УДК 004.056.53

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ

С.В. Голубев, кандидат экономических наук, доцент,
тел. 8(8422)55-95-54, des-s@mail.ru,
С.А. Голубева, кандидат экономических наук, доцент,
тел. 8(8422)55-95-54, golubevas83@mail.ru,
Е.А. Голубева, кандидат экономических наук, доцент,
тел. 8(8422)55-95-54, golubevaea@mail.ru
ФГБОУ ВО Ульяновская ГСХА

Ключевые слова: *автоматизированные системы управления, информационная безопасность, обеспечение безопасности, шифрование, вычислительные сети.*

Данная работа посвящена вопросам обеспечения информационной безопасности в автоматизированных системах управления. Описываются и анализируются методы обеспечения информационной безопасности в автоматизированных системах управления. Рассматривается отечественное и зарубежное законодательство в сфере информационной безопасности. Даются рекомендации по повышению безопасности информации в автоматизированных системах управления.

Вопросы обеспечения безопасности автоматизированных систем управления технологическим процессами становятся всё более актуальными. Если несколько лет назад эта тема поднималась в основном среди узкого круга специалистов, то сейчас она стала интересна собственникам систем управления, специалистам, занимающимся их эксплуатацией, разработкой и внедрением.

Все эксперты в области информационной безопасности соглашаются, что обеспечение безопасности автоматизированных систем управления технологическим процессами отличается от обеспечения безопасности корпоративных информационных систем. Обычно говорится о том, что необходимо уделять внимание не только обеспечению конфиденциальности, но также о том, что жизненный цикл у них отличается, и о том, что технологические окна у корпоративных информационных систем совсем не такие.

Российская нормативная база ориентирована на защиту информации. ФСТЭК в своей действующей нормативной документации ведет речь о безопасности информации в ключевых системах информационной ин-

фраструктуры. То есть в основе требований находится предположение, что необходимо защищать именно информацию в системе управления.

Зарубежные стандарты и практики предусматривают еще более широкое понятие объекта защиты – это вся информация, программно-технические средства и персонал, влияющий на технологический процесс.

В случае с автоматизированной системой управления технологическими процессами специалист по информационной безопасности чаще всего появляется уже на этапе промышленной эксплуатации. То есть перед специалистом по информационной безопасности есть система управления, которая в ряде случаев не может быть адекватно проанализирована, осмыслена и не может быть изменена. Лица, эксплуатирующие систему, и специалисты по безопасности могут только ей доверять и наблюдать за тем, как она работает. Это сильно ограничивает количество и качество мер, которые специалист может применить.

Традиционно самым слабым звеном всех технологических систем является человек. Это касается и обеспечения безопасности автоматизированных систем управления технологическим процессами. Их особенности не позволяют использовать специалиста с навыками защиты корпоративных информационных систем для защиты. Требуются другие базовые знания, применяются другие меры и ответственность.

Как следствие, специалисты по безопасности и эксплуататоры автоматизированных систем управления технологическим процессами в качестве защитной меры выбирают изоляцию системы. Но добиться изоляции практически невозможно. Связано это с тем, что современный бизнес требует получения оперативной информации о параметрах технологических процессов. Это подразумевает наличие канала связи сегментов сети автоматизированных систем управления технологическим процессами и корпоративных информационных систем.

Процессы создания системы управления защитой автоматизированных систем управления технологическим процессами от киберугроз, анализа и управления рисками во многом схожи с аналогичными, заданными стандартом ISO 27001 для ИТ-систем, с учетом специфики реализации. Основой для определения требований, предъявляемых к проектируемой системе, является анализ рисков. Краеугольными камнями анализа рисков являются идентификация, классификация и оценка. Выбор методики оценки рисков остается на усмотрение владельца автоматизированных системы управления технологическим процессами и зависит от специфики используемых систем.

Стандарт IEC 62443 предусматривает внедрение хорошо известных специалистам, знакомым с семейством ISO 27000, процессов: управление инцидентами, управление изменениями, управление конфигурациями, планирование восстановления деятельности и непрерывности бизнеса, повышение осведомленности и т. д. И IEC 62443, как и все стандарты и в области информационной безопасности, подразумевает непрерывный жизненный цикл процессов безопасности, поддерживаемый на всех стадиях существования объекта защиты.

Реализовывать технические меры обеспечения безопасности в автоматизированных системах управления технологическим процессами следует прежде всего – сегментированием. Технические средства, доступные на рынке, позволяют осуществлять его на верхних и средних уровнях архитектуры. Сегментирование позволит при необходимости исключить неисправные или зараженные контроллеры, устройства связи, серверы и автоматизированные рабочие места управления из сети управления. Также с помощью таких устройств можно доставить функционал в сеть управления технологическими процессами и осуществлять фильтрацию не только на уровне сетевых адресов оборудования в, но и на уровне объектов, протоколов передачи данных и управления.

Шифрование трафика в сетях также является приоритетной задачей. Более того, международные стандарты рекомендуют его реализовывать. Речь не идет об использовании сертифицированных по требованиям ФСБ криптографических средств, но обеспечить передачу трафика по «закрытому» каналу связи возможно. Однако не стоит забывать, что шифрование трафика оказывает влияние на характеристики канала. В ряде случаев (например, в электроэнергетике) увеличение задержки на определенных типах каналов является недопустимым. Средства защиты IP сетей, применяемые при выходе каналов передачи данных за пределы контролируемой зоны, также применимы, при этом необходимо помнить о требованиях по обеспечению надежности.

Средства сбора и передачи событий от источников АСУ ТП тоже существуют. Это делает возможным применение корпоративных систем сбора и анализа событий информационной безопасности.

Обеспечить изоляцию сети автоматизированных систем управления технологическим процессами от других в современных условиях практически невозможно, поэтому задачи контроля сетевого периметра важны. Однако необходимо не только контролировать потоки по атрибутам сетевого и транспортного уровня, но и осуществлять контроль содержания передаваемой информации. Большинство протоколов

взаимодействия устройств низкого уровня не поддерживают взаимную аутентификацию устройств или проверку содержимого передаваемых пакетов. Отсутствие контроля подлинности передаваемых данных и их источников приводит к появлению ряда уязвимостей, успешно использованных при реализации атак. Развитие современных технологий в области обеспечения безопасности позволяет обеспечить такой контроль.

Вопросы обеспечения физической безопасности еще более актуальны. Необходимо применять более совершенные системы контроля доступа, видеонаблюдения и пр.

Необходимость строгого регламентирования процессов обеспечения безопасности имеет ничуть не меньшую важность, чем реализация технических мер, это отмечается и в рекомендациях соответствующих стандартов.

Важность освещенной в статье темы и возрастающее внимание к ней говорит о том, что рынок будет и дальше активно развиваться. Стоит ожидать появления новых средств для обеспечения безопасности, совершенствования стандартов и рекомендаций.

Библиографический список

1. ФЗ № 149 «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.09.2015)
2. Борисов М. А., Заводцев И. В., Чижов И. В. Основы программно-аппаратной защиты информации. (Гриф УМО по классическому университетскому образованию). Изд.2. - М.: Книжный дом «ЛИБРОКОМ», 2013. — 376 с.
3. Борисов М. А., Романов О. А. Основы организационно-правовой защиты информации. (Гриф УМО по дополнительному профессиональному образованию). №2. Изд.3, перераб. и доп. - М.: Книжный дом «ЛЕНАНД», 2014. — 248 с.
4. Будников С.А., Паршин Н.В. Информационная безопасность автоматизированных систем: Учебное пособие, издание второе, дополненное - Издательство им. Е.А.Болховитинова. - Воронеж, 2011
5. Гафнер В.В. Информационная безопасность: учеб. пособие. – Ростов на Дону: Феникс, 2010. - 324 с.
6. Малюк А.А. Теория защиты информации. — М.: Горячая линия - Телеком, 2012. — 184 с.

INFORMATION SECURITY IN AUTOMATED CONTROL SYSTEMS

Golubev S.V., Golubeva S.A., Golubeva E.A.

Keywords: *automated control systems, information security, security, encryption, computer networks.*

This work is devoted to the issues of information security in automated control systems. It describes and analyzes the methods of information security in automated control systems. We consider the domestic and foreign legislation in the field of information security. Recommendations for improving information security in automated control systems.