УДК 004.056.53

С.В. Кирсанов

Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли

Предложен метод оценки угроз информационной безопасности в автоматизированных системах управления технологическим процессом (АСУ ТП) газовой отрасли на основе международных стандартов, его роль в процессе оценивания рисков безопасности и способ применения. Выделены источники угроз для АСУ ТП газотранспортных предприятий. Предложено применение для оценки угроз адаптированного для АСУ ТП стандарта системы оценки уязвимостей CVSS. Приведен положительный пример применения описанного метода на примере ООО «Газпром трансгаз Томск».

Ключевые слова: автоматизированная система управления технологическим процессом, информационная безопасность, уровень безопасности.

Актуальность проблемы. Для крупных промышленных объектов с повышенной техногенной опасностью, к которым относятся в том числе и объекты магистральных газопроводов, важнейшим является требование повышенной надежности систем автоматизации, поскольку в данном случае недопустимы даже мелкие аварии из-за возможного значительного экологического и материального ущерба. Следовательно, решения, направленные на выполнение этого требования, имеют наивысший приоритет как при выборе программно-аппаратных средств, так и при выборе методов управления, используемых на всех уровнях автоматизации. Автоматизация управления объектами газоснабжения, в частности автоматизация управления технологическими процессами газотранспортных предприятий, как любая другая, несет угрозу реализации деструктивного воздействия на информационную и телекоммуникационную инфраструктуры со стороны злоумышленников. При проведении любых работ по автоматизации деятельности предприятий немаловажным и заслуживающим особого внимания является вопрос обеспечения информационной безопасности (ИБ) автоматизированных систем управления. Поддерживание приемлемого уровня ИБ автоматизированных систем – процесс перманентный, это связано с постоянным появлением новых уязвимостей и угроз или модернизацией существующих систем. При этом возникает необходимость оценить и классифицировать угрозы ИБ АСУ ТП для принятия дальнейших защитных мер.

Угрозы ИБ АСУ ТП. Под угрозами ИБ АСУ ТП понимается возможность возникновения такого явления или события, следствием которого могут быть негативные воздействия на информацию, обрабатываемую в АСУ ТП.

В качестве базовых негативных воздействий на информацию рассматривается нарушение следующих свойств обрабатываемой в АСУ ТП информации:

- конфиденциальность информации;
- целостность информации;
- доступность информации.

Угрозы ИБ используют уязвимости компонентов АСУ ТП для реализации негативных воздействий на информацию, обрабатываемую в АСУ ТП. Одна угроза ИБ или группа угроз ИБ могут использовать одну уязвимость или группу уязвимостей.

Под источником угроз ИБ понимается непосредственный исполнитель угрозы ИБ в плане ее негативного воздействия на информацию [1, 7, 8, 10]. Все источники угроз ИБ классифицируются следующим образом:

- по отношению к АСУ ТП: на внутренние и внешние;
- по происхождению: на естественные (стихийные и техногенные) и антропогенные.

Список возможных источников угроз ИБ АСУ ТП представлен в табл. 1.

Существует много методов оценки угроз ИБ информационных систем, но немногие из них применимы для АСУ ТП ввиду того, что системы АСУ ТП состоят из большого количества взаимосвязей от простейших датчиков и механизмов до систем верхнего уровня (систем диспетчерского

управления и сбора данных (аббр. от англ. Supervisory Control And Data Acquisition – SCADA-система) [2]. Поэтому, чтобы выполнить оценку угроз ИБ АСУ ТП, необходимо проводить адаптацию существующих методов [9].

Таблица 1

Источники угроз ИБ АСУ ТП

Источники угроз ИБ	Акроним	Наименование источника угроз ИБ
Внутренние антропогенные	ПЕР	Вспомогательный персонал
	ТЕХ	Инженерно-технический персонал
	ПОЛ	Пользователи АСУ ТП
	РАЗ	Разработчики компонентов АСУ ТП
	АДМ	Администраторы (системные, сетевые), ответственный за обеспечение ИБ
	РУК	Руководители (отделов, отделений, лабораторий)
Внешние антропогенные	ПОС	Посетители (клиенты, партнеры, подрядчики, аудиторы и др.)
	ОБС	Обслуживающие организации
	УВС	Уволенные сотрудники
	ВНЕШ	Внешние злоумышленники (конкуренты, криминал)
Внутренние техногенные	ВНУТ	Количественная или качественная недостаточность компонентов АСУ ТП (аппаратные средства, программные средства, инженерно-технические средства)
Внешние техногенные	ВНЕТ	Внешний техногенный источник угроз (энергетические сети, инженерные сети, средства связи, транспорт)
Стихийные	СТХ	Стихийный источник угроз (наводнение, ураган, землетрясение, климатические явления)

Для составления перечня возможных угроз ИБ используется каталог угроз, приведенный в стандарте по анализу и управлению рисками ИБ CRAMM версии 5.1 (CCTA Risk Analysis and Management Method) [3].

Угрозы ИБ используют уязвимости для реализации негативных воздействий на ресурсы АСУ ТП. Возможность реализации угрозы ИБ и степень воздействия на ресурсы АСУ ТП определяют уровень угрозы ИБ – степень критичности для газотранспортных предприятий.

Для определения уровня угрозы ИБ применим адаптированный для оценки угроз стандарт системы оценки уязвимостей CVSS [4–6, 10].

Каждой угрозе ИБ присваивается уровень влияния (Impact), характеризующий степень воздействия угрозы ИБ на конфиденциальность, целостность и доступность информации, обрабатываемой в АСУ ТП. Каждая угроза ИБ характеризуется возможностью реализации (Exploitability).

Уровень влияния и возможность реализации задают базовый уровень угрозы ИБ (BS – Base Score). Расчет базового уровня угрозы ИБ осуществляется по следующей формуле:

$$BS = ((0{,}6 * \mathrm{Im}\,pact) + (0{,}4 * Exploitability) - 1{,}5 * f(\mathrm{Im}\,pact), \quad (1)$$

где результат округляется с точностью до десятых.

Уровень влияния угрозы ИБ рассчитывается по следующей формуле:

$$\mathrm{Im}\,pact = 10{,}41 * (1 - (1 - Conf\,\mathrm{Im}\,pact) * (1 - Integ\,\mathrm{Im}\,pact) * (1 - Avail\,\mathrm{Im}\,pact)), \quad (2)$$

где результат округляется с точностью до десятых.

Возможность реализации угрозы ИБ рассчитывается по следующей формуле:

$$Exploitability = 20 * AccessVector * AccessComplexity * Authentication, \quad (3)$$

где результат округляется с точностью до десятых.

В табл. 2 приведены параметры, используемые для расчета базового уровня угроз ИБ АСУ ТП газотранспортных предприятий.

Уровень угрозы ИБ АСУ ТП принимает следующие значения:

- низкий, если базовый уровень угрозы ИБ меньше 4;
- средний, если базовый уровень угрозы ИБ находится в диапазоне от 4 до 6,9;
- высокий, если базовый уровень угрозы ИБ находится в диапазоне от 7 до 9,9;
- критический, если базовый уровень угрозы ИБ равен 10.

Таблица 2

Параметры формулы базового уровня угроз ИБ АСУ ТП

Параметр	Значение
f(Impact)	Характеризует актуальность угрозы ИБ и принимает следующие значения: 0 – если Impact = 0; 1,176 – если Impact ≠ 0
ConfImpact	Confidentiality Impact – влияние на конфиденциальность. Определяет степень воздействия угрозы ИБ на конфиденциальность информации АСУ ТП и может принимать следующие значения: 0 – угроза ИБ не влияет на конфиденциальность; 0,275 – при определенных условиях угроза ИБ влияет на конфиденциальность; 0,66 – угроза ИБ влияет на конфиденциальность
IntegImpact	Integrity Impact – влияние на целостность. Определяет степень воздействия угрозы ИБ на целостность информации АСУ ТП и может принимать следующие значения: 0 – угроза ИБ не влияет на целостность; 0,275 – при определенных условиях угроза ИБ влияет на целостность; 0,66 – угроза ИБ влияет на целостность
AvailImpact	Availability Impact – влияние на доступность. Определяет степень воздействия угрозы ИБ на доступность информации АСУ ТП и может принимать следующие значения: 0 – угроза ИБ не влияет на доступность; 0,275 – при определенных условиях угроза ИБ влияет на доступность; 0,66 – угроза ИБ влияет на доступность
Access-Vector	Вектор доступа. Определяет отношение источника угрозы к компонентам АСУ ТП и может принимать следующие значения: 0,395 – угроза ИБ может быть реализована при наличии локального (либо физического) доступа к компонентам АСУ ТП; 0,46 – угроза ИБ может быть реализована из сети передачи данных (СПД) газотранспортного предприятия (либо угроза может быть реализована внутри территории предприятия); 1 – угроза может быть реализована из внешних по отношению к СПД предприятия сетей (угроза может быть реализована вне территории предприятия)
Access-Complexity	Сложность доступа и реализации угрозы. Характеризует наличие контрмер угрозам ИБ АСУ ТП и может принимать следующие значения: 0,35 – существующие контрмеры значительно затрудняют реализацию угрозы ИБ АСУ ТП; 0,61 – существующие контрмеры недостаточны для противодействия угрозе ИБ АСУ ТП; 0,71 – контрмеры отсутствуют
Authentica-tion	Аутентификация. Определяет права доступа источника угрозы, необходимые для реализации угрозы ИБ, и может принимать следующие значения: 0,45 – угроза может быть реализована при постоянном доступе к АСУ ТП (либо источник угрозы является компонентом АСУ ТП); 0,56 – угроза может быть реализована при временном (однократном) доступе (либо источник угрозы поддерживает функционирование АСУ ТП); 0,704 – угроза реализуется при отсутствии санкционированного доступа (источник угрозы не принадлежит предприятию)

Проведя анализ полученных результатов организационно-административного и технического обеспечения АСУ ТП по описанному выше методу, можно выявить, существуют ли противоречия между сложностью решаемых задач, высоким уровнем угроз и требований ИБ к АСУ ТП, с одной стороны, и существующим уровнем защищенности АСУ ТП, отсутствием комплексных решений в области построения системы защиты информации и наличием ограничений существующей АСУ ТП – с другой стороны.

Применение описанного метода оценки угроз ИБ АСУ ТП осуществлено при проектировании подсистемы обеспечения информационной безопасности систем автоматизации магистральных га-

зопроводов на участке, входящем в эксплуатационную зону ответственности ООО «Газпром трансгаз Томск».

Литература

1. Котенко И.В. Методы оценивания уязвимостей: использование для анализа защищенности компьютерных систем / И.В. Котенко, Е.В. Дойникова // Защита информации. Инсайд. – СПб.: Изд. дом «Афина». – 2011. – № 4. – С. 74–81.

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

3. CCTA Risk Analysis and Management Method [Электронный ресурс]. – Режим доступа: www.cramm.com/capabilities/risk.htm, свободный (дата обращения: 10.06.2013).

4. Котенко И.В. Система оценки уязвимостей CVSS и ее использование для анализа защищенности компьютерных систем/ И.В. Котенко, Е.В. Дойникова // Защита информации. Инсайд. – СПб.: Изд. дом «Афина». – 2011. – № 5. – С. 54–60.

5. A Complete Guide to the Common Vulnerability Scoring System Version 2.0 [Электронный ресурс]. – Режим доступа: http://www.first.org/cvss/cvss-guide.html, свободный (дата обращения: 15.04.2013).

6. Астахов А.М. Искусство управления информационными рисками. – М.: ДМК-Пресс, 2010. – 312 с.

7. 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.

8. Шелупанов А.А. Метод построения графа связи альтернатив с исходами и графа предпочтений в задаче принятия решений/ А.А. Шелупанов, Т.Ю. Зырянова // Вестник Тюмен. Гос. ун-та. – 2007. – № 5. – С. 101–106.

9. 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.

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

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 method for assessment of information security threats for APCS of the gas industry

The method for assessment of information security threats for APCS of the gas industry based on international standards, the role of this method in assessment process of security risks and its applying are suggested. The sources of information security threats for APCS of the gas transmission companies are identified. The applying of adapted standard of Common Vulnerability Scoring System (CVSS) for assessment of information security threats is suggested. And the positive example of using this method in Gazprom transgaz Tomsk LLC. is described.

Keywords: automated process control system (APCS), information security, security level.