УДК 004.056

С.Л. Зефиров, А.Ю. Щербакова

Оценка инцидентов информационной безопасности

Рассматривается способ оценки инцидентов информационной безопасности, основанный на факторах событий информационной безопасности. Предложены алгоритм оценки инцидентов информационной безопасности и его программная реализация.
Ключевые слова: инцидент, информационная безопасность, фактор, первичная оценка, вторичная оценка, анализ.

С ростом числа информационных систем и совершенствованием информационных технологий растёт и число инцидентов информационной безопасности (ИБ), под которыми понимается одно или несколько нежелательных событий (событий ИБ), которые влияют на информационную безопасность активов систем и могут привести к негативным последствиям. Такими последствиями могут быть, например, нарушение конфиденциальности, целостности и доступности информационных активов, прерывание бизнес-процессов и др.

Международный стандарт ISO 27001:2005 [1] обращает особое внимание на необходимость создания процедуры управления инцидентами информационной безопасности – очевидно, что без своевременного реагирования на инциденты ИБ, устранения их последствий и возможных причин невозможно эффективное управление информационной безопасностью. В международном стандарте ISO/IEC 27035 [2] и национальном стандарте ГОСТ Р ИСО/МЭК 18044:2007 [3] приводятся процессы управления инцидентами информационной безопасности. Рассматриваются вопросы обеспечения нормативно-распорядительной документацией, ресурсами, даются рекомендации по необходимым процедурам для реализации этих процессов, в том числе по классификации инцидентов ИБ, распределению ролей при обработке инцидента ИБ, порядку обработки инцидентов ИБ. Схема управления обработкой инцидентов ИБ в соответствии с [2, 3] приведена на рис. 1.

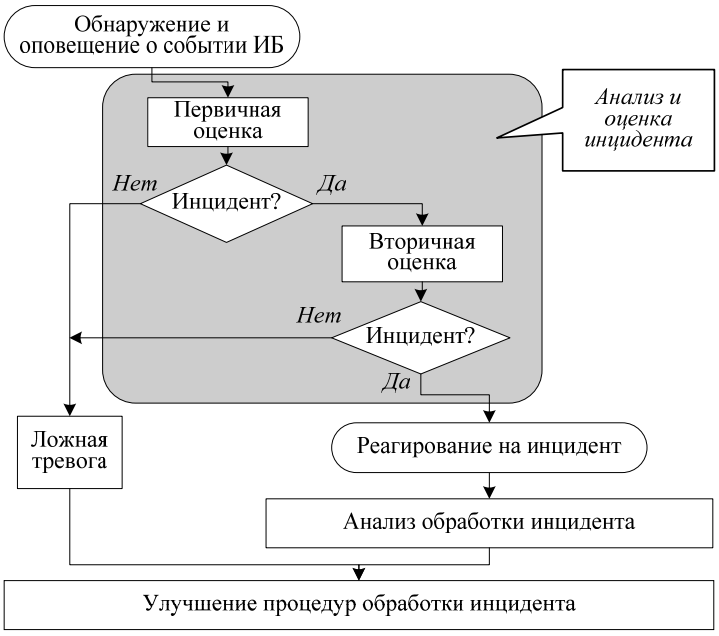

Рис.1. Управление обработкой инцидентов ИБ

Постановка задачи. Обнаружение, анализ и оценка инцидента ИБ являются определяющими этапами при управлении инцидентами ИБ, поскольку от своевременности и достоверности информации, полученной на этих этапах для принятия решения по реагированию на инцидент, зависит успешность его обработки.

Зачастую в организациях отсутствует методика обнаружения инцидентов ИБ, сотрудники не знают, какие события могут являться инцидентами ИБ, поскольку они не всегда связаны с прерываниями основной деятельности. Анализ и оценка инцидентов ИБ также могут быть затруднительны из-за недостаточности информации о произошедших инцидентах, их причинах и последствиях. Существует необходимость в создании и поддержке актуальной базы событий и инцидентов ИБ. База событий и инцидентов ИБ может быть создана на основе собственного опыта обработчиков инцидентов ИБ и сведений о произошедших инцидентах из различных источников. Сведения об инцидентах ИБ, произошедших в организациях, особенно в крупных фирмах, компаниях, обычно не публикуются, чтобы избежать риска повторных атак на их системы и потери репутации. Но аналитики ИБ при исследовании проблем обеспечения информационной безопасности, например на промышленных и других предприятиях [4], приводят обзоры обнаруженных уязвимостей информационных технологий, статистику инцидентов ИБ за определенный период, например [5,6], без указания организаций, в которых эти инциденты происходили. Подобные сведения позволяют регулярно обновлять базу инцидентов ИБ для поддержания её в актуальном состоянии.

Анализ и оценка инцидента ИБ представляют сложность ввиду большого объема информации, необходимой для идентификации событий ИБ как инцидентов, определения причин и источников этих событий, а также возможного развития их негативных последствий, поэтому эти процедуры должны быть формализованы и автоматизированы.

Задачей настоящей работы является разработка способа повышения оперативности анализа и оценки инцидентов ИБ с помощью их автоматизации и обеспечения адекватности принятия решения по обработке инцидентов ИБ за счет информационного обеспечения процедур их обнаружения, анализа и оценки на основе базы данных о произошедших событиях и инцидентах ИБ.

Оценка инцидентов информационной безопасности на основании их факторов. Первичная оценка идентификации события ИБ как инцидента ИБ может осуществляться на основании факторов событий ИБ, указывающих на определённый вид инцидента. Фактор события ИБ – признак события ИБ, указывающий на возможное нарушение ИБ или аварию защитных мер (средств), а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью. Факторы событий могут быть выявлены обработчиками инцидентов ИБ техническими средствами в процессе мониторинга систем и плановых проверок или сотрудниками организации в ходе выполнения ими основной деятельности.

Так как нежелательные события в системе, например замедление работы, отказы и сбои программного обеспечения и т.д., не всегда свидетельствуют об инциденте ИБ, необходимо подтверждение актуальности их факторов, для чего должна осуществляться вторичная оценка. По результатам вторичной оценки принимается решение, является ли инцидент ложным, реальным или потенциальным [7]. Для потенциальных инцидентов ИБ можно вычислить их вероятность, зная частость нежелательных событий в их сценариях и результативность защитных мер, направленных на предотвращение инцидентов ИБ, выбранных по результатам оценки рисков [8].

Для автоматизации процесса анализа и оценки инцидентов ИБ было разработано программное средство, алгоритм которого представлен на рис. 2.

С целью идентификации инцидентов ИБ обработчику необходимо на основе полученных от источника данных об обнаруженных событиях ИБ отметить в предустановленных списках соответствующие факторы инцидентов ИБ. Списки факторов инцидентов ИБ составляются на основе базы данных о произошедших событиях и инцидентах ИБ и регулярно обновляются. Затем обработчику необходимо выбрать вид инцидента для детального рассмотрения. В соответствии с выбранным видом инцидента ИБ программой строятся его сценарии.

В разработанном программном средстве предусмотрена функция вторичной оценки, которая представляет собой сбор дополнительной информации относительно обнаруженных факторов и соответствующих им событий для подтверждения их актуальности. В комментариях к каждому событию приводятся сведения о том, например, какая дополнительная информация нужна для подтверждения или опровержения факторов, и источник этой информации. Программа перестраивает сценарий инцидента в соответствии с подтвержденными при вторичной оценке факторами. Кроме того, программное средство позволяет построить все возможные сценарии инцидента, факторы которых отмечены не были (рис. 3). Эта функция позволяет обработчику инцидентов произвести сбор дополнительных сведений по рассматриваемому инциденту ИБ и повысить достоверность информации для принятия решения о мерах по реагированию на него.

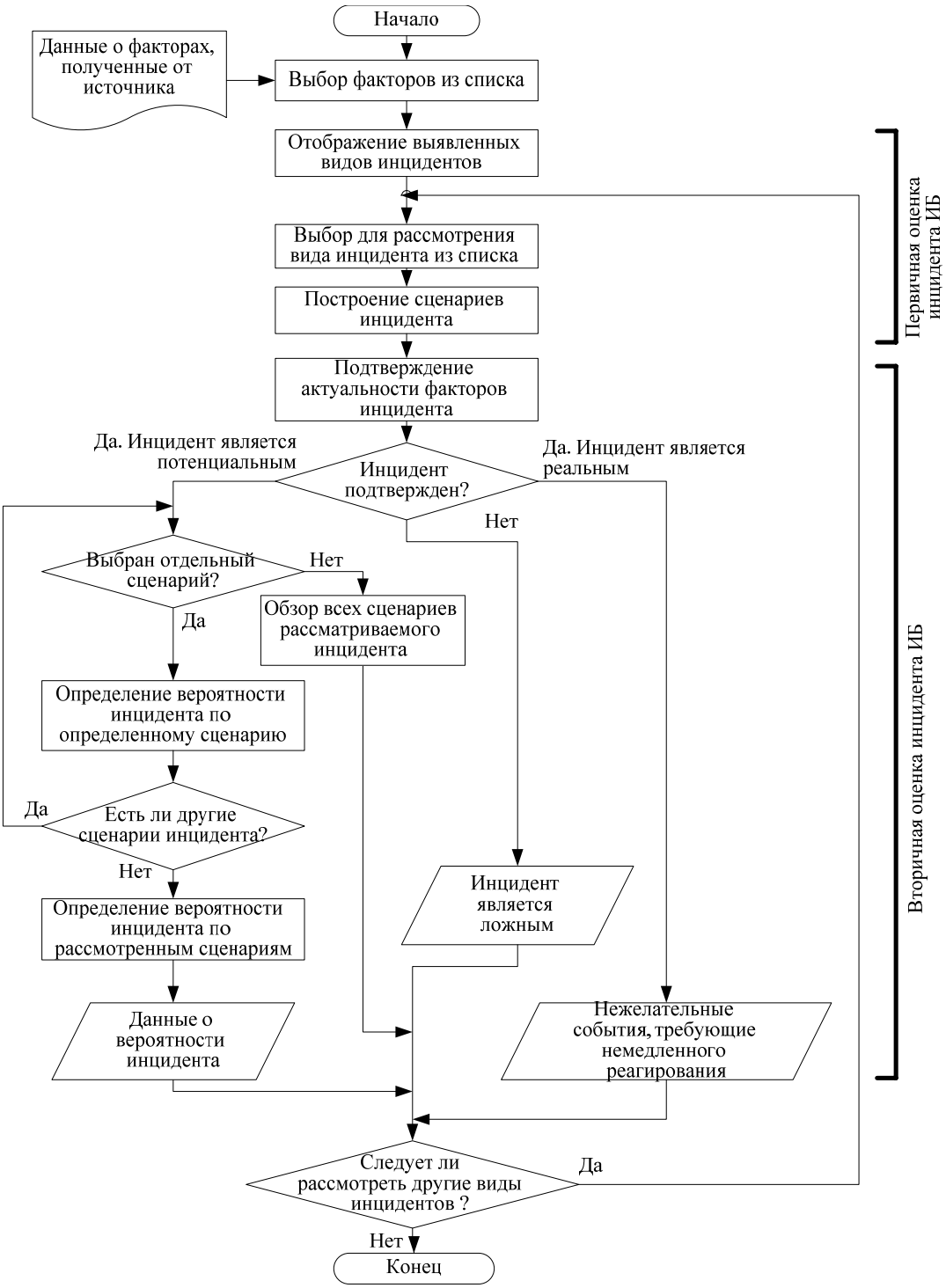

Рис. 2. Алгоритм работы программного средства

Программное средство позволяет оценить вероятность потенциального инцидента по отдельным его сценариям в соответствии с частотой нежелательных событий и уровнем защитных мер по их предотвращению. Для этого в программе установлено 5 уровней защитных мер – от 0 (защитные меры отсутствуют) до 4 (защитные меры предотвращают нежелательное событие в сценарии инцидента). Каждому уровню соответствует коэффициент результативности защитных мер – z. Например, если выбран «шаг» между уровнями, равный 0,25, то для защитных мер с уровнем 1 коэффициент результативности будет равен 0,75 (т.е. применение этих защитных мер снижает вероятность события инцидента на 0,25), а для защитных мер с уровнем 2 коэффициент будет равен 0,5 (т.е. применение этих защитных мер снижает вероятность события инцидента на 0, 5) и т.д. Вероят-

ность нежелательного события в сценарии инцидента в соответствии с [8] определяется следующим образом:

$$P_{HC} = h_i z_i \,, \tag{1}$$

где P_{HC} – вероятность нежелательного события; $i = \overline{1,n}$, где n – количество нежелательных событий в сценарии инцидента; h_i – частость события, являющегося причиной нежелательного события; z_i – коэффициент результативности защитных мер, направленных на предотвращение нежелательного события в сценарии инцидента.

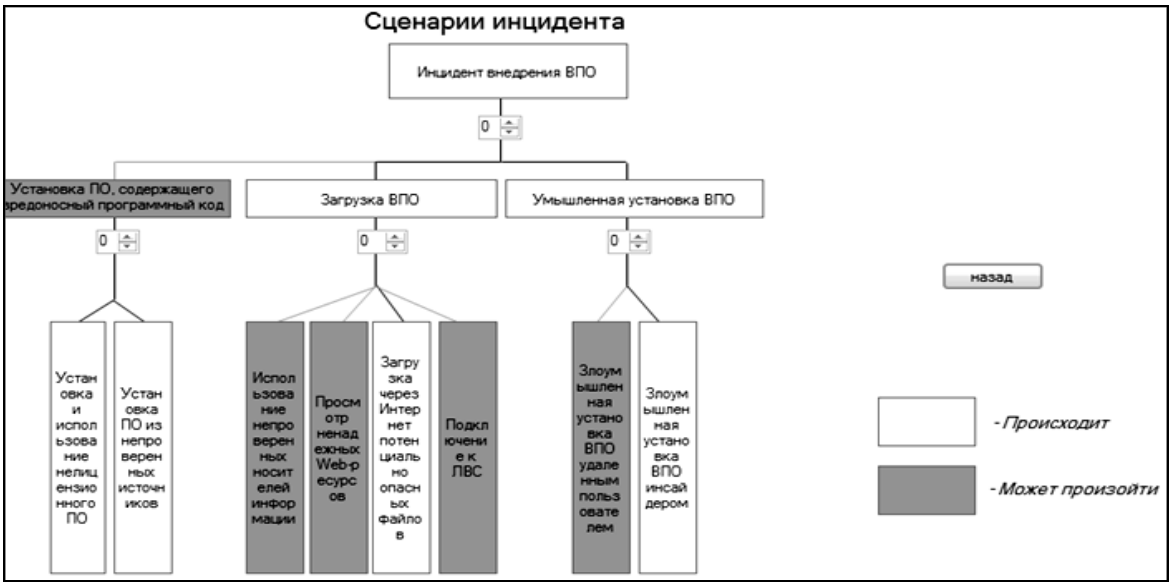

Рис. 3. Обзор сценариев инцидента внедрения ВПО

Вероятность инцидента по отдельному сценарию $P_И$ в соответствии с [8] определяется следующим образом:

$$P_И = \prod_{i=1}^{n} h_i z_i \,. \tag{2}$$

Результат определения вероятности инцидента ИБ по его отдельному сценарию на примере инцидента внедрения вредоносного программного обеспечения (ВПО) приведен на рис. 4.

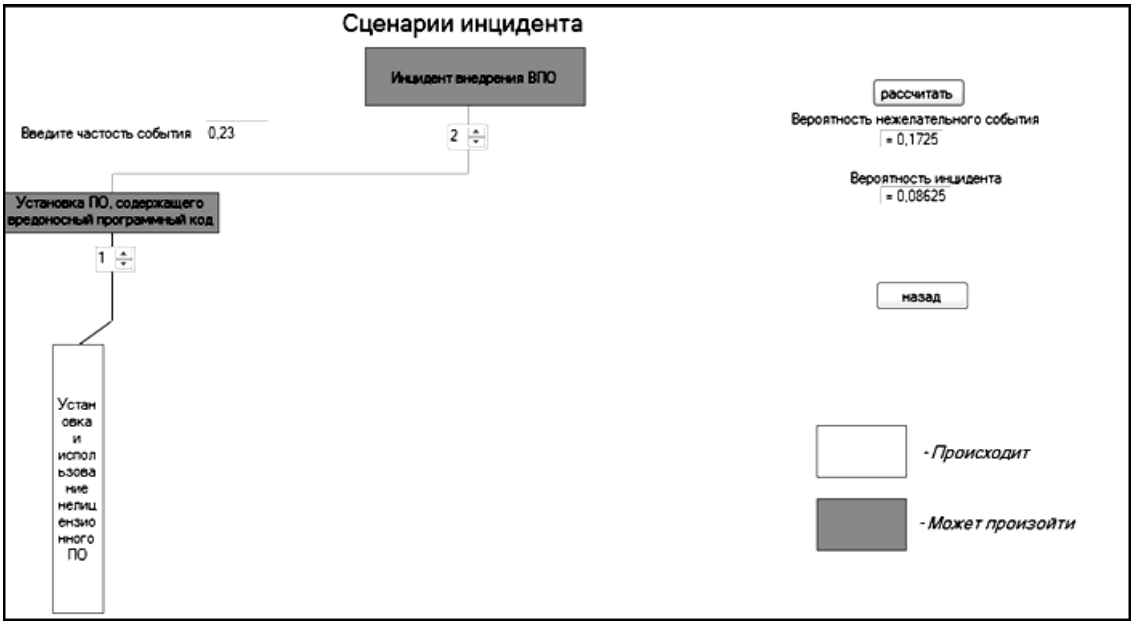

Рис. 4. Результат определения вероятности инцидента внедрения ВПО

Заключение. Таким образом, способ, реализуемый программным средством, позволяет по наблюдаемым факторам выделить соответствующий инцидент ИБ, рассмотреть наглядно его возможный сценарий, подсчитать вероятность инцидента, с учетом условных уровней защитных мер. Также программа даёт возможность просмотреть возможные нежелательные события инцидента, которые не были выявлены пользователем.

Разработанное программное средство дает возможность оценить происходящие в системе инциденты ИБ на основе актуальной базы данных о произошедших событиях и инцидентах ИБ, тем самым способствуя существенному уменьшению времени и повышению достоверности информации для адекватного принятия решения по обработке обнаруженных инцидентов ИБ.

Литература

1. ISO/IEC 27001:2005. Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования. – 2005. – 54 с.

2. ISO/IEC 27035:2011. Информационные технологии. Метод обеспечения безопасности. Управление случайностями в системе информационной безопасности. – 2011. – 78 с.

3. ГОСТ Р ИСО/МЭК 18044:2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – М.: Стандартинформ, 2009. – 50 с.

4. Утечки конфиденциальной информации (итоги 2013 года) [Электронный ресурс]. – Режим доступа: http://www.banki.ru/news/research/?id=6242078, свободный (дата обращения: 19.06.2013).

5. Обзор инцидентов информационной безопасности АСУ ТП зарубежных государств [Электронный ресурс]. – Режим доступа: http://www.securitylab. ru/analytics/398184.php, свободный (дата обращения: 19.06.2013).

6. ИБ инциденты СНГ 2011 г. [Электронный ресурс]. – Режим доступа: http://www. security-scripts.ru/download/books/ib-incidenty.pdf, свободный (дата обращения: 19.06.2013).

7. Щербакова А.Ю. Алгоритм обнаружения и анализа инцидентов информационной безопасности на основании их факторов // Открытые инновации – вклад молодежи в развитие региона: сб. матер. рег. молодежного форума (г. Пенза, 6 декабря 2013 г.). – Пенза: Изд-во ПензГУ, 2013. – Т. 1. – С. 225–226.

8. Щербакова А.Ю. Вероятностная оценка последствий инцидентов информационной безопасности // Труды междунар. симпозиума «Надежность и качество – 2013». – Пенза: Изд-во ПензГУ, 2013. – Т. 1. – С. 125–128.

Зефиров Сергей Львович
Канд. техн. наук, доцент, зав. каф. информационной безопасности систем и технологий
Пензенского государственного университета (ПензГУ)
Тел.: 8 (841-2) 36-82-23
Эл. почта: ibst@pnzgu.ru

Щербакова Анастасия Юрьевна
Аспирант каф. «Информационная безопасность систем и технологий» ПензГУ
Тел.: 8 (841-2) 36-82-23

Zefirov S.L., Shcherbakova A.Y.
Information security incidents assessment

A way of information security incidents assessment based on information security events' factors is considered in this paper. An algorithm and its program implementation are suggested.
Keywords: incident, information security, factor, first assessment, second assessment, analysis.