Интернет-журнал «Науковедение» ISSN 2223-5167 http://naukovedenie.ru/

Том 8, №5 (2016) http://naukovedenie.ru/index.php?p=vol8-5

URL статьи: http://naukovedenie.ru/PDF/55TVN516.pdf

Статья опубликована 07.11.2016.

Ссылка для цитирования этой статьи:
Цапко Г.П., Вериго А.А., Каташев А.С. Анализ рисков безопасности автоматизированных систем управления технологическими процессами // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 8, №5 (2016) http://naukovedenie.ru/PDF/55TVN516.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 004.056

Цапко Геннадий Павлович
ФГАОУ ВО «Национальный исследовательский Томский политехнический университет», Россия, Томск[1]
Профессор кафедры «Автоматики и компьютерных систем»
Доктор технических наук
E-mail: tsapkogp@gmail.com

Вериго Андрей Александрович
ФГАОУ ВО «Национальный исследовательский Томский политехнический университет», Россия, Томск
Аспирант кафедры «Автоматики и компьютерных систем»
E-mail: andrey_verigo@mail.ru

Каташев Андрей Сергеевич
ФГАОУ ВО «Национальный исследовательский Томский политехнический университет», Россия, Томск
Аспирант кафедры «Автоматики и компьютерных систем»
E-mail: katashev_as@mail.ru

Анализ рисков безопасности автоматизированных систем управления технологическими процессами

Аннотация. В данной работе проведен обзор основных подходов к анализу и управлению рисками безопасности автоматизированных систем управления технологическими процессами. Цель исследования заключалась в анализе рисков безопасности автоматизированных систем управления технологическими процессами. Основные методы исследования включали: структурный, сравнительный и системный анализ. Авторами определены основные угрозы безопасности в автоматизированных системах управления технологическими процессами, а также их источники. В качестве примера рассмотрены подходы к анализу и управлению рисками безопасности автоматизированных систем управления технологическими процессами на российских предприятиях, а также обеспечению безопасности в специальной операционной системе, разработанной Всероссийским научно-исследовательским институтом автоматизации управления в непромышленной сфере. Сделан вывод о необходимости проведения мероприятий для снижения рисков нарушения безопасности автоматизированных системах управления технологическими процессами на системном уровне. Построение защищенной автоматизированной системы управления технологическими процессами на базе отечественной специализированной операционной системы на промышленных предприятиях выглядит разумным решением не только с позиции обеспечения безопасности, но и снижения

[1] 634050, Россия, г. Томск, проспект Ленина, дом 30

зависимости от импортных ИТ-решений, что крайне важно для крупных коммерческих организаций, заинтересованных в гарантированной защите конфиденциальной информации.

Ключевые слова: безопасность; риск; автоматизированная система управления технологическими процессами

В современных условиях развития информационных технологий (ИТ), когда документооборот ведется в преимущественно электронной форме, для обменена информацией широко используются глобальные сети. Использование современных ИТ-решений, с одной стороны, обеспечивает повышение эффективности решения различных задач по управлению технологическими процессами, но с другой стороны приводит к существенному увеличению риска нарушения существующей системы информационной безопасности (ИБ).

Для противодействия угрозам нарушения ИБ на промышленных объектах создаются специализированные системы защиты информации (СЗИ). Сегодня для решения задачи обеспечения ИБ объекта специалистами разрабатываются такие модели, которые позволяют не только оценивать процесс распространения информации, но и процесс устранения угроз ИБ объекта [1, с. 59].

При построении СЗИ промышленного предприятия необходимо учитывать его системную структуру. В наиболее общем случае объект включает: локальные вычислительные сети (ЛВС), отдельные автоматизированные рабочие места (АРМ), а также различные вспомогательные технические средства и системы. При этом каждый указанный элемент предприятия может выступать объектом воздействия со стороны нарушителей или может быть вовлечен в процесс распространения угроз ИБ в связи с существующим технологическим (техническим) взаимодействием и территориальным расположением между различными элементами информационной системы (ИС) объекта [2, с. 27].

Важно учитывать, что источники угроз при взаимодействии с отдельными элементами ИС промышленного предприятия могут порождать различные виды угроз для этих элементов. Исходя из цели воздействия на ИС, специалисты выделяют три основных типа угроз безопасности в автоматизированных системах управления (АСУ):

- нарушение конфиденциальности информации;
- нарушение целостности информации;
- нарушение работоспособности ИС (отказы в обслуживании) [10, с. 289].

Проведенный анализ литературных источников и мнений экспертов [3, 5-6, 8] показывает, что с позиции построения СЗИ и возможных рисков нарушения безопасности информационного обмена в любом объекте информатизации можно выделить следующие основные компоненты:

- совокупность различных информационных средств, которые различаются техническими возможностями и характеристиками, используемыми видами информационных ресурсов и способами обработки/обмена информацией;
- совокупность необходимых вспомогательных технических средств, которые обеспечивают устойчивое функционирование ИС;
- сотрудники (персонал организации), имеющие различный уровень доступа к получению, обработке и использованию информации.

В свою очередь каждый из указанных компонентов возможно дополнительно разделить на множество составляющих элементов, которые могут подвергаться различным угрозам ИБ. Таким образом, можно сделать вывод, что объект информатизации представляет собой многоуровневую иерархическую систему, совокупность технических средств и пользователей, которая может быть подвержена различным рискам ИБ. Важно учитывать, что между различными элементами ИС объекта информатизации существуют взаимоотношения различного вида, что может способствовать распространению угроз ИБ. Взаимоотношения между отдельными элементами ИС выступают проявлением осуществляемых политик безопасности, используемых на данном предприятии.

Автоматизированные системы управления технологическими процессами (АСУТП, SCADA) активно используются на множестве предприятий/организаций как производственных, так и непроизводственных секторов экономики. Современные АСУТП включают в себя следующие звенья:

- управляемая/контролируемая аппаратура, представленная датчиками и исполнительными механизмами;
- специализированные контроллеры;
- программное обеспечение (ПО) управления АСУ ТП;
- сети взаимодействия указанных компонентов друг с другом и с диспетчерскими службами [7].

В современной практике информационно-вычислительные сети АСУТП не являются изолированными и используют общие технологии передачи информации (TCP/IP со специализированными прикладными протоколами верхнего уровня).

Актуальность задач защиты сетей АСУТП обусловлена следующими факторами:

- универсальность используемых технологий и протоколов;
- невозможность изоляции технологических сетей от остальной ИТ-инфраструктуры предприятия/организации;
- использование на российских предприятиях иностранного оборудования и ПО;
- высокая стоимость ущерба в случае целенаправленных атак на АСУТП;
- совершенствование нормативных требований по защите АСУТП в России[2].

Основными регулятивными требованиями в области безопасности АСУТП являются: Федеральный закон от 21 июля 2011 года №256-ФЗ «О безопасности объектов топливно-энергетического комплекса», а также требования ФСТЭК России [9, с. 37].

Так, например, приказом ФСТЭК России от 14 марта 2014 года № 31[3] утверждены требования к обеспечению защиты информации в АСУТП. Данные требования касаются

[2] Романченко Д. Обеспечение безопасности автоматизированных систем управления технологическими процессами (АСУТП) [Электронный ресурс] – Режим доступа: http://www.ibs.ru/it-infrastructure/information-security/obespechenie-bezopasnosti-avtomatizirovannykh-sistem-upravleniya-tekhnologicheskimi-protsessami-asutp/#open-tab-1.

[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» // Российская газета. – 2014. – 6 августа.

критически важных и потенциально опасных объектов, а также представляющих повышенную опасность для жизни или здоровья людей и для окружающей природной среды. Согласно нормативных подходов разрабатываемые на предприятиях организационно-распорядительные документы по защите информации (ЗИ) должны охватывать, в том числе, и области анализа угроз безопасности информации в АСУТП и соответствующих рисков их реализации.

К основным угрозам безопасности АСУТП следует отнести:

- внешнее проникновение с выведением АСУТП и управляемых объектов из строя;
- внешнее несанкционированное управление технологическими объектами с определенными целями;
- блокирование управления АСУТП и управляемыми объектами;
- несанкционированное обновление ПО для изменения режимов работы технологических объектов[4].

Каким образом решаются вопросы анализа рисков безопасности АСУТП рассмотрим на примере из практики управления отечественными предприятиями.

Так, специалистами Rusal Global Management было обследовано 5 предприятий концерна и 269 задач (подсистем) АСУТП. Было установлено, что 212 задач (78,8%) имеют непосредственное воздействие на технологическое оборудование через программируемые логические контроллеры (Programmable Logic Controller, PLC) т.е. возможно прямое деструктивное воздействие на технологический процесс различными методами атак. Через остальные задачи (57 или 21,2%) прямое воздействие невозможно, но, информация, обрабатываемая этими системами, влияет на принятие решение технологами (управление ходом производственного процесса)[5].

Для оценки рисков информационной безопасности систем АСУТП была использована экспертная оценка рисков, включающая идентификацию источников угроз, методов реализации угроз и текущих уязвимостей систем АСУТП. В дальнейшем проводилась обработка рисков, предполагающая принятие решений по снижению, уклонению, передачи или принятию рисков, а также управление рисками - формирование плана по мерам воздействия на риски.

Проведенная оценка рисков безопасности показала, что из 212 задач, оказывающих непосредственное воздействие на технологическое оборудование через PLC:

- 10 имеют самый высокий риск, величина возможных потерь, при вредоносном воздействии на технологию, превосходит критический уровень, реализация угрозы способна привести к значительным финансовым потерям или утрате конкурентных преимуществ;

[4] Романченко Д. Обеспечение безопасности автоматизированных систем управления технологическими процессами (АСУТП) [Электронный ресурс] – Режим доступа: http://www.ibs.ru/it-infrastructure/information-security/obespechenie-bezopasnosti-avtomatizirovannykh-sistem-upravleniya-tekhnologicheskimi-protsessami-asutp/#open-tab-1.

[5] Трушкин С.Б. Планирование мероприятий по воздействию на риски ИБ для систем автоматизации производства и информационно-технологических систем предприятий [Электронный ресурс] – Режим доступа: http://www.infosecurity-forum.ru/download/Trushkin.pdf.

- 45 задач имеют такие свойства, что реализация информационных атак может привести вследствие нарушения целостности, конфиденциальности или доступности критичных информационных активов АСУТП, существенному ущербу;
- при негативном воздействии на 50 задач потери не будут серьезными, но влияние на производственно-технологические и бизнес-процессы может быть ощутимо;
- остальные 107 таковы, что потери в случае реализации атак являются несущественными либо возможность реализации атак чрезвычайно мала, либо влияние на основные производственно-технологические и бизнес- процессы предприятий незначительно.

Можно сделать вывод, что порядка 5% задач имеют критический риск и около 50% незначительны или маловероятны.

Анализ распределения вероятных источников угроз показал, что в наибольшей степени они могут быть отнесены к рискам, связанным с работой персонала предприятий:

- основной персонал (пользователи) - 34%;
- основной технический персонал - 22%.

Кроме этого 30% совокупных рисков приходятся на внешних пользователей, не являющихся работниками предприятия:

- персонал, участвующий в разработке АСУТП (18%);
- подрядчики (12%).

Оставшиеся 14% совокупных рисков пришлись на:

- нелояльные структуры (конкуренты, иностранные спецслужбы и пр.) - 8%;
- криминал (хакеры, кибертеррористы и пр.) - 4%;
- силовые и регулирующие государственные органы - 2%.

Таким образом, проведенный анализ рисков АСУТП на 5 предприятиях показал, что наиболее вероятными источниками угроз безопасности АСУТП выступает персонал предприятия. В качестве основных факторов, влияющих на защищенность АСУТП являются отсутствие развитых средств ИБ в составе технической инфраструктуры АСУТП, характерной для современных ИТ-систем, игнорирование требований ИБ при осуществлении модернизации и технического обслуживания, слабая организационная составляющая обеспечения ИБ, а также отсутствие единого центра компетенции АСУТП в компании.

Для снижения рисков нарушения безопасности АСУТП возможно использование разработок отечественной оборонной промышленности. Так, Всероссийским научно-исследовательским институтом автоматизации управления в непромышленной сфере (ВНИИНС) на базе дистрибутива GNU/Linux разработана операционная система (ОС) МСВС, в которой используются встроенные технологии защиты информации на основе мандатного управления доступом, списков контроля доступа, использования ролевой модели, а также развитые средства аудита (протоколирования событий)[6].

[6] Изделия ВНИИНС – ОС МСВС 3.0 и СУБД «Линтер - ВС» 6.0 получили положительное заключение ФСБ России [Электронный ресурс] – Режим доступа: http://www.vniins.ru/about_certificates.

ОС МСВС обеспечивает многоуровневую систему приоритетов с вытесняющей многозадачностью, виртуальную организацию памяти и полную сетевую поддержку; работает с многопроцессорными (symmetrical multiprocessing, SMP) и кластерными конфигурациями на платформах Intel, MIPS и SPARC.

В марте 2014 года ВНИИНС был подтвержден статус ведущей организации в области защиты информации получением положительного заключения экспертной организации на ОС МСВС 3.0 о соответствии системы требованиям безопасности информации ФСБ России[7].

Важнейшим моментом с точки зрения обеспечения целостности системы защиты МСВС выступает операция регистрации новых пользователей, когда происходит определение атрибутов пользователя, включая атрибуты безопасности, в соответствии с которыми в дальнейшем система управления доступом контролирует работу пользователя. При этом основой для мандатной модели составляет та информация, которая вводится пользователем при регистрации в системе.

В МСВС в целях реализации дискреционного управления доступом используются механизмы бит прав доступа и списков прав доступа (ACL - access control list). При этом оба указанных механизма реализуются на уровне файловой системы МСВС и служат для задания прав доступа к объектам файловой системы, исходя из категорий пользователей системы (владелец, группа, остальные).

Особенность МСВС заключается в децентрализации функций суперпользователя. При этом задача администрирования системы разделена на несколько составных частей, для выполнения которых выделены системные администраторы разных категорий исходя из функциональной направленности (конфигурирование, безопасность и аудит). С точки зрения ОС указанные администраторы выступают обычными пользователями, но им предоставлена возможность запуска специальных административных программ и доступ к соответствующим конфигурационным файлам[8].

Важным функциональным преимуществом встроенной СЗИ ОС МСВС является протоколирование всех событий, имеющих отношение к безопасности, в том числе и действия администраторов.

Децентрализация функций суперпользователя в ОС МСВС позволяет реализовать принцип «четырех глаз», при котором осуществляется дублирование важнейших операций доступа к системе. Так, при регистрации нового пользователя МСВС администратор конфигурирования создает новую учетную запись, а администратор безопасности затем регистрирует нового пользователя в базе данных СЗИ. Только после проведения этой комплексной двухэтапной операции новый пользователь способен осуществить вход в систему.

Использование МСВС выглядит важным, учитывая то, что согласно проведенному анализу АСУТП на предприятиях РУСАЛ, основные риски нарушения безопасности приходятся на внутренних пользователей. Следует полагать, что данная ситуация типична для большинства промышленных предприятий.

В качестве технических мер повышения защищенности АСУТП и снижения рисков нарушения безопасности можно предложить следующие мероприятия:

---

[7] Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере им. В.В. Соломатина [Электронный ресурс] – Режим доступа: http://www.vniins.ru.

[8] Тюлин А., Жуков И., Ефанов Д. На страже конфиденциальной информации // Открытые системы [Электронный ресурс] – Режим доступа: http://www.osp.ru/os/2001/10/180520.

- использование межсетевого экранирования между уровнями корпоративной системы и АСУТП;
- защита удаленного доступа (BYOD);
- автоматизированный инструментальный анализ защищенности;
- антивирусная защита;
- обнаружение вторжений (IDS/IPS);
- централизованный сбор и анализ событий безопасности;
- централизованное управление конфигурациями устройств.

По нашему мнению, наиболее эффективным методом защиты безопасности АСУТП является построение комплексной системы защиты АСУТП, которая должна реализовывать следующие функции:

- идентификацию и управление доступом субъектов к объектам защиты;
- целостность программной среды;
- защиту машинных носителей информации;
- антивирусную защиту;
- регистрацию событий и расследование инцидентов ИБ;
- межсетевое экранирование;
- обнаружение/противодействие вторжениям/атакам различной природы;
- контроль/анализ защищенности информационных систем;
- защиту среды виртуализации;
- обеспечение безопасной разработки прикладного ПО;
- управление обновлениями программного обеспечения;
- обеспечение доступности технических средств и информации;
- защиту автоматизированной системы и ее компонентов.

Это позволит добиться следующих результатов:

- снизить риски отказа или внештатного функционирования систем АСУТП и контролируемых/управляемых объектов;
- обеспечить соответствие требованиям законодательства России и нормативным требованиям ФСТЭК России по защите АСУТП;
- создать эшелонированную систему выявления и подавления современных таргетированных атак;
- даст возможность оперативного консолидированного мониторинга и расследования атак и инцидентов, в том числе в реальном времени.

Таким образом, для снижения рисков нарушения безопасности АСУТП необходимо проведение мероприятий на системном уровне. Построение защищенной АСУТП на базе ОС МСВС на промышленных предприятиях выглядит разумным решением не только с позиции обеспечения безопасности, но и снижения зависимости от импортных ИТ-решений, что

крайне важно для крупных коммерческих организаций, заинтересованных в гарантированной защите конфиденциальной информации.

ЛИТЕРАТУРА

1. Андрианов В.В. Обеспечение информационной безопасности бизнеса / В.В. Андрианов, С.Л. Зефиров, В.Б. Голованов. - М.: ЦИПСиР, 2011. - 373 с.
2. Астапчук В.А. Архитектура корпоративных информационных систем / В.А. Астапчук, П.В. Терещенко. – Новосибирск: НГТУ, 2015. - 75 с.
3. Дубинин Е.А. Оценка относительного ущерба безопасности информационной системы: монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.
4. Дятлов С.А. Информационно-сетевая экономика: структура, динамика, регулирование: Монография / С.А. Дятлов, В.П. Марьяненко, Т.А. Селищева - М.: НИЦ ИНФРА-М, 2016. - 414 с.
5. Комплексная безопасность бизнеса в условиях экономической нестабильности: материалы науч.-практ. конф. / отв. ред. Е.В. Стельмашонок, С.Н. Максимов. – СПб.: Изд-во СПбГЭУ, 2014. – 151 с.
6. Малюк А.А. Теория защиты информации. - М.: Гор. линия-Телеком, 2012. – 184 с.
7. Прокопенко А.В. Синтез систем реального времени с гарантированной доступностью программно-информационных ресурсов: монография / А.В. Прокопенко, М.А. Русаков, Р.Ю. Царев. - Красноярск: Сиб. федер. ун-т, 2013. - 92 с.
8. Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза: монография. - М.: ЮНИТИ-ДАНА: Закон и право, 2012. - 159 с.
9. Хабриева Т.А. Закон. Обеспечение безопасности и реальной экономики - М.: НИЦ ИНФРА-М, 2015. - 48 с.
10. Шаньгин В.Ф. Информационная безопасность и защита информации. – М.: ДМК Пресс, 2014. – 702 с.

Tsapko Gennady Pavlovich
National research Tomsk polytechnic university, Russia, Tomsk
E-mail: tsapkogp@gmail.com

Verigo Andrey Aleksandrovich
National research Tomsk polytechnic university, Russia, Tomsk
E-mail: andrey_verigo@mail.ru

Katashev Andrey Sergeevich
National research Tomsk polytechnic university, Russia, Tomsk
E-mail: katashev_as@mail.ru

Security risk analysis process control systems

Abstract. In this paper, a review of the main approaches to the analysis of safety and risk management of automated process control systems. The purpose of the study was to analyze the security risks of automated process control systems. The main research methods include: structural, comparative and systematic analysis. The authors identified the main threats to security in process control systems, as well as their sources. As an example, consider approaches to the analysis of risk and safety of the automated process control systems management in Russian companies, as well as security in a special operating system, developed by the All-Russian Scientific Research Institute of Control Automation in the industrial field. The conclusion about the need for measures to reduce the risk of a security breach of automated process control systems at the system level. Building a secure automated process control system based on national specialized operating systems in industrial plants looks reasonable solution, not only from the standpoint of safety, but also reduce dependence on imports of IT solutions, which is essential for large commercial organizations interested in the guaranteed protection of confidential information.

Keywords: safety; risk; automated process control system