечивать [13]:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность автоматизированной системы управления и информации;
- доступность технических средств и информации;
- защиту среды виртуализации;
- защиту технических средств и оборудования;
- защиту автоматизированной системы и ее компонентов;
- безопасную разработку прикладного и специального программного обеспечения;
- управление обновлениями программного обеспечения;
- планирование мероприятий по обеспечению защиты информации;
- обеспечение действий в нештатных (непредвиденных) ситуациях;
- информирование и обучение персонала;
- анализ угроз безопасности информации и рисков от их реализации;
- выявление инцидентов и реагирование на них (управление инцидентами);
- управление конфигурацией автоматизированной системы управления и ее системы защиты.

4. Заключение

В заключение можно сказать, что на сегодняшний день существует не мало методов защиты информации с использованием различных программных и программно-аппаратных средств защиты информации, не стоит забывать, что они корректно будут выполнять свои функции только при правильной настройке и эксплуатации. Помимо средств защиты на предприятиях должны быть использованы и организационные меры, соответствующие требованиям правовых регуляторов и внутренних нормативных документов, таких как: политика безопасности, служебные предписания и должностные инструкции для сотрудников, регулирующих обеспечение защиты информации. Необходимо и четкое распределение доступа по ролям для персонала.

Сегодня перед научным сообществом в документе "Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации"[14], утвержденном Президентом РФ 03.02.2012 N 803, поставлены определенные задачи в области развития фундаментальной и прикладной науки, технологий и средств обеспечения безопасности.[2]

Вопрос информационной безопасности АСУ ТП по прежнему актуален, так как промышленность постоянно развивается, каждый год разрабатываются и внедряются новые средства автоматизации, в которых также могут присутствовать недостатки в виде уязвимостей, с каждым днем появляются новые угрозы и атаки, бороться с которыми необходимо. Работать в этой области еще есть над чем. Необходимо разрабатывать стратегии обеспечения информационной безопасности на предприятиях по отраслям, учитывая их специфичность.

Acknowledgments

Оргкомитет благодарит РФФИ за содействие в проведении конференции.

Список используемых источников

1. Сафрошкин О. Ю., Защита АСУ ТП // Информационная безопасность, Москва, 2014, с. 18-19.
2. Пищик Б.Н., Безопасность АСУ ТП // Компьютерные технологии, Новосибирск: Институт вычислительных технологий Сибирского отделения РАН, 2013, том 18, с. 170-175.
3. ICS-CERT (Industrial Control Systems Cybersecurity Emergency Response Team). Доступно on-line: https://ics-cert.us-cert.gov/, дата обращения 21.03.2018.
4. Пилиджан Крейг, Мелтон Кит, Свиержинский Дуэйн. Промышленный шпионаж. 2013 г. Доступно on-line: http://lifeinbooks.net/chto-pochitat/ofisnyiy-shpionazh-kreyg-pilidzhan-kit-melton-dueyn-svierzhinskiy/, дата обращения 21.03.2018.
5. Воронцов А.Н., Автоматизированные системы управления технологическими процессами // Вопросы безопасности: информационная бюллетень компании “Инфосистемы Джет”. Информационная безопасность промышленных объектов. Доступно on-line: http://www.jetinfo.ru/stati/asu-tp-voprosy-bezopasnosti, дата обращения 21.03.2018.

6. Лукацкий А. Стандарты безопасности АСУ ТП // Cisco Systems, Москва, 2012. с. 5-15, Доступно on-line: http://www.slideshare.net/ CiscoRu/ss-8690963, дата обращения 21.03.2018.
7. The North American Electric Reliability Corporation (NERC). Доступно on-line: http://www.nerc.com, дата обращения 21.03.2018.
8. The Chemical Information Technology Center (ChemITC®). Доступно on-line: https://chemitc.americanchemistry.com/, дата обращения 21.03.2018.
9. Cisco. Доступно on-line: http://www.cisco.com, дата обращения 21.03.2018.
10. ISA Industrial Automation and Control Systems Security. Доступно on-line: https://www.isa.org/isa99/, дата обращения 21.03.2018.
11. NIST National Institute of Standards and Technology. Доступно on-line: https://www.nist.gov/, дата обращения 21.03.2018.
12. International Electrotechnical Commission. Доступно on-line: http://www.iec.ch/, дата обращения 21.03.2018.
13. Приказ ФСТЭК №31 от 14.03.2014 г., // Доступно on-line: http://fstec.ru/normotvorcheskaya/ akty/53-prikazy/868-prikaz-fstek-rossii-ot, дата обращения 21.03.2018.
14. "Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации" (утв. Президентом РФ 03.02.2012 N 803). Доступно on-line: http://www.consultant.ru/document/cons_doc_LAW_150730/, дата обращения 21.03.2018.