УДК 004.056.53

С.В. Кирсанов

Защита информационной технологии удаленного управления объектами газотранспортной системы

Предложен общий методологический подход организации защиты технологий удаленного управления объектами газотранспортной системы (ГТС), а также влияние внедрения технологии удаленного управления на информационную безопасность газотранспортного предприятия. Приведена модель автоматизированного предприятия. Сгруппированы основные функции процессов, влияющих на информационную безопасность и автоматизированную систему управления технологическим процессом.

Ключевые слова: автоматизированная система управления технологическим процессом, информационная безопасность, малолюдные технологии, удаленное управление.

Актуальность проблемы. Технологии удаленного управления в газовой отрасли также называют «малолюдными технологиями». Внедрение технологий удаленного управления объектами ГТС направлено на оптимизацию процессов хозяйственной деятельности и на повышение уровня безопасности технологических объектов.

Внедрение информационных технологий (процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [1]) удаленного управления на предприятии позволяет решать широкий спектр задач, таких как:

- оптимизация финансовых, материальных и других видов затрат;
- централизация процессов управления;
- централизованный сбор и агрегация данных;
- визуализация технологических процессов;
- сокращение требований по наличию на местах высококвалифицированного персонала, необходимого для обеспечения процесса эксплуатации;
- уменьшение рисков возникновения и развития аварийных ситуаций.

«Малолюдные технологии» затрагивают решения в области автоматизации, информатизации и связи. Процессы внедрения направлены на модернизацию средств и систем автоматизации, информатизации и связи и осуществляются в рамках строительства новых объектов, а также реконструкции, модернизации, переоснащения и ремонта существующих введенных в эксплуатацию объектов.

Технологии удаленного управления интегрируются в автоматизированные системы управления технологическим процессом (АСУ ТП) и системы диспетчерского сбора информации и управления объектами газотранспортной системы.

Учитывая тот факт, что технологические объекты газотранспортных предприятий часто находятся на территории нескольких субъектов Российской Федерации и географически удалены от диспетчерской службы предприятия, можно утверждать, что задача удаленного диспетчерского мониторинга и управления объектами ГТС становится особо актуальной и значимой.

Существует два подхода к решению задачи удаленного управления:

- внедрение отдельных проектных решений связи, автоматизации и информатизации, направленных на реализацию поставленной задачи;
- внедрение на базе существующей технологической, информационной и телекоммуникационной инфраструктуры готовых решений и информационных технологий (ИТ) удаленного управления.

Первый вариант трудоемок, долгосрочен и требует больших финансовых затрат, а для реализации второго необходимо провести исследование, апробирование, испытания информационных технологий в готовом исполнении, доступных на момент начала решения задачи.

Обеспечение информационной безопасности. Для безопасного удаленного управления объектами газотранспортной системы необходимо разработать и провести комплекс мероприятий по информационной безопасности (ИБ) [4–7].

Сфера задач, решаемых в рамках обеспечения ИБ при внедрении технологий удаленного управления в АСУ ТП, смещается от традиционного обеспечения конфиденциальности в сторону обеспечения целостности, доступности, безотказности и других важных свойств газотранспортных систем. Это объясняется тем, что информация в АСУ ТП представлена в виде потоков данных (информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека [2]), которые обрабатываются в системах в виде и объеме, не подпадающем под определение конфиденциальной информации. Потоки данных в системах автоматизации сводятся, обрабатываются и передаются в иерархически вышестоящие информационные системы. И в результате лишь малую часть сведенных данных можно отнести к информации, подпадающей под определение конфиденциальности [8, 9]. Такие сведения в большинстве случаев накапливаются и обрабатываются уже на совершенно ином инфраструктурном уровне информационных систем (совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [1]), не связанном с АСУ ТП (как правило, с участием человека) [3], что соответствует согласно приведенной на рис. 1 модели автоматизированного предприятия.

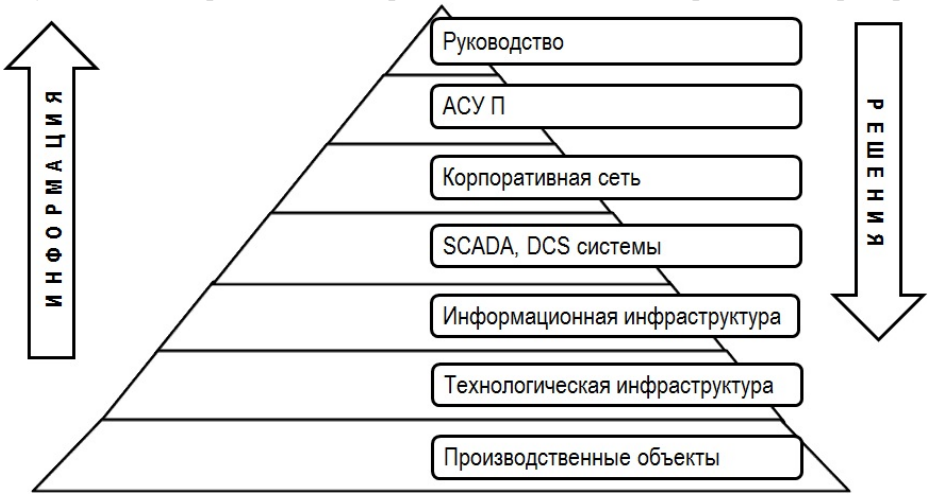

Рис. 1. Модель автоматизированного предприятия

При разработке мероприятий ИБ необходимо учитывать то, что угрозы безопасности появляются и становятся актуальными всегда, когда в информационной системе возникает возможность реализации неблагоприятных или опасных условий, способных повлиять на ее работоспособность.

Информационные технологии в готовом исполнении, являющиеся неотъемлемой частью любой информационной системы, с точки зрения информационной безопасности – это объекты, требующие внимательного изучения и анализа [10, 11].

Для систем АСУ ТП можно выделить две группы угроз безопасности, которые при их реализации могут повлиять на безопасность объектов газотранспортной системы (рис. 2):

– угрозы несанкционированного доступа;

– угрозы несанкционированного воздействия.

Другая важная составляющая часть, которую необходимо учитывать при разработке мероприятий защиты, – это риски информационной безопасности, определяющие возможность реализации угроз безопасности. В отличие от угроз риски возникают, растут или

Рис. 2. Модель угроз безопасности

уменьшаются по мере проявления тех или иных скрытых факторов (внутренних или внешних) и изменений в условиях функционирования информационной системы.

Деятельность по обеспечению ИБ направлена на снижение уровня рисков ИБ и недопущение возможностей реализации угроз безопасности для информационных систем ГТС. Вышеописанные цели обеспечения ИБ достигаются решением различных групп задач:

- защита информационных ресурсов (уровень частных задач);
- защита информационных технологий (уровень общих инфраструктурных задач);
- защита информационных систем (уровень групповых задач).

Для решения задач защиты необходимо выделить в составе исследуемых систем и технологий объекты защиты. Проведя анализ структуры комплексов АСУ ТП и систем диспетчерского управления, можно выделить перечень объектов защиты:

1) в информационных системах: информационные технологии хранения и обработки информации (общесистемное и прикладное программное обеспечение (ПО), информационные технологии удаленного управления объектом информатизации (специализированное ПО);

2) в системах связи: средства связи локальных вычислительных сетей и региональной сети передачи данных (далее – ЛВС и РСПД);

3) в системах автоматизации: объекты информатизации комплексов АСУ ТП, информационные системы, системы связи.

При интеграции информационных технологий удаленного управления в состав систем комплекса АСУ ТП актуальными становятся угрозы несанкционированного воздействия на системы автоматизации и входящие в их состав компоненты. Перечислим следующие подсистемы и компоненты интегрированной системы удаленного управления объектом ГТС:

1) на уровне АСУ ТП: объекты информатизации комплекса АСУ ТП, объекты ГТС, объекты информатизации центральной системы диспетчерского управления;

2) на уровне информационных систем диспетчерского управления: система диспетчерского управления технологическим процессом объекта ГТС (в составе комплекса АСУ ТП), центральная система диспетчерского управления;

3) на уровне средств и систем связи: ЛВС АСУ ТП, ЛВС Центральной диспетчерской службы, РСПД;

4) на уровне информационных технологий: специализированное ПО удаленного управления объектами информатизации;

5) на уровне информационных потоков: поток данных, содержащий визуальную информацию объекта удаленного управления и информацию о передаваемых на удаленный объект управляющих воздействий.

Реализация угроз несанкционированного воздействия на системы автоматизации и входящие в их состав компоненты может привести к нарушению режима функционирования или сбою в технологическом процессе.

В рассматриваемых условиях информационные ресурсы – это потоки данных, содержащие информацию о состоянии объектов газотранспортной системы. Системы диспетчерского управления устроены таким образом, что вся необходимая для диспетчерского управления информация поступает и визуализируется на автоматизированном рабочем месте (АРМ) диспетчера.

Защита информационных ресурсов в АСУ ТП достигается путем ограничения физического и логического доступа к средствам управления объектами ГТС [12–16].

При этом, проводя анализ целей, задач и ролей подразделений, ответственных за обеспечение информационной безопасности и автоматизации производственной деятельности, указывает на множество функций, сгруппировав которые, можно сформировать типовые для этих подразделений процессы:

- организация и обеспечение производственных объектов и технологических процессов средствами автоматизации, телемеханизации, пожарной безопасности и прочими средствами АСУ ТП;
- организация и обеспечение состояния защищенности интересов, ресурсов и объектов производства основных процессов газотранспортного предприятия.

Вышеописанные процессы можно выразить в виде функций:

- $B(bp1, bp2, ..., Ib, Ap, Z, \Pr, ..., bpn)$ – основной процесс газотранспортного предприятия;
- $B(bp1, bp2, ..., Ib, Ap, Z, \Pr, ..., bpn) = \sum_{i=1}^{n} Bpi + Ap + Ib - Z - \Pr - Rp$;

– $Ib(p1,p2,p3,...,pn)$ – процесс ИБ;

– $Ap(p1,p2,p3,...,pm)$ – процесс АСУ ТП;

– $Z(c1,c2,...,cn)$ – цели и задачи злоумышленника;

– $\Pr(c1,c2,c3...,cm)$ – прогресс ИТ, ИБ, АСУ ТП, тенденции и развитие, требования свыше;

– $Rp(p1,p2,p3,...,pk)$ – расходы на ведение бизнеса.

Задача предприятий состоит в достижении максимума значения функции: $\max B(bp1,bp2,...,Ib,Ap,Z,\Pr,...,bpn)$.

В алгоритме расчета функции *B* функция *Ap* вносит вклад больше, чем функция *Ib:* $Ap(p1,p2,p3,...,pm) \geq Ib(p1,p2,p3,...,pn)$. Это связано с тем, что функция *Ap* максимизирует и оптимизирует работу технологических процессов, а функция *Ib* минимизирует риски и затраты функции *B*. Это продолжается до тех пор, пока вклад функции *Z* не внесет свои коррективы в алгоритм расчета значений функции B, $Z(c1,c2,...,cn) \geq Ap + \Pr + \sum_{1}^{k} Bp$, либо до тех пор, пока себя не проявит функция $\Pr(c1,c2,c3...,cm) \geq Ap + \Pr + \sum_{1}^{k} Bp$. В данном случае коррективами могут быть планы на развитие, внедрение «малолюдных технологий» на других объектах, организация централизованного управления объектами производства, увеличение территории ответственности.

Заключение. В сфере информационных технологий основополагающим фактором, способным оказывать влияние на ИБ, является то, что в программном обеспечении существуют ошибки, наличие которых приводит к появлению в вычислительной системе возможности нарушения целостности ПО или изменения режима функционирования системы. Описанное явление становится уязвимостью для любой вычислительной системы, где используется это программное обеспечение.

При организации защиты информационных систем необходимо учитывать протекающие в системе информационные потоки, а также структуру взаимосвязи объектов автоматизации, связи и информатизации. Необходимо рассмотреть и изучить все компоненты информационной системы, выявить критически важные информационные процессы и компоненты системы, в которых реализация угроз безопасности может повлиять на структурную целостность и способность системы исполнять свои функции.

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=147341, свободный (дата обращения: 10.06.2013).

2. ГОСТ 15971–90 «Системы обработки информации. Термины и определения» [Электронный ресурс]. – Режим доступа: http://www.vashdom.ru/gost/15971-90/, свободный (дата обращения: 10.06.2013).

3. Нестеров А.Л. Проектирование АСУТП: метод. пособие. – Кн. 1. – М.: ДЕАН, 2006. – 552 с.

4. Прищеп С.В. Подходы и критерии оценки рисков информационной безопасности/ С.В. Прищеп, С.В. Тимченко, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 15–21.

5. Оценка рисков информационной безопасности телекоммуникационной системы / А.А. Кускова, А.А. Шелупанов, Р.В. Мещеряков, С.С. Ерохин // Информационное противодействие угрозам терроризма. – 2009. – № 13. – С. 90–92.

6. Миронова В.Г. Методология формирования угроз безопасности конфиденциальной информации в неопределенных условиях их возникновения / В.Г. Миронова, А.А. Шелупанов // Изв. Южного федерального ун-та. Технические науки. – 2012. – Т. 137, № 12. – С. 39–45.

7. Епифанцев Б.Н. Conception of interconnecting security system for trunk pipelines against intended threats / Б.Н. Епифанцев, А.А. Шелупанов // Электронный научный журнал «Нефтегазовое дело». – 2011. – № 1. – С. 20–34.

8. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1. – С. 28–35.

9. Автоматизированная система предпроектного обследования информационной системы персональных данных «Аист-П» / А.А. Шелупанов, В.Г. Миронова, С.С. Ерохин, А.А. Мицель // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2010. – № 1-1. – С. 14–22.

10. Исхаков С.Ю. Разработка методического и программного обеспечения для мониторинга работы локальных сетей / С.Ю. Исхаков, А.А. Шелупанов // Телекоммуникации. – 2013. – № 6. – С. 16–20.

11. Крайнов А.Ю. Модель надежности передачи информации в защищенной распределенной телекоммуникационной сети / Ю.А. Крайнов, А.А. Шелупанов // Изв. Том. политех. ун-та. – 2008. – Т. 313, № 5. – С. 60–63.

12. Сабанов А.Г. Требования к системам аутентификации по уровням строгости / А.Г. Сабанов, А.А. Шелупанов, Р.В. Мещеряков // Ползуновский вестник. – 2012. – № 2–1. – С. 61–67.

13. Миронова В.Г. Реализация модели Take-Grant как представление систем разграничения доступа в помещениях / В.Г. Миронова, А.А. Шелупанов, Н.Т. Югов // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2011. – № 2–3. – С. 206–210.

14. Мещеряков Р.В. Характеристики надежности распределенных криптографических информационно-телекоммуникационных систем с ограниченными ресурсами / Р.В. Мещеряков, А.А. Шелупанов, Т.Ю. Зырянова // Вычислительные технологии. – 2007. – Т. 12, спец. выпуск 1. – С. 62–67.

15. Встраивание криптографических функций в систему связи с ограниченными ресурсами / С.К. Росошек, Р.В. Мещеряков, А.А. Шелупанов, С.С. Бондарчук // Вопросы защиты информации. – 2004. – № 2. – С. 22–25.

16. Технология прямого поиска при решении задач прикладной математики / В.А. Архипов, С.С. Бондарчук, И.Г. Боровской, А.А. Шелупанов // Вычислительные технологии. – 1995. – Т. 4, № 10. – С. 19.

Кирсанов Сергей Владимирович
Зам. нач. отд. информационной безопасности
ООО «Газпром трансгаз Томск»
Тел.: 8 (383-2) 60-36-36
Эл. почта: S.Kirsanov@gtt.gazprom.ru

Kirsanov S.V.

The protection of information technology of remote control by objects of the gas transmission system

The common methodological approach to protection organization of the technology of remote control by objects of the gas transmission system and influence of introduction the technology of remote control on information security of the gas transmission company are suggested at this article. The model of automatized company is described. The basic functions of the processes affecting the information security and the automated process control system are grouped.

Keywords: automated process control system (APCS), information security, minimally-manned operations, remote control.