УДК 004.056.53

А.К. Новохрестов, А.А. Конев

Россия, Томск, Томский государственный университет
систем управления и радиоэлектроники

ОБЗОР ПОДХОДОВ К ПОСТРОЕНИЮ МОДЕЛЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ И УГРОЗ ЕЕ БЕЗОПАСНОСТИ

При проектировании и разработке информационных систем возникает вопрос обеспечения безопасности обрабатываемой информации и самой системы. Одним из важнейших этапов оценки защищенности является выявление угроз информации и системе. В настоящей статье рассматриваются подходы к построению модели угроз и модели информационной системы.

Ключевые слова: информационная безопасность, угроза, модель угроз, компьютерная сеть.

Введение

Защита информации является одной из главных задач современного общества. Немаловажную роль в распространении информации играет человеческий фактор. Но так как полностью контролировать действия человека невозможно, необходимо обезопасить информационную систему, в которой обрабатывается информация.

Прежде чем переходить к минимизации возможности неавторизованного воздействия на систему необходимо оценить защищенность разрабатываемой системы [1]. Одними из важнейших этапов оценки защищенности являются построение модели угроз безопасности рассматриваемой системы [2], а также построение модели нарушителя [3]. Однако, построение моделей угроз и нарушителя требует максимально точного описания системы, другими словами наличия модели информационной системы.

1. Модели информационной системы

Рассматриваются математические модели, которые используются в общественных, технических и естественных науках, также при решении различных

задач проектирования. Такие модели описываются с помощью формул и графов.

В работе [4] информационная система представляется, как система 152нносового обслуживания, в которую поступают угрозы (заявки). На вход системы поступают угрозы одного типа. При этом предполагают, что данная угроза не может быть реализована или не может наступить несколько раз в один и тот же момент времени. Если эта ситуация соблюдена, то система может находиться в трех состояниях:

1) угроза не поступала, а значит, не была реализована;

2) угроза поступала, но не была реализована;

3) угроза поступала и была реализована.

Также в работе отмечается, что у данной системы отсутствуют поглощающие состояния. Это значит, что реализация угрозы либо не повлияет на работу системы, либо выведет из строя на недолгий промежуток времени один из ее сегментов.

Недостаток данной модели заключается в том, что не известно, чем являются объекты информационной системы, как они взаимодействуют друг с другом, так как модель представлена в виде черного ящика.

В работе [5] описывается модель взаимодействия объектов распределенной вычислительной системы в проекции на физический, канальный и сетевой уровень модели OSI. На вход модели подается адрес объекта, с которого идет передача сообщения, и адрес, на который идет передача сообщения. На выходе получаем результат, а именно доставлено или нет передаваемое сообщение. Главная задача этой модели состоит в том, чтобы сформировать путь между заданными входными параметрами модели.

Модель информационной системы построена при помощи ориентированного графа, в котором описывается взаимодействие объектов распределенной вычислительной системы на физическом, канальном и сетевом уровне модели OSI. В рассмотренной модели учтены не все уровни эталонной модели OSI, так как в ней не рассматривается взаимодействие между программным обеспечение и операционными системами в сети.

В результате рассмотрения данных моделей можно сказать, что с их помощью невозможно подробно описать, чем являются объекты в информационной системе, а также, как они между собой взаимодействуют. Не пред-ставляется возможным описать многоуровневую информационную систему, которая бы включала в себя взаимодействие на всех уровнях модели OSI.

2. Модели угроз

Существует множество частных моделей угроз информации, которые используют организации. Самые известные из них в России: базовая модель угроз персональным данным [6]; модель угроз, приведенная в отраслевом стандарте Банка России [7]; модель угроз от Digital Security [8].

Модель [6] содержит перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

В [7] содержится обобщенное описание угроз безопасности персональных данных для каждой их категории.

На [8] основывается методика оценки риска из состава Digital Security Office. Данная модель определяет защищенность каждого важного ресурса с помощью анализа угроз, которые действуют на определенный ресурс, и уязвимостей, через которые могут быть реализованы эти угрозы. Проводится анализ информационных рисков ресурсов предприятия с помощью оценки вероятностей реализации для важного ресурса угроз, а также степени влияния угрозы на ресурсы.

Три основных зарубежных модели угроз: ISO/IEC 27002 [9]; The STRIDE Threat Model [10]; NIST Special Publication 800-30 [11].

Стандарт [9] дает практические советы по менеджменту информационной безопасности для тех людей, которые отвечают за создание, воплощение в жизнь или обслуживание систем менеджмента информационной безопасности. Информационная безопасность определяется стандартом, как сохранение конфиденциальности, целостности и доступности информации.

В [10] описан подход к созданию защищенных систем на основе моделирования угроз, применяемый компанией Microsoft.

Документ [11] – руководство по управлению рисками для IT-систем. В данном руководстве на этапе идентификации угроз предоставляется только описание злоумышленников (источников угроз) и их вероятных действий.

Ключевой недостаток всех моделей заключается в том, что ни в одной из них нет описания угроз информационной системе в явном виде. Все внимание уделяется угрозам информации, обрабатываемой в определенной информационной системе, например, в информационной системе персональных дан-ных.

Каждая из рассмотренных российских моделей может учитывать те или иные угрозы, которые не описаны в другой.

В зарубежных моделях нет формального описания угроз, составление перечня угроз предоставляется на реализацию экспертам, которые, зачастую, не имеют прямого отношения к организации.

Также в рассмотренных моделях нет математической формализации, т.е. все модели описаны посредством словесных перечней и указаний, что может привести к тому, что каждый из экспертов может трактовать одну и ту же методику по-разному.

Заключение

Для оценки защищенности информационных систем необходима модель системы и модель ее угроз. Существующие модели информационных систем и угроз имеют недостатки, из-за которых становится затруднительно построить формализованную и независимую от субъективного мнения и профессионального эксперта методику оценки защищенности.

К основным недостаткам моделей информационных систем, которые необходимо устранить можно отнести отсутствие описания объектов информационной системы и их взаимодействия между собой, а также невозможность описания многоуровневой системы.

К недостаткам моделей угроз, требующим устранения, относится отсутствие полноты и недостаточное внимание к угрозам информационной системе – в большинстве моделей рассматриваются только угрозы информации.

Литература

1 Новохрестов А.К., Конев А.А. Оценка качества защищенности компьютерных сетей // Динамика систем, механизмов и машин: Материалы XI Международной научно-технической конференции. – Омск: ФГБОУ ВПО «Омский государственный технический университет», 2014. – № 4. – С. 85–87.

2. 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.

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

4. Математическая модель воздействия угроз на информационную систему обработки персональных данных [Электронный ресурс]. – Режим доступа:

http://www.fundamental-research.ru/ru/article/view?id=32312, свободный (дата обращения: 20.04.2017).

5. Модели механизмов реализации типовых угроз безопасности РВС [Электронный ресурс]. – Режим доступа: https://bugtraq.ru/library/books/attack/chapter03/02.html?k=9, свободный (дата обращения: 20.04.2017).

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: 20.04.2017).

7. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/credit/Gubzi_docs/rs-24-xx.pdf, свободный (дата обращения: 20.04.2017).

8. Методика оценки риска ГРИФ 2006 из состава Digital Security Office [Электронный ресурс]. – Режим доступа: http://dsec.ru/ipm-research-center/article/risk_assessment_method_vulture_2006_from_the_composition_of_the_digital_security_office/, свободный (дата обращения: 20.04.2017).

9. Международный стандарт ISO/IEC 27002. Информационные технологии. Свод правил по управлению защитой информации [Электронный ресурс]. – Режим доступа: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27002-2005.pdf, свободный (дата обращения: 20.04.2017).

10. The STRIDE Threat Model [Электронный ресурс]. – Режим доступа: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx, свободный (дата обращения: 20.04.2017).

11. NIST Special Publication 800-30. Risk Management Guide for Information Technology Systems [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, свободный (дата обращения: 20.04.2017).