УДК 004.056 + 002:004.056

ДОВЕРИЕ К ПОЛЬЗОВАТЕЛЮ ИНФОРМАЦИОННОЙ СИСТЕМЫ КАК КОМПОНЕНТ ДОВЕРИЯ К ЕЕ БЕЗОПАСНОСТИ

Л.В. Астахова

В статье обоснована актуальность использования категории «доверие» к оценке кадровой безопасности информационной системы. Охарактеризован подход к применению оценочных уровней доверия, указанных в ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. Разработан подход к оценке доверия к кадровой безопасности информационной системы на основе достижений гуманитарных наук.

Ключевые слова: доверие, кадровая безопасность, информационная безопасность, оценка, пользователь, информационная система.

Человек как важнейшее звено информационной системы серьезно недооценивается в практике обеспечения защиты информации, о чем свидетельствует статистика. За I-е полугодие 2014 года Аналитическим центром InfoWatch зарегистрировано 654 случая утечки конфиденциальной информации, что на 32 % больше, чем за аналогичный период 2013 г. При этом в 71 % случаев виновниками утечек информации были сотрудники компаний – настоящие или бывшие (69,2 % и 1,4 % соответственно) [1].

Причина такого положения дел видится нам в принципиальной сложности формализации процессов идентификации и оценки кадровых уязвимостей информационной безопасности и на этапе проектирования информационной системы (ИС), и на этапе ее эксплуатации. А это значит, что в решении проблемы сотрудников компаний как виновников инцидентов информационной безопасности главным императивом деятельности выступает кадровая безопасность.

Полагаем, что высоким эвристическим потенциалом в решении этой проблемы является подход, связанный с категорией доверия, используемой в сфере информационной безопасности. Согласно ISO/IEC 15408-3:2008 «Information technology – Security techniques – Evaluation criteria for IT security – Part 3. Security assurance components» [2] и идентичного ему ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», «доверие – основа для уверенности в том, что продукт ИТ отвечает целям безопасности» [3].

Традиционным способом достижения доверия является оценка (активное исследование) продукта информационных технологий (ИТ), который должен соответствовать определенным критериям безопасности. Названный стандарт выделяет **7 оценочных уровней доверия (ОУД)** для оценки уровня доверия к объекту оценки (ОО). Каждый последующий ОУД представляет более высокое доверие, чем любой из предыдущих. Увеличение доверия от предыдущего ОУД к последующему достигается заменой какого-либо компонента доверия иерархичным компонентом из того же семейства доверия (т.е. увеличением строгости, области охвата и/или глубины оценки) и добавлением компонентов из других семейств доверия (т.е. добавлением новых требований).

Оценочные уровни доверия состоят из определенной комбинации компонентов доверия, которые сгруппированы в 6 классов доверия к безопасности ИТ: разработка, руководства, поддержка жизненного цикла, оценка задания по безопасности (ЗБ), тестирование, оценка уязвимостей. Методы их оценки включают в себя: анализ и проверку процесса (процессов) и процедуры (процедур); проверку того, что процесс (процессы) и процедура (процедуры) действительно применяются; анализ соответствия между представлениями проекта ОО; анализ соответствия каждого представления проекта ОО требованиям; верификацию доказательств; анализ руководств; анализ разработанных функциональных тестов и предоставленных результатов; независимое функциональное тестирование; анализ уязвимостей, включающий предположения о недостатках; тестирование проникновения.

Оценочный уровень доверия 1 (ОУД1) предусматривает функциональное тестирование; ОУД2 – структурное тестирование; ОУД3 – методическое тестирование и проверку; ОУД4 – методическое проектирование, тестирование и углубленную проверку; ОУД5 – полуформальное проектирование и тестирование; ОУД6 – полуформальную верификацию и тестирование проекта; ОУД7 – формальную верификацию проекта и тестирование.

Согласно логике стандарта, можно предположить, что человек как пользователь информационной системы организации должен выступать объектом оценки на всех оценочных уровнях доверия к безопасности информационной системы.

Функциональное тестирование (ОУД1) ИС как объекта оценки должно предусматривать: анализ Руководств различных категорий пользователей по эксплуатации (AGD_OPE.1); установление требований кадровой безопасности в задании по безопасности (ASE_REQ.1); анализ и обзор кадровых уязвимостей (AVA_VAN.1) и др. Это означает значимое увеличение доверия по сравнению с продуктом ИТ, не подвергавшимся оценке.

Структурное тестирование (ОУД2) ИС как объекта оценки должно предполагать: тестирование кадрового обеспечения ИС и анализ кадровых уязвимостей разработчиком (помимо изучения общедоступных источников информации), а также независимое тестирование, основанное на более де-

тализированных спецификациях ОО. Это демонстрирует способность противостояния ИС попыткам проникновения нарушителей, обладающих базовым потенциалом нападения.

Методическое тестирование и проверка (ОУД3) ИС как объекта оценки должны предполагать: более полное покрытие тестированием функциональных возможностей и механизмов кадровой безопасности и/или процедур кадровой безопасности. Это демонстрирует способность противостояния ИС попыткам проникновения нарушителей, обладающих базовым потенциалом нападения.

Методическое проектирование, тестирование и углубленная проверка (ОУД4) ИС как объекта оценки должны предполагать: более детальное описание проекта, представление реализации для всех ФБО и улучшенные механизмы и/или процедуры по обеспечению кадровой безопасности. Это демонстрирует способность противостояния ИС попыткам проникновения нарушителей, обладающих усиленным базовым потенциалом нападения.

Полуформальное проектирование и тестирование (ОУД5) ИС как объекта оценки должны предполагать: полуформальное описание проекта, более структурированную (и, следовательно, лучше анализируемую) архитектуру и улучшенные механизмы и/или процедуры кадровой безопасности. Это демонстрирует способность противостояния ИС попыткам проникновения нарушителей, обладающих умеренным потенциалом нападения.

Полуформальная верификация и тестирование проекта (ОУД6) ИС как объекта оценки должны предполагать: проведения более всестороннего анализа, структурированное представление реализации, более стройную структуру (например, с разбиением на уровни), более всесторонний независимый анализ уязвимостей, а также улучшенное управление конфигурацией и улучшенный контроль среды разработки. Это демонстрирует способность противостояния ИС попыткам проникновения нарушителей, обладающих высоким потенциалом нападения.

Формальная верификация проекта и тестирование (ОУД7) ИС как объекта оценки должны предполагать: тестирование, основанное на функциональной спецификации и представлении реализации, полное независимое подтверждение результатов тестирования разработчиком и независимый анализ кадровых уязвимостей, демонстрирующие способность противостояния ИС попыткам проникновения нарушителей с Высоким потенциалом нападения. Это требует более всестороннего анализа, использующего формальные представления и формальное соответствие, а также всестороннее тестирование кадровой безопасности информационной системы.

Из сказанного следует, что система кадровой безопасности – это обязательный элемент информационной безопасности организации, а доверие к пользователям информационной системы организации – неотъемлемый

компонент доверия к ее информационной безопасности. Стандартная структура оценочных уровней доверия к безопасности ИС содержит в себе потенциальные возможности для оценки кадровой безопасности, однако в теории и практике информационной безопасности этот вопрос не разработан.

Примечателен факт, что в ИСО/МЭК 15408 не отрицаются и не комментируются относительные достоинства других способов получения доверия, поскольку исследования альтернативных путей достижения доверия продолжаются. По словам разработчиков стандарта (п.5.2.), альтернативные подходы могут в дальнейшем быть включены в ИСО/МЭК 15408, который структурно организован так, что предусматривает такую возможность [3].

В целях развития закрепленных стандартом оценочных уровней доверия к безопасности ИС считаем необходимым разработку и включение в действующий стандарт системы оценки доверия к кадровой безопасности ИС. Считаем также, что адекватной мерой противодействия растущим объемам ИБ-инцидентов по вине сотрудников организации является разработка отдельного стандарта по системе оценки доверия к кадровой безопасности ИС.

Для разработки названной системы нецелесообразно опираться только на техническое знание. Необходимо использовать все богатство накопленных гуманитарными науками достижений в изучении доверия. К таким наукам относятся философия, психология, экономика и др.

Анализ российских и зарубежных источников по проблеме доверия к технике показал, что большинство исследователей осознают большое значение человеческого фактора для доверия к технике, высокую роль компетентности самого пользователя / оператора, а также компетентности других людей (создателей техники, смежников и т.д.).

Основой системы могут быть основные структурные элементы модели доверия / недоверия к социотехническим системам, разработанной российским экспертом А.Б. Купрейченко. К этим элементам автор относит:

• доверие / недоверие к принципам организации и правилам функционирования системы;

• доверие / недоверие к отдельным функциональным блокам (иерархическим уровням, материально-технической базе, технологиям, отдельным узлам и элементам);

• доверие / недоверие к различным категориям людей, обеспечивающим функционирование системы (создателям, организаторам, модераторам системы и другим заинтересованным сторонам);

• доверие / недоверие к себе как профессионалу или пользователю;

• доверие / недоверие к условиям функционирования системы.

В качестве основных детерминантов доверия / недоверия социальным и социотехническим системам автор называет личностные и социально-групповые факторы: базовое доверие / недоверие к миру, к другим людям, к себе, общее отношение к социальному и техническому прогрессу; интернальность, ответственность, склонность к риску, отношение к новизне и т.д. Кроме того, мы согласны с ученым и в том, что весомый вклад в проблему вносят культурно-исторические, социально-экономические и научно-технические факторы, в том числе культура доверия / недоверия в обществе и их уровень. [4, с. 435–436].

Нетрудно заметить, что перечень компонентов доверия к ИС как к социотехнической системе в рамках экономического подхода гораздо шире, чем идентичный перечень, представленный в стандарте ГОСТ Р ИСО/МЭК 15408-3-2013. Это позволяет говорить о необходимости расширения критериев оценки доверия к кадровой безопасности ИС за счет включения в их состав: 1) оценки доверия субъекта оценки (оценщика): к различным категориям пользователей ИС; к самому себе; к условиям функционирования ИС; 2) оценки доверия пользователей ИС: друг к другу; к себе; к миру, научно-техническому прогрессу; 3) оценки уровня культуры доверия в организации и др.

Другие ученые считают, что подход к доверию технике как психологическому отношению предполагает выделение в его структуре когнитивной, эмоционально-оценочной и поведенческой компонент, которые, на наш взгляд, также могут играть роль компонентов доверия к кадровой безопасности информационной системы. Когнитивная компонента включает знание о надежности работы техники; представление о вероятности ее работы без сбоев и отказов в разных условиях и при решении разных задач; представление о мере освоенности техники ее пользователями. Эмоциональная компонента содержит эмоциональную оценку степени уверенности в работе техники, а также степени уверенности в своих возможностях управления техникой. Поведенческая компонента предусматривает оценку готовности к выполнению определенных действий, обеспечивающих эффективное выполнение профессиональных задач в разных условиях [4, с. 465].

В основу системы оценки доверия к ИС могут быть также положены три группы факторов, влияющие на организационное доверие, выделенные B. Uzzi:

- организационные факторы (характеристики организации) – структура, политика организации в отношении персонала, организационная культура;
- факторы отношений (характеристики ситуации) – первичное взаимодействие, ожидания, «стоимость обмена»;
- индивидуальные факторы (личностные характеристики субъекта доверия) – склонность к доверию, самоэффективность, ценности [5].

Без сомнения, названные факторы должны исследоваться в процессе оценки доверия к кадровой безопасности ИС.

Таким образом, пользователь ИС как виновник инцидентов информационной безопасности – проблема кадровой безопасности этой системы. Кадровая безопасность является императивом деятельности по обеспечению информационной безопасности, а потому важнейшим объектом оценки. Высоким эвристическим потенциалом в решении этой проблемы является подход, связанный с категорией доверия, используемой в сфере информационной безопасности по отношению к ИС. Оценочные уровни доверия к безопасности ИС должны быть дополнены компонентами доверия к кадровой безопасности. Целесообразна также разработка специального стандарта по критериям оценки доверия к кадровой безопасности информационной системы.

Библиографический список

1. Глобальное исследование утечек конфиденциальной информации в I-м полугодии 2014 года. – URL: http://www.infowatch.ru/report2014_half.

2. ISO/IEC 15408-3:2008 «Information technology – Security techniques – Evaluation criteria for IT security – Part 3. Security assurance components». – URL: http://www.iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413.

3. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. – М.: Стандартинформ, 2014. –151 с.

4. Доверие и недоверие в условиях развития гражданского общества / отв. ред. А.Б. Купрейченко, И.В. Мерсияновой. – М.: Издательский дом НИУ ВШЭ, 2013. – 564 с.

5. Uzzi B. Social Structure and Competition in Interfirm Networks: The Paradox of Embeddedness // Administrative Science Quarterly. – 1997. – Vol. 42. – No. 1. – P. 35–67.

К содержанию