МИССИОЦЕНТРИЧЕСКИЙ ПОДХОД К КИБЕРБЕЗОПАСНОСТИ АСУ ТП

***Гордейчик Сергей Владимирович**, г. Москва*

В статье предлагается использование миссоцентрического подхода к кибербезопасности АСУ ТП через призму промышленной, функциональной и информационной безопасности. Кибербезопасность определяется как процесс обеспечения функционирования объекта управления, при котором отсутствуют опасные отказы и недопустимый ущерб, обеспечивается заданный уровень экономической эффективности и надежности с учетом целенаправленного негативного антропогенного информационного воздействия.

***Ключевые слова**: кибербезопасность, функциональная безопасность, промышленная безопасность, надежность, анализ рисков, SIL, АСУ ТП, уязвимости.*

MISSION-CENTRIC APPROACH TO ICS/SCADA CYBERSECURITY IN TERMS OF INDUSTRIAL

***Sergey Gordeychik**, Moscow*

This article covers a mission-centric approach to ICS/SCADA cybersecurity in terms of industrial, functional and information security. Cybersecurity is defined as a process that ensures control object operation with no dangerous failures or damage, but with a set economic efficiency and reliability level maintained in the light of adverse anthropogenic information influence.

Введение

В последнее время в среде специалистов широко обсуждаются вопросы кибербезопасности применительно к системах автоматизированного управления технологического процесса (АСУ ТП). Целью данной статьи является попытка определения предмета кибербезопасности АСУ ТП и его места в обеспечении промышленной безопасности и экономической эффективности.

Актуальность кибербезопасности АСУ ТП

Сложная геополитическая обстановка и развитие средств проведения компьютерных атак заставляют пересмотреть используемые для анализа защищенности и построения средств защиты модели угроз. В ходе выявленной в 2014 году комплексной кибератаки Havex [1] злоумышленники компрометировали сайты компаний-производителей компонентов АСУ ТП для подмены дистрибутивов программного обеспечения, загружаемого пользователем. Таким образом, специализированное вредоносное ПО загружалось с официальных репозиториев производителя и устанавливалось в сегментах АСУ ТП самим оператором системы.

Практический анализ защищенности ряда широко используемых систем АСУ ТП [2] продемонстрировал наличие дефектов и уязвимостей, использование которых злоумышленником позволяет не только снижать ключевые показатели надежности и обходить механизмы функциональной безопасности, но и реализовывать атаки, напрямую влияющие на промышленную безопасность и стать причиной техногенных катастроф. Примечательно, что, с точки зрения информационной и функциональной безопасности, данные системы соответствуют всем выдвигаемым требованиям, имеют все необходимые международные, отраслевые и государственные сертификаты.

Текущее состояние кибербезопасности АСУ ТП

Основным направлением направления развития кибербезопасности АСУ ТП являются попытки адаптации опыта, наработанного в области информационной безопасности по трем направлениям:

- анализ и оценка защищенности кибербезопасности АСУ ТП;
- разработка нормативного и методического обеспечения;
- разработка специализированных методов и средств обеспечения кибербезопасности.

Анализ и оценка кибербезопасности систем АСУ ТП не носит систематический характер. Подобные работы часто проводятся в рамках корпоративного заказа, и в данном случае результаты исследований не публикуются. Однако, в некоторых случаях информация об уязвимостях открыто обсуждается на научно-практических конференциях. В настоящее время доступны подробные анализ уязвимостей различных систем [3].

Одной из проблем в данной области является отсутствие скоординированной активности в данной области. Частично проблему пытаются решить государственные и отраслевые команды реагирования на инциденты компьютерной безопасности (Computer emergency response teams, CERT). Наиболее авторитетной организацией в данном отношении является ICS-CERT [4], являющийся подразделением Министерства Внутренней Безопасности США (US Department of Homeland Security), отслеживающий информацию о публикуемых уязвимостях промышленных систем и координирующий взаимодействие производителей и исследователей. Однако подотчётность данной организации DHS накладывает ряд ограничений на взаимодействие с нею.

Кроме открытого сообщества существует ряд организаций, специализирующихся на выявлении и перепродаже информации о выявленных уязвимостях и методов проведения атак. Примерами подобных организацией является компания Exodus Intelligence из США, европейские ReVuln, Vupen.

В части нормативного обеспечения наиболее ярким представителем является семейство стандартов ANSI/ISA-62443, адаптированный в качестве ГОСТ Р МЭК 62443. Ряд требований к безопасности АСУ ТП изложен в документе ФСТЭК России «Требования 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». Однако, данный документ построен на привычной концепции обеспечения «целостности», «доступности» и «конфиденциальности» информации, что не совпадает с основными задачами промышленной безопасности.

Отраслевые документы в области безопасности АСУ ТП наиболее хорошо развиты в энергетической отрасли США. В большинстве случаев основой для этого является NERC CIP. На железнодорожном транспорте требования по кибербезопасности изложены в технических регламентах Таможенного Союза «О безопасности железнодорожного подвижного состава» (ТР ТС 001/2011), «О безопасности высокоскоростного железнодорожного транспорта» (ТР ТС 002/2011). Однако данные документы выдвигают достаточно поверхностные требования сводящиеся к обеспечению «защищенности от компьютерных вирусов, несанкционированного доступа, последствий отказов, ошибок и сбоев при хранении, вводе, обработке и выводе информации, возможности случайных изменений информации». Как видим, в данном случае речь идет в основном о «случайных воздействиях», не учитывающих целенаправленную атаку. Однако, в документе присутствует упоминание «несанкционированного доступа», что косвенно вводит антропогенный фактор

Таким образом, нормативные, организационные и технические вопросы кибербезопасности современных систем АСУ ТП проработаны достаточно слабо, и существует разрыв между подходами и методами обеспечения информационной безопасности и практикой решения задач промышленной безопасности.

Миссоцентрический подход кибербезопасности

В настоящее время ряд исследователей предлагает рассматривать кибербезопасность через призму цели или мисси, для которой создается информационная система [5]. Это позволяет анализировать угрозы и уязвимости информационной системы не в контексте обеспечения целостности, доступности и конфиденциальности, но в терминах предметной области, для автоматизации которой используется АСУ.

В рамках развития этой концепции предлагается рассматривать вопрос кибербезопасности, используя методический аппарат трех дисциплин: промышленной безопасности, функциональной безопасности и информационной безопасности.

Необходимость синтеза различных научных направлений обусловлено с одной стороны, возможностью применения наработанных научных и методических инструментариев, а с другой стороны рядом ограничений, не позволяющих применять каждую из дисциплин самостоятельно для решения поставленных задач. Так функциональная безопасность связана с непреднамеренно вызванными отказами в выполнении отдельных функций системы и не учитывает целенаправленных угроз, а информационная безопасность на-

Рис. 1. *Дисциплины, связанные с кибербезопасностью*

правлена на обеспечение целостности, доступности и конфиденциальности информации, что напрямую не связанно с задачами промышленной безопасности.

Основными преимуществами данного подхода является возможность интеграции предмета кибербезопасности в существующие процессы проектирования, разработки и внедрения систем АСУ ТП, используя зарекомендовавшие себя наработки (см. Таблица 1).

Основой обеспечения безопасности является корректное определение угроз. Использование миссиоцентрического подхода позволяет выделить три основных класса угроз кибербезопасности АСУ ТП.

1. Нарушение промышленной безопасности: реализация угроз непосредственно влияет на промышленную безопасность, может являться причиной техногенной катастрофы.
2. Снижение эффективности производственного процесса: реализация угроз явно снижает количественные экономические показатели процесса, автоматизируемого с помощью АСУ ТП.
3. Другие нарушения функциональной безопасности и надежности: реализация угроз непосредственно не влияет на промышленную безопасность и оказывает косвенное влияние на качественные или количественные показатели эффективности, надежности и безопасности (SIL, наработка на отказ и т.д.).

Таблица 1 *– Определение кибербезопасности АСУ ТП через смежные дисциплины*

Дисциплина	**Используемые методики**
Промышленная безопасность	Требования к уровню безопасности Доказательства безопасности Функциональные требования к МПСУ
Функциональная безопасность и теория надежности	Методический аппарат анализа рисков Методы доказательства безопасности Оценка эффективности средств защиты
Информационная безопасность	Методический аппарат моделирования угроз Методики анализа защищенности Процессы, средства и механизмы защиты Оценка эффективности средств защиты

Это позволяет определить кибербезопасность как процесс обеспечения функционирования АСУ ТП, при котором отсутствуют опасные отказы и недопустимый ущерб, обеспечивается заданный уровень экономической эффективности, функциональной безопасности и надежности с учетом вероятности целенаправленного негативного антропогенного информационного воздействия на компоненты АСУ ТП.

Подобный подход позволяет при анализе кибербезопасности АСУ ТП строить частную модель угроз, исходя из требований промышленной и функциональной безопасности, выдвигаемых к данному классу систем.

Заключение

Таким образом, при проектировании, разработке и внедрении систем АСУ ТП требуется учет возможности целенаправленного антропогенного воздействия, негативно влияющего на промышленную безопасность и экономическую эффективность. Определение предмета кибербезопасности через дисциплины промышленной безопасности, функциональной безопасности и информационной безопасности позволяет перейти к учету отраслевой специфики и оценивать влияние негативных воздействий в терминах опасных отказов (SIL) и теории надежности, что позволяет встроить процессы кибербезопасности в существующие процессы обеспечения промышленной безопасности, экономической эффективности и надежности.

Литература:

1. SecurityLab.ru, FireEye obnaruzhila boviy variant Havex, scaniruushiy OPC-servery, http://www.securitylab.ru/news/455022.php
2. Sergey Gordeychik, “WinCC Under X-Rays”, http://www.digitalbond.com/blog/2013/03/21/s4x13-video-wincc-under-x-rays-by-sergey-gordeychik/, S4 Conference, Miami, USA
3. Глеб Грицай, Александр Тиморин, Юрий Гольцев, Роман Ильин, Сергей Гордейчик, Антон Карпин, «Безопасность промышленных систем в цифрах», http://www.ptsecurity.ru/download/SCADA_analytics_russian.pdf
4. The Industrial Control Systems Cyber Emergency Response Team https://ics-cert.us-cert.gov/
5. Gabriel Jakobson, Mission-Centricity in Cyber Security: Architecting Cyber Attack Resilient Missions

References:

1. SecurityLab.ru, FireEye obnaruzhila boviy variant Havex, scaniruushiy OPC-servery, http://www.securitylab.ru/news/455022.php
2. Sergey Gordeychik, “WinCC Under X-Rays”, http://www.digitalbond.com/blog/2013/03/21/s4x13-video-wincc-under-x-rays-by-sergey-gordeychik/, S4 Conference, Miami, USA
3. Gleb Gritsai, Alexander Timorin, Yury Goltsev, Roman Ilyin, Sergey Gordeychik, Anton Karpin, «Bezopasnost promyshlennyh system v tsyfrah», http://www.ptsecurity.ru/download/SCADA_analytics_russian.pdf
4. The Industrial Control Systems Cyber Emergency Response Team https://ics-cert.us-cert.gov/
5. Gabriel Jakobson, Mission-Centricity in Cyber Security: Architecting Cyber Attack Resilient Missions