УДК 004.056.53

А.К. Новохрестов, Д.С. Никифоров, А.А. Конев, А.А. Шелупанов

Модель угроз безопасности автоматизированной системы коммерческого учета энергоресурсов

Статья посвящена модели угроз безопасности автоматизированной системы коммерческого учета энергоресурсов. В качестве модели системы для описания угроз используется многоуровневая модель, построенная с помощью атрибутивного метаграфа вложенности 3. Рассматриваются аппаратный и программный уровни системы. Комплексно учитываются угрозы конфиденциальности, целостности и доступности информации, а также угрозы конфиденциальности и целостности информационной системы. Таким образом, был составлен максимально полный перечень, для разрабатываемой системы, состоящий из более 80 угроз.

Ключевые слова: информационная безопасность, угроза, модель угроз.
doi: 10.21293/1818-0442-2016-19-3-111-114

В настоящее время значительную роль при проектировании и разработке информационных систем играет обеспечение безопасности информации, передаваемой при работе этих систем по сети. Это относится и к разрабатываемой автоматизированной системе коммерческого учета энергоресурсов (АСКУЭ), задача создания которой осложняется большим количеством узлов учёта конечных потребителей и рассредоточением их на значительной территории [1]. Неавторизованное воздействие на элементы системы может нарушить конфиденциальность, целостность или доступность передаваемых данных или даже функционирование системы в целом.

Однако прежде чем переходить к минимизации возможности неавторизованного воздействия на систему, необходимо оценить защищенность разрабатываемой системы [2]. Одними из важнейших этапов оценки защищенности являются построение модели угроз безопасности рассматриваемой системы, а также построение модели нарушителя [3]. Задачей настоящей работы является создание максимально полного перечня угроз безопасности разрабатываемой системы и обрабатываемой в ней информации в условиях, когда известна структура системы, но не известен ее состав.

Применяется подход к построению модели угроз безопасности информационной системы, который описан в [4] и [5].

Существующие модели угроз безопасности, такие как в [6, 7] а также в[8, 9], в явном виде не описывают угрозы безопасности информационной системы. Каждая из рассмотренных моделей может учитывать те или иные угрозы, которые не описаны в другой.

В большинстве рассмотренных моделей нет математической формализации, т.е. все угрозы безопасности описаны посредством словесных перечней и указаний, что может привести к тому, что разные эксперты, использующие эти модели при оценке защищенности, могут трактовать их по-своему.

Структура системы

В качестве модели системы для описания угроз безопасности используется многоуровневая модель, построенная с помощью атрибутивного метаграфа вложенности 3. Взаимодействие между объектами в модели информационной системы происходит по правилам взаимодействия объектов в эталонной модели OSI. Использование метаграфов при построении модели позволяет получить полный перечень угроз безопасности информации и системы. Подход к построению модели системы описан в [10], он предполагает разделение системы на уровень сетей, уровень операционных систем и уровень программного обеспечения (ПО). В данном случае из-за отсутствия полной информации об использующемся аппаратном и программном обеспечении используется упрощенный вариант модели системы, предполагающий разделение на аппаратный и программный уровни.

АСКУЭ можно представить совокупностью объектов трех типов:

– центральный сервер (ЦС);
– устройство сбора и передачи данных (УСПД);
– устройство учета энергоресурсов (УУЭ).

Простейший вариант системы представлен на рис. 1.

Рис. 1. Структура системы

Система имеет древовидную структуру, то есть ЦС взаимодействует с несколькими УСПД, УСПД взаимодействует с несколькими УУЭ. Все правила взаимодействия между элементами системы могут быть описаны в понятиях модели OSI. Пользователи системы могут напрямую работать с каждым объектом. Формулировка «пользователь» обозначает не самого оператора системы, а устройство, с помощью которого он с ней взаимодействует.

Рассматриваются аппаратный и программный уровни системы. К аппаратному уровню системы относятся все устройства системы, линии связи и протоколы низкого уровня. К программному уровню системы относятся операционные системы и про-

граммное обеспечение устройств, протоколы высокого уровня, программы конфигурирования устройств.

Согласно [10] двухуровневую систему G можно представить как совокупность множества устройств X_1 (в него входят ЦС, а также все УСПД и УУЭ), множества программного обеспечения устройств X_2, множества связей на аппаратном уровне E_1 и множества связей на программном уровне E_2:

$$G=(X_1,X_2,E_1,E_2). \quad (1)$$

Угрозы безопасности информации

Информация в системе передается от объекта к объекту по каналу связи и хранится на объектах системы. Учитываются угрозы конфиденциальности, целостности и доступности информации [11]. При этом система из двух объектов, соединенных каналом связи, подвержена следующим угрозам:

– угроза целостности информации вследствие получения информации из неавторизованного источника;

– угроза конфиденциальности информации вследствие отправления информации неавторизованному объекту;

– угроза конфиденциальности и целостности информации вследствие воздействия на канал связи;

– угроза конфиденциальности и целостности информации из-за уязвимости канала;

– угроза доступности информации вследствие перегрузки или разрушения канала.

Применительно к АСКУЭ данный перечень необходимо рассмотреть для каждой связанной пары объектов, представленной на рис. 1, при этом стоит учитывать, что угрозы могут быть реализованы на различных уровнях. Далее рассмотрены примеры угроз безопасности информации.

Угроза целостности информации вследствие получения информации из неавторизованного источника на аппаратном уровне выражается возможностью ошибки выбора области памяти при отправке данных, на программном уровне – возможностью обработки команды от неавторизованного источника (УСПД, ЦС или пользователя) или получения данных от неавторизованного УУЭ, УСПД или ЦС.

Угроза конфиденциальности информации вследствие отправления информации неавторизованному объекту на аппаратном уровне выражается возможностью ошибки выбора области памяти при отправке данных, на программном – в возможности отправки команды на неавторизованное устройство либо отправки данных неавторизованному пользователю.

Угроза конфиденциальности информации вследствие воздействия на канал связи на аппаратном уровне выражается в возможности высокочастотного навязывания на канале связи, на программном уровне – в возможности проведения атаки «человек посередине».

Угроза целостности информации вследствие воздействия на канал связи на аппаратном и программном уровнях выражается в возможности внедрения в канал ложных пакетов информации.

Угроза конфиденциальности информации из-за уязвимости канала на аппаратном уровне обусловлена наличием паразитного электромагнитного излучения, на программном уровне – в возможности существования ошибок в протоколах передачи данных.

Угроза целостности информации из-за уязвимости канала на аппаратном уровне может быть реализована вследствие большого количества помех в канале связи, на программном уровне – вследствие возможности возникновения ошибок в работе протоколов передачи данных.

Угроза доступности информации на аппаратном уровне выражается в возможности уничтожения канала связи, на программном – в возможности проведения атаки на отказ в обслуживании.

Угрозы безопасности системы

Угрозы, которым подвергается автоматизированная система, – это угрозы, связанные с несанкционированным изменением структуры этой системы, или угрозы, связанные с несанкционированным изменением параметров элементов системы. Угрозы можно разделить на две группы: угрозы безопасности самой информационной системы и угрозы безопасности средств защиты информации [11]. В данный момент, так как система защиты еще не разрабатывалась, угрозы безопасности средств защиты информации не рассматриваются.

К угрозам конфиденциальности относятся угрозы, связанные со сбором информации о системе. К данной информации могут относиться список идентификаторов устройств, версии программного обеспечения, политики разграничения доступа, аутентификационные данные и т.д.

К угрозам целостности информационной системы относятся угрозы:

– несанкционированное добавление объекта в систему;

– несанкционированное удаление объекта из системы;

– подмена авторизованного объекта системы неавторизованным;

– создание несанкционированного канала связи между двумя объектами;

– уничтожение канала связи между объектами системы;

– подмена канала связи между двумя объектами;

– изменение атрибутов элементов системы и связей между элементами.

Данный перечень необходимо рассмотреть для каждой связи и объекта, представленных на рис. 1. В данном случае пользователь как часть системы не рассматривается.

Возможные способы реализации каждой угрозы из представленного перечня кратко расписаны для аппаратного уровня в табл. 1 и для программного уровня в табл. 2.

Рассмотрим примеры некоторых угроз целостности для системы, представленной в (1). Согласно [5] и [12] угроза удаления элемента из множества устройств, составляющих систему, будет выражена, как (2):

$$G'=(X_1 \setminus x_1^l, X_2, E_1, E_2), \quad (2)$$

где x_1^l – один из элементов системы (l – номер элемента).

Если взять в качестве удаляемого элемента УУЭ (x_1^l), тогда данное выражение будет соответствовать угрозе «несанкционированное удаление УУЭ» из табл. 1.

Угроза добавления элемента во множество устройств системы будет выражена, как (3):

$$G''=(X_1 \cup x_1^{m+1}, X_2, E_1, E_2), \quad (3)$$

где m – количество элементов системы.

Если взять в качестве добавляемого элемента УУЭ (x_1^{m+1}), тогда данное выражение будет соответствовать угрозе «несанкционированное добавление УУЭ» из табл. 1.

Угроза подмены элемента множества устройств системы выражается как последовательность из действий (2) и (3).

Таблица 1

Угрозы системе на аппаратном уровне

Элементы системы	Н/с* добавление элемента	Н/с удаление элемента	Подмена объекта системы	Создание н/с канала связи	Уничтожение канала связи	Подмена канала связи	Изменение атрибутов
Связь УУЭ – УСПД	Н/с добавление УУЭ или УСПД	Н/с удаление УУЭ или УСПД	Подмена УУЭ или УСПД	Использ-е н/с линии связи	Повреждение линии связи, помехи на линии связи	Использ-е н/с линии связи вместо санкционир.	Изменение MAC-адреса УУЭ или УСПД
Связь УСПД – ЦС	Н/с добавление УСПД или ЦС	Н/с удаление УСПД или ЦС	Подмена УСПД или ЦС	Использ-е н/с линии связи	Повреждение линии связи, помехи на линии связи	Использ-е н/с линии связи вместо санкционир.	Изменение MAC-адреса УУЭ или УСПД
УУЭ	Подключение н/с оборудования	Н/с удаление компонента УУЭ	Н/с замена компонента УУЭ	Создание н/с связей между комп. УУЭ	Уничтожение связей между комп. УУЭ	Изменение связей между комп. УУЭ	Н/с изменение крит. парам. УУЭ
УСПД	Подключение н/с оборудования	Н/с удаление компонента УСПД	Н/с замена компонента УСПД	Создание н/с связей между комп. УСПД	Уничтожение связей между комп. УСПД	Изменение связей между комп. УСПД	Н/с изменение крит. парам. УСПД
ЦС	Подключение н/с оборудования	Н/с удаление компонента ЦС	Н/с замена компонента ЦС	Создание н/с связей между комп. ЦС	Уничтожение связей между комп. ЦС	Изменение связей между комп. ЦС	Н/с изменение крит. парам. ЦС

* Несанкционированное.

Таблица 2

Угрозы системе на программном уровне

Элементы системы	Н/с добавление элемента	Н/с удаление элемента	Подмена объекта системы	Создание н/с канала связи	Уничтожение канала связи	Подмена канала связи	Изменение атрибутов
Связь УУЭ – УСПД	Н/с добавление УУЭ или УСПД (в логическую сеть)	Н/с удаление УУЭ или УСПД (на прогр. уровне)	Подмена УУЭ или УСПД	Использ-е н/с драйвера или протокола	DoS-атака, удаление драйвера	Использ-е н/с драйвера или протокола	Изменение IP-адреса УУЭ или УСПД
Связь УСПД – ЦС	Н/с добавление УСПД или ЦС (в логическую сеть)	Н/с удаление УСПД или ЦС (на прогр. уровне)	Подмена УСПД или ЦС	Использ-е н/с драйвера или протокола	DoS-атака, удаление драйвера	Использ-е н/с драйвера или протокола	Изменение IP-адреса УУЭ или УСПД
УУЭ	Внедрение н/с ПО	Н/с удаление ПО	Н/с замена ПО	Создание н/с связей между комп. УУЭ	Уничтожение связей между комп. УУЭ	Изменение связей между комп.	Н/с изменение крит. парам. УУЭ
УСПД	Внедрение н/с ПО	Н/с удаление ПО	Н/с замена ПО	Создание н/с связей между ПО	Уничтожение связей между ПО	Изменение связей между ПО	Н/с изменение крит. парам. УСПД
ЦС	Внедрение н/с ПО	Н/с удаление ПО	Н/с замена ПО	Создание н/с связей между ПО	Уничтожение связей между ПО	Изменение связей между ПО	Н/с изменение крит. парам. ЦС

Механизмы защиты от угроз

Следующим шагом после описания угроз безопасности идет описание механизмов защиты, которые должны присутствовать в системе для минимизации возможности неавторизованного воздействия. Далее приведен перечень механизмов защиты для аппаратного уровня системы.

Так, для защиты от угроз несанкционированного добавления элемента в систему и подмены элемента системы должна быть реализована идентификация и аутентификация устройств системы, а также контроль целостности каждого отдельного устройства.

Минимизировать возможность реализации угрозы удаления элемента системы, а также уничтожения канала связи можно только организационными методами защиты.

Для защиты от создания несанкционированного канала связи, подмены канала, а также изменения атрибутов системы необходимо реализовать иден-

тификацию и аутентификацию пользователей системы в совокупности с разграничением доступа к параметрам системы.

Заключение

Таким образом, для разрабатываемой АСКУЭ на основе математических моделей угроз безопасности информации и информационной системы был составлен перечень, состоящий из более 80 угроз. В нем учтены все угрозы, приведенные в моделях угроз безопасности [6–9], при этом из описания модели угроз исключена модель нарушителя.

Дальнейшая работа с моделью угроз будет производиться после выбора протоколов и технологий взаимодействия между элементами, а также реализации самих элементов системы. Для выбранных протоколов и технологий можно будет выделить угрозы, зависящие от особенностей их построения и работы, а также выделить из рассмотренного перечня актуальные и неактуальные угрозы. Возможность реализации актуальных угроз должна быть устранена или сведена к минимуму после разработки и внедрения системы защиты. При этом комплексный подход к составлению модели угроз позволил разработчикам конкретизировать требования к наличию необходимых механизмов защиты уже на этапе проектирования системы.

Однако необходимо учитывать, что с развитием сетевых технологий появляются новые способы неавторизованного воздействия, а также выявляются необнаруженные ранее уязвимости использующихся технологий. Следовательно, существует необходимость периодической переоценки защищенности и обновления списка актуальных угроз с последующей модернизацией системы защиты.

Работа выполнена при финансовой поддержке Минобрнауки РФ по контракту № 02.G25.31.0107 от 14 августа 2014.

Литература

1. Сапронов А.А. Требования, критерий оптимальности и функция цели АСКУЭ для бытового и мелкомоторного сектора электрических сетей напряжением 0,4 кВ // Энергосбережение и водоподготовка. – 2006. – № 6. – С. 57–58.

2. Новохрестов А.К. Оценка качества защищенности компьютерных сетей / А.К. Новохрестов, А.А. Конев // Динамика систем, механизмов и машин: матер. XI Междунар. науч.-техн. конф. – Омск: ФГБОУ ВПО «Омский государственный технический университет», 2014. – № 4. – С. 85–87.

3. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1 (31). – С. 28–35.

4. Конев А.А. Подход к построению модели угроз защищаемой информации // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2012. – Т. 1, № 2. – С. 34–39.

5. Новохрестов А.К. Математическая модель угроз информационной системе / А.К. Новохрестов, А.А. Конев // Перспективы развития фундаментальных наук [Электронный ресурс]. – Режим доступа: http://science-persp.tpu.ru/Arch/Proceedings_2016_vol_7.pdf, свободный (дата обращения: 02.09.2016). – С. 99–101.

6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]. – Режим доступа: http://fstec.ru/component/attachments/download/289 свободный (дата обращения: 10.09.2016).

7. The STRIDE Threat Model [Электронный ресурс]. – Режим доступа: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx, свободный (дата обращения: 10.09.2016).

8. Модели механизмов реализации типовых угроз безопасности РВС [Электронный ресурс]. – Режим доступа: http://bugtraq.ru/library/books/attack/chapter03/02.html?k=9, свободный (дата обращения: 10.09.2016).

9. Yuill J. Intrusion-detection for incident-response, using a military battlefield-intelligence process / J. Yuill, F. Wu, J. Settle, F. Gong // Computer Networks. – 2000. – No. 34. – P. 671–697.

10. Новохрестов А.К. Многоуровневая модель информационной системы на основе атрибутивных метаграфов / А.К. Новохрестов, А.А. Конев // Электронные средства и системы управления: сб. тр. XI Междунар. науч.-практ. конф. – Томск: ТУСУР, 2015. – № 1, 2. – С. 184–188.

11. Шелупанов А.А. Основы информационной безопасности / А.А. Шелупанов, Р.В. Мещеряков, Е.Б. Белов, В.П. Лось. – М.: Горячая линия – Телеком, 2011. – 558 с.

12. Basu A. Metagraphs and their applications / A. Basu, R. Blanning. – New York: Springer US, 2007. – 174 p.

Новохрестов Алексей Константинович
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: +7 (382-2) 70-15-29, внут. 2966
Эл. почта: nak1@keva.tusur.ru

Никифоров Дмитрий Сергеевич
Аспирант каф. КИБЭВС
Тел.: +7 (382-2) 70-15-29, внут. 2981
Эл. почта: nds@csp.tusur.ru

Конев Антон Александрович
Канд. техн. наук, доцент каф. КИБЭВС
Тел.: +7 (382-2) 70-15-29, внут. 2980
Эл. почта: kaa1@keva.tusur.ru

Шелупанов Александр Александрович
Д-р техн. наук, профессор каф. КИБЭВС
Тел.: +7 (382-2) 70-15-29, внут. 2950
Эл. почта: saa@keva.tusur.ru

Novokhrestov A.K., Nikiforov D.S.,
Konev A.A., Shelupanov A.A.

Model of threats to automatic system for commercial accounting of power consumption

Development of information system requires consideration of the issues of information security. Security system designing requires a preliminary assessment of the protected object. One of the most important phases of the security assessment is to identify threats to information and system. This article discusses the model of threats to automatic system for commercial accounting of power consumption.

Keywords: information security, security assessment, model of threats, integrity of information system.