# Информационная безопасность в АСУТП – основная проблема при использовании Web-технологий в задачах автоматизации

Е.В. Егоров, М.В. Зайцев (ООО "ЭФО")

*Двадцать лет назад в России находилось немного людей, способных ответить на вопрос: «Что такое Internet?» Тем более, мало кто мог предположить, что этот «зверь» будет доступен каждому, что развитие промышленности во многом будет зависеть от уровня развитости Internet-технологий. Сегодня мир Internet и информационных технологий охватывает все аспекты нашей жизни. Построенная для этого глобальная инфраструктура связи уязвима для различных атак. Угрозы кибератак на любом уровне, тем более и на уровне объектов АСУТП с каждым годом вызывают все большее беспокойство не только специалистов, но и различные государственные структуры. Сейчас уже многие понимают, что последствия кибератак для командно-управляемых систем автоматики могут оказаться особенно разрушительными. Цель статьи - не просто констатировать существующие проблемы, но и привлечь внимание читателей к проблемам информационной безопасности в АСУТП.*

*Ключевые слова: Internet, информационные системы, безопасность, кибератака, системы автоматизации, Web-технологии.*

Web-технологии стали неотъемлемой частью нашей жизни и работы, их использование уже принесло грандиозное расширение возможностей и сулит еще большее в будущем. Это утверждение в полной мере применимо к интеграции Web-технологий и автоматических систем управления производством.

В феврале 2009 г. в журнале "Автоматизация в промышленности" был опубликован небольшой обзор [1], в котором предполагалось, что использование инфраструктуры публичных сетей передачи данных для решения задач удаленного мониторинга и управления обладает исключительной привлекательностью, так как позволяет сэкономить огромные средства на построении физической сети передачи как таковой. Так оно и вышло — внедрения диспетчерских систем и систем автоматики с применением Web-технологий пошли лавиной, соответствующие публикации были, в том числе и в нашем журнале — ссылок не приводим, чтобы не перегружать изложение списком литературы, желающие легко найдут информацию о подобных внедрениях в своей области с помощью все тех же Web (Internet)-технологий. В том же обзоре было сделано предположение, что основную специфику и главную проблему при внедрении Web-технологий для решения задач автоматизации и диспетчеризации ТП составят вопросы контроля доступа и обеспечения информационной безопасности. Так оно и получилось на самом деле. Принято считать, что первой серьезной кибератакой на системы технологического управления явилась история с вирусом Stuxnet, появившегося в 2010 г. и наиболее прославившегося выводом из строя центрифуг ядерного центра в Иране [2]. Этот случай, однако, далеко не первый. Например, еще в августе 2005 г. все заводы Daimler-Chrysler в США были вынуждены остановить сборочные конвейеры из-за проникновения в сеть незамысловатого вируса Zotob, видимо, с зараженного ноутбука кого-то из сервисных инженеров. В 2003 г. вирус Slammer блокировал диспетчерскую систему на АЭС Дэвис-Бесс в штате Огайо (США). Управляющий сервер диспетчерской системы был недоступен на протяжении 6 часов! По счастью, вирус не затронул тогда систем управления РВ, и технологических сбоев, которые могли бы потребовать вмешательства операторов, не случилось.

Список примеров этим не исчерпывается. Stuxnet получил особую известность лишь потому, что на сегодня это единственный пример вредоносного ПО, по всей видимости, специально созданного для атаки конкретного объекта, остальные случаи связаны с проникновением в сеть обычных неспециализированных Internet-червяков (ясно, что от этого не легче). Ненаучно-фантастические произведения на эту тему, правда, появились много ранее: в 2004 г. некие Рид и Швайцер издали в США книгу под названием "Над бездной: холодная война глазами участника", в которой изложили вполне бредовую историю о взрыве в 1982 г. газопровода в Уренгое с помощью секретного кода, заложенного в нелегально поставленное ПО АСУТП станции газоперекачки и приведенного в действие командой по каналу телеуправления. Это очевидная байка потому что, во-первых, не очень понятно, какие именно каналы телеуправления могли быть в этом случае задействованы, а во-вторых и в главных, оригинальные специализированные программно-аппаратные комплексы для АСУТП насосных станций прекраснейшим образом разрабатывались и производились в самом СССР и совершенно непонятно, зачем надо было закупать что-то из этого в Америке, тем более нелегально. Тем не менее сам факт сочинения такой сказки показателен и говорит о том, что в определенных кругах идея носится в воздухе, причем со времен, много предшествующих повсеместному распространению публичной сети Internet. Поэтому угроза совершенно реальна и для защиты от нее необходимо принимать целый комплекс мер и отслеживать современные тенденции в этой области; в противном случае возможны серьезные финансовые потери, «утечка» конфиденциальной информации, парализация работы предприятия и нанесение ущерба окружающей среде.

В свете изложенного не кажется удивительным, что проблемой занялись на самом высоком уровне. 4 июля 2012 г. на сайте Совета Безопасности появил-

ся интересный документ — "Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ". В самом начале документа написано, что эти направления разработаны в целях реализации основных положений Стратегии национальной безопасности РФ, в соответствии с которой одним из аспектов обеспечения информационной безопасности страны является совершенствование защиты информационных и телекоммуникационных систем критически важных объектов инфраструктуры. Документ этот написан грамотно — беглый анализ показывает, что в нем охвачены все ключевые темы, в том числе и требования к разработчикам АСУТП. Видимо, характер регулируемой темы в условиях засилья западных решений вызывает серьезное беспокойство и заставляет пересмотреть сложившуюся практику пренебрежительного отношения к ПО технологических систем.

Банально, но для начала определим, что представляет собой типовая АСУТП. Для этого откроем «Справочник инженера по АСУТП» Ю. Н. Федорова.

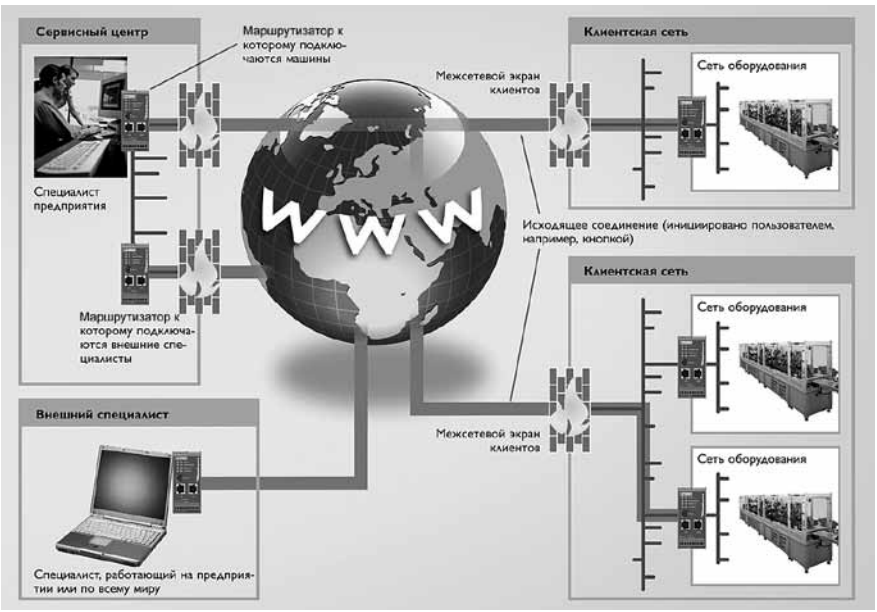
Все производственные АСУТП обычно строятся по трехуровневому принципу.

Нижний уровень (полевой уровень, field) АСУТП представляет собой различные датчики (сенсоры) и исполнительные механизмы.

Средний уровень (уровень контроллеров) состоит из ПЛК, принимающего полевые данные и выдающего команды управления на нижний уровень. Управление в ПЛК осуществляется по заранее разработанному алгоритму, который исполняется циклически (прием данных — обработка — выдача управляющих команд).

Верхний уровень — это визуализация, диспетчеризация (мониторинг) и сбор данных. На этом уровне задействован человек, то есть оператор (диспетчер). Если он осуществляет контроль локального агрегата (машины), то для его осуществления используется так называемый человеко-машинный интерфейс. Если оператор осуществляет контроль за распределенной системой машин, механизмов и агрегатов, то для таких диспетчерских систем часто применим термин SCADA (Supervisory Control And Data Acqusition — диспетчерское управление и сбор данных) В обоих случаях верхний уровень АСУТП обеспечивает сбор, а также архивацию важнейших данных, поступающих от ПЛК, их визуализацию, то есть наглядное (в виде мнемосхем, часто анимированных) представление на экране существо и параметры происходящего процесса. При получении данных система самостоятельно сравнивает их с граничными параметрами (уставками) и при выходе за границы уведомляет оператора с помощью тревог. Оператор, который для начала работы должен авторизоваться (зарегистрироваться), запускает ТП, имеет возможность остановить его полностью или частично, может изменить режимы работы агрегатов (изменяя уставки) и т. п. При этом система записывает все происходящее, включая действия оператора, обеспечивая "разбор полетов" в случае аварии или другой нештатной ситуации. Тем самым обеспечивается персональная ответственность управляющего оператора.

Важнейшим элементом АСУТП являются сети, по которым передаются данные и команды управления. Часто нижний и средний уровни АСУТП объединяются «полевой шиной», которая представляет собой сеть с гарантированным временем доставки пакетов, что позволяет создать распределенную систему управления, работающую в режиме РВ. Приложения на верхнем уровне АСУТП обычно не требуют работы в режиме РВ, поэтому компьютеры здесь связаны между собой сетью Ethernet, что позволяет АСУТП легко интегрировать с системами управления уровня АСУ предприятия, отправляя производственные данные в БД предприятия.




*Концепция применения межсетевых экранов при удаленном управлении*

В настоящее время многие производители оборудования КИПиА, то есть того оборудования, которое устанавливается на нижнем уровне, имеют возможность комплектовать свои датчики не только полевыми шинами, но и протоколами более высокого уровня, например, Ethernet. Тем самым данные нижнего уровня могут быть доступны на верхнем уровне и даже на уровне АСУ предприятия. С одной стороны это существенно упрощает процесс разработки АСУТП, а с другой — заставляет разработчиков систем предусматривать допол-

нительные меры защиты от внешнего вмешательства в пределах системы автоматики и сохранения целостности данных. Для этого, как правило, применяются межсетевые экраны, позволяющие разделить сети АСУТП от общепроизводственных сетей, создаются виртуальные сети (VPN) (рисунок). В некоторых случаях, на особо ответственных и опасных производствах АСУТП функционируют отдельно, будучи отделены физически от основных сетей.

Но технологии не стоят на месте, а вместе с ними увеличиваются запросы заказчиков, которые хотят иметь возможность удаленно мониторить производственные процессы через общедоступные каналы связи, в том числе и Internet. Большинство современных программируемых контроллеров имеют в своем составе встроенные Web-серверы, на которых можно разрабатывать собственные страницы, отражающие состояние процесса в виде мнемосхем, примерно так же, как их представляют в SCADA-системах. Многие панели оператора (ЧМИ) также обладают такими ресурсами. Применение подобного оборудования существенно расширяет возможности удаленного управления. Одним из главных достоинств такого подхода, кроме универсальности связи с ПЛК, был отказ от использования SCADA-систем. Web-сервер в данном случае содержится в контроллере, который подключен непосредственно к сети Internet. Содержащийся в контроллере сопроцессор осуществляет формирование необходимых HTML-страниц и связывает их с данными, поступающими с объекта. Однако в данном случае основная тяжесть работы по обработке данных ложится на плечи самого контроллера, который вынужден уже кроме первичной обработки данных осуществлять и вторичную обработку, что может потребовать применения гораздо более мощного процессора ПЛК, чем в случае работы без Web-сервера. Существует возможность снизить загрузку процессора ПЛК за счет применения Java-апплетов, которые будут осуществлять вторичную обработку данных уже на компьютере-клиенте. С помощью штатного встроенного ПО контроллеров можно создавать мнемосхемы как на полноценной SCADA-системе. У них существует даже возможность разделения доступа между пользователями к тем или иным операциям. Многие панели оператора (HMI) также обладают такими ресурсами. Применение подобного оборудования существенно расширяет возможности удаленного управления. По сути реализованная таким образом система является способом удаленного управления через Internet и основана на делении SCADA пакета на серверную и клиентскую части. В роли SCADA выступает интегрированный Web-сервер в ПЛК. Клиентская часть представляет собой Web-браузер, который просматривает специализированную Web-страницу, находящуюся на Web-сервере. На этой странице создается специализированный интерфейс с графикой и анимацией. Анимация выполняется с помощью JScript, VBScript, Java апплетов,

*Безопасность это процесс, а не результат.*
Bruce Schneier

Flash и анимированных GIF-файлов. Поскольку основная часть визуальной динамики пользовательского интерфейса исполняется на клиентском компьютере, а с сервера передаются только данные об объекте автоматизации, существенно снижаются требования к пропускной способности Internet-канала.

JavaScript или VBScript применяются в таких системах для создания динамических Web-страниц (с вращающимися лопастями вентиляторов, с движением жидкости в трубах и т. п.), для оперативной проверки правильности действий пользователя при заполнении форм до передачи страницы на сервер, для взаимодействия с пользователем при решении таких задач, которые не требуют обращения к серверу.

Web-страница может воспринимать действия пользователя, например, нажатие кнопок, заполнение форм и передавать их серверу. Сервер в ответ формирует новую Web-страницу с элементами, измененными в соответствии с действиями пользователя. Выполняется это с помощью CGI-сценария (Common Gateway Interface)

Если сама по себе организация удаленного доступа к АСУТП по Web-каналам в настоящее время не представляет большой трудности благодаря огромному разнообразию решений от различных производителей ПЛК, то защита от несанкционированного доступа через Internet и не только — это проблема. История со Stuxnet'ом это блестяще продемонстрировала. SCADA система оказалась столь же уязвимой для вирусной атаки, как и любое другое ПО, работающее под ОС Windows ("какая неожиданность, кто бы мог подумать" — о сомнительной пригодности платформы Wintel для ответственных приложений только ленивый в последние 10 лет не писал, нет, куда там сформированная навязчивой рекламой привычка свыше нам дана...). Впрочем, сам по себе червяк Stuxnet тоже оказался не так прост — он содержал целевой код, удовлетворяющий целому ряду специфических требований и реализующий полноценную атаку на АСУТП производства известной европейской компании. В частности, для реализации потенциала нападения вирус требовал наличия в составе АСУТП частотных преобразователей производства совершенно определенных компаний (одна из которых иранская), работающих на частотах 807...1210 Гц. Наличие подобных требований позволило большинству экспертов, исследовавших данный код, сделать вывод о том, что вирус предназначался для точечной атаки вполне определенного производства или ряда производств.

Проблематика защиты автоматизированных систем технологического управления обсуждается в специализированной прессе и в выступлениях ведущих экспертов по информационной безопасности (ИБ)

## Опасно чувствовать себя безопасно в Internet-е.

Журнал «Автоматизация в промышленности»

достаточно давно. Тем не менее, заметного прогресса в защите систем этого класса за прошедшие 10 лет не произошло. И вот почему. "Романтика" периода "холодной войны" уступила холодному расчету эпохи финансового бандитизма. Многочисленные приключенческие фильмы с участием плеяды блистательных Джеймсов Бондов показывают нам маньяков, шантажирующих мир проникновением в системы управления ядерным оружием с целью его (мира) уничтожения. Но реальная киберпреступность — штука куда более приземленная и направлена, прежде всего, на получение денежной выгоды от реализации тех или иных атак на инфраструктуру. При этом с точки зрения преступной экономики АСУТП малопривлекательны, так как затраты на производство вредоносного ПО те же самые, а результат принесет в лучшем случае извращенное моральное удовлетворение. Время гениальных одиночек кончилось и в этой области, современный вирус — штука сложная и затратная, требующая командной работы высококвалифицированных специалистов. Посему появление серьезных угроз для промышленной инфраструктуры возможно при наличии заинтересованного платежеспособного заказчика, руководствующегося внеэкономическими мотивами. Почему-то считается, что такая ситуация маловероятна. А зря. Stuxnet это отлично продемонстрировал.

Как же защитить АСУТП? Меры эти, в общем, общеизвестны:

— управление доступом и полномочиями;

— обеспечение безопасного межсетевого взаимодействия;

— антивирусная защита;

— анализ степени существующей защищенности;

— своевременное обнаружение вторжений;

До последнего времени специфика контроллерного оборудования технологического уровня позволяла обеспечить достаточно надежную защиту вполне элементарными средствами. ПО практически любого контроллера позволяет защитить паролем доступ к конфигурационному порту, а интерфейсы программирования большинства ПЛК работали по протоколу RS-485. Такая аппаратная конфигурация сама по себе является надежной защитой от хакерской атаки — пока злоумышленник будет с помощью специального софта подбирать 32-разрядный пароль на скорости обмена 9600 бод, у него отрастет очень длинная борода. Однако сегодня скоростной Ethernet все более и более используется как единая среда передачи данных вплоть до самого нижнего уровня АСУТП — уровня датчиков и исполнительных механизмов, подключаемых по протоколам Modbus/TCP, EtherNet/IP, PROFInet и др. Поэтому на простую реализацию программно-аппаратной защиты, когда роль межсетевого экрана играет сам контроллер, рассчитывать уже не приходится. Необходимо использовать специальные аппаратные средства — маршрутизаторы, обеспечивающие отслеживание таких воздействий, как:

— прослушивание трафика (с использованием атак переполнения таблицы MAC);

— подмена адресов участников информационного обмена (с использованием атак подделки сообщений протокола ARP, подделки IP-адресов, подделки MAC-адресов);

— несанкционированная передача трафика в другие виртуальные сегменты сети (с использованием атак прохождения VLAN);

— атака на сам коммутатор и сеть (с использованием особенностей протокола Spanning Tree, передачи анормального трафика и др.).

Использование современных маршрутизаторов с функциями межсетевых экранов вполне достаточно для защиты локальных сегментов сети предприятия, например, для отделения технологического сегмента от диспетчерского уровня. Оборудование с такими функциями предлагается многими поставщиками, причем для некоторых эта область деятельности является узкой специализацией, что говорит о востребованности продукта рынком. Предлагается такое оборудование и "универсальными" производителями.

В некоторых случаях целесообразно использование технологии аутентификации устройств и/или пользователей при подключении к коммутируемой сети (например, по стандарту 802.1x). Наличие возможности дополнительной аутентификации на рабочих станциях, Web-страницах SCADA-систем или ПЛК существенно снижают вероятность вывода злоумышленником из строя системы автоматики.

Однако не следует забывать, что при осуществлении взаимодействия средств АСУТП через сети общего пользования (например, с ЛВС предприятия) обязательным является создание доверенного (защищенного) канала связи между взаимодействующими объектами с использованием выделенных каналов связи межсетевых экранов и криптографических средств.

Для индивидуальной защиты децентрализованно распределенных систем автоматизации многие производители сетевого оборудования предлагают различные промышленные межсетевые экраны/маршрутизаторы с целым рядом превентивных и диагностических функций, позволяющих быстро и надежно распознать попытки несанкционированного сетевого доступа и изменений в вычислительных системах. Это оборудование является универсальным (все в одном) и совмещает функции файрвола, маршрутизатора и VPN-сервиса. Благодаря этому, появляется возможность простого и надежного дистанционного обслуживания устройств через открытые сети, например, Internet.

Web-технологии привлекательны в первую очередь своей дешевизной, общедоступностью и простотой. Пока мы не можем представить все области их применения. Ясно, что Internet будет широко применяться в промышленных АСУ разного класса

и назначения, но представляется также очевидным, что Internet и Web-доступ позволит выйти за пределы сферы привычного нам применения АСУТП. В качестве примера нестандартного применения WWW можно привести систему, которую в свое время (2005–2006 гг.) разместила на своем сайте компания Echelon. Данный ресурс позволял в on-line режиме управлять, освещением, кондиционированием в специальной демонстрационной комнате компании. Но тогда Internet-технологии в автоматике еще только развивались и ни кто не предполагал, что открытость таких систем может представлять серьезную опасность для отдельных компаний и экономики целых государств. Может нам пора взглянуть на Internet в АСУТП несколько шире и задуматься о проблемах, которые могут возникнуть?

Уже после того, как текст этой статьи ушел в печать, в Internet на сайте РБК (http://top.rbc.ru/economics/13/12/2012/836311.html) появился интереснейший материал в точности по обсуждаемой теме. Корреспондент РБК К. Петрова со ссылкой на специалистов "Лаборатории Касперского" (к сожалению, анонимных) в статье с несколько претенциозным заглавием "Кибероружие: империя наносит ответный удар" рассказала о необычайно высоких темпах прогресса в области разработок вредоносного ПО, специально предназначенного для поражения инфраструктуры. Оказывается, пресловутый Stuxnet был только первой пташкой. В 2012 г. в Иране и в Катаре зарегистрировано несколько атак на системы управления нефтяными терминалами, в результате которых работа этих предприятий парализовывалась на длительное время. На компьютерах, подвергшихся атаке предприятий, обнаруживаются уже не отдельные вирусы, а чуть ли не полноценные вредоносные операционные системы, например, Flameи Gauss. Они способны по команде удаленного оператора перехватывать и направлять вовне любую информацию о происходящих в системе процессах, а также размещать в зараженной системе модули для выполнения по команде извне определенных "клиенто-ориентированных" действий. Интересно, что, по мнению специалистов, коды этих систем очень похожи на код Stuxnet, что позволяет сделать вывод об их происхождении от одной и той же команды разработчиков. Пока, правда, распространение всех этих ужасов ограничено странами Ближнего Востока. Статья на РБК заканчивается оптимистическим утверждением, что Россия в обозримом будущем не должна стать лакомой целью для подобных атак. Хотелось бы верить — только вот непонятно, почему мы должны стать исключением... в общем, даже если утверждение насчет империи и является журналистским преувеличением, исключительная актуальность вопросов обеспечения информационной безопасности в задачах АСУТП получила еще одно подтверждение.

**Список литературы**


1. *Егоров Е.В.* Область применимости Internet-технологий в системах диспетчерской автоматики//Автоматизация в промышленности. 2009. № 2.
2. *Фрейдман А.В.* Stuxnet и промышленная безопасность//Автоматизация в промышленности. 2011. № 11.



***Егоров Евгений Валентинович** – канд. физ.-мат. наук, начальник отдела промышленной автоматики,*
***Зайцев Михаил Вячеславович** – инженер-консультант отдела промышленной автоматики ООО "ЭФО".*
*Контактный телефон (812) 331-09-64.*
*E-mail: eve@efo.ru mivz@efo.ru*