Л И Т Е Р А Т У Р А

1. **Епифанов, В. И.** Технология обработки алмазов в бриллианты / В. И. Епифанов, А. Я. Песина, Л. В. Зыков. – М.: Высш. шк., 1987. – 335 с.

2. **Устройство** для обработки алмаза: пат. РБ № 1447 / М. Г. Киселев, В. Т. Минченя, Г. А. Галенюк.

3. **Экспериментальная** оценка интенсифицирующего воздействия ультразвука на производительность механического распиливания хрупких материалов / М. Г. Киселев [и др.] // Теоретические и технологические основы упрочнения и восстановления изделий машиностроения: сб. науч. тр. – Полоцк: Полоцкий государственный университет, 2002. – С. 633–637.

4. **Дроздов, А. В.** Влияние виброударного режима взаимодействия режущего инструмента и обрабатываемой заготовки на условия формирования ее шероховатости при механическом распиливании хрупких и твердых материалов / А. В. Дроздов, М. Г. Киселев // Инженерно-физический журнал. – 2005. – № 2. – С. 171–176.

5. **Быковский, И. М.** Основы теории вибрационной техники / И. М. Быковский. – М.: Машиностроение, 1968. – 362 с.

Поступила 3.03.2008

УДК 004.932

МЕТОДИЧЕСКИЙ ПОДХОД К АНАЛИЗУ И ОЦЕНКЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ, ОСНОВАННЫЙ НА ОПАСНОСТИ УЯЗВИМОСТЕЙ

Канд. техн. наук КРОТЮК Ю. М., КАМЛЮК В. А.

ОИПИ НАН Беларуси,
Лаборатория Касперского, г. Москва

Общепринятым подходом к проведению оценки информационной безопасности информационных систем (ИС) является использование общего методологического подхода, закрепленного в качестве международного стандарта ИСО/МЭК 15408–99 «Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3», который получил название «Общие критерии» и в качестве предстандарта введен в Республике Беларусь.

Методология «Общих критериев» предусматривает необходимость проведения анализа возможных источников угроз и уязвимостей, их сопоставления друг с другом, анализа рисков нарушения информационной безопасности, связанных с причинением ущерба владельцам информационных ресурсов.

Вопросам анализа и оценки угроз уязвимостей, анализа и оценки рисков нарушения информационной безопасности посвящены работы ряда авторов [1–3]. Предлагаются схемы как качественной оценки угроз [1], так и их количественной оценки, основанной на использовании методов экспертных оценок [2]. В указанных работах объектами экспертной оценки становятся события в целом и не проводится структурная декомпозиция события с целью уточнения оценки, определения типовых этапов реализации события и оценки сложности реализации этих этапов с дальнейшей интегральной оценкой события в целом.

Настоящая статья направлена на рассмотрение методического подхода к анализу и оценке безопасности информации в ИС, основанного на анализе уязвимостей и их опасности. Под опасностью уязвимости понимается сложность ее эксплуатации в составе информационной системы.

Угрозы безопасности ИС проявляются через уязвимости конкретного объекта ИС, последние, в свою очередь, обусловливаются свойствами и особенностями принятых проектных решений, связанных со способами и механиз-

мами реализации основных целевых задач (вариантов использования ИС), применяемым общесистемным программным обеспечением и аппаратной платформой.

Источники угроз могут использовать уязвимости для нарушения безопасности информации в ИС. Устранение или ослабление уязвимостей, присущих ИС, влияет на возможность реализации угроз, а следовательно, непосредственно определяет степень защищенности информации в ИС.

Для удобства дальнейшего рассмотрения воспользуемся классификацией уязвимостей, приведенной в [2].

Уязвимости могут быть разделены на: объективные – зависящие от особенностей построения и технических характеристик оборудования, использующего на защищаемом объекте; субъективные – зависящие от некомпетентных действий сотрудников, осуществляющих взаимодействие с ИС (актеров); случайные – зависящие от особенностей окружающей объект среды и непредвиденных обстоятельств, связанных с этой средой.

Последний класс уязвимостей связан с малопредсказуемыми факторами и, как правило, в равной степени присущ всем возможным вариантам реализации ИС, а их устранение – с проведением комплекса мероприятий, направленных на создание безопасных условий функционирования ИС.

В связи с этим при дальнейшем анализе будут рассматриваться уязвимости первых двух классов – объективные и субъективные, механизмы противодействия которым в наибольшей степени закладываются непосредственно в ИС на этапе технического проектирования.

Не останавливаясь подробно на методических вопросах анализа и поиска уязвимостей в составе ИС, отметим лишь, что в этом вопросе существуют два основных подхода [1]: логический (ручной) анализ проектных решений, конфигурационных файлов, маршрутизаторов, серверов, других критических элементов сети; тестирование системы защиты ИС с использованием сетевых сканеров, располагающих базами данных об известных уязвимостях, и программных агентов.

Под эффективностью системы защиты информации в ИС будем понимать отсутствие либо степень опасности уязвимых мест, присутствующих в системе, эксплуатация которых источниками угроз может привести к нарушению целостности, доступности или конфиденциальности информации.

На практике получение точных значений характеристик степени опасности уязвимостей затруднено, так как понятие сопротивляемости механизмов защиты внешним атакам трудно формализуемо и требует анализа сценариев реализации атаки в процессе эксплуатации конкретных уязвимостей.

Описанный в настоящей работе подход позволяет получить количественную оценку защищенности ИС на основе предлагаемых схем реализации типовых атак для выделенных классов уязвимостей.

Основой предлагаемого подхода является интуитивно понятное предположение о том, что для реализации угрозы безопасности информации в ИС источнику угрозы необходимо осуществить ряд воздействий на ИС, в результате которых будут преодолены защитные механизмы ИС. Указанные воздействия (в дальнейшем такое воздействие будем называть этапом атаки при эксплуатации уязвимости) представляют собой не что иное, как варианты использования системы злоумышленником. Основным элементом такого воздействия является посылка в систему сообщения, результатом которого будет являться либо нарушение состояния безопасности информации, либо получение от системы дополнительной информации, необходимой для посылки очередного сообщения. Конечной целью указанной последовательности сообщений является нарушение состояния безопасности информации в ИС.

В этом случае степень защищенности информации в ИС может быть оценена по совокупному количеству уязвимостей, выявленных на этапе анализа ИС и по степени опасности этих уязвимостей, выраженной в количестве необходимых элементарных воздействий, которые необходимо произвести на ИС для нарушения ее безопасного состояния.

Защищенность ИС S от всех возможных угроз безопасности определяется количеством уязвимостей и прочностью барьеров (механизмов защиты), перекрывающих эти уязвимости.

В идеале каждый механизм защиты должен исключать путь реализации угрозы через уязвимость.

В действительности механизмы защиты обеспечивают лишь определенную степень сопротивляемости ИС угрозам безопасности.

Защищенность ИС S^{Γ} от выделенных в процессе анализа условий функционирования и активов, группы угроз безопасности определяется количеством уязвимостей E^{Γ}, которые могут быть использованы для реализации выделенной группы угроз, и прочностью барьеров, перекрывающих эти уязвимости.

Таким образом, в качестве характеристик защищенности информационной системы выступают следующие показатели: $E=\{E_i\}$ – множество уязвимостей, каждая уязвимость E_i, $i=\overline{1, I}$, может потребовать n_i этапов проведения атаки для ее эксплуатации ($n_i=\overline{1, N}$); N – размерность множества E.

В простейшем случае под этапом проведения атаки для эксплуатации уязвимости можно рассматривать сообщение, посланное злоумышленником и направленное на эксплуатацию уязвимости.

В условиях введенных обозначений в качестве критерия оценки защищенности информации в ИС может быть использован критерий вида

$$S=\prod_{i=1}^{N}\left(1-\frac{1}{n_i}\right). \qquad (1)$$

Легко убедиться, что критерии указанного вида позволяют проводить оценку защищенности ИС и работают на всем множестве возможных состояний системы. Так, в пограничных случаях при наличии в системе одной уязвимости для эксплуатации которой достаточно реализовать один этап атаки (посылка одного элементарного воздействия), защищенность такой системы S считается равной 0. Чем больше этапов необходимо реализовать злоумышленнику в процессе проведения атаки, тем выше уровень защищенности ИС.

На практике получение значений количества этапов n_i, необходимых для эксплуатации i-й уязвимости, затруднено, так как процесс реализации атаки зависит от большого количества факторов.

Вместе с тем анализ значительного количества известных уязвимостей позволяет построить типовые модели реализации атак, определить последовательность действий нарушителя в процессе реализации атак, а следовательно, и количество этапов, которые необходимо преодолеть для эксплуатации уязвимости.

Рассмотрим более подробно механизмы реализации атак, направленных на эксплуатацию уязвимостей.

Под уязвимостью системы защиты ИС будем понимать возможность реализации угрозы в отношении ИС. На практике под уязвимостью системы защиты ИС обычно понимают не саму возможность осуществления угрозы безопасности, а те свойства системы, которые способствуют успешному осуществлению угрозы либо могут быть использованы злоумышленником для осуществления угрозы.

Обобщенную модель, иллюстрирующую необходимые и достаточные условия эксплуатации уязвимости, можно представить в виде схемы (рис. 1).

Для оценки защищенности системы необходимо выделить ряд уязвимостей этой системы и произвести их количественную оценку. Для решения задачи количественной оценки уязвимости предлагается рассмотреть обобщенную модель реализации атаки и выделить из этой модели часть, соответствующую конкретной рассматриваемой уязвимости. После этого необходимо пройти по всем элементарным этапам или сообщениям, составляющим модель (отображаемым в виде овалов с названием этапа снизу) по направлениям, отмеченным стрелками сверху вниз, и экпертным путем оценить веса элементарных этапов с учетом специфики и сложности прохождения этапов для рассматриваемой уязвимости.

Полученная модель реализации атаки с весовыми коэффициентами сложности реализации ее этапов может быть использована при количественной оценке защищенности ИС по отношению к конкретной уязвимости. Обобщенная модель реализации атак приведена на рис. 2.

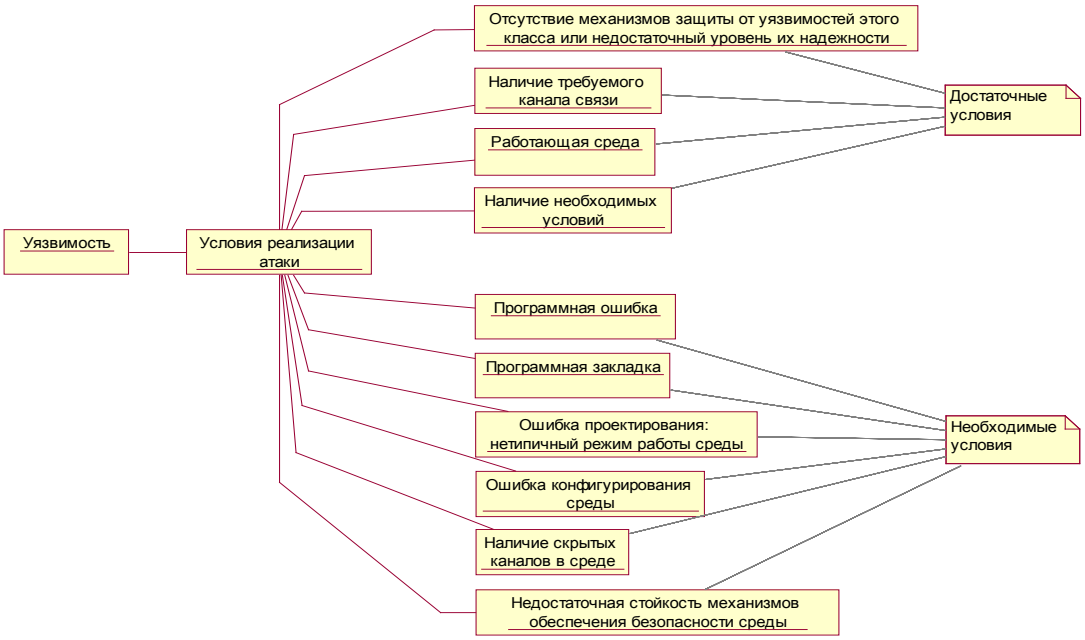

Рис. 1. Необходимые и достаточные условия эксплуатации уязвимости

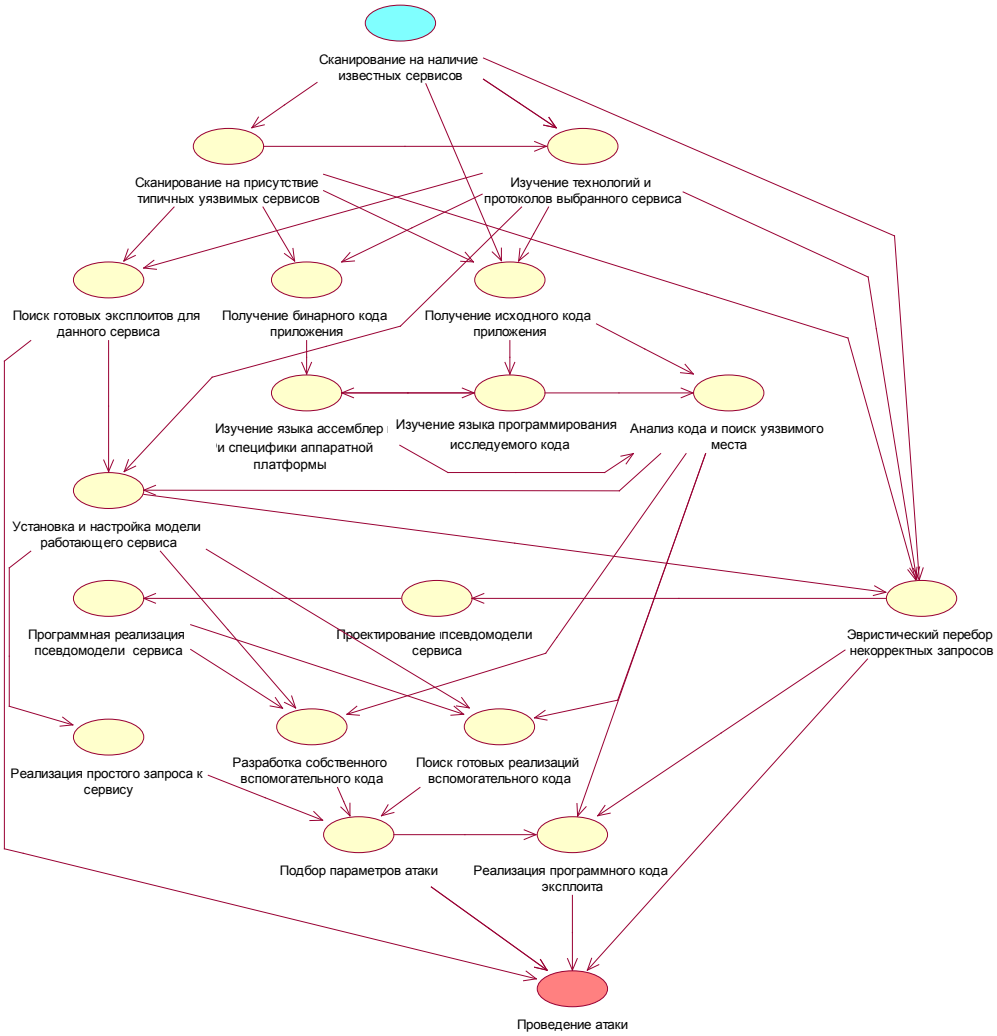

Рис. 2. Обобщенная модель реализации атак

Типовые модели реализации атак для ряда часто встречающихся уязвимостей могут быть выделены из обобщенной модели. На рис. 3 в качестве примера приведена модель реализации атаки типа переполнения стека (Stack Overflow Attack), показывающая, как необходимо производить выбор модели для конкретной уязвимости из обобщенной модели. Аналогичным образом из обобщенной модели могут быть построены модели реализации атак: атаки для сервера MS IIS (IIS Unicode Bug); атаки для CGI приложений (Attack to CGI); атаки типа отказ в обслуживании (Denial of Service Attack) и др.

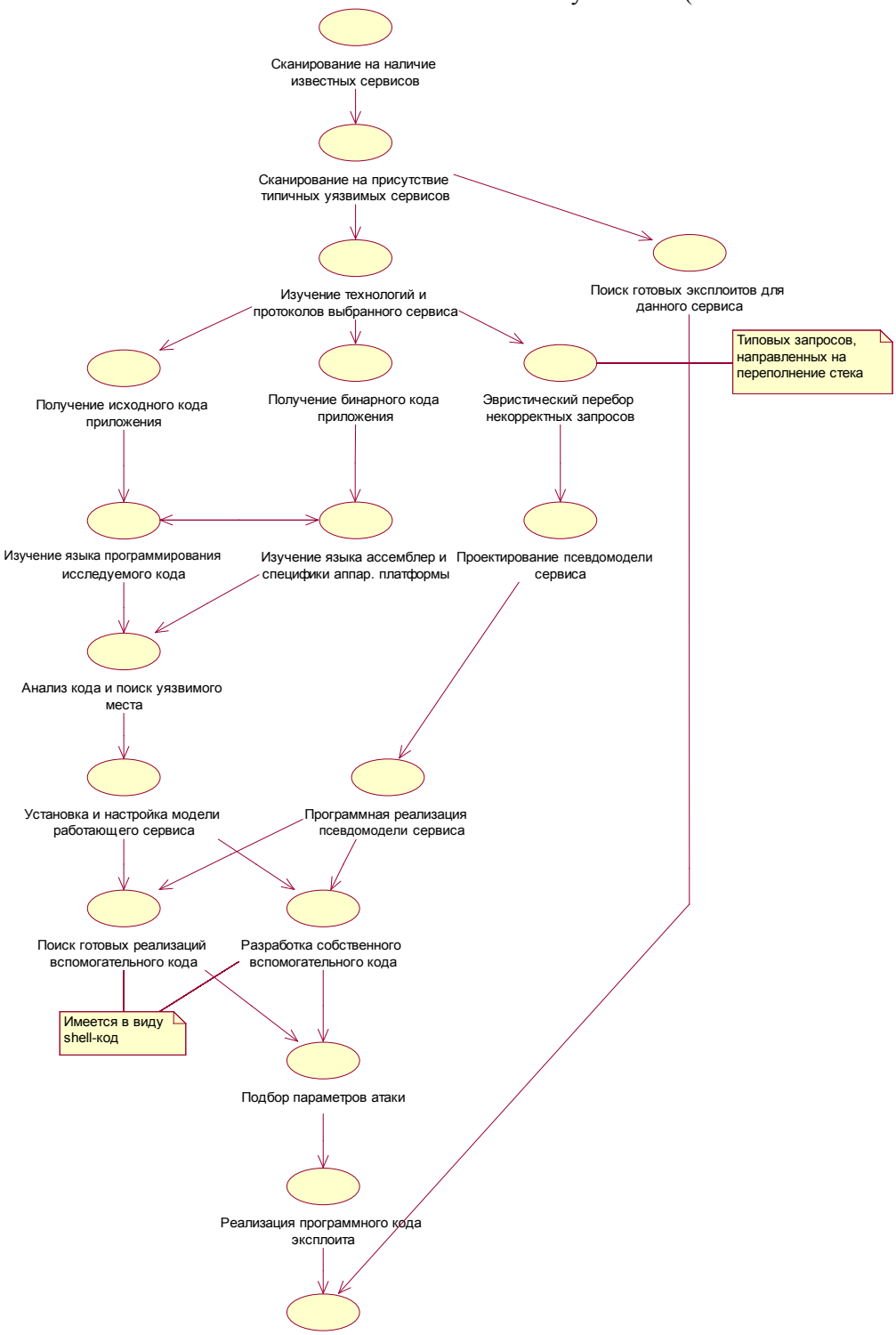

Рис. 3. Модель реализации атаки типа переполнения стека (Stack Overflow Attack)

Для более полной количественной оценки опасности уязвимости необходима оценка сложности реализации каждого из этапов, которая может производиться с привлечением экспертов путем назначения весовых коэффициентов.

Представленные схемы модели реализации атак содержат возможные варианты реализации атаки, выбор которых остается за нарушителем и зависит от его предшествующего опыта. В процессе экспертной оценки сложности реализации этапов уязвимости производится выделение возможных путей реализации атаки, для которых выполняются необходимые и достаточные условия. Затем осуществляется оценка этапов для каждого из выделенных путей. При оценке уязвимости ИС возможны различные процедуры выбора показателей. В случае предположения о том, что нарушитель будет следовать стратегии использования варианта, являющегося наиболее простым с точки зрения его реализации, в качестве критерия оценки защищенности ИС в отношении конкретной уязвимости может использоваться критерий вида

$$D_i = \min_{l \in L_i} \sum_{j=1}^{m_l} K_{ij}^l, \qquad (2)$$

где D_i – интегральный показатель сложности реализации атаки при эксплуатации i-й уязвимости; L_i – множество возможных вариантов реализации атаки при эксплуатации i-й уязвимости; K_{ij}^l – весовой коэффициент сложности подготовки и реализации j-го этапа проведения атаки, направленной на эксплуатацию i-й уязвимости для варианта реализации атаки l, $0 < k_{ij}^l \le 1$, $j = 1, m_l$.

Наличие многовариантности реализации атаки для эксплуатации i-й уязвимости повышает вероятность обнаружения пути реализации атаки нарушителем и может быть учтено в оценке сложности реализации атаки. В этом случае в качестве критерия оценки защищенности ИС в отношении конкретной уязвимости может использоваться критерий вида

$$D_i = \prod_{l=1}^{L_i} \sum_{j=1}^{m_l} K_{ij}^l, \qquad (3)$$

где m_l – количество этапов при реализации l-го варианта атаки для i-й уязвимости.

В этом случае критерий оценки защищенности системы S будет иметь вид

$$S = \prod_{i=1}^{N} \left(1 - \frac{1}{D_i}\right), \qquad (4)$$

где k_{ij} – весовой коэффициент сложности подготовки и реализации j-го этапа проведения атаки, направленной на эксплуатацию i-й уязвимости, $0 < k_j \le 1$.

ВЫВОД

Методический подход использован при выборе вариантов реализации механизмов защиты в ИС, а также при оценке безопасности информации в действующих ИС.

Предложенный подход может служить основой для выработки методики оценки защищенности информации в ИС различного назначения.

ЛИТЕРАТУРА

1. **Астахов, А. А.** Анализ защищенности корпоративных систем / А. А. Астахов // Открытые системы. – 2002. – Июль – август. – С. 44–49.

2. **Вихорев, С. В.** Как узнать откуда напасть и откуда исходит угроза безоапасности / С. В. Вихорев, Р. Ю. Кобиев // Конфидент. – 2002. – Февраль. – С. 44–49.

3. **Симонов, С.** Современные технологии анализа рисков в информационных системах / С. Симонов // PC Week «Компьютерная неделя». – 2001. – № 37 (307).

Поступила 3.03.2008