УДК 004.056
DOI 10.33764/2618-981X-2023-8-1-126-133

С. В. Десятов[1]*

Обеспечение информационной безопасности автоматизированных систем управления технологических процессов (АСУ ТП) как важнейший элемент устойчивого функционирования и развития высокотехнологичных отраслей экономики Российской Федерации

[1]Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация,
*e-mail: s.v.desyatov@sgugit.ru

Аннотация. в статье рассматриваются вопросы обеспечения информационной безопасности АСУ ТП. Проанализированы основные виды уязвимостей, рассмотрены возможные реальные последствия выхода АСУ ТП из строя. Предложены наиболее эффективные меры по организации их защиты.

Ключевые слова: информационная безопасность, транспортные и промышленные предприятия, АСУ ТП, программное обеспечение, угрозы, уязвимости, средства защиты информации

S. V. Desyatov[1]*

Safety Information for Automated Process Control Systems (APCS) as an Essential Element of Sustainable Functioning and Development of High-Tech Branches of the Economy of the Russian Federation

[1]Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
*e-mail: s.v.desyatov@sgugit.ru

Abstract. The article deals with issues of ensuring the information security of automated process control systems. The main types of vulnerabilities are analyzed, the possible real consequences of failure are considered. The most effective measures for organizing their protection are proposed.

Keywords: information security, transport and industrial enterprises, process control systems, software, threats, vulnerabilities, information security tools

Введение

Политический и экономический суверенитет любой страны невозможен без суверенитета технологического. Актуальность этого утверждения очень четко подтвердила начавшаяся в феврале 2022 Специальная военная операция. Как показывает мировая история, победа над противником куется в тылу, и этому есть огромное количество примеров. Самые понятные и правдивые – Великая отечественная война 1941–1945 гг.

Как это вообще соотносится с заявленной темой работы? Во-первых, история повторяется. Во-вторых, 2022 год показал, что «коллективный» Запад, управляемый США, уже несколько лет не скрывает своих целей: ослабить, разделить, а то вообще стереть с лица земли Российскую Федерацию. По понятным

причинам политическая составляющая начинает играть все более заметную роль в технологических аспектах нашей экономики.

Целью данной работы является практический анализ вопросов обеспечения информационной безопасности автоматизированных систем управления технологическим процессом (АСУ ТП) как важный элемент устойчивого функционирования и развития высокотехнологичных отраслей экономики РФ.

К данной посылке есть конкретные подтверждения: более десяти лет автор отвечал за информационную, экономическую и физическую безопасность значимого объекта критической информационной инфраструктуры (ЗОКИИ). В технологических процессах данного предприятия в значительных объемах используются взрывчатые вещества (ВВ) и взрывчатые материалы (ВМ). Принимал участие в расследовании различных чрезвычайных происшествий. Вопросы организации взаимодействия IT-специалистов, производственников и «безопасников» на примере конкретного предприятия оборонно-промышленного комплекса г. Новосибирска можно экстраполировать на конкретную отрасль экономики РФ, после чего сделать конкретные выводы и прогнозы.

Рост рынка решений для обеспечения кибербезопасности прямо пропорционален возросшему количеству угроз. Несмотря на то, что рынок технологий информационной безопасности (ИБ) ежегодно растет, количество способов атак на корпоративные сети не уменьшается. Это немного напоминает ситуацию с коронавирусной инфекцией. Не успели сделать вакцину, опробовали, запустили в производство, а вирус мутировал – надо делать новую…

Российские специалисты, анализируя зарубежный опыт в сфере ИБ, в целом, соглашаются с предложенными выводами и выделяют несколько основных видов киберпреступлений в мире.

1. Преступление в качестве услуги: «подпольные цифровые услуги» подкрепляются моделью «преступление-в-качестве-услуги», которая становится все более популярной и востребованной.

2. Банковские «трояны», позволяющие осуществить переводы денежных средств со счетов банковских клиентов, являются главными угрозами среди вредоносного программного обеспечения (ПО).

3. Платежное мошенничество. Число атак, направленных на банкоматы, постоянно увеличивается.

4. Преступное использование данных посредством использования программ-вымогателей: данные остаются ключевым товаром для киберпреступников.

5. Атаки на промышленные предприятия со взломом АСУ ТП, в том числе и вымогательство террористических, экстремистских и враждебно настроенных групп с целью вывода из строя критических важных объектов. Интересный момент: главной угрозой становятся атаки против представителей руководства предприятий и организаций!

6. Виртуальные валюты: криптовалюты остаются тем средством, которое мошенники предпочитают для оплаты за приобретение незаконных товаров и услуг в «темной» сети.

Ситуация в России практически не отличается от мировой. Из всех киберпреступлений, совершенных на территории Российской Федерации за последние несколько лет, специалисты выделяют основные векторы атак.

1. DDoS-атаки: данный вид информационной атаки отличается высокой эффективностью и крайне труден в прогнозировании.

2. Программы-вымогатели: в последнее время корпоративный сектор в нашей стране все чаще подвергается атакам со стороны этой категории программ, которые, по мнению аналитиков ИБ, являются доминирующим видом вредоносного ПО. Главная их опасность заключается в том, что они «эволюционируют».

3. Атаки на АСУ ТП: в настоящее время это одна из ключевых угроз ИБ. Фиксируется кратный рост неизвестных «зловредов», атакующих АСУ ТП.

Суммируя все вышесказанное, можно сделать вывод: обеспечение надежного функционирования АСУ ТП требует самого серьезного подхода к обеспечению ИБ.

Что такое АСУ ТП, и кто их должен защищать?

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 №187-ФЗ в статье 2 дает определения основных понятий. В частности, автоматизированная система управления (АСУ) – комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и/или производственным оборудованием (испытательными устройствами) и производственными процессами, а также для управления такими оборудованиями и процессами.

Понятия автоматизированной системы управления технологическими процессами в этом законе нет. Что вообще следует под этим понимать?

АСУ ТП – группа технологических и программных средств, предназначенных для автоматизации и управления технологическим оборудованием на промышленных предприятиях. Это целостное, комплексное решение для автоматизации основных операций технологического процесса. Проще говоря, АСУ ТП – это система промышленной автоматизации, которая, так или иначе, связана с той средой, в которой она функционирует.

К субъектам критической информационной инфраструктуры (КИИ) этот ФЗ относит и промышленные предприятия различных сфер деятельности, которые на праве собственности, аренды или ином законном основании, принадлежат информационная система (ИС), информационно-телекоммуникационная сеть и АСУ.

Следует заметить, что принятие Федерального закона «О безопасности КИИ РФ» от 26.07.2017 №187 и ввод его в действие вызвал неоднозначную реакцию всех, кто имел отношение к данной проблеме. Правительство Новосибирской области проводило соответствующие семинары, на которых представители ФСТЭК России, ФСБ и ведущие специалисты различных институтов разъясняли порядок выполнения требований данного федерального закона.

Этот документ регулирует все, что связано с безопасностью КИИ, то есть всех IT-инфраструктур на критически важных объектах (КВО), к которым, в

первую очередь, относятся энергетические, нефтегазовые, транспортные, и другие промышленные предприятия. В КИИ отдельно выделяются ЗОКИИ – значимый объект критической информационной инфраструктуры. АСУ ТП также может являться ЗОКИИ.

Практика показала, что руководители многих предприятий, даже формально не подпадающих под определение КВО, прекрасно понимая возможные риски и угрозы, предпринимают конкретные действия в этом направлении.

Как тут не вспомнить известного политического деятеля прошлого века сэра Уинстона Черчиля: «За безопасность нужно платить, а за ее отсутствие расплачиваться!».

По мнению некоторых специалистов, рынок защиты АСУ ТП в настоящее время еще до конца не сформировался.

Главными действующими лицами в вопросе обеспечения безопасности АСУ ТП являются две стороны: специалисты по АСУ, и специалисты по ИБ. Первые прекрасно разбираются в технологических процессах, но часто не задумываются об их безопасности. Вторые хорошо знают методы защиты, но не очень хорошо ориентируются в самих технологических процессах. И те, и другие прекрасно понимают, что проблема действительно существует, так как последствия могут катастрофическими, следовательно, необходимо предпринимать конкретные совместные действия, чтобы их избежать или снизить их уровень.

Статья 10 №187-ФЗ от 26.07.2017 четко определяет обязанности субъекта КИИ по созданию системы безопасности такого объекта и ее функционирования. Основными задачами безопасности значимого объекта КИИ являются:

– предотвращение неправоверного доступа к информации, обрабатываемой значимыми объектами КИИ;

– недопущение воздействия на технические средства обработки информации;

– восстановление функционирования значимого объекта КИИ;

– непрерывное взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

Для специалистов в области ИБ всегда был интересен вопрос количества инцидентов в западных странах, США и у нас, в РФ, связанных с безопасностью АСУ ТП. В связи с отсутствием достоверной информации какие-либо выводы делать сложно. Но если судить о размерах проблем по количеству доступных из Интернета данных об АСУ ТП, то больше всего их в США, Россия находится где-то в середине списка.

В каких отраслях и насколько серьезные существуют последствия. Известные примеры

Вопросы организации и обеспечения надежной защиты АСУ ТП наиболее актуальны и «жизненно» необходимы для технологических процессов критичных отраслей промышленности. Это те, где возможен максимальный экологический ущерб, и может пострадать максимальное количество людей. В первую оче-

редь, это предприятия топливно-энергетического комплекса – здесь возможны любые негативные сценарии: экологические, экономические, гуманитарные. Сюда же относится и химическая промышленность. Не стоит забывать об отраслях, связанных с жизнеобеспечением. Потенциальная угроза здесь просто огромна. Очень чувствительной отраслью к возможности несанкционированного вмешательства в управление является транспорт.

Если раньше обычно говорили про наземный транспорт, то в настоящее время приводят некоторые примеры (правда, не подтвержденные официально) вмешательства в управление самолетом. Очень неприятный инцидент произошел в США. Неизвестный злоумышленник через мультимедийную (развлекательную) систему в самолете смог подключиться к АСУ и ненадолго изменить тягу одного из двигателей, в результате самолет некоторое время летел боком… Можно не верить и сомневаться, но просто невозможно себе представить экономические и имиджевые потери авиакомпании, если бы данный факт стал достоянием гласности! Хорошо, что данный инцидент обошелся без последствий.

На сегодняшний день можно привести немало конкретных примеров вмешательства в работу АСУ ТП, которое повлекло за собой серьезные потери. Следует заметить, что большинство информации о таких инцидентах получено по материалам зарубежных источников. В качестве показательного примера вспомним один и самых серьезных инцидентов вмешательства в работу АСУ ТП, который произошел с оборудованием немецкой компании «Siemens». Речь идет об известном вирусе «Stuxnet». Интерес к нему обусловлен двумя причинами: это, наверное, первый случай, когда вирус приносит физическое разрушение. Изменение скорости вращения центрифуги приводило к физическому выходу ее из строя. Червь был настроен на конкретный тип контроллеров от компании «Siemens». После инцидента «Siemens», как очень большая и серьезная компания, предприняла все возможные меры, чтобы как-то сгладить ситуацию. Все желающие могли получить доступ к контроллерам, в результате чего было выявлено много серьезных уязвимостей. Для исправления сложившейся ситуации был создан специальный центр по их анализу и реагированию. Обращает на себя внимание одно обстоятельство. Почему-то не пишут, в какой стране и на каком объекте это произошло, хотя секрета здесь никакого нет.

Диагноз поставлен. Как лечить?

Основы технологических процессов систем управления различных предприятий составляют, в общем-то, схожие компоненты: это испытательные и запоминающие устройства. Степень критичности и влияния приостановки или даже частичного изменения технологических процессов на конкретных предприятиях, в первую очередь, стоит оценивать с позиций их уязвимости. Возможные материальные потери адекватно могут оценить только собственники организации. Чаще всего истинные суммы скрываются. Понятно, что в силу специфики производственной деятельности материальный ущерб от нарушения технологических процессов может быть самый разнообразный. Но в первую очередь надо рассматривать экологический аспект и последствия ограничения предоставления населению жизненно важных услуг.

Рассматривая безопасность АСУ ТП, российские специалисты в области защиты информации пришли к выводу, что осуществить удаленное подключение к отдельным компонентам систем из Интернета не составляет большого труда. Масштабы открытых возможностей просто поражают! Не стоит «расслабляться» и тем предприятиям, для которых целенаправленная атака маловероятна.

Высокий уровень открытости промышленных сетей в Интернете свидетельствует о том, что данному вопросу на протяжении многих лет попросту не уделялось должного внимания. Но здесь имеется одна существенная деталь: удаленный доступ к АСУ ТП через Интернет обусловлен требованиями заказчика (производителя, которому периодически необходимо обновлять ПО, поддерживать оборудование в работоспособном и т.п.). С течением времени имеющиеся (хоть и небольшие) разграничения между сегментами ИТ и АСУ стирались. Позже пришло понимание, что необходимо было сразу использовать защищенный канал связи.

К числу других уязвимостей следует отнести отсутствие разграничения между технологическим процессом в офисных и промышленных сетях. Дело в том, что используемые методы и средства защиты этих систем серьезно различаются. В данной статье рассматриваются промышленные варианты.

Объективно оценивая сложившуюся ситуацию с обеспечением безопасности АСУ ТП можно прийти к простому выводу: основная угроза системам управления заключается в отсутствии должного внимания к этой проблеме. Это и бесконтрольное использование периферийных устройств, флеш-носителей, отсутствие локальных нормативно-правовых актов (НПА) по защите АСУ ТП. Не стоит забывать, что технологические процессы достаточно статичны (модернизация проводится редко), оборудование устаревает. В основном, используются старые версии программных продуктов и операционных систем, которые содержат в себе множество различных уязвимостей.

Самые главные первые шаги

По глубокому убеждению автора, «не стоит изобретать велосипед». Наиболее эффективный, действенный и проверенный метод – это применение комплексного подхода защиты АСУ ТП. Необходимо применять как традиционные (классические) средства защиты, так и специализированные. Важный элемент: так как чаще всего производственный процесс непрерывный, то защитные средства следует применять очень аккуратно, дабы не нарушать сам процесс.

Практика показывает, что при выборе средств защиты предпочтение следует отдавать аппаратным средствам, а потом дополнительным. Обязательные условия: наличие документов и сертификата соответствия ФСТЭК. Еще одно «золотое правило»: вне зависимости от того, какие средства защиты АСУ ТП используются, необходимо в обязательном порядке производить обучение и переподготовку сотрудников, ответственных за безопасность автоматизированных систем управления.

Следующим шагом должно стать решение руководства организации о разработке локального НПА. Как правило, это политика безопасности. После при-

нятия решения о необходимости защиты АСУ ТП необходимо произвести инвентаризацию, в рамках которой обследуются все системы, подсистемы и их связи, имеющиеся средства защиты, а также основное и прикладное ПО. В ходе проведения этих мероприятий не следует забывать об одном существенном моменте: все имеющиеся в настоящее время средства защиты условно можно разделить на два типа. К первому типу относятся системы, реализующие только мониторинг (системы обнаружения вторжений, IDS). Второй тип составляют системы, реагирующие на тот или иной инцидент (системы предотвращения вторжений, IPS). Это условное разделение на типы очень важно для определения дальнейших шагов, в частности, установление очередности приоритета защиты основных свойств информации.

Рассмотрим подробнее средства защиты, относящиеся к этим типам. Первые ничего не блокируют, их основная задача – мониторинг происходящих событий. Они в режиме реального времени отслеживают все возникающие угрозы, аномалии в сети и проблемы, фиксируют их и уведомляет соответствующие подразделения (ОПИТРиЗИ – отдел по противодействию иностранным техническим разведкам и технической защите информации или кибербезопасности). По большому счету, это технология (процесс) обнаружения компьютерных атак, каких-либо аномальных поведений в сети, контроль целостности данных и ПО, т.е. мониторинг событий ИБ.

Основная функция средств защиты второго типа состоит в организации управления потоками информации, контроля доступа команд и действий пользователей. Как показывает практика, хорошим решением здесь является использование межсетевых экранов, защита конечных узлов, управление доступом к сети и т.д.

Как было отмечено выше, условное разделение используемых средств защиты на типы позволяет выделить приоритет (очередность) в организации защиты классических сетей и АСУ ТП.

В чем же состоит разница приоритетов? Для классической системы информационной безопасности в порядке снижения уровня приоритетности следуют: конфиденциальность, целостность и доступность. Первичная задача «уберечь» конфиденциальность! Для АСУ ТП, с точностью «до наоборот», самое важное – это доступность, далее целостность, а потом конфиденциальность. Поэтому, исходя из этого, следует выбирать средства защиты.

Заключение

Время показывает, что вопросам обеспечения безопасности АСУ ТП необходимо уделять самое пристальное внимание. Только комплексный подход в обеспечении ИБ АСУ ТП может гарантировать устойчивую и надежную работу промышленности и транспорта. Самую большую цену приходится платить за нештатные ситуации. Будь то приостановка работы, либо выход из строя отдельных участков технологических процессов и т.д. Хочется обратить внимание на еще один немаловажный аспект: организация защиты АСУ ТП – это отдельный вид ИБ и поэтому требует специфического подхода.

В статье рассмотрены, в основном, «внутренние проблемы» обеспечения ИБ АСУ ТП. Сейчас в мире полным ходом идет научно-техническая война. Это война и за новое знание и влияние. Кто первым «добежит» и первым получит новую технологию, тот и обеспечит себе конкурентное преимущество, опередив других игроков лет на десять-пятнадцать. Война подразумевает и непорядочные средства ведения. Если не получается добиться преимущества в открытой борьбе, то в ход идут «подлые и грязные» методы. События 2022 года это прекрасно показали. Не будем забывать о т.н. незадекларированных возможностях импортного оборудования, включая ПО.

Приказ ФСТЭК от 14.03.2014 №31 определяет много правильных решений, но он больше подходит для работы в «мирных» условиях. Очевидно, необходимы очень серьезные решения органа государственного управления, чтобы принять превентивные меры по усилению ИБ АСУ ТП, предупредить наступление негативных последствий.

Было бы правильно «смоделировать» работу АСУ ТП в условиях «военного времени» четко понимая, откуда взялась угроза.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Жмуров, Д. Б. Анализ угроз безопасности информации в автоматизированных системах управления технологическими процессами / Д. Б. Жмуров // Актуальные проблемы обеспечения информационной безопасности : труды Межвузовской научно-практической конференции, Самара, 20–24 мая 2017 года. – Самара: Инсома-Пресс, 2017. – С. 90-95.

2. Дементьев, А. В. Анализ проблем информационной безопасности автоматизированных систем управления технологическими процессами / А. В. Дементьев // Студенческий. – 2020. – № 21-1(107). – С. 37-40.