УДК 004.056 + 004.7 Вестник УрФО № 1(27) / 2018, с. 77–83

Вотинов М. В.

ТЕОРЕТИЧЕСКИЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ФУНКЦИОНИРОВАНИЯ ПРОМЫШЛЕННЫХ КОМПЛЕКСОВ С ЦЕЛЬЮ УЛУЧШЕНИЯ ИХ ЭКСПЛУАТАЦИОННЫХ ХАРАКТЕРИСТИК В ЧАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Работа посвящена актуальным вопросам обеспечения защиты информации, обрабатываемой в промышленных комплексах на критически важных и потенциально опасных объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей природной среды. В работе на примере программно-аппаратного комплекса малогабаритной сушильной установки, содержащего в себе не только систему автоматического управления технологическим процессом, но и средства удалённого доступа и мобильного контроля в рамках концепции Промышленного интернета вещей (IIoT), выделены уровни обработки информации, показано определение класса защищённости, и соответствующего набора мер защиты информации, которым должен соответствовать комплекс согласно руководящим документам ФСТЭК России. Представлена реализация определённых мер защиты информации, направленная на повышение общего уровня безопасности технологического процесса.

Ключевые слова*: защита информации, информационные системы, вычислительные сети.*

THEORETICAL ANALYSIS AND STUDY OF THE OPERATION OF INDUSTRIAL COMPLEXES WITH THE AIM OF IMPROVING THEIR PERFORMANCE IN TERMS OF INFORMATION SECURITY

The work is devoted to topical issues of ensuring the protection of information processed in the industrial complexes on the critical and potentially dangerous objects, representing an increased danger to life and health of people and the natural environment. In the example hardware-software complex of small dryer, which contains not only the automatic control system of technological process, but remote access tools and mobile control in the framework of the concept of Industrial Internet of things (IIoT), dedicated levels of information processing, shows the definition of the class of security, and relevant set of information protection measures, which must conform to the complex in accordance with the guiding documents of the FSTEC of Russia. Are the implementation of certain security policies aimed at improving the overall security of the process.

Keywords: *information security, information systems, computer network.*

Введение

С развитием вычислительной техники и технологий все большее количество сфер жизнедеятельности человека подвергается информатизации. Сейчас практически вся информация тем или иным способом хранится и обрабатывается в рамках компьютерных информационных систем с использованием информационных технологий. Мы находимся на пороге времени, когда все больше услуг начинает предоставляться в электронном виде. Стремимся к полной информатизации своей деятельности. Уже невозможно представить отрасль хозяйства, где бы не использовались информационные технологии и информационные системы.

Информатизация общества активно поддерживается и на правительственном уровне. Так, Министерством связи и массовых коммуникаций РФ разработана государственная программа «Информационное общество», которая предполагает, что к 2020 году 85 % населения России будет пользоваться услугами в электронном виде.

Однако развитие информационных технологий порождает вопросы, связанные с защитой информации. Действительно, когда большая часть информации «оцифрована», содержится и обрабатывается в информационных системах, всегда будет существовать круг лиц, заинтересованных в её использовании в своих корыстных целях.

В связи с этим параллельно развитию информационных технологий развивается и система нормативно-правовых документов по обеспечению защиты информации. Система основывается на Конституции Российской Федерации, федеральных законах, нормативной базе органов исполнительной власти, государственных отраслевых стандартах и так далее. В частности, Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» регламентирует права субъекта персональных данных, обязанности оператора системы по обработке персональных данных. Закон РФ от 21 июля 1993 г. № 5485-I «О государственной тайне» регламентирует перечень сведений, составляющих государствен-

ную тайну, защиту государственной тайны, а также контроль и надзор данной сфере.

Вопросы защиты информации охватывают не только конкретные виды информации, но и являются приоритетными при рассмотрении безопасности страны в целом. Так, Указом Президента России от 5 декабря 2016 г. № 646 утверждена доктрина информационной безопасности Российской Федерации, представляющая собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

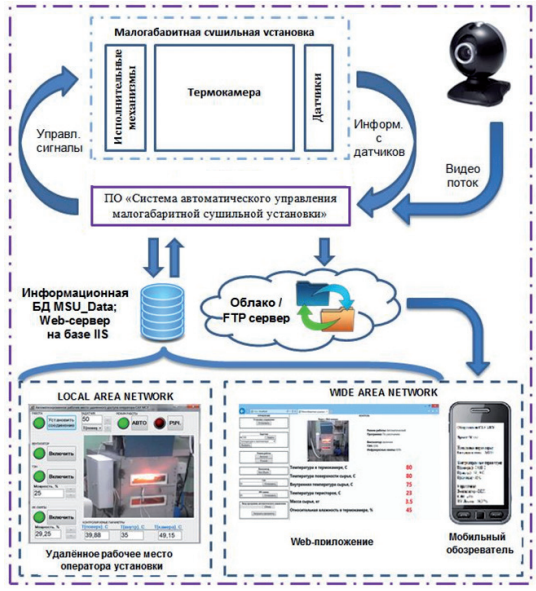
В общем случае обеспечение безопасности представляет собой комплекс мероприятий, начиная от прогнозирования угроз безопасности, их анализа и оценки и заканчивая их выявлением и ликвидацией.

Вместе с тем, помимо классических информационных систем, включающих в себя базу данных и клиентское программное обеспечение, например: автоматизированная система управления кадровыми ресурсами (АСУКР), автоматизированная система управления предприятием (АСУП), сайт в сети интернет, – в которых довольно просто определить вид хранящейся информации и необходимую степень защиты информации, существует отдельный класс систем, до недавнего времени не в полной мере охваченный требованиями по защите информации. Речь пойдёт о промышленных комплексах, в состав которых входят автоматизированные системы управления технологическими процессами.

Следует понимать, что промышленные комплексы также являются источниками информации. Обеспечение информационной безопасности таких комплексов, в зависимости от того, какую важность и опасность представляют они собой для жизни и здоровья людей и окружающей природной среды, является актуальной на сегодняшний день задачей, как и привитие будущим специалистам (студентам и магистрантам) понимания того, что не достаточно построить информационную систему, создать автоматизированную систему управления технологическим процессом, проложить вычислительную сеть, необходимо ещё в полной мере задуматься над вопросами защиты обрабатываемой в них информации.

Описание используемого комплекса

В учебно-экспериментальном цехе Мурманского государственного технического университета функционирует программно-аппаратный комплекс для тепловой обработки рыбного сырья (сушка, вяление, копчение рыбы). Комплекс представлен малогабаритной сушильной установкой [1] и содержит в себе не только систему автоматического управления технологическим процессом, но и оснащён в рамках концепции IIoT современными средствами удалённого доступа и мобильного контроля собственной разработки, позволяющими в режиме реального времени по телекоммуникационным каналам связи отслеживать проводимый технологический процесс [2]. Общая структурная схема комплекса приведена на рисунке.



Информационные потоки программного комплекса

Программная часть комплекса позволяет организовывать удалённый доступ и управление технологическим процессом по локальной сети с использованием программного обеспечения «Удалённое рабочее место оператора установки» (ПО «АРМ»), а также по глобальной сети с использованием Web-приложения. Мониторинг параметров технологического процесса возможен с любого мобильного устройства (мобильные телефоны, планшетные компьютеры и так далее) с использованием разработанного мобильного обозревателя.

Вместе с тем, в составе программной части комплекса находится Web-камера, которая передаёт видео поток во все используемые средства и, тем самым, позволяет визуализировать протекающий технологический процесс находящемуся на удалении операто-

ру-технологу или преподавателю, контролирующему ход выполнения лабораторной работы.

В состав аппаратной части комплекса входит оборудование отечественного производителя автоматики, фирмы «ОВЕН», центробежный вентилятор, инфракрасные лампы, трубчатые электронагреватели, датчики температуры и влажности.

Подробно останавливаться непосредственно на реализации комплекса не будем, отметив только то, что аппаратная и программная части комплекса сведены воедино программным обеспечением «Система автоматического управления малогабаритной сушильной установкой» (ПО «САУ МСУ»). Данное программное обеспечение выполняет функции системы автоматики, обеспечивая управление технологическим процессом с помощью исполнительных механизмов на основании информации с датчиков, а также обеспечивает функционирование средств удалённого доступа и мобильного контроля, работая с информационной базой данных MSU_Data и передавая информацию о технологическом процессе через FTP-сервер на мобильный обозреватель системы. Таким образом, можно с уверенностью сказать, что в составе комплекса функционирует как система автоматического управления, так и классическая информационная система, состоящая из базы данных и клиентских средств удалённого доступа и мобильного контроля.

По представленной схеме функционируют многие промышленные комплексы, взять, к примеру, работающие под управлением TRACE MODE Data Center или использующие для удалённого управления беспроводные системы связи стандарта GSM, выпускаемые фирмами Овен, Siemens, MOXA, TELEOFIS.

Использование средств, обеспечивающих удалённый доступ к промышленным комплексам, управление технологическим процессом или просто его мониторинг, приводит к возникновению рисков утечки информации и негативным последствиям на сложных технологических операциях.

Федеральной службой по техническому и экспортному контролю (ФСТЭК России) принят приказ № 31 от 14 марта 2014 г., утверждающий требования по обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных и потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей природной среды [3].

Приказ не содержит положений, устанавливающих обязательную аттестацию автоматизированных систем управления производственными и технологическими процессами [4], однако игнорировать его требования крайне не целесообразно.

Хотя малогабаритная сушильная установка и не является критически важным производством, для неё был обеспечен ряд требований в соответствии с руководящими документами ФСТЭК.

Определение мер по защите информации

Системы автоматического управления, обеспечивающие функционирование потенциально опасных производств и технологических процессов относятся к ключевым системам информационной инфраструктуры [4]. Для таких систем мероприятия по обеспечению защиты информации подразумевают определение актуальных угроз безопасности информации, формирование базовой модели угроз и нарушителей, а также определение мер защиты информации.

Нормативные документы, касающиеся ключевых систем информационной инфраструктуры носят закрытый характер и не находятся в общем доступе в сети «Интернет», однако, в состав нашего комплекса входят информационные системы в виде средств удалённого доступа и мобильного контроля. Таким образом, для обеспечения их защиты вполне возможно, по крайней мере, в образовательных целях, пользоваться нормативными документами, регламентирующими обеспечение защиты информационных систем общего пользования.

Что касается мер защиты информации непосредственно систем автоматического управления, то они регламентированы приказом ФСТЭК России № 31 от 14 марта 2014 г. и зависят от класса защищённости. Выделяется три класса защищённости К1-К3. Отнесение программно-аппаратного комплекса к тому или иному классу зависит от уровня значимости обрабатываемой информации.

В малогабаритной сушильной установке можно выделить три уровня обработки информации:

– нижний уровень, на котором обрабатывается информация с датчиков и формируются управляющие сигналы для исполнительных механизмов;

– средний уровень, на котором осуществляется функционирование ПО «САУ МСУ»;

– верхний уровень, на котором осуществляется функционирование средств удалённого доступа и мобильного контроля.

Для определения класса защищённости комплекса необходимо для каждого уровня обработки определить уровень защищённости информации, ориентируясь по оценке возможной степени ущерба для целостности, доступности и конфиденциальности обрабатываемой информации.

Так как технологические процессы, протекающие в малогабаритной сушильной установке, не попадают под определение «критически важных», то для всех свойств безопасности информации были определены низкие степени ущерба, и, как следствие, определён третий, самый низкий уровень значимости информации, обрабатываемой на всех уровнях исследуемого программно-аппаратного комплекса.

Третьему уровню значимости информации соответствует третий класс защищённости системы автоматического управления малогабаритной сушильной установки. Согласно определённому классу защищённости в соответствии с приложением № 2 приказа ФСТЭК России № 31 от 14 марта 2014 г. был выявлен состав мер защиты информации, которые необходимо реализовать для защиты рассматриваемого программно-аппаратного комплекса.

Состав мер защиты информации в системах автоматического управления включает в себя двадцать положений, каждое из которых разбито на несколько пунктов, выбор которых зависит от класса защищённости системы.

Важно понимать, что программно-аппаратный комплекс малогабаритной сушильной установки действует на территории учебно-экспериментального цеха, а его средства удалённого доступа и мобильного контроля отчасти интегрированы в вычислительную сеть университета. Поэтому некоторые меры защиты информации, как то антивирусная защита, обновление базы данных признаков вредоносных компьютерных программ, контроль доступа лиц в помещение цеха изначально были реализованы.

Анализ мер защиты информации заставил серьёзно подойти к вопросам идентификации, аутентификации пользователей, управления доступом к программной части комплекса. В частности, в ПО «САУ МСУ» и ПО «АРМ» были интегрированы механизмы парольной защиты, налажена система рангов доступа, при которой операторы-технологи, студенты и разработчики имеют различные права при работе и обслуживании комплекса. Так, полные права доступа имеют разработчики комплекса, операторы-технологи могут помимо технологического процесса, управлять настройками архивирования информации, студентам доступны только основные функции по ведению технологического процесса.

Доступ к рабочей станции, на которой установлены программные модули системы, также осуществляется с применением политики учётных записей пользователей, позволяя ограничивать их права и возможности при работе в операционной системе, в частности, это позволяет уменьшить риски, связанные с установкой неразрешённого программного обеспечения.

Доступ к управлению технологическим процессом по средствам Web-приложения осуществляется по закрытым каналам связи по протоколу Secure Socket Layer (SSL).

Помимо стандартной регистрации событий, которая осуществляется операционной системой MS Windows, в программной части комплекса реализована регистрация событий безопасности в системе автоматики малогабаритной сушильной установки. Регистрируются возможные случаи отказа датчиков, необоснованное повышение рабочих температур в силовом блоке установки, выход температуры технологического процесса за рамки допустимого коридора. В случае возникновения ошибок происходит срочное информирование персонала, работающего за малогабаритной сушильной установкой и, при необходимости, останов технологического процесса. Регистрация событий необходима для проведения дальнейшего анализа инцидентов, в том числе определения источников и причин возникновения инцидентов, а также оценки их последствий 3.

В целях обеспечения целостности и доступности информации в рамках определённых мер защиты информации осуществляется с помощью бесплатного программного обеспечения xStarter периодическое резервное копирование программных модулей на резервные машинные носители информации.

Немаловажную роль в обеспечении информационной защиты программно-аппаратного комплекса играют организационные

меры. В частности, целесообразно проводить информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты программно-аппаратного комплекса, о возможных нештатных ситуациях и необходимых действиях при их возникновении.

Стоит отметить, что организационные меры по своей значимости не уступают остальным, так как только грамотное поведение персонала в нештатных ситуациях позволяет существенно снизить на потенциально опасных объектах риски, связанные с повышенной опасностью для жизни и здоровья людей и окружающей природной среды.

Заключение

Таким образом, на примере программно-аппаратного комплекса малогабаритной сушильной установки была выполнена реализация мер по защите информации в соответствии с регламентирующими документами ФСТЭК России.

Установка не является критически важным или потенциально опасным объектом, не требует проведения аттестации на соответствие требованиям по защите информации, однако включает, помимо системы автоматического управления, средства удалённого доступа и мобильного контроля, которые делают её уязвимой в плане утечки информации, стороннего вмешательства в технологический процесс, что может привести к негативным последствиям.

Согласно ГОСТ Р 51898-2002 «Аспекты безопасности»: Безопасность – отсутствие недопустимого риска. В этой связи, выполнение мер по защите информации позволило поднять общий уровень безопасности разработанного программно-аппаратного комплекса, снизив вероятность возможных недопустимых рисков, тем самым улучшив его эксплуатационные характеристики.

Практика применения мер по защите информации согласно третьему классу защищённости показала, что поднять уровень информационной безопасности возможно средствами самой операционной системы и используемого программного обеспечения. Вместе с тем, вопросами обеспечения защиты таких комплексов необходимо заниматься ещё на этапе их разработки и внедрения, предусматривая выполнения некоторых мер в рамках уже действующих на предприятиях и организациях системах защиты информации.

Практическая направленность работы состоит во внедрении её результатов не только в технологический, но и в учебный процесс при подготовке студентов и магистрантов по специальности «Автоматизация технологических процессов и производств» для углубления знаний в области защиты разрабатываемых ими систем автоматического управления.

Литература

1. Пат. 135234 Рос. Федерация, МПК A 23 B 4/03. Малогабаритная сушильная установка / Вотинов М. В. ; заявитель и патентообладатель ФГОУВПО «Мурм. гос. техн. ун-т». – № 2013132112/13 ; заявл. 10.07.13 ; опубл. 10.12.13, Бюл. № 34. – 2 с. : ил.

2. Вотинов М.В. Оснащение систем автоматического управления современными информационными средствами удалённого доступа и мобильного контроля // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2017. – Т. 17, № 2. – С. 141–148.

3. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

4. Информационное сообщение ФСТЭК России от 25.07.2014 № 240/22/2748 «По вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

References

1. Pat. 135234 Ros. Federaciya, MPK A 23 V 4/03. Malogabaritnaya sushil'naya ustanovka / Votinov M. V. ; zayavitel' i patentoobladatel' FGOUVPO «Murm. gos. tekhn. un-t». – № 2013132112/13 ; zayavl. 10.07.13 ; opubl. 10.12.13, Byul. № 34. – 2 s. : il.

2. Votinov M.V. Osnashchenie sistem avtomaticheskogo upravleniya sovremennymi informacionnymi sredstvami udalyonnogo dostupa i mobil'nogo kontrolya: Vestnik YUUrGU. Seriya «Komp'yuternye tekhnologii, upravlenie, radioehlektronika». – 2017. – T. 17, № 2. – S. 141–148.

3. Prikaz FSTEC Rossii ot 14.03.2014 № 31 «Ob utverzhdenii Trebovanij k obespecheniyu zashchity informacii v avtomatizirovannyh sistemah upravleniya proizvodstvennymi i tekhnologicheskimi processami na kriticheski vazhnyh ob»ektah, potencial'no opasnyh ob»ektah, a takzhe ob»ektah, predstavlyayushchih povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudej i dlya okruzhayushchej prirodnoj sredy» .

4. Informacionnoe soobshchenie FSTEC Rossii ot 25.07.2014 № 240/22/2748 «Po voprosam obespecheniya bezopasnosti informacii v klyuchevyh sistemah informacionnoj infrastruktury v svyazi s izdaniem prikaza FSTEC Rossii ot 14 marta 2014 g. № 31 «Ob utverzhdenii trebovanij k obespecheniyu zashchity informacii v avtomatizirovannyh sistemah upravleniya proizvodstvennymi i tekhnologicheskimi processami na kriticheski vazhnyh ob»ektah, potencial'no opasnyh ob»ektah, a takzhe ob»ektah, predstavlyayushchih povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudej i dlya okruzhayushchej prirodnoj sredy».

ВОТИНОВ Максим Валерьевич, ФГБОУ ВО «Мурманский государственный технический университет», доцент кафедры автоматики и вычислительной техники, кандидат технических наук. 183010, г. Мурманск, ул. Спортивная, 13. E-mail: votinovmv@yandex.ru

VOTINOV Maksim, FSEI HE «Murmansk state technical university», docent of department of Automatic and Computer Engineering, PhD. 183010, Murmansk, Sportivnaya street, 13. E-mail: votinovmv@yandex.ru