О ПРИЗНАКАХ ПОТЕНЦИАЛЬНО ОПАСНЫХ СОБЫТИЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

***Жидков Игорь Васильевич**, кандидат технических наук, доцент*
Кадушкин Иван Викторович

Статья посвящена вопросам, касающимся проблем безопасности программного обеспечения и созданных на его основе информационных систем. Рассмотрены проблемные вопросы выявления выявлению недекларированных возможностей. Предложена иерархическая классификации нарушений целостности, доступности и целостности. Предложен подход по выявлению потенциально–опасных событий, основанный на сочетании структурного анализа и функционального тестирования.

***Ключевые слова**: сертификация, потенциально опасные события, недекларированные возможности, безопасность программ.*

ABOUT THE SIGNS OF POTENTIALLY DANGEROUS EVENTS IN INFORMATION SYSTEMS

***Igor Zhidkov**, Ph.D., Associate Professor*
Ivan Kadushkin

The issues related to information security systems are discussed. The problem of identify of software security defects is considered. The hierarchical classification of violations of integrity, availability, and integ–rity is proposed. An approach to identify potentially dangerous events based on a combination of structural analysis and functional testing is offered.

***Keywords**: certification, information security defects, undeclared features, software security.*

В настоящее время проблема безопасности программного обеспечения (ПО) и созданных на его основе информационных систем (ИС) стоит как никогда актуально [4,5].

По требованиям безопасности ПО и ИС проверяются с целью контроля функционального соответствия, защиты от несанкционированного доступа, выявления недекларированных возможностей (НДВ), реализующих события, опасные с точки зрения безопасности информации. Проверки могут осуществляться как независимыми представителями заказчика или самого разработчика в процессе разработки и производства ПО, так и экспертами испытательных лабораторий или каких-либо аттестационных комиссий на испытаниях ПО и ИС.

Порядок и требования к проведению сертификационных испытаний описаны в Руководящих документах Гостехкомиссии России (ныне ФСТЭК России) [8].

Рассмотрим более подробно проблему выявления НДВ.

Бытует мнение, что при наличии необходимой документации на ПО (исходных текстов, описания программ, описания применения и др.) на сертификационных или иного рода испытаниях и проверках достигается гарантированное выявление всех НДВ. Однако, это мнение принципиально ошибочное. Дело в том, что изначально вообще неизвестно, внесены НДВ в ПО или нет. В разных испытательных лабораториях при проведении проверок используются принципиально различные технологии, которые по большому счету нельзя признать совершенными из-за научной незавершенности проблемы выявления вредоносных функций ПО. Эти технологии реализуются специалистами неодинакового уровня квалификации, сроки проверки ПО могут оказаться весьма жестко ограниченными, что сказывается на качестве проводимых работ и т.д. Наконец, исходная достоверная документация вообще может не представляться [2,3]. Ситуация в полной мере напоминает «поиск черной кошки в темной комнате». В итоге всегда существует остаточный риск того, что после проверки в ПО сохранятся невыявленные ошибки и функциональные возможности, осуществляющие опасные воздействия на обрабатываемую информацию [9].

В реальности требуемая документация на ПО (в первую очередь, исходные тексты, подробные описания программ и их применения) может отсутствовать в объеме, достаточном для детальной проверки. В этом случае приходится анализировать функциональность и безопасность ПО путем выявления и анализа ПОС в ходе имитации процессов его функционирования.

Таким образом, своевременное выявление и устранение опасных событий на этапе тестирования ПО способно предотвратить или существенно снизить ущерб, возникающий в результате наличия в ПО вредоносного кода.

Одним из основных признаков обеспечения безопасности информации в ИС является сохранение ее целостности, конфиденциальности и доступности.

В ГОСТ РВ 51987-2002 «Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества функционирования информационных систем. Общие положения» введены следующие определения [1, 6]:

- целостность информации – состояние информации, при котором обеспечивается достижение целей ее функционального применения;

- конфиденциальность информации – свойство используемой информации быть сохраненной в течение заданного объективного периода конфиденциальности от ознакомления лицами, к ней не допущенными, и/или от несанкционированного считывания техническими средствами;

- доступность информации – это состояние информации, ее носителей и технологий обработки, при котором обеспечивается санкционированный доступ к ней и надежность представления требуемой информации.

Рассмотрим классификационные признаки потенциально-опасных событий (ПОС) при функционировании ПО.

Признаки потенциально опасных событий, связанных с нарушением целостности информации

В соответствии с требованиями руководящими документами Гостехкомиссии России в ИС должна быть обеспечена целостность программных средств, обрабатываемой информации, а также неизменность программной среды.

Основываясь на данном требовании к ИС можно сформулировать типовые способы программного нарушения целостности информации:

1) нарушение целостности информационного ресурса ИС:

- нарушение целостности файлов;

- нарушение целостности записей (полей записей);

- нарушение целостности каталогов и папок.

2) нарушение целостности программного ресурса ИС:

- нарушение целостности программ;

- нарушение размещения программ на внешних носителях информации.

3) нарушение целостности программной среды:

- нарушение целостности активных процессов;

- активизация несанкционированных процессов;

- несанкционированное удаление активных процессов.

Вышеприведенные способы программного нарушения целостности информации базируются на следующем множестве событий, являющихся высшим уровнем детализации классификационных признаков нарушения целостности информации:

- несанкционированная модификация информации;

- несанкционированное уничтожение информации;

- несанкционированное перемещение информации.

Анализ сформированного множества событий нарушения целостности информации позволяет определить характерные последствия при их реализации в ИС:

- отсутствие возможности активизации программного ресурса ИС;

- отсутствие возможности использования информационного ресурса ИС;

- изменение декларируемого алгоритма программ;

- неверное выполнение расчетных задач по причине модификации информационного ресурса;

- изменение штатного алгоритма активного процесса;

- изменение состава необходимых активных процессов;

программные сбои ИС и возникновение исключительных ситуаций в процессах.

Причинно-следственная связь между способами программного нарушения целостности и последствиями реализации ПОС, направленных на нарушение целостности информации иллюстративно представлена на рисунке 1.

Одним из основных требований к проводимым испытаниям ПО является выявление НДВ, реализующих несанкционированные функции нарушения целостности информационного и программного ресурса (ИПР) в ИС.

Выполненный анализ и опыт проведения испытаний ПО позволяет построить иерархическую структуру классификационных признаков нарушения целостности информации, представленную на рисунке 2.

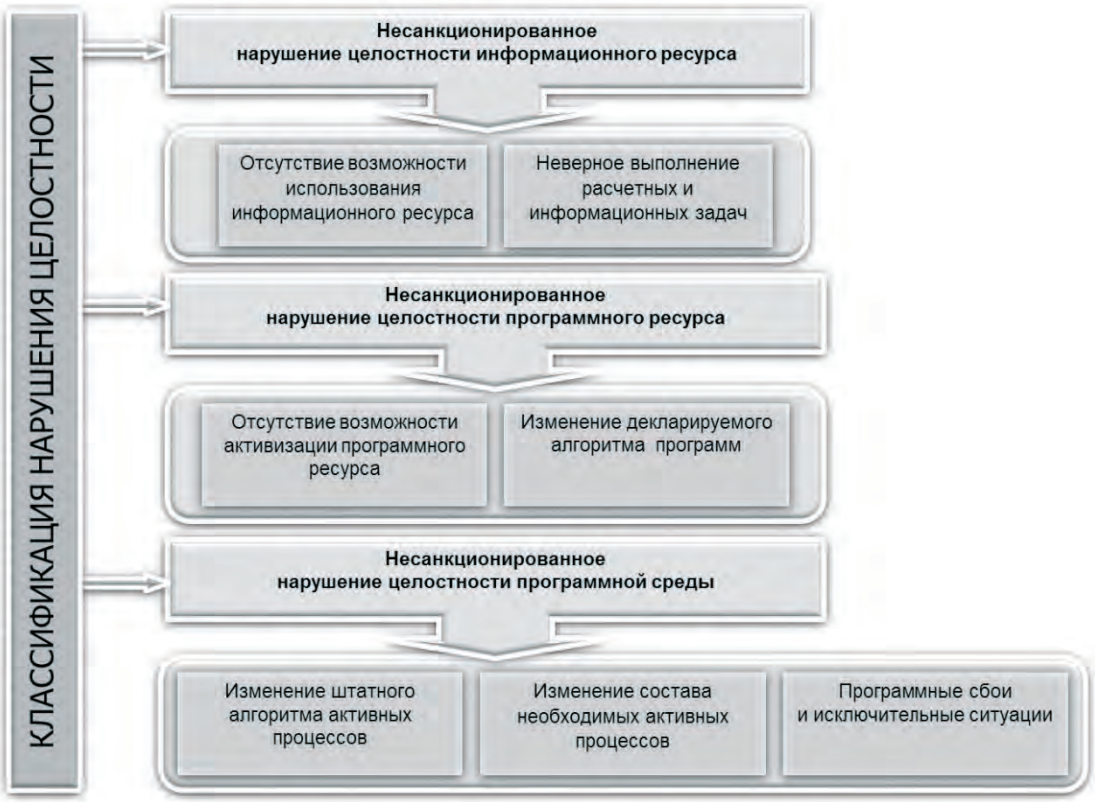

Рис. 1. *Связь между способами и последствиями реализации опасных событий, направленных на нарушение целостности информации*

Рис. 2. *Иерархич еская структура классификационных признаков нарушения целостности ИПР*

Признаки потенциально опасных событий, связанных с нарушением конфиденциальности информации

Нарушение конфиденциальности информации напрямую связано с реализацией угрозы несанкционированного доступа к ИС и является следствием нарушения системы защиты информации.

Угрозы нарушения конфиденциальности, как правило, выступают в форме несанкционированного обращения.

Термин «несанкционированное обращение» означает активные действия, направленные на сбор или хищение ценной информации, закрытой для доступа посторонних лиц.

Опыт эксплуатации показывает, что около 80% попыток НСД к конкретной ИС осуществляют лица, работающие или работавшие с данной системой [7]. Поэтому будем считать, что потенциальный нарушитель имеет достаточно высокую квалификацию и ему известны принципы функционирования ИС.

К типовым способам нарушения конфиденциальности можно отнести:

- уничтожение или вывод из строя ПО с целью вывода из строя СЗИ или системы передачи данных;
- изменение программно-информационного обеспечения с целью нарушения штатных режимов функционирования ИС;
- захват прав доступа авторизованных пользователей;
- использование уязвимостей в ПО и операционных системах или ошибок, допущенных при администрировании;
- использование доверия между хостами (хост – хост) и сетями (сеть – сеть);
- использование средств, реализующих недекларированные возможности – "троянцы", лазейки (дыры), вирусы и т.д.;
- использование ошибок и особенностей сетевых протоколов или инфраструктуры сети;
- перехват информации в ходе сетевых взаимодействий;
- перехват информации из оперативной памяти.

Все приведенные способы нарушения конфиденциальности приводят хотя бы к одному из следующих событий, составляющих первый уровень иерархии классификационных признаков нарушения конфиденциальности:

- несанкционированное копирование защищаемых ИПР (естественный способ нарушения конфиденциальности; копирование может осуществляться на жесткий диск, на отчуждаемый носитель информации, на удаленный объект сети и в оперативную память);
- несанкционированное ознакомление с защищаемыми ИПР (под ознакомлением понимается вывод информации на средства отображения: дисплей, печатающее устройство);
- несанкционированная модификация программных средств защиты ИПР (изменения могут вноситься в файлы, отвечающие за обеспечение работы системы разграничения доступа, в атрибуты защищаемых информационных объектов и в другие данные, определяющие работоспособность системы защиты информации; цель этих манипуляций состоит в нарушении правил разграничения доступа);
- несанкционированное перемещение защищаемых ИПР (перемещение может осуществляться на жесткий диск, на отчуждаемый носитель информации, на удаленный объект сети и в оперативную память; кроме того, перемещение или удаление некоторых объектов, отвечающих за работоспособность системы защиты информации может привести к нарушению принятых правил разграничения доступа).

Анализ способов нарушения конфиденциальности показал, что при правильной настройке системы защиты администратор безопасности может получить множество данных (признаков), указывающих на то, что в защищаемой системе была произведена попытка доступа к конфиденциальной информации. Таким образом, чем большими возможностями обладает система защиты, тем больше возможных признаков нарушения конфиденциальности она может обнаружить. Основой для поиска признаков нарушения конфиденциальности является информация, хранящаяся в системных журналах, журналах администрирования и прочих подобных банках данных.

Множество признаков нарушения конфиденциальности напрямую зависит от множества способов эту конфиденциальность нарушить. В то же время, если реализованная система безопасности не сможет обнаружить известных ей признаков, неизвестная системе атака станет осуществимой, и конфиденциальность будет нарушена.

В ходе анализа способов получения несанкционированного доступа к конфиденциальной информации были выявлены следующие характерные последствия реализации опасных событий, направленных на нарушение конфиденциальности в ИС:

1) Нарушение целостности информационно-программных ресурсов.

Нарушение целостности защищаемых данных – первый признак нарушения конфиденциальности, ведь изменение данных возможно только после получения к ним доступа. Нарушение целост-

ности системы защиты информации сигнализирует о возможном изменении характеристик функционирования системы защиты и, как следствие, о возможном нарушении конфиденциальности.

2) Нарушение доступности информационно-программных ресурсов.

Нарушение доступности, как и нарушение целостности, является прямым указанием на попытки осуществления несанкционированного доступа к защищаемым ресурсам, за исключением тех случаев, когда доступность нарушена вследствие случайных событий, связанных со сбоями в ПО или аппаратуре.

3) Заражение программными вирусами.

Многие программные вирусы, особенно распространенные сейчас так называемые «троянские кони» написаны именно с целью ознакомления с конфиденциальными данными.

4) Несанкционированное обращение к устройствам вывода информации.

Это событие связано с отображением информации на устройства вывода – монитор либо печатающее устройство. Данное событие может быть и не замечено обычным пользователем, особенно при наличии сетевого принтера. В этом случае обнаружение нарушения конфиденциальности производится на основе анализа системных журналов.

5) Манипуляции или неправильное использование файлов с информацией.

Сюда относятся и попытки прямого копирования информации, и вывод ее на внешние носители, и печать, и простое ознакомление путем открытия файлов на чтение. Также возможно копирование файлов, содержащих конфиденциальную информацию, в незащищенные области диска. Информация об этих манипуляциях обычно хранится в журналах аудита.

6) Разработка компьютерных программ для неслужебного использования.

Появление неизвестного исполняемого файла может привести к выполнению запрещенных в ИС действий.

7) Сообщения об ошибках в ходе аутентификации.

Если в течение короткого промежутка времени произошло несколько ошибок при аутентификации, это может свидетельствовать о попытках несанкционированного доступа. Кроме того, авторизованный пользователь может обнаружить

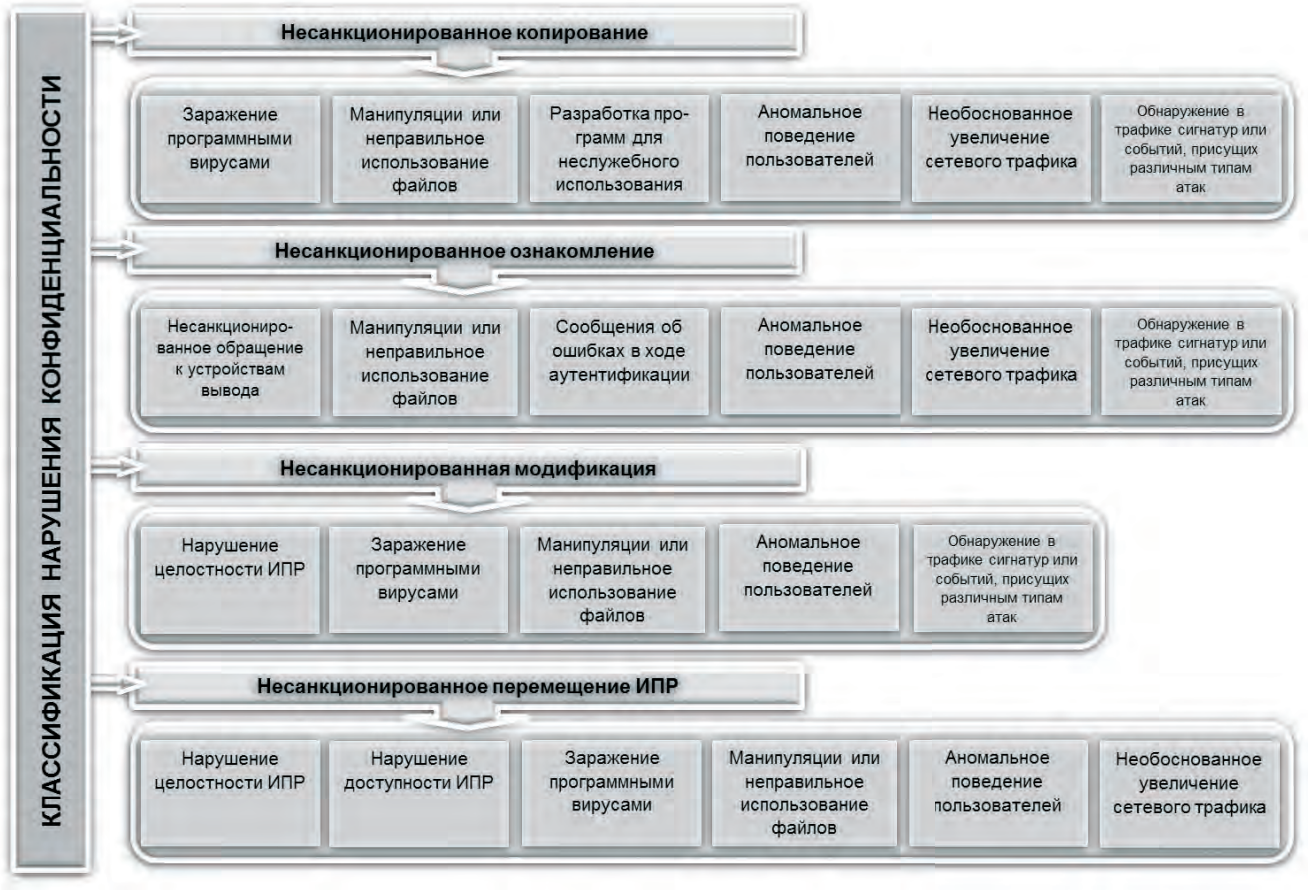

Рис. 3. *Связь между способами и последствиями реализации опасных событий, направленных на нарушение конфиденциальности ИПР*

несанкционированное вхождение в систему от его имени, проанализировав время последнего входа в систему.

8) Аномальное поведение пользователей.

Основной принцип обнаружения аномалий состоит в том, что атаки отличаются от нормального поведения. Скажем, определенную повседневную активность пользователей можно смоделировать достаточно точно. Допустим, конкретный пользователь обычно регистрируется в системе около десяти часов утра, читает электронную почту, выполняет транзакции баз данных, уходит на обед около часа дня, допускает незначительное количество ошибок при доступе к файлам и так далее. Если система отмечает, что тот же самый пользователь зарегистрировался в системе в три часа ночи, начал использовать средства компиляции и отладки и делает большое количество ошибок при доступе к файлам, она должна пометить эту деятельность как подозрительную.

9) Необоснованное увеличение сетевого трафика.

Увеличение исходящего сетевого трафика может свидетельствовать об утечке информации на удаленный объект сети. Увеличение входящего сетевого трафика может свидетельствовать о несанкционированной записи на диск объектов сомнительного содержания, которые могут представлять опасность для функционирования системы защиты информации.

10) Обнаружение во входящем сетевом трафике сигнатур или событий, присущих различным типам атак.

На этом принципе работают программы, реализующие защиту посредством межсетевых экранов.

Связь между способами и последствиями реализации опасных событий, направленных на нарушение конфиденциальности, представлена на рисунке 3.

В ходе испытаний и тестирования ПО по требованиям безопасности информации необходимо дать подтверждение отсутствия в ПО НДВ, реализующих возможности по нарушению конфиденциальности информации. В результате анализа способов, реализующих механизмы нарушения конфиденциальности, предложена иерархическая структура классификационных признаков нарушения конфиденциальности ИПР, изображенная на рисунке 4.

Рис. 4. *Иерархическая структура классификационных признаков нарушения конфиденциальности*

Признаки потенциально опасных событий, связанных с нарушением доступности информации

Для обеспечения гарантированной доступности и сохранности информации как правило применяют многоуровневое резервирование и дублирование каналов передачи данных и внешних носителей информации.

Реакция ответственных служб на нарушения доступности ИПР преследует две главные цели: локализация нарушения и уменьшение наносимого ущерба, и недопущение повторных нарушений.

Планирование восстановительных работ, являясь частным случаем проработки реакции на нарушение доступности, позволяет подготовиться к потенциально опасным событиям, уменьшить ущерб от них и сохранить способность к функционированию критически важных сервисов.

Процесс планирования восстановительных работ можно подразделить на следующие этапы:

- выявление критически важных сервисов, их ранжирование по степени критичности;
- идентификация ресурсов, необходимых для функционирования критически важных сервисов;
- определение перечня потенциально опасных событий;
- разработка плана восстановительных работ;
- подготовка к реализации разработанного плана;
- проверка плана.

И при подготовке мер реагирования на нарушение доступности, и при планировании восстановительных работ необходимо проводить измерения, показывающие, за какое время то или иное действие может быть выполнено на практике. Располагая временной метрикой элементарных действий, можно оценивать продолжительность более сложных мероприятий. Если не удается уложиться в отведенное время, нужно или повысить подготовку персонала, или пересмотреть накладываемые ограничения, или разработать альтернативные, возможно, более дорогостоящие процедуры.

Признаками нарушения доступности информации могут выступать следующие события:

- отсутствие доступа на чтение ресурса;
- отсутствие доступа на запись ресурса;
- отсутствие доступа на исполнение ресурса;
- отсутствие доступа на удаление ресурса;
- отсутствие доступа на перемещение ресурса;
- блокирование определенных функций ПО;
- блокирование вывода информации.

В ходе испытаний на функциональную безопасность ПО необходимо дать подтверждение отсутствия в ПО недекларированных возможностей, реализующих нарушение доступности информации.

В результате анализа признаков нарушения доступности информации можно сформулировать множество ПОС, приводящих к нарушению доступности ИПР. Иллюстративно признаки ПОС, приводящих к нарушению доступности информации представлены на рисунке 5.

Рис. 5. *Признаки ПОС, приводящих к нарушению доступности*

В соответствии с предложенной схемой возникновение каждого из признаков нарушения доступности ИПР является следствием возникновения ПОС, реализацией которых являются системные вызовы операционной системы.

Как видно из предложенных структур, нижним уровнем классификационных признаков ПОС, влияющих на целостность, конфиденциальность и доступность ИПР, являются системные вызовы используемой операционной системы.

В испытательной лаборатории информационных систем и программного обеспечения 3 ЦНИИ МО РФ проведен анализ системных вызовов линек ОС Windows и ОС МСВС. Сформирован перечень потенциально опасных системных вызовов, который используется при проведении сертификационных испытаний по требованиям безопасности информации.

Для выявления описанных ПОС на этапе тестирования и испытаний ПО предлагается совместное использование проверок, как по поиску НДВ, так и на соответствие требованиям по защите от НСД, представленное на рисунке 6.

Заключение

Сложность современных ИС измеряется не столько количеством комплектующих элементов и механических соединений, сколько бесконечным множеством возможных сценариев функционирования подобных систем, семантическим многообразием исходной формализованной информации, подлежащей оперативной обработке в режиме реального времени, и множеством функций программного обеспечения, реализующего эту обработку и подлежащего соответствующим проверкам на испытаниях.

Предлагаемый подход направлен на повышение эффективности выявления ПОС при проведении испытаний ИС на соответствие требованиям безопасности информации.

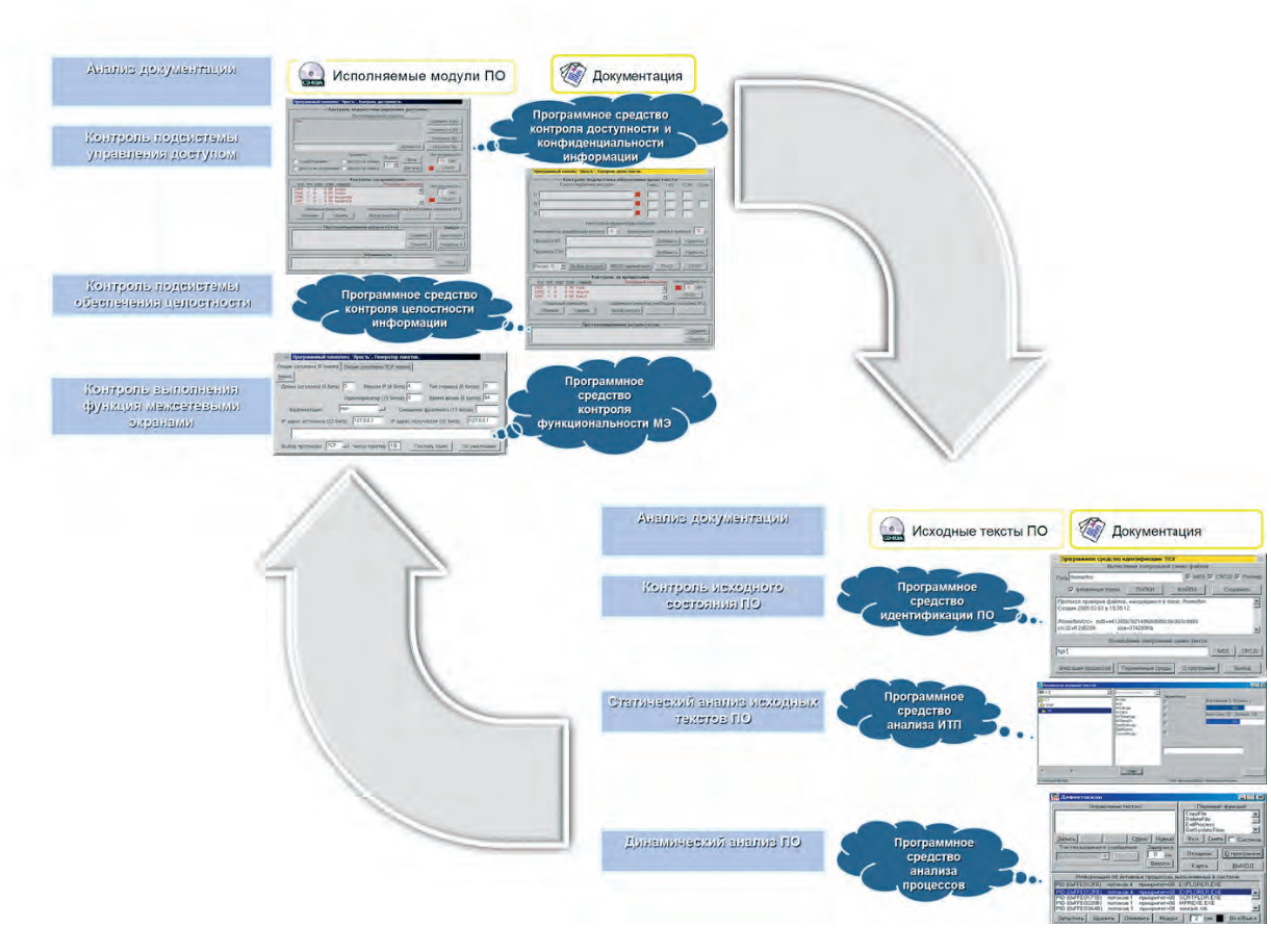

Рис. 6. *Порядок выявления потенциально-опасных событий на этапе тестирования и испытаний ПО*

Литература

1. Бойко А.А., Гриценко С.А., Храмов В.Ю. Система показателей качества баз данных автоматизированных систем. // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2010. № 01. С. 39-45.
2. Жидков И.В., Львов В.М., Федорец О.Н. Применение программно-инструментальных средств автоматизированного тестирования в процессе сертификационных испытаний // Информационное противодействие угрозам терроризма. 2008. № 10. С. 170-176.
3. Жидков И.В., Федорец О.Н. Проблема создания безопасного программного обеспечения и предложения по ее решению // Доклады Томского государственного университета систем управления и радиоэлектроники. 2008. Т. 2. № 1. С. 32-33.
4. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. № 1 (1). С.10-16.
5. Зубарев И.В. Сертификация как направление повышения безопасности информационных систем и программного обеспечения // Известия Южного федерального университета. Технические науки. 2003. Т. 33. № 4. С. 48-53.
6. Костогрызов А.И., Зубарев И.Ю., Родионов В.Н. и др. Методическое руководство по оценке качества функционирования информационных систем (в контексте стандарта ГОСТ РВ 51987). М.: Изд-во 3 ЦНИИ, 2004, 352 с.
7. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность / Справочник. – М.: Новый юрист, 1998. С. 48-57.
8. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.
9. Diomidis Spinellis. Code Quality: The Open Source Perspective. - Addison Wesley, 2006. 569 p.

References

1. Boyko A.A., Gritsenko S.A., Khramov V.Yu. Sistema pokazateley kachestva baz dannykh avtomatizirovannykh sistem, Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Sistemnyy analiz i informatsionnyye tekhnologii, 2010, No 01, pp. 39-45.
2. Zhidkov I.V., Lvov V.M., Fedorets O.N. Primeneniye programmno-instrumentalnykh sredstv avtomatizirovannogo testirovaniya v protsesse sertifikatsionnykh ispytaniy, Informatsionnoye protivodeystviye ugrozam terrorizma, 2008, No 10, pp. 170-176.
3. Zhidkov I.V., Fedorets O.N. Problema sozdaniya bezopasnogo programmnogo obespecheniya i predlozheniya po yeye resheniyu, Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki, 2008, Vol. 2, No 1, pp. 32-33.
4. Zubarev I.V., Zhidkov I.V., Kadushkin I.V. Kiberbezopasnost avtomatizirovannykh sistem upravleniya voyennogo naznacheniya, Voprosy kiberbezopasnosti (Cybersecurity Issues), 2013, No 1(1), pp.10-16.
5. Zubarev I.V. Sertifikatsiya kak napravleniye povysheniya bezopasnosti informatsionnykh sistem i programmnogo obespecheniya, Izvestiya Yuzhnogo federalnogo universiteta. Tekhnicheskiye nauki, 2003, Vol. 33. No 4, pp. 48-53.
6. Kostogryzov A.I., Zubarev I.Yu., Rodionov V.N. and etc. Metodicheskoye rukovodstvo po otsenke kachestva funktsionirovaniya informatsionnykh sistem (v kontekste standarta GOST 51987), Moscow, 2004, 352 p.
7. Kurushin V.D., Minayev V.A. Kompyuternyye prestupleniya i informatsionnaya bezopasnost / Spravochnik, Moscow, Novyy yurist, 1998, pp. 48-57.
8. Markov A.S., Tsirlov V.L., Barabanov A.V. Metody otsenki nesootvetstviya sredstv zashchity informatsii, Moscow, Radio i svyaz, 2012. 192 p.
9. Diomidis Spinellis. Code Quality: The Open Source Perspective. Addison Wesley, 2006, 569 p.