D.S. Simonenkova

Modeling and Security Threat Assessments of Data Processed in Cloud Based Information Systems

Keywords: information security, cloud based information systems, security threat assessments.

The subject of the research is modeling and security threat assessments of data processed in cloud based information systems (CBIS). This method allow to determine the current security threats of CBIS, state of the system in which vulnerabilities exists, level of possible violators, security properties and to generate recommendations for neutralizing security threats of CBIS.

Д.С. Симоненкова

МОДЕЛИРОВАНИЕ И ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОНЫХ СИСТЕМАХ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Введение

Облачные вычисления представляют собой модель предоставления повсеместного и удобного сетевого доступа по требованию к разделяемому множеству конфигурируемых вычислительных ресурсов (сети, серверы, память, приложения и сервисы), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами и (или) обращениями к провайдеру [1].

Несмотря на все преимущества информационных системах, построенных с использованием технологий облачных вычислений (ИСОТ), под которыми понимаются информационные системы (ИС), предназначенные для реализации облачных услуг, переход к ним несет новые угрозы и уязвимости безопасности, выявлению и устранению которых необходимо уделять особое внимание.

Для обеспечения должного уровня безопасности информации необходимо с особой важностью отнестись к проектированию системы защиты информации в ИСОТ. Отправной точкой для проектирования является моделирование и оценка угроз безопасности ИСОТ.

По результатам проведенного анализа существующих методик моделирования угроз безопасности информации (БИ) [2, 4] можно сделать вывод о том, что построение моделей угроз представляет собой, в большинстве случаев, процесс составления таблиц или перечней на основе формирования описаний угроз из определенных наборов источников угроз, уязвимостей, способов реализации угроз, объектов воздействия и деструктивных свойств, а также проведения оценок опасности угроз БИ.

В последнее время всё чаще приходится учитывать требования различных стандартов в области информационной безопасности (ИБ) при построении системы защиты. Соответственно, несомненным достоинством методики моделирования и оценки угроз безопасности ИСОТ является возможность оценки степени соответствия мер защиты, реализованных в ИСОТ, требованиям, предъявляемым современными нормативными документами.

В настоящий момент не существует общепринятой методики моделирования и оценки угроз безопасности ИСОТ, а существующие методики ориентированы на стандартные ИС и не позволяют учитывать особенности ИСОТ [5].

Нарушители безопасности ИСОТ

Построение любой модели угроз БИ не представляется возможным без описания нарушителей БИ.

В данной работе нарушители безопасности ИСОТ классифицируются по уровню возможностей, предоставляемых им штатными средствами системы. Выделены три уровня таких возможностей. Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего уровня. Типы нарушителей и краткое описание их способностей приведены в таблице.

Таблица. Нарушители и их возможности

№ п/п	Наименование нарушителя	Возможности нарушителя
1	Первый уровень	Имеет доступ к общедоступному веб-интерфейсу
2	Второй уровень	Имеет доступ к интерфейсу самообслуживания в полном объеме
3	Третий уровень	Имеет доступ к интерфейсу управления ресурсами ИСОТ

Нарушители, имеющие физический доступ к аппаратной части, а также угрозы, реализуемые такими нарушителями в данной работе, не рассматриваются в виду отсутствия в таких угрозах и нарушителях, а также методах и средствах защиты от них какой-либо специфики ИСОТ и предполагается, что оператором ИСОТ приняты все необходимые меры для защиты ИСОТ на данном уровне.

Математическая модель представления функциональных возможностей ИСОТ

На основе анализа различные модели ИСОТ по версиям NIST, Microsoft, IBM, Microsoft TechNet[0], описания которых доступны в открытых источниках, результатов исследования наиболее популярных функциональных возможностей, существующих ИСОТ, был сформирован набор функциональных возможностей ИСОТ, которые могут быть реализованы в предложенной модели ИСОТ.

Для представления функциональных возможностей предложенной модели ИСОТ в виде динамической системы в качестве математического аппарата были выбраны сети Петри [0], [0].

Построенная сеть Петри, описывающая функциональные возможности предложенной модели описания ИСОТ, состоит из 248 позиций и 314 переходов. Множества состояний обозначим P, $P = \{p_1, p_2, \dots, p_{248}\}$, а множество переходов T, $T = = T = \{t_1, t_2, \dots, t_{3\ 14}\}$.

В качестве иллюстрации построенного в работе графа сети Петри, на рисунке представлен подграф графа сети Петри, описывающий 1 из 18 функциональных возможностей предложенной модели описания ИСОТ.

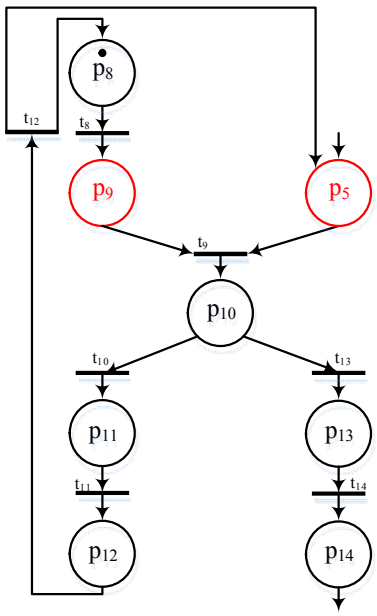

Рис. Подграф графа сети Петри, описывающий процесс получения доступа к личному кабинету подписчика

Каждому состоянию системы p_j ставится в соответствие набор параметров:

c_{p_j} – конфиденциальность;

i_{p_j} – целостность;

a_{p_j} – доступность, такfz, что $c_{p_j}, i_{p_j}, a_{p_j} \in \{0,1\}, j = \overline{1,248}$.

c_{p_j} = 1 (аналогично i_{p_j}= 1 и a_{p_j}= 1), если в состоянии p_j обеспечивается конфиденциальность (соответственно целостность и доступность) информации, обрабатываемой в ИСОТ. В случае если нарушается какой-либо из параметров, то он принимает нулевое значение.

Таким образом, состоянию системы p_j ставится в соответствие вектор свойств безопасности состояния ИСОТ $s_{p_j} = (c_{p_j}, i_{p_j}, a_{p_j}) \in S$.

Состояние p_j, в котором $c_{p_j} = i_{p_j} = a_{p_j} = 1$ называется безопасным состоянием ИСОТ ($s^+{}_{p_j} = (c_{p_j}, i_{p_j}, a_{p_j}) \in S^+$).

Состояние p_j, в котором хотя бы один из параметров $c_{p_j}, i_{p_j}, a_{p_j} \neq 1$, называется небезопасным состоянием ИСОТ ($s^-{}_{p_j} = (c_{p_j}, i_{p_j}, a_{p_j}) \in S^-$).

На рис. 1 p_5 и p_9 – состояния системы, в которых существуют уязвимости, в случаях, когда необходимые меры защиты не приняты. Множество состояний, в которых такие уязвимости существуют, обозначим P'.

Множество уязвимостей V может быть описано следующим образом:

$$V \subseteq I \times P', \quad (1)$$

где I – множество уровней нарушителей, которые могут реализовать угрозу; P'– множество состояний системы, в которых уязвимости существуют.

После того как все уязвимости определены, описание каждой из них было дополнено краткими рекомендациями по ее устранению. Множество рекомендаций обозначим R.

Методика моделирования и оценки угроз безопасности ИСОТ

В разработанной методике моделирования и оценки угроз безопасности ИСОТ предлагается использовать построенную базовую модель угроз безопасности ИСОТ.

Базовая модель угроз безопасности ИСОТ представляет собой множество описаний угроз безопасности ИСОТ, состоящих из перечней уязвимостей, состояний системы, в которых такие уязвимости существуют, нарушителей, обладающих возможностями для реализации описываемой угрозы путем эксплуатации уязвимости, а также нарушаемые свойства безопасности. Помимо этого, базовая модель угроз безопасности ИСОТ содержит набор рекомендаций, позволяющих нейтрализовать выявленные актуальные угрозы безопасности. Использование такой базовой модели угроз безопасности ИСОТ позволяет избавиться от необходимости составления и проверки корректности всевозможных описаний угроз, тем самым давая возможность осуществлять моделирование угроз безопасности ИСОТ без привлечения экспертов.

Описание функциональных возможностей ИСОТ в терминах теории сетей Петри позволяет на основе дальнейшего анализа построенного графа сети Петри сформировать описания угроз, из которых и состоит базовая модель угроз безопасности ИСОТ. Такое описание угроз может быть представлено следующим образом:

$$D \subseteq I \times V \times P' \times S^{-}, \quad (2)$$

где S^{-} – множество векторов свойств безопасности небезопасных состояний ИСОТ; D – множество угроз безопасности ИСОТ.

Таким образом, предлагаемая в работе методика моделирования и оценки угроз безопасности ИСОТ может быть описана последовательностью следующих шагов.

Входные данные:

базовая модель угроз ИСОТ;

функциональные возможности ИСОТ;

ПО, используемое на уровне виртуализации ИСОТ;

меры защиты, используемые в ИСОТ.

Шаг 1. Выбор из базовой модели угроз ИСОТ описаний угроз, которые могут быть реализованы в исследуемой ИСОТ.

Шаг 2. Определение актуальных угроз безопасности ИСОТ с учетом информации о ПО и мерах защиты, используемых в ИСОТ(множество актуальных угроз обозначим $D_{\text{акт}}$).

Шаг 3. Оценивание уровня защищенности ИСОТ.

Оценка уровня защищенности ИСОТ $L_{\text{защ}}$ определяется по следующей формуле:

$$L_{\text{защ}} = \frac{|D_{\text{акт}}|}{|D_{\text{ИСОТ}}|} 100\ \%, \quad (3)$$

где $|D_{\text{акт}}|$ – мощность множества актуальных угроз безопасности ИСОТ, $D_{\text{акт}} \subseteq D_{\text{ИСОТ}}$; $|D_{\text{ИСОТ}}|$ – мощность множества всех угроз, существующих в ИСОТ, $D_{\text{ИСОТ}} \subseteq D$.

Таким образом, уровень защищенности ИСОТ определяется по следующему правилу:

$L_{\text{защ}} \geq 50\ \%$ – низкий уровень защищенности ИСОТ;

$30\% \leq L_{\text{защ}} < 50\ \%$ – средний уровень защищенности ИСОТ;

$L_{\text{защ}} < 30\ \%$ – высокий уровень защищенности.

Шаг 4. Оценивание уровня опасности актуальных угроз безопасности ИСОТ, в зависимости от свойств безопасности, обеспечение которых особенно важно для ИСОТ.

Вычисление уровня опасности *j*-ой актуальной угрозы безопасности ИСОТ определяется по следующей формуле:

$$\mathrm{A}_{D_{\text{акт}_j}} = k_{c_j} + k_{i_j} + k_{a_j}, \tag{4}$$

где коэффициенты k_{c_j}, k_{i_j}, k_{a_j} определяются для каждого из свойства безопасности (конфиденциальность, целостность, доступность соответственно) с использованием вектора свойств безопасности небезопасных состояний ИСОТ, по следующему правилу:

$$k_{c_j}, k_{i_j}, k_{a_j} = \begin{cases} 1{,}5, \text{ если обеспечение свойства безопасности приоритетно и нарушено;} \\ 1, \text{ если обеспечение свойства безопасности приоритетно, но не нарушено;} \\ 0{,}5, \text{ если обеспечение свойства безопасности не приоритетно, но нарушено;} \\ 0, \text{ если обеспечение свойства безопасности не приоритетно и не нарушено.} \end{cases}$$

Уровень опасности *j*-й актуальной угрозы может принимать значения от 0,5 до 4,5 с шагом 0,5. Если угроза не актуальна, то уровень ее опасности для ИСОТ принимает нулевое значение.

Шаг 5. Оценивание степени соответствия мер, принятых в ИСОТ, требованиям, предъявляемым стандартами $L_{\text{соот}}$:

$$L_{\text{соот}} = \frac{|R'_{\text{акт}}|}{|R'_{\text{ИСОТ}}|} 100\%, \tag{5}$$

где $|R'_{\text{акт}}|$ – мощность множества мер, реализованных в ИСОТ, $R'_{\text{акт}} \subseteq R'_{\text{ИСОТ}}$; $|R'_{\text{ИСОТ}}|$ – мощность множества всех требований стандарта, реализация которых возможна в ИСОТ, $R'_{\text{ИСОТ}} \subseteq R'$, где R' – множество всех требований стандарта.

Таким образом, уровень защищенности ИСОТ определяется по следующему правилу:

$L_{\text{соот}} \geq 50\ \%$ – низкий уровень защищенности;

$30\ \% \leq L_{\text{соот}} < 50\ \%$ – средний уровень защищенности;

$L_{\text{соот}} < 30\ \%$ – высокий уровень защищенности.

На момент написания работы существует два проекта нормативных документов, содержащих правила для защиты данных, обрабатываемых в ИСОТ. Принятие первого проекта стандарта планировалось на 2014 год, обсуждение первой редакции второго документа проводилось в период с 30 июня по 22 августа 2015 года. Таким образом, проведение оценки степени соответствия мер, реализованных в ИСОТ, требованиям указанных стандартов, позволит в будущем быстрее адаптироваться под требования, предъявляемые вводимыми нормативными документами.

Шаг 6. Формирование рекомендаций по устранению актуальных угроз.

Выходные данные: модель угроз безопасности ИСОТ и оценки угроз безопасности ИСОТ.

Заключение

Разработанная методика моделирования и оценки угроз безопасности ИСОТ позволяет выявить актуальные угрозы безопасности ИСОТ, состояния системы, в которых существуют уязвимости, а также формировать рекомендации по нейтрализации выявленных актуальных угроз безопасности ИСОТ. Также методика, представленная в данной работе, позволяет проводить ранжирование угроз безопасности ИСОТ в зависимости от приоритетности обеспечения каждого из свойств безопасности, оценивать уровень защищенности ИСОТ и степень соответствия мер защиты, реализованных в ИСОТ, требованиям нормативных документов.

СПИСОК ЛИТЕРАТУРЫ:

1. NIST SP 800-145. The NIST Definition of Cloud Computing / Recommendations of the National Institute of Standards and Technology. – NIST, 2011.
2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). – Введ. 2008.02.15. ФСТЭК России, 2008.
3. РС БР ИББС-2.4-2010 Стандарт банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации.– Введ. 2010.06.21. М.: Банк России, 2010.
4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. – Введ. 2008.02.14. М.: ФСТЭК РФ, 2008.
5. Симоненкова Д.С. Исследование нормативных документов, описывающих порядок построения модели угроз безопасности данных при их обработке в информационных системах. / Симоненкова Д.С. // XVI Международной телекоммуникационной конференции молодых ученых и студентов «Молодежь и наука». Тезисы докладов. Ч. 3. М.: НИЯУ МИФИ, 2013, с. 15.
6. Симоненкова Д.С. Об информационных системах, построенных с использованием технологий облачных вычислений». / Симоненкова Д.С., А. Н. Велигура // Материалы XX Всероссийская научно-практическая конференция «Проблемы информационной безопасности в системе высшей школы». М.: БИТ. 2013. № 1. С. 121–122.
7. Сети Петри – инструмент для описания и исследования динамических систем [Электронный ресурс]: Режим доступа к ресурсу: http://www.asterisk.by/node/1625 (дата обращения 25.01.2016).
8. Симоненкова Д.С. Визуальное представление модели угроз безопасности информационных систем, построенных с использованием технологий облачных вычислений / Симоненкова Д.С., Велигура А.Н. // Научная визуализация. № 2. 2015. С. 81–95.

REFERENCES:

1. NIST SP 800-145. The NIST Definition of Cloud Computing / Recommendations of the National Institute of Standards and Technology. – NIST, 2011.
2. Bazovaja model' ugrozbezopasnostipersonal'nyhdannyhpriihobrabotke v informacionnyhsistemahpersonal'nyhdannyh (vypiska). – Vved. 2008.02.15 – FSTJeK Rossii, 2008.
3. RS BR IBBS-2.4-2010 StandartbankaRossii. Obespechenie informacionnoj bezopasnosti organizacij bankovskoj sistemy Rossijskoj Federacii. Otraslevaja chastnaja model' ugrozbez opasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh organizacij bankovskoj sistemy Rossijskoj Federacii.–Vved. 2010.06.21 M.: Bank Rossii, 2010.
4. Metodika opredelenija aktual'nyh ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyhsistemahpersonal'nyhdannyh. – Vved. 2008.02.14. M.: FSTEHK RF, 2008.
5. Simonenkova D.S. Issledovanie normativnyh dokumentov, opisyvajushh ih porjadok postroenija modeli ugroz bezopasnosti dannyh pri ih obrabotke v informacionnyh sistemah. / Simonenkova D.S. // XVI Mezhdunarodnoj telekommunikacionnoj konferencii molodyh uchenyh i studentov «Molodezh' inauka». Tezisy dokladov. Ch. 3. M.: NIYAU MIFI, 2013. S. 15.
6. Simonenkova D.S. Ob informacionnyh sistemah, postroennyh s ispol'zovaniem tehnologij oblachnyh vychislenij. / Simonenkova D.S., A. N. Veligura // Materialy XX Vserossijskaja nauchno-prakticheskaja konferencija «Problemyinformacionnojbezopasnosti v sistemevysshejshkoly». M.: BIT. 2013. № 1. S. 121–122.
7. Seti Petri – instrument dljaopisanijaissledovanijadinamicheskihsistem [Jelektronnyjresurs]: - Rezhimdostupa k resursu: http://www.asterisk.by/node/1625 (data obrashhenija 25.01.2016).
8. Simonenkova D.S. Vizual'noe predstavlenie modeli ugrozbez opasnosti informacionnyh sistem, postroennyh s ispol'zovaniem tehnologij oblachnyh vychislenij / Simonenkova D.S., Veligura A.N. // Nauchnajavizualizacija. 2015. № 2. S. 81–95.