УДК 004.056:061.68

М.А. Колтик

МЕТОДЫ И СПОСОБЫ РЕАЛИЗАЦИИ АВТОМАТИЗИРОВАННОЙ ПОДДЕРЖКИ ПРОВЕДЕНИЯ ИСПЫТАНИЙ КОМПЬЮТЕРНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ (КСЗИ)

Рассматриваются этапы создания КСЗИ, описывается их технология проведения испытаний КСЗИ, а также подход к разработке программного средства поддержки проведения испытаний КСЗИ, выделяются задачи, которые могут быть реализованы с использованием автоматизированного средства поддержки. Также, предлагается возможная методология (алгоритм) автоматизированного проведения испытаний и краткая характеристика функциональных модулей входящих в предложенный алгоритм работы программы. Проводится анализ основных требований к программе, которые должны учитываться при ее разработке.

Введение

В современных условиях, во всех сферах жизнедеятельности, все большее значение приобретает информационный ресурс, наряду с уже традиционными ресурсами, такими как: материальные, трудовые, финансовые.

Специфика информации, как и любого другого не материального актива, состоит в том, что она не имеет материальной формы и, как правило, жесткой привязки к носителю, а ее хищение может быть произведено путем простого копирования, то есть без физического изъятия объекта. Такие особые свойства, а также ценность информационного ресурса заставляет уделять все больше внимания вопросам защиты информации.

Среди угроз, которые могут привести к потере или разглашению информации, особое место занимает несанкционированный доступ к информации, которая циркулирует в информационно-телекоммуникационных системах.

Очевидным является тот факт, что проблемы связанные с безопасностью информации, требуют для своего решения комплексного подхода, суть которого – учет всех возможных угроз безопасности информации и одновременное использование взаимосвязанной совокупности правовых, организационных, математических, программных, технических методов и средств защиты информации путём создания (КСЗИ).

Создание КСЗИ подразумевает проведение определенного перечня работ, среди которых можно выделить следующие этапы:

1) обследование информационной инфраструктуры Заказчика;

2) разработка организационно-распорядительной документации;

3) разработка Плана защиты информации;

4) разработка Технического задания на создание КСЗИ;

5) разработка Проекта КСЗИ;

6) приведение информационной инфраструктуры Заказчика в соответствие с Проектом КСЗИ;

7) разработка эксплуатационной документации КСЗИ;

8) внедрение КСЗИ;

9) предварительные испытания КСЗИ;

10) проведение государственной экспертизы КСЗИ, которая является отдельным этапом приёмочных испытаний АС;

11) поддержка и обслуживание КСЗИ [1].

Испытания КСЗИ являются одним из важнейших этапов в её создании, который дает возможность оценить уровень защищенности автоматизированной системы. В качестве критериев оценки могут выступать существующие нормативные документы и стандарты или требования,

© М.А. Колтик, 2013

выдвигаемые собственником автоматизированной системы (АС) или информации, которая в ней обрабатывается.

Испытания КСЗИ представляют собой процесс подтверждения эффективности её работы и соответствия положениям, определённым в «Техническом задании на создание КСЗИ» или других нормативных документов используемых в качестве критериев оценки.

После успешного завершения испытаний КСЗИ может быть введена в эксплуатацию в составе автоматизированной системы или же должны быть устранены выявленные в ней недостатки, с учётом предложенных дополнительных мер по доработке КСЗИ.

В Украине наблюдается устойчивая тенденция к увеличению потребности в разработке КСЗИ для различных автоматизированных систем. Поэтому проблема качественного проведения испытаний КСЗИ является на сегодня достаточно актуальной.

Проблемы, связанные с проведением испытаний КСЗИ и возможные пути их решения

Для проведения отдельных видов работ, связанных с испытанием КСЗИ, актуальной и своевременной задачей является разработка и применение средств их автоматизированной поддержки.

Актуальность данного решения обусловлена рядом проблем, которые возникают при проведении подобных видов работ традиционным способом, с привлечением специалистов в этой области. Их проведение связано с целым рядом трудностей, как экономического, так и психологического характера [2].

При анализе защищенности автоматизированных систем необходимо учитывать большое количество различных факторов и проводить большое количество рутинных операций, что в свою очередь приводит к увеличению вероятности появления ошибок, которые допускаются специалистами во время проведения испытаний КСЗИ.

Необходимость массового построения КСЗИ и их дальнейшего сопровождения, в чем в настоящий момент нуждается все больше компаний отечественного рынка и государственных организаций, также порождает проблему, которая связана с необходимостью привлечения достаточно большого количества специалистов в сфере защиты информации. Их подготовка требует больших затрат организации, которая проводит переподготовку своих работников. К тому же подготовка квалифицированного специалиста занимает достаточно много времени.

Данные проблемы подталкивают организации, создающие и оценивающие КСЗИ различных автоматизированных систем, к поиску их решений. И одним из таких решений является разработка и использование при проведении испытаний КСЗИ автоматизированных средств поддержки (АСР), что является, бесспорно, конкурентным преимуществом любого предприятия за счёт оптимизации расходов и полученных результатов при выполнении проектов.

Автоматизированные средства поддержки испытаний позволяют облегчить реализацию поставленных задач, повысить качество выполняемых работ, уменьшить рабочую нагрузку на специалистов, особенно, молодых и не имеющих достаточного опыта работы, помочь менее опытным работникам выполнять более сложные задачи.

Использование автоматизированных средства поддержки ведёт к уменьшению сроков выполнения проекта, оптимизации количества и уровня квалификации специалистов, выполняющих проект, обеспечивает эффективное руководство процессом реализации проекта за счёт оперативного исправления проблем и негативных тенденций, которые появляются.

В основе разработки соответствующего программного обеспечения лежит анализ специфики основных видов работ, выделяемых при проведении испытаний КСЗИ, выявление методов и способов формализации соответствующих задач.

Цель данной работы – рассмотрение возможных методов и средств, примени-

мых для реализации автоматизированной поддержки испытаний КСЗИ.

Задачи: провести анализ технологии проведения испытаний КСЗИ, разработать методологию автоматизированного проведения испытаний КСЗИ, разработать требования к программному обеспечению автоматизированной поддержки проведения испытаний КСЗИ.

Понятие защищенности и характеристика оценки уровня защищенности автоматизированной системы

Защищенность является одним из важнейших показателей эффективности функционирования автоматизированной системы, наряду с такими показателями как надежность, отказоустойчивость, производительность и т. п.

Под защищенностью системы подразумевается ее способность противодействовать несанкционированному вмешательству в нормальный процесс её функционирования, а также попыткам хищения, незаконной модификации, использования, копирования или разрушения информации, а также других ее составляющих входящих в состав системы, доступных в процессе выполнения задач или заложенных в систему во время разработки [3].

Под защищенностью автоматизированной системы (АС) будем понимать степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации.

Под угрозами безопасности информации традиционно понимается возможность нарушения таких свойств информации, как конфиденциальность, целостность и доступность.

Можно выделить несколько факторов, которые определяют защищенность автоматизированной системы. В идеале каждый путь осуществления угрозы должен быть перекрыт соответствующим механизмом защиты. Данное условие является первым фактором, определяющим защищенность автоматизированной системы. Вторым фактором является “прочность” существующих механизмов защиты, характеризующаяся степенью устойчивости этих механизмов к попыткам их обхода либо преодоления. Третьим фактором является величина ущерба, наносимого владельцу автоматизированной системы в случае успешного осуществления угроз безопасности [4].

Чтобы гарантировать эффективную защиту от информационных угроз, необходимо иметь объективную оценку текущего уровня информационной безопасности. Именно для этих целей и применяется оценка уровня защищенности системы.

Официально признаваемой оценкой защищенности АС являются классы защищенности, описание которых приведено в стандартах защищенности [5]. К таким стандартам можно отнести: НДТЗІ 2.5-005-99, НДТЗІ 2.5-004-99.

Оценка уровня защищенности – это процесс проведения конкретных мероприятий направленных на получение объективной информации о состоянии информационной безопасности в АС.

В большинстве случаев оценка уровня защищенности автоматизированной системы, которая реализуется КСЗИ, требуется, когда автоматизированная система предназначена для обработки информации с ограниченным доступом.

Следует отметить, что оценку уровня защищенности рекомендуется проводить периодически, так как состояние любой автоматизированной системы изменяется с течением времени и к моменту очередной оценки она может не иметь ничего общего с тем, что было зафиксировано ранее. Как правило, повторную оценку уровня защищенности проводят при изменении архитектуры автоматизированной системы, при изменении ее конфигурации, при выявлении недостаточности реализованных средств защиты, а также, в случае если в автоматизированной системе изменяются требования к защищенности той информации, которая в ней циркулирует [6].

Характеристика технологии проведения испытаний КСЗИ

Технология испытаний КСЗИ проводимая экспертами, состоит из отдельных взаимосвязанных процедур, а именно:

1) анализ совокупности показателей об автоматизированной системе и реализованных в ней средствах защиты информации;

2) анализ циркулирующей в автоматизированной системе информации;

3) выбор критериев для оценивания защищенности автоматизированной системы;

4) анализ проектной документации по созданию КСЗИ предоставленной собственником АС;

5) проведение испытаний в соответствии с разработанной программой и методикой;

6) предоставление выводов о реализованных средствах защиты и рекомендациях, которые касаются устранения выявленных недостатков КСЗИ.

Испытания могут проводиться, как КСЗИ в целом, так и отдельных ее модулей или компонентов.

Испытания КСЗИ проводится в соответствии с критериями, выбранными ее собственником. Выбор критериев, как правило, осуществляется, в соответствии с теми задачами, которые должна выполнять автоматизированная система, частью которой является КСЗИ.

Для АС, собственником которой является государственная организация, критерием оценивания выступают, как правило, государственные нормативные документы по защите информации. Если собственником АС выступает коммерческая организация, а собственником информации, которая циркулирует в автоматизированной системе, является государство, то такая КСЗИ, также должна отвечать государственным стандартам по защите информации, которые прописаны в соответствующих нормативных документах.

КСЗИ может проходить испытания на соответствие национальным критериям, а также международным или внутренним. Однако, национальные критерии защищенности информации, в большинстве случаев, являются основными для подтверждения качества защищенности информации в автоматизированной системе, которая функционирует на территории Украины.

Автоматизация процесса проведения испытаний КСЗИ или отдельных ее процедур, при использовании национальных критериев оценки защищенности системы, является достаточно актуальной задачей, результатом которой будет являться разработка и внедрение в эксплуатацию специального программного обеспечения.

Описание похода к разработке автоматизированной поддержки испытаний КСЗИ

Данный подход описывает основные принципы, которые должны быть реализованы в программном обеспечении для автоматизированной поддержки проведения испытаний в соответствии с государственными стандартами НД ТЗИ и определить достаточность и полноту применяемых средств защиты, с предоставлением результатов испытаний КСЗИ пользователю.

Применение данного подхода должно относиться к компонентам входящих в состав КСЗИ направленным на устранение угроз от несанкционированного доступа (НСД).

Разработка программного обеспечения для автоматизированной поддержки проведения испытаний КСЗИ должна быть реализована в соответствии с такими принципами:

1) программное обеспечение должно позволять вводить и обрабатывать совокупность показателей, характеризующих конкретную автоматизированную систему (объект испытаний (ОИ)) и средства ее защиты;

2) в программном обеспечении должны быть реализованы критерии оценки, под которыми следует понимать совокупность требований (шкалы оценки), которые используются для оценки эффективности функций защиты информации и корректности их реализации;

3) программное обеспечение должно быть разработано в соответствии с определенной методологией оценки, которая определяет последовательность действий (алгоритм), выполняемый программой при проведении оценки уровня защищенности системы, эффективности и корректности реализации функций защиты информации;

4) в программном обеспечении должна быть реализована форма представления результатов оценки, которая включает совокупность показателей, характеризующих уровень защищенности АС, их достаточность и полноту;

5) программное обеспечение должно предоставлять пользователю интуитивно понятный интерфейс.

Результатом проведенных испытаний должно быть соответствующее заключение, на основании которого владельцы АС и обрабатываемых в них информационных ресурсов могут принимать решения о приемлемости и достаточности, принятых мер и реализованных средств касающихся защищенности системы [7].

Описанный подход позволяет получать количественные и качественные оценки уровня защищенности АС, путем сопоставления характеристик, свойств и параметров АС и ее комплексных средств защиты с многократно апробированными на практике и стандартизированными национальными критериями оценки защищенности, которые используются в качестве критериев.

Методика (алгоритм) функционирования программного обеспечения для автоматизированной поддержки проведения испытаний КСЗИ

Данное программное обеспечение должно состоять из следующих функциональных модулей:

первый модуль – ввод пользователем информации об автоматизированной системе, реализованных в ней средствах защиты и вывод (предоставление) пользователю, обработанной информации об автоматизированной системе. Информация, которая вводится пользователем, должна содержать описание подсистем автоматизированной системы и ее элементов, а также характеристику информации, которая циркулирует в этих элементах и требует защиты;

второй модуль – ввод-вывод данных об угрозах для информации, которая обрабатывается в системе. Данный модуль должен предоставить пользователю возможность создать поле угроз (модель угроз) для информации и осуществить их классификацию по нескольким параметрам. Модель угроз должна предоставлять возможность пользователю определить вероятность реализации угроз и относительный уровень ущерба при их реализации;

третий модуль – ввод-вывод данных о нарушителях безопасности. Данный модуль должен предоставить пользователю возможность построения модели нарушителя с их классификацией. Модель нарушителя должна быть разработана при взаимодействии с моделью угроз и пользователь должен иметь возможность определить, какую из угроз может реализовать отдельный вид нарушителя;

четвертый модуль – ввод-вывод данных об отношении между ОИ с циркулирующей в нём информацией, угрозами для ОИ, определения функций защиты, которые должна реализовать КСЗИ, услуг и функционального профиля защищенности;

пятый модуль – пользователь должен определить механизмы защиты в составе ОИ, проанализировать и оценить целесообразность их применения, в соответствии с выделенной моделью угроз, выделенными функциями защиты, которые формируют услуги определенных уровней, входящих в функциональный профиль защищенности. Пользователь должен иметь возможность ввести или выбрать те средства защиты, которые должны быть реализованы в ОИ, а также определить, какие функции защиты они выполняют и от каких угроз защищают;

шестой модуль – пользователю предоставляется оценка уровня защищенности системы. Она выражается в предос-

тавлении пользователю количественных показателей (данных о количестве угроз, которые были устранены и их характеристика) и качественных показателей (данных об оценке вероятности возникновения этих угроз) касающихся устраненных угроз.

В случае если программа выявила угрозы, которые не устранены с помощью указанных средств защиты, программа рассматривает это как уязвимость ОИ и предоставляет пользователю количественную и качественную оценку защищенности, с учетом выявленных уязвимостей. Пользователю предоставляется информация о количественных показателях (данных о количестве обнаруженных уязвимостей и их характеристика) и качественных показателях (вероятность их реализации и уровень относительного ущерба в случае их реализации) уязвимостей ОИ.

Также, пользователю предоставляется сводная информация об устраненных угрозах, выявленных уязвимостях и их характеристика;

седьмой модуль – пользователю предоставляется возможность доработать КСЗИ и сохранить проект.

Пользователю предоставляется возможность после выявления уязвимостей, выбрать функции защиты, которые должны реализовываться КСЗИ для защиты ОИ и устранения выявленных уязвимостей, после чего данные функции должны быть включены в состав услуг и функциональный профиль защищенности. Выбор новых функций может повлиять на уровень определенных услуг, входящих в функциональный профиль защищенности.

На основе выбранных функций пользователю предоставляется возможность указать средства защиты, которые должны будут реализовывать эти функции. После чего, программа предоставляет пользователю обновленные показатели уровня защищенности системы.

Пользователю также предоставляется возможность просмотра средств защиты, которые входят в состав КСЗИ и реализуют указанные функции защиты.

На рис. 1 представлен алгоритм работы и взаимодействия проектных модулей программного обеспечения по автоматизированной поддержке проведения испытаний КСЗИ.

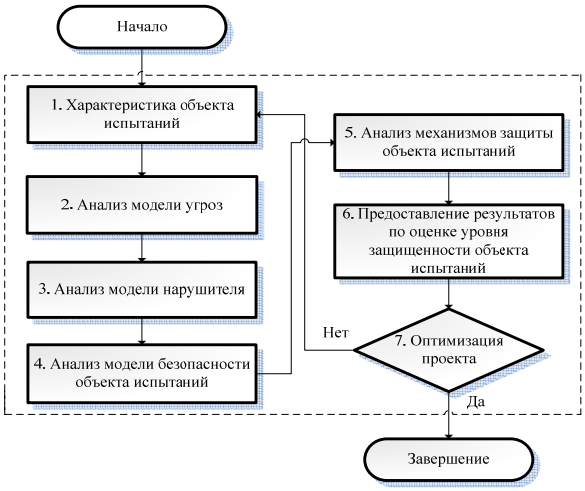

Рис. 1. Характеристика алгоритма работы и взаимодействия проектных модулей программного обеспечения по автоматизированной поддержке проведения испытаний КСЗИ

Характеристика структурно-функциональных модулей алгоритма

S1 – Начало алгоритма;

Первый модуль – ввод-вывод данных относительно архитектуры ОИ, реализованных средств защиты и информации, которая в нем циркулирует.

Операция R1 – ввод данных пользователем относительно архитектуры ОИ, реализованных средств защиты и информации, которая в нем циркулирует;

Операция Z1 – анализ вводимых данных программным обеспечением. В случае ввода некорректных данных, программа отказывается переходить на следующий этап работы и выводит пользователю на экран соответствующее сообщение;

Операция P1 – обработка программой данных введенных пользователем относительно архитектуры ОИ, реализованных средств защиты и информации, которая в нем циркулирует;

Операция R2 – вывод данных относительно архитектуры ОИ, реализованных средств защиты и информации, которая в нем циркулирует.

Второй модуль – Ввод-вывод данных об угрозах для информации, которая обрабатывается в ОИ. Создание пользователем модели угроз, анализ вероятности их реализации и относительного уровня ущерба.

Операция R3 – ввод данных пользователем об угрозах для информации, которая обрабатывается в ОИ;

Операция Z2 – анализ вводимых данных программным обеспечением. В случае ввода некорректных данных, программа отказывается переходить на следующий этап работы и выводит пользователю на экран соответствующее сообщение;

Операция P2 – обработка программой данных введенных пользователем относительно угроз для информации, которая обрабатывается в ОИ, формирование модели угроз;

Операция P3 – анализ вероятности реализации выявленных угроз и относительного уровня ущерба в случае их реализации;

Операция R4 – вывод данных относительно сформированной модели угроз, анализа вероятности реализации выявленных угроз и относительного уровня ущерба в случае их реализации.

Третий модуль – ввод-вывод данных о нарушителях безопасности. Построение модели нарушителя и осуществление их классификации. Определение взаимосвязи класса нарушителей и возможного перечня рисков, которые могут быть ими реализованы.

Операция R5 – ввод данных пользователем об нарушителях безопасности;

Операция Z3 – анализ вводимых данных программным обеспечением. В случае ввода некорректных данных, программа отказывается переходить на следующий этап работы и выводит пользователю на экран соответствующее сообщение;

Операция P4 – обработка программой данных введенных пользователем относительно нарушителей безопасности, формирование модели нарушителя;

Операция P5 – определение взаимосвязи перечня угроз и класса нарушителей, которые могут их реализовать;

Операция R6 – вывод данных относительно сформированной модели нарушителей и перечня угроз, которые могут быть ими реализованы.

Четвертый модуль – ввод-вывод данных об отношении между ОИ и реализованными в нем средствами защиты, а также угрозами для объекта экспертизы, на основе данного взаимоотношения пользователем определяются функции защиты, которые должны быть реализованы КСЗИ, а также уровень услуг и функциональный профиль защищенности.

Операция R7 – ввод (выбор) данных пользователем о функциях защиты, которые реализованы в соответствии с реализованными средствами защиты, а также функции защиты, которые должны быть реализованы КСЗИ данного ОИ;

Операция Z4 – анализ вводимых данных программным обеспечением. В случае ввода некорректных данных, программа отказывается переходить на следующий этап работы и выводит пользователю на экран соответствующее сообщение;

Операция P6 – обработка программой данных введенных пользователем относительно функций защиты, которые реализованы в ОИ, а также тех функций защиты, что должны быть реализованы для обеспечения более полной защищенности ОИ;

Операция P7 – определение программой реального и необходимого уровня услуг и функционального профиля защищенности;

Операция P8 – определение программой соотношения между ОИ, угрозами для ОИ и функциями защиты которые уже реализованы и должны быть реализованы;

Операция R8 – вывод данных относительно соотношения между ОИ, угрозами для ОИ и функций защиты которые должны быть реализованы. Программа предоставляет сформированный функцио-

нальный профиль защищенности. Программа предоставляет сообщения, в случае если пользователь выбрал (или указал) не достаточное количество функций защиты для минимально необходимого уровня услуги.

Пятый модуль – ввод-вывод данных, в процессе которого пользователь должен определить дополнительные или лишние механизмы (средства) защиты ОИ от определенного ранее перечня угроз, на основе выделенных функций защиты, которые формируют определенные уровни услуг и функциональный профиль защищенности. Пользователь выбирает или вводит средства защиты, которые должны быть реализованы в ОИ, а также определяет, какие функции защиты они выполнят и от каких угроз защищают.

Операция R9 **–** ввод (или выбор) данных пользователем относительно необходимых механизмов (средств) защиты ОИ;

Операция Z5 **–** анализ вводимых данных программным обеспечением. В случае ввода некорректных данных, программа отказывается переходить на следующий этап работы и выводит пользователю на экран соответствующее сообщение;

Операция P9 – обработка программой данных введенных пользователем относительно необходимых механизмов (средств) защиты ОИ;

Операция P10 – определение программой соотношения между ОИ, угрозами для ОИ, функциями защиты которые должны быть реализованы и необходимыми механизмами (средствами) защиты ОИ;

Операция R10 – вывод данных относительно соотношения необходимых и реализованных механизмов (средств) защиты ОИ, а также соотношения между ОИ, угрозами для ОИ, функциями защиты, которые уже реализованы, а также должны быть реализованы указанными механизмами (средствами) защиты ОИ.

Шестой модуль – ввод-вывод данных, в котором пользователю предоставляется оценка уровня защищенности ОИ. Данная оценка выражается в предоставлении пользователю количественных и качественных показателей касающихся устраненных угроз и выявленных уязвимостей.

Операция R11 **–** выбор пользователем данных относительно количественных и качественных показателей уровня защищенности ОИ;

Операция P11 – определение программой выбранных пользователем параметров относительно количественных и качественных показателей уровня защищенности ОИ;

Операция R12 – вывод данных программой относительно выбранных пользователем параметров количественных и качественных показателей уровня защищенности ОИ. Предоставление пользователю количественных показателей (данных о количестве угроз, которые были устранены и их характеристика) и качественных показателей (данных об оценке вероятности возникновения этих угроз) касающихся устраненных угроз. Предоставление пользователю количественных показателей (данных о количестве обнаруженных уязвимостей и их характеристика) и качественных показателей (вероятность их реализации и уровень относительного ущерба в случае их реализации) уязвимостей данного ОИ. Предоставление пользователю информации об устраненных угрозах, выявленных уязвимостях и их характеристика.

Седьмой модуль – выбор процедуры позволяющей пользователю доработать проект.

Операция Z6 – выбор пользователем механизма отката программы на первоначальный этап работы, для доработки проекта по оценке уровня защищенности ОИ. Предоставление пользователю возможности заново провести ввод необходимой информации на первом и последующих этапах работы.

S2 – Конец алгоритма.

На рис. 2 показана структурно-функциональная схема автоматизированной поддержки проведения испытаний КСЗИ.

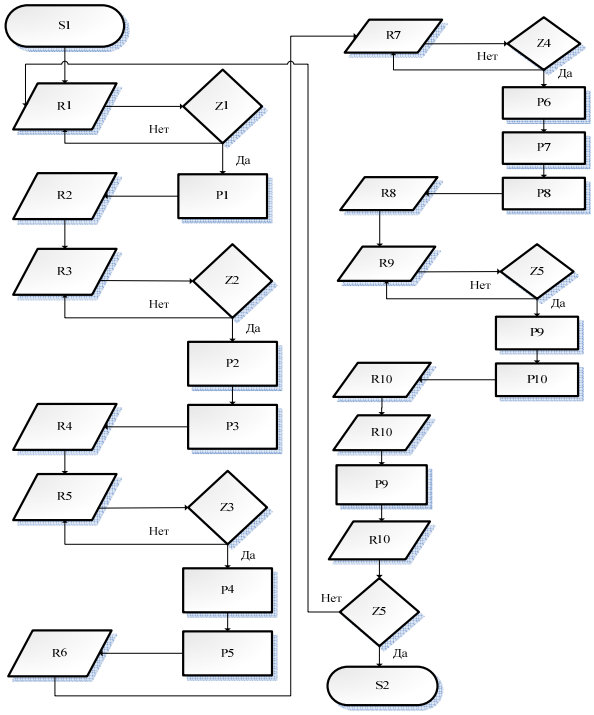

Рис. 2. Структурно-функциональная схема (модель) автоматизированной поддержки проведения испытаний КСЗИ

Описание требований к разрабатываемой программе по автоматизированной поддержке проведения испытаний КСЗИ

Цель создания программного обеспечения – предоставление пользователю (эксперту, разработчику КСЗИ) возможности автоматизированной поддержки при проведении испытаний КСЗИ.

Объектом автоматизации является процесс проведения испытаний КСЗИ.

Предназначение программного обеспечения. Программное обеспечение предназначено для автоматизированного решения определенных задач, реализуемых в ходе проведения испытаний КСЗИ и оценки уровня защищенности АС.

Характеристика объекта автоматизации. Реализация автоматизированной поддержки проведения испытаний КСЗИ подразумевает проектирование, разработку, внедрение в эксплуатацию и дальнейшее использование в работе специалиста, программного обеспечения, с помощью которого решается отдельная задача или группа задач выполняемых при проведении испытаний КСЗИ, что в дальнейшем позволяет сделать выводы о полноте и достаточности уровня защищенности автоматизированной системы.

Общие требования к программному обеспечению

Данное программное обеспечение должно выполнять следующие общие требования:

1) предоставлять пользователю интуитивно понятный и простой интерфейс взаимодействия с программой;

2) предоставлять пользователю возможность диалогового взаимодействия с программой;

3) в случае некорректного ввода данных предоставлять пользователю соответствующие предупреждения;

4) предоставлять пользователю вспомогательные сообщения для корректного ввода данных;

5) предоставлять нескольким пользователям возможность пользоваться данной программой, с возможностью сохранения своих проектов, в том числе не доработанных;

6) предоставлять пользователю возможность начать работу со своим проектом с того шага на котором он был завершен, без необходимости начинать его заново.

Функциональные требования к программному обеспечению для автоматизированной поддержки проведения испытаний КСЗИ

Этап ввода данных об автоматизированной системе.

Качество проводимого оценивания безопасности во многом зависит от полноты и точности информации, которая получена в процессе сбора исходных данных.

Данный этап должен предоставлять пользователю возможность ввести информацию, характеризующуюся ОИ в целом, его предназначение и основные задачи.

Пользователь должен иметь возможность:

1) выбора наиболее приоритетных свойств информации (конфиденциальность, целостность, доступность, наблюдаемость) для каждого из видов информации, которая циркулирует в ОИ;

2) ввести информацию, которая характеризует подсистемы ОИ, элементы подсистем ОИ входящие в их состав.

Последовательность операций входящих в состав алгоритма проведения испытаний должна включать ввод основных данных описывающих ОИ, а именно:

1) ввод данных характеризирующих основные функциональные модули и элементы ОИ;

2) ввод данных характеризирующих функциональные подсистемы и элементы комплекса средств защиты, реализованные в ОИ;

3) ввод данных характеризирующих объекты-пользователи, объекты-процессы, пассивные объекты и их атрибуты доступа [7].

Характеристика ОИ и реализованных средств защиты, должна рассматриваться на нескольких уровнях:

1) аппаратный;
2) BIOS;
3) операционная система;
4) сетевой;
5) СУБД;
6) прикладного программного обеспечения.

Пользователь должен иметь возможность:

1) на основе введенных данных об ОИ и его элементах построить архитектуру и представить ее в графическом виде;

2) добавить новый элемент в разработанную архитектуру ОИ, в случае если она была уже сформирована.

В результате, пользователь должен получить общее представление об ОИ и элементах, которые в него входят.

На основе вводимых данных должен осуществляется следующий этап анализа ОИ.

Этап ввода данных об обрабатываемой в автоматизированной системе информации

На данном этапе необходимо предоставлять пользователю возможность ввести характеристики информации, которая циркулирует в ОИ и той информации, которая требует защиты.

Также, пользователю необходимо указать все виды информации, которая циркулирует в ОИ (например, открытая, с ограниченным доступом).

Пользователь должен иметь возможность указать те подсистемы и их элементы, в которых требующая защиты информация циркулирует.

Этап ввода данных об угрозах для информации

Пользователь должен иметь возможность построения модели угроз для информации, которая циркулирует в ОИ.

После окончания этапа ввода информации об ОИ, его подсистемах и обрабатываемой информации, которая в данном ОИ циркулирует, пользователь должен перейти к следующему этапу ввода информации об угрозах.

Программное обеспечение должно предоставлять возможность для ОИ в целом и его отдельных элементов, учитывая циркулирующую в нем информацию, ввести возможные угрозы для его безопасности, которые касаются несанкционированных действий (доступа, копирования, модификации, подмены или удаления информации, блокирования доступа до информации, потери наблюдаемости за информацией).

Необходимо, также иметь возможность провести классификацию выявленных угроз по нескольким категориям (угрозы природного или техногенного происхождения, угрозы для секретной, конфиденциальной или открытой информации, угрозы для конфиденциальности, целостности, доступности, наблюдаемости информации, угрозы для элемента 1, элемента 2 и т.д.).

Информация должна быть представлена, как в текстовом, табличном так и графическом виде.

Необходимо предусмотреть возможность добавить новую угрозу в разработанную модель, в случае если модель была уже сформирована.

Данный этап должен предоставить пользователю возможность создать поле угроз (модель угроз) для информации и осуществить их классификацию по нескольким параметрам, а именно:

1) разделение угроз по видам;
2) разделение угроз по типам;
3) по результатам влияния на информацию;
4) по пути их реализации.

Модель угроз должна предоставлять возможность пользователю определить вероятность реализации угроз и относительный уровень ущерба при их реализации.

Этап ввода данных о нарушителях безопасности информации

На данном этапе необходимо предусмотреть для пользователя возможность:

1) построения модели нарушителя для информации, которая циркулирует в ОИ;
2) после окончания этапа ввода данных об угрозах для информации, перейти к следующему этапу построения модели нарушителя;
3) на основе построенной модели угроз для информации построить модель нарушителя;
4) на основе построенной модели угроз, для каждого вида угроз и отдельно взятой угрозы, определить потенциального нарушителя;
5) провести классификацию выявленных нарушителей по нескольким категориям (внешний или внутренний нарушитель, цель или мотив нарушителя);
6) провести классификацию выявленных нарушителей по уровню их возможностей, знаний, методам и способам нарушений, месту совершения действия.

Информация должна быть представлена, как в текстовом, табличном так и графическом виде.

Пользователь должен иметь возможность добавить нового нарушителя в разработанную модель, в случае если модель была уже сформирована.

Этап определения подсистем и элементов автоматизированной системы, угроз для них, а также путей и механизмов их защиты

Программное обеспечение должно предоставлять возможность:

1) на основе построенной архитектуры ОИ и построенной модели угроз, определить объекты и элементы, которые требуют защиты;
2) на следующем этапе работы с программным обеспечением, на основе построенной модели угроз и определенных подсистем и элементов ОИ, требующих защиты, выбрать из предложенного программой списка те функции защиты, которые отвечают выявленным угрозам и выделенным элементам ОИ;
3) на основе выбранных функций защиты, определить на следующем этапе работы с программным обеспечением те услуги защищенности, к которым они относятся;
4) на основе выбранных услуг защищенности, сформировать функциональный профиль защищенности;
5) сравнения необходимого и реализованного уровня защищенности (сравнение заданного и реализованного функционального профилей защиты);
6) на основе выбранных функций защиты и анализа архитектуры ОИ, выделенных подсистем и их элементов, выбрать те средства защиты, которые входят в состав ОИ и реализуют выделенные функции защиты.

Программа должна определять, какой подсистеме или элементу ОИ соответствует отдельное средство защиты, какую полноту защиты это средство обеспечивает, является ли оно достаточным для защиты данного объекта.

Этап классификации не устраненных угроз (уязвимостей системы)

В случае выявления пользователем отсутствия средств защиты, которые реализуют выбранные функции защиты, необходимо иметь возможность определить те угрозы, которые являются не устраненными.

После выявления пользователем не устраненных угроз (уязвимостей системы), он должен иметь возможность классифицировать данные угрозы, установить рейтинг опасности этих угроз для ОИ, используя определенные критерии, на пример: по вероятности реализации угроз и степени ущерба, который может быть нанесен их реализацией.

Этап вывода результатов испытаний и оценки защищенности автоматизированной системы

После проведенной классификации не устраненных угроз (уязвимостей системы), программа должна предоставить пользователю в текстовом, табличном или графическом виде:

1) результаты данной классификации, а также предоставить перечень событий и нарушителей, которые могут способствовать реализации данных угроз;

2) информацию о состоянии достаточности и полноты защищенности ОИ, перечень защищенных, частично защищенных и незащищенных подсистем и элементов ОИ;

3) результат оценки степени защищенности как ОИ в целом, так и отдельных его подсистем и элементов.

Необходимо предусмотреть возможность предоставления рекомендации по совершенствованию средств защиты ОИ. Такие рекомендации должны включать в себя следующие типы действий, направленных на минимизацию выявленных уязвимостей:

1) уменьшение риска за счёт использования дополнительных средств защиты, позволяющих снизить вероятность проведения атаки или уменьшить возможный ущерб от неё;

2) уклонение от риска путём изменения архитектуры или схемы информационных потоков ОИ, что позволяет исключить возможность проведения той или иной атаки;

3) принятие риска в том случае, если он уменьшен до того уровня, на котором он не представляет опасности для ОИ.

Результаты данной процедуры должны оформляться в виде отчётного документа, который предоставляется Заказчику. В общем случае этот документ состоит из следующих основных разделов:

1) описание границ, в рамках которых был проведён аудит безопасности;

2) описание структуры ОИ Заказчика;

3) описание выявленных уязвимостей и недостатков, включая уровень их риска;

4) рекомендации по совершенствованию КСЗИ;

5) предложения по плану реализации первоочередных мер, направленных на минимизацию выявленных рисков [8].

Этап доработки и сохранения проекта

В случае выявления новых угроз или уязвимостей, необходимости в повышении уровня защищенности ОИ, а также изменения его архитектуры, программа должна предоставлять возможность пользователю ввести новую информацию, которая касается необходимых изменений ОИ, и провести доработку по оценке уровня его защищенности, с сохранением всех необходимых параметров.

После проведения доработки классификации угроз, пользователь должен иметь возможность перейти к следующему этапу работы с программой и выбрать или указать новые средства защиты, которые должны входить в состав КСЗИ ОИ, определить новые функции защиты, которые они должны будут выполнять и пересмотреть уровень услуг к которым данные функции будут относиться.

После выбора услуг, которые должны быть реализованы в КСЗИ, пользователь должен иметь возможность составить новый профиль защищенности ОИ, в соответствии с новыми выбранными уровнями услуг.

После доработки КСЗИ, пользователь должен иметь возможность просмотреть результаты проведенных доработок.

Программа, должна предоставлять возможность:

1) сохранить результаты своей работы. Сохранение результатов проведенных испытаний, позволит проводить даль-

нейший анализ ОИ в случае изменения, каких либо из его характеристик;

2) сохранять результаты проведенных испытаний, даже если проект не был завершен до конца;

3) сохранять историю проводимых изменений ОИ, а также создавать архив из проектов, которые были реализованы полностью или частично.

Дальнейший анализ ОИ, в случае последующих изменения его архитектуры, изменения требований к защите информации, которая циркулирует в ОИ или других его характеристик.

Требования пользователей к программному обеспечению для автоматизированной поддержки проведения испытаний КСЗИ

При проектировании интерфейса должна учитываться проектируемая функциональность программного обеспечения.

Работа пользователя должна начинаться со стартовой страницы программы. На стартовой странице должны быть обеспечены средства изменения языка отображения информации.

На стартовой странице должна предоставляться справочная информация относительно предназначения программы, ее версии, названия, правила и последовательность работы пользователя с программой.

Интерфейс пользователя при проведении испытаний КСЗИ должен быть ориентирован на специалиста в вопросах защиты информации относительно вопроса информационного наполнения и на обычного пользователя в вопросах простоты использования.

Интерфейс программы должен иметь три основные компонента:

1) диалог;
2) ввод;
3) вывод.

Интерфейс пользователя должен обеспечивать пошаговое использование соответствующих процедур, с предоставлением оперативной справочной и аналитической информации пользователю о результатах проведенной работы.

Диалоговые решения определяют путь, которым пользователь направляет работу программы, выполняя введение данных. Диалог должен быть разработан для поддержки пользователя в его основной работе, без отвлечения его внимания дополнительной работой, обусловленной спецификой программы. Разработка диалогового меню должна использоваться при разработке структуры меню.

При разработке введения информации определяются способы введения информации (цифровая клавиатура, функциональные ключи и т.д.). ISO 9241–14 содержит рекомендации относительно использования средств ввода информации, а также относительно способов и требований к предоставлению информации пользователю.

Вывод информации должен обеспечивать однозначное восприятие информации.

При разработке интерфейса пользователя необходимо учитывать семь принципов построения диалога, которые имеют принципиальное значение для проектирования и оценивания диалога пользователя с программой, а именно:

1) соответствие заданию;
2) информативность;
3) управляемость;
4) соответствие ожиданиям пользователя;
5) не чувствительность к ошибкам;
6) способность к индивидуализации;
7) способность к обучению.

Принципы диалога необходимо применять, учитывая такие характеристики пользователя как:

1) объем внимания пользователя;
2) границы краткосрочной памяти;
3) обучаемость пользователя;
4) квалификация и опыт пользователя;
5) имеющиеся убеждения пользователя относительно основной структуры и предназначения системы, с которой он будет взаимодействовать.

Выполнение задания обеспечивается особенностями системного диалога [9].

Требования к защите данных циркулирующих в программном обеспечении для автоматизированной поддержки проведения испытаний КСЗИ

Вход в программу должен обеспечиваться по логину пользователя и его специальному паролю.

Программное обеспечение должно предусматривать защиту данных от несанкционированного доступа на уровне разграничения различных прав доступа.

Все операции, проводимые в программе пользователем должны "привязываться" к его профилю доступа.

В программе должен быть предусмотрен механизм обработки незавершенных транзакций.

В программном обеспечении должна быть реализована процедура резервного копирования и восстановления содержимого баз данных.

Ошибки в работе программы или аварийное завершение работы программного обеспечения, не должны вызывать потерю, частичное или полное разрушение базы данных системы.

В программе должно быть предусмотрена журнализация всех операций, а также функций, перечень которых будет определен в дальнейшем.

Выводы

Испытания являются одним из ключевых этапов при создании КСЗИ, который осуществляется для получения полной информации о текущем состоянии защищённости АС и для выявления уязвимостей информационной безопасности. Кроме того, результаты испытаний КСЗИ являются основой для формирования стратегии развития защищенности автоматизированной системы (ОИ) и обеспечения информационной безопасности организации.

Однако, необходимо отметить, что оценка уровня защищенности не является однократной процедурой и должна проводиться на регулярной основе. Только в этом случае работа будет приносить реальную отдачу и способствовать повышению уровня информационной безопасности. В связи с этим использование специализированного программного обеспечения для проведения испытаний КСЗИ более чем актуально.

В данной статье проведен анализ этапов создания КСЗИ, описана технология проведения испытаний КСЗИ, описан поход к разработке программного средства поддержки, выделены задачи, которые могут быть реализованы с использованием автоматизированного средства поддержки. Также, рассматривается возможная методология автоматизированного проведения испытаний и краткая характеристика функциональных модулей входящих в предложенный алгоритм работы программы. Также, рассматриваются основные требования к программе, которые должны учитываться при ее разработке.

Анализ методологии функционирования программного средства поддержки проведения испытаний КСЗИ, а также анализ требований к его реализации, являются необходимым условием на начальном этапе создания.

В дальнейшем планируется провести более детальный анализ методологии оценивания защищенности ОИ, а также провести разработку математического алгоритма и проектирование модели программного обеспечения для автоматизированной поддержки проведения испытаний КСЗИ.

1. *www*.atmnis.com/files/user_files/kszi.pdf
2. *Замятин Д., Прокофьев М.* Алгоритмические особенности экспертных систем, ориентированных на проблемы защиты информации // Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине. – Киев: НТУ Украины “КПИ”. – 2000. – Вып. 1. – С. 252–253.
3. *http*://software-testing.ru/library/testing/security/87
4. *www*.info-system.ru/security/Analysis_security_cis.doc
5. *http:*//www.jurnal.org/articles/2008/inf33.html

6. *Барсуковский Ю.* Аудит систем информационной безопасности – проблемы и решения // Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине. – Киев: НТУ Украины “КПИ”. – 2002. – Вып. 4. – С. 29–33.
7. *Методичні* вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. – НД ТЗІ 2.7 -009-09, ДС СЗЗІ України Київ, 2009.
8. *Домарев В.В.* Безопасность информационных технологий. Системный подход. – Киев: ООО ”ТИД “ДС”, 2004. – 992 с.
9. *http:*//i-novice.net/sostavlyaem-trebovaniya-k-po/

Получено 30.04.2012

Об авторе:

Колтик Максим Анатолиевич,
аспирант.

Место работы автора:

Институт программных систем
НАН Украины,
03187, Киев-187,
Проспект Академика Глушкова, 40.
Тел.: 067 218 2809
E-mail: maxfaktor@ua.fm