УДК 004.056:061.68

Е.Н. Боровская, М.А. Колтик

ХАРАКТЕРИСТИКА ИНФОРМАЦИОННЫХ ПОТОКОВ ПРОГРАММНЫХ МОДУЛЕЙ ВХОДЯЩИХ В СОСТАВ ПРОГРАММНОГО СРЕДСТВА ДЛЯ АВТОМАТИЗИРОВАННОЙ ПОДДЕРЖКИ ПРОВЕДЕНИЯ ИСПЫТАНИЙ КСЗИ

В данной работе описывается информация, которая циркулирует в структурно-функциональных модулях программного обеспечения. Выделяются виды информационных потоков, а также, проанализированы уровни информационного взаимодействия для модулей программного обеспечения, автоматизированной поддержки проведения испытаний КСЗИ.

Введение

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 комплексной системы защиты информации (КСЗИ).

При создании КСЗИ для различных автоматизированных систем (АС), важной задачей для организаций, которые специализируются на данном виде деятельности, наряду с временными и количественными показателями, является обеспечение качества выполняемых работ на различных этапах её создания.

Можно выделить следующие основные этапы создания КСЗИ:

1) обследования информационной инфраструктуры АС;

2) разработки моделей угроз информации и нарушителей безопасности информации;

3) формирования требований к КСЗИ;

4) проектирования КСЗИ, разработка документации;

5) настройка информационной инфраструктуры в соответствии с проектом КСЗИ;

6) испытания КСЗИ (предварительные испытания и государственная экспертиза).

Одним из методов, который способствует решению задач связанных с улучшением качества выполняемых работ при создании КСЗИ, сокращением времени на реализацию проекта, уменьшением рутинных операций для специалиста, является автоматизация работ, выполняемых на этапах путём использования специально разработанного программного обеспечения.

После проведенного анализа этапов создания КСЗИ следует отметить, что одним из наиболее перспективных в плане автоматизации является этап проведения испытаний, так как на этом этапе анализируется большой объём информации по результатам предыдущих этапов и проводится большое количество рутинных операций.

Автоматизация данного этапа позволит повысить производительность труда, снизить трудозатраты, частично или полностью снять функции оперативного управления процессом с работника, улучшить контроль и диагностику процесса проведения испытаний КСЗИ, повысить управляемость как проведением испытаний КСЗИ, так и всем технологическим процессом ее создания.

В работе [1] рассмотрен технологический процесс проведения испытаний КСЗИ, методика функционирования программного обеспечения для автоматизиро-

ванной поддержки проведения испытаний КСЗИ.

Цель данной работы – анализ информационных потоков и их взаимодействия для функциональных модулей программного средства автоматизированной поддержки проведения испытаний КСЗИ.

Задачи: провести анализ информации, циркулирующей в структурно-функциональных модулях программного обеспечения, описать уровни основных потоков информации и методику информационного взаимодействия для модулей программного обеспечения автоматизированной поддержки проведения испытаний КСЗИ.

Общая характеристика информационных потоков программного средства для автоматизированной поддержки проведения испытаний КСЗИ

Информацию, которая циркулирует в программном средстве для автоматизированной поддержки проведения испытаний КСЗИ, можно разделить на шесть уровней:

1) характеристика объекта испытаний;
2) характеристика модели угроз;
3) характеристика модели нарушителя;
4) характеристика модели безопасности;
5) характеристика модели механизмов защиты;
6) Предоставление результатов относительно оценки уровня защищенности объекта испытаний.

На первом уровне проводится ввод пользователем информации о подсистемах и уровнях объекта испытаний (ОИ) (аппаратный, программный, сетевой), элементах объекта испытаний (объектах, процессах, каналах связи), информации, которая в них обрабатывается. После чего проводится анализ введенной информации и вывод (предоставление) пользователю структурированных данных об архитектуре объекта испытаний, выделенных объектах защиты, определяется класс информации в соответствии с НДТЗИ 2.5 – 005-99, циркулирующей в объекте испытаний.

На втором уровне проводится ввод пользователем информации об угрозах для информации, которая циркулирующей в ОИ. Пользователю предоставляется возможность осуществить классификацию угроз по нескольким параметрам, после чего проводится анализ введенной информации и создается поле угроз (модель угроз) для ОИ. Модель угроз формируется на основе вводимой пользователем информации об угрозах и ранее обработанной информации об ОИ. Модель угроз должна предоставлять возможность пользователю определить вероятность реализации угроз, относительный уровень ущерба при их реализации, определить необходимость их нейтрализации.

На третьем уровне проводится ввод пользователем информации о нарушителях безопасности. Пользователю предоставляется возможность осуществить классификацию нарушителей по нескольким параметрам, после чего проводится анализ введенной информации и создается модель нарушителя. Модель нарушителя должна быть разработана при взаимодействии с моделью угроз и пользователь должен иметь возможность определить, какую из угроз может реализовать отдельный вид нарушителя.

На четвертом уровне проводится ввод пользователем информации об основных мерах по защите информации, о функциях защиты, которые должны быть реализованы, услугах и их уровнях в соответствии с НДТЗИ 2.5 – 005-99, после чего проводится анализ введенной информации и создается функциональный профиль защищенности объекта испытаний. Функциональный профиль защищенности формируется на основе вводимой пользователем информации о необходимых для реализации функциях защиты, уровнях услуг, а также ранее обработанной информации об основных мерах по защите информации и угрозах для ОИ.

На пятом уровне проводится ввод пользователем информации о механизмах защиты, которые необходимы для защиты

информации в ОИ. Пользователю предоставляется возможность проанализировать и оценить целесообразность их применения, с помощью коэффициента важности. После ввода необходимых данных проводится анализ введенной информации и вывод (предоставление) пользователю структурированных данных о модели механизмов защиты информации в объекте испытаний. Модель механизмов защиты информации ОИ формируется на основе вводимой пользователем информации об необходимых механизмах защиты, а также, в соответствии с формированной моделью угроз и моделью безопасности. Пользователь должен иметь возможность ввести или выбрать средства защиты и определить, какие функции защиты они выполняют и от каких угроз защищают.

На шестом уровне проводится выбор пользователем необходимых параметров для получения структурированной информации об уровне защищенности объекта испытаний. Пользователю предоставляются количественные показатели (данные о количестве угроз, которые были устранены и их характеристика) и качественных показателей (данных об оценке вероятности осуществления 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 и качественных показателях угроз, определение вероятности осуществления той или иной угрозы, определения уровня убытков при осуществлении угроз, определение уровня риска информационной безопасности и определение наличия уязвимостей в системе защиты ОИ.

На рисунке показана общая схема информационных потоков для программных модулей входящих в состав программного средства для автоматизированной поддержки проведения испытаний КСЗИ.

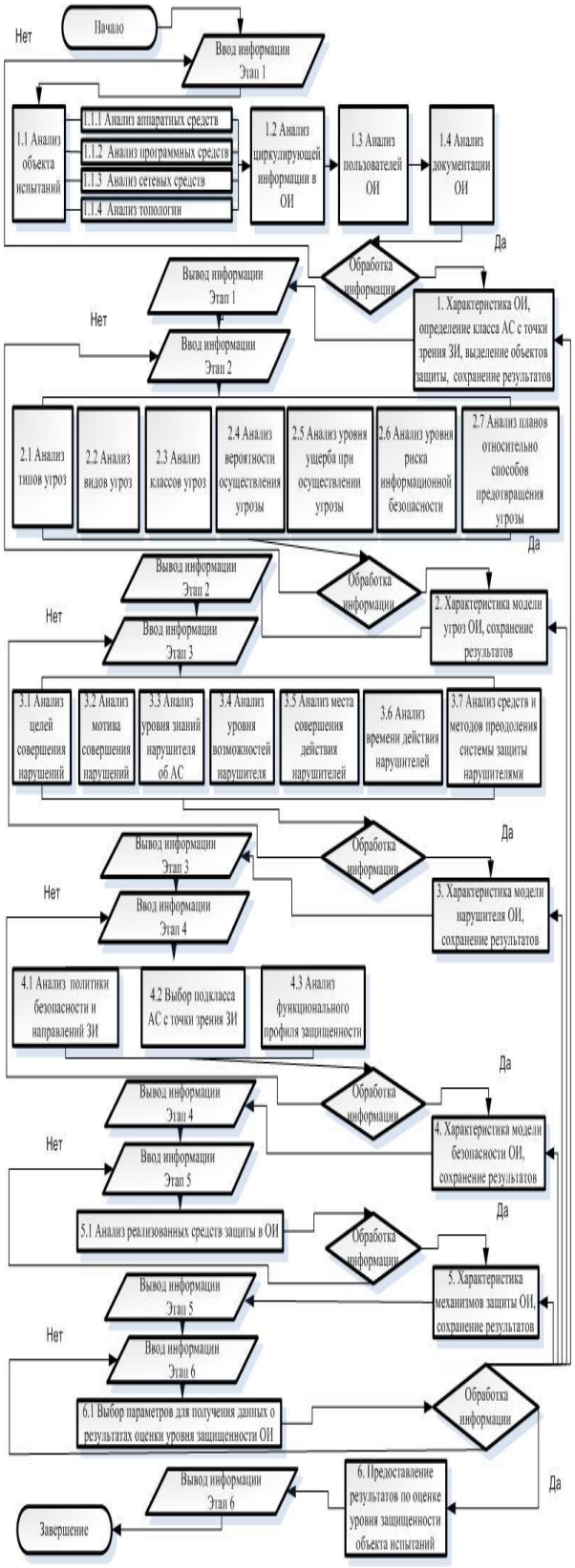

Рисунок. Общая схема информационных потоков для программных модулей входящих в состав программного средства для автоматизированной поддержки проведения испытаний КСЗИ

Характеристика информационных потоков программного модуля – характеристика объекта испытаний

Процесс взаимодействия с данным программным средством на первом этапе подразумевает ввод информации об объекте испытаний (автоматизированной системе). После чего, программа обрабатывает полученную информацию и на выход (на дисплей рабочей станции пользователя) предоставляет данные об архитектуре и конфигурации объекта испытаний, с указанием элементов, где циркулирует критическая информация и выделением объектов защиты.

Выделяются следующие виды информации, которая вводится на данном этапе:

1) характеристика объекта испытаний;

2) характеристика циркулирующей информации;

3) характеристика пользователей;

4) характеристика документации.

Для **объекта испытаний** определены следующие уровни информации, характеризующие:

1.1) **аппаратные средства,** входящие в его состав;

1.2) **программные средства** (общесистемные, прикладные) входящие в его состав;

1.3) **сетевые средства,** входящие в его состав;

1.4) **топологию** объекта испытаний.

В свою очередь, каждый из информационных уровней объекта испытаний делится на соответствующие категории информации.

Уровень информации, характеризующий **аппаратные средства**, входящие в состав объекта испытаний включает следующие категории:

1.1.1) количество и типы аппаратного оборудования (в том числе периферийное оборудование, средства печати, и хранения информации);

1.1.2) типы процессоров используемых в системе;

1.1.3) описание функций BIOS.

Уровень информации, характеризующий **программные средства**, входящие в состав объекта испытаний включает следующие категории:

1.2.1) описание общесистемного программного обеспечения и основных его функций (ОС серверов, универсальных высокопродуктивных ЭВМ, рабочих станций, обеспечивающие выполнение сетевых функций, СКБД и т.д.);

1.2.2) описание прикладного программного обеспечения и основных его функций.

Уровень информации, характеризующий **сетевые средства**, входящие в состав объекта испытаний включает следующие категории:

1.3.1) аппаратное коммутационное оборудование (коммутаторы, маршрутизаторы и т.д.);

1.3.2) типы используемых кабельных систем (кабель, беспроводная связь);

1.3.3) программное обеспечение коммутационного оборудования.

Уровень информации характеризующей **топологию объекта испытаний** и описывающий расположение и соединение сетевых устройств, включает следующие категории:

1.4.1) карта локальной (или распределенной) вычислительной сети АС, включающей схему распределения серверов и рабочих станций по сегментам сети;

1.4.2) информация о направлении информационных потоков передаваемых по сети автоматизированной системы;

1.4.3) информация о типах каналов связи используемых в автоматизированной системе;

1.4.4) информация об используемых в автоматизированной системе сетевых протоколах.

Для описания информации, **которая циркулирует** в объекте испытаний, выделяются такие уровни вводимых данных:

2.1) степень ограничения доступа информации, циркулирующей в объекте

испытаний (открытая информация, информация с ограниченным доступом: конфиденциальная, секретная: особой важности, совершенно секретная, секретная);

2.2) описание критической информации, которая подлежит защите;

2.3) описание модулей и элементов объекта испытаний, в которых циркулирует критическая информация;

2.4) описание технологии обработки и передачи информации (интернет технологии, описание протоколов взаимодействия, которые используют в сети и т.д.).

Характеристика **пользователей (персонала)** определяется такими уровнями информации:

3.1) функциональные обязанности пользователя;

3.2) уровень квалификации пользователя;

3.3) полномочия пользователя по доступу к информационным ресурсам АС;

3.4) полномочия пользователя по доступу к программным и аппаратным компонентам АС;

3.5) полномочия пользователя по доступу к физической среде АС;

3.6) полномочия пользователя по управлению КСЗИ АС;

3.7) степень доступа пользователя к конфиденциальной информации.

Для **документации** можно выделить следующие уровни, которые её характеризируют:

4.1) нормативно-методическая и организационная документация;

4.2) проектная документация;

4.3) эксплуатационная документация.

Характеристика информационных потоков программного модуля – модель угроз информации

После ввода параметров, характеризующих объект испытаний, и их успешной обработки функциональным программным модулем «**Характеристика объекта испытаний**», осуществляется переход к модулю «**Модель угроз информации»**.

Угроза информации – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности, целостности и наблюдаемости информации, которая циркулирует в АС.

Модель угроз для информации – это абстрактное формализованное или неформализованное описание методов и средств реализации угроз для информации в конкретных условиях функционирования АС [2, 3].

Модель угроз для информации – описание способов и средств осуществления существенных угроз для информационных ресурсов с указанием уровней предельно допустимых потерь, связанных с их возможными проявлениями в конкретных или тех условиях применения, которые предусмотрены АС [4].

Необходимо выделить следующие виды информации, которая вводится (или выбирается) на этапе формирования модели угроз:

1) тип угрозы;

2) вид угрозы;

3) классы угроз (в соответствии с влиянием реализации угрозы на информацию и систему ее обработки);

4) вероятность осуществления угрозы;

5) определение уровня ущерба при осуществлении угрозы;

6) определения уровня риска информационной безопасности;

7) планы относительно осуществления способов предотвращения угрозы.

Угрозы для информации, которая обрабатывается в АС, зависят от характеристик вычислительной системы, физической среды, среды пользователей, технологий обработки информации и других факторов. Они могут иметь объективную (природные угрозы) или субъективную (техногенные угрозы) природу. Угрозы, которые имеют субъективную природу,

делятся на случайные (неумышленные) и преднамеренные, а преднамеренные угрозы по месту размещения источника угроз относительно подсистем подразделяются на дистанционные и контактные [5].

Исходя из этого, все угрозы можно отнести к четырем следующим **типам**:

1) угрозы природного происхождения;

2) случайные угрозы техногенного происхождения;

3) преднамеренные угрозы техногенного происхождения дистанционного действия;

4) преднамеренные угрозы техногенного происхождения контактного действия.

Эта классификация легла в основу модели угроз в соответствии с НД ТЗИ 1.1-002-99, НД ТЗИ 1.4-001-2000 и НД ТЗИ 1.6-003-04.

При анализе угроз информации выделены следующие их **виды**:

1) **угрозы природного происхождения со стороны физической среды** (стихийные бедствия (землетрясение, наводнение, пожар) или другие случайные события, связанные с изменением условий физической среды, которые могут привести к большим разрушительным последствиям);

2) **случайные техногенные угрозы со стороны физической среды** (аварии или другие случайные события, связанные с изменением условий физической среды, которые могут привести к большим разрушительным последствиям);

3) **случайные техногенные угрозы со стороны вычислительной системы** (сбои и отказы, которые имеют наиболее серьезные последствия);

4) **случайные техногенные угрозы со стороны среды пользователей при разработке подсистем** (ошибки при проектировании и разработке компонентов подсистемы (технических средств, технологии обработки информации, программных средств, средств защиты, структур данных и т.п.), т. е., угрозы, направленные на нарушение конфиденциальности, целостности, доступности информации, а также нарушение наблюдаемости и управляемости системы);

5) **случайные техногенные угрозы со стороны среды пользователей** при эксплуатации подсистем (ошибки персонала (пользователей) системы при эксплуатации, классифицируются как случайные угрозы субъективной природы);

6) **умышленные техногенные дистанционные угрозы со стороны среды пользователей** (умышленные угрозы, т.е. попытки потенциальных внешних нарушителей);

7) **умышленные техногенные контактные угрозы со стороны среды пользователей** (умышленные угрозы, т.е. попытки потенциальных внутренних нарушителей).

По результатам воздействия на информацию и систему ее обработки угрозы делятся на четыре **класса** [6, 7]:

1) **нарушение конфиденциальности информации** (получение информации пользователями или процессами вопреки установленным правилам доступа);

2) **нарушение целостности информации** (полное или частичное уничтожение, искажение, модификация, навязывание ложной информации);

3) **нарушение доступности информации** (частичная или полная утрата трудоспособности, блокирование доступа к информации);

4) **потеря наблюдаемости или управляемости** системой обработки (нарушение процедур идентификации и аутентификации пользователей и процессов, предоставления им полномочий, осуществления контроля за их деятельностью, отказ от получения или пересылки сообщений).

Для анализа угроз информации выделена следующая качественная шкала для определения вероятности осуществления угрозы (табл. 1).

Таблица 1. Качественная шкала определения вероятности осуществления угрозы

№	Вероятность осуществления угрозы	Описание
1	Очень низкая	Угроза практически никогда не будет реализована. Уровень соответствует числовому интервалу вероятности [0, 0.25]
2	Низкая	Вероятность осуществления угрозы достаточно низкая. Уровень соответствует числовому интервалу вероятности [0.25, 0.5]
3	Средняя	Вероятность реализации угрозы приблизительно равна 0,5
4	Высокая	Угроза, скорее всего, будет реализована. Уровень соответствует числовому интервалу вероятности [0.5, 0.75]
5	Очень высокая	Угроза почти наверняка будет реализована. Уровень соответствует числовому интервалу вероятности [0.75, 1]

При анализе угроз информации выделяется следующая качественная шкала для определения уровня убытков при осуществлении угроз (табл. 2)

Таблица 2. Качественная шкала определения уровня убытков при осуществлении угроз

№	Уровень ущерба	Описание
1	Малый ущерб	Осуществление угрозы приводит к незначительным потерям материальных активов, которые быстро восстанавливаются, или к незначительному влиянию на репутацию компании
2	Умеренный ущерб	Осуществление угрозы вызывает заметные потери материальных активов или к умеренному влиянию на репутацию компании
3	Ущерб средней тяжести	Осуществление угрозы приводит к существенным потерям материальных активов или значительному урону репутации компании
4	Большой ущерб	Осуществление угрозы вызывает большие потери материальных активов и наносит большой урон репутации компании
5	Критический ущерб	Осуществление угрозы приводит к критическим потерям материальных активов или к полной потере репутации компании на рынке, что делает невозможным дальнейшую деятельность организации

После анализа вероятности осуществления угроз и определения возможного уровня убытков в случае их реализации, необходимо определить уровни рис-

ков информационной безопасности. Для этого используется «Таблица определения уровня рисков информационной безопасности».

При построении модели угроз в табл. 3 определяются следующие риски:

Таблица 3. Таблица определения уровня риска информационной безопасности

Вероятность осуществления угрозы / Уровень ущерба	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Малый ущерб	Низкий риск	Низкий риск	Низкий риск	Средний риск	Средний риск
Умеренный ущерб	Низкий риск	Низкий риск	Средний риск	Средний риск	Высокий риск
Ущерб средней тяжести	Низкий риск	Средний риск	Средний риск	Средний риск	Высокий риск
Большой ущерб	Средний риск	Средний риск	Средний риск	Средний риск	Высокий риск
Критический ущерб	Средний риск	Высокий риск	Высокий риск	Высокий риск	Высокий риск

В данной таблице, в первом столбце задаются понятийные уровни ущерба, а в первой строке – вероятность осуществления угрозы. Ячейки же таблицы, расположенные на пересечении первой строки и столбца, содержат уровень риска безопасности. Размерность таблицы зависит от количества концептуальных уровней вероятности осуществления угрозы и уровня ущерба [8].

Каждая из выявленных угроз оценивается по данной таблице и определяется степень рисков, которые она несет в случае ее реализации. В соответствии с этим выстраиваются планы и приоритеты по предотвращению угроз, которые несут высокие риски для информационной безопасности объекта испытаний.

При анализе угроз информации выделяется следующая качественная шкала для определения планов СЗИ относительно применения предупредительных мер против выявленных угроз или о не применении таких мер, поскольку в них нет необходимости (табл. 4).

Таблица 4. Качественная шкала для определения планов СЗИ относительно применения предупредительных мер против выявленных угроз

№	Приоритет предотвращения угрозы	Описание
1	Обязательно	Риски, которые несет угроза высокие. Необходимо обязательно предотвратить возможность их реализации
2	Желательно	Риски, которые несет угроза среднего уровня. Рекомендуется предотвратить возможность их реализации
3	Не обязательно	Риски, которые несет угроза низкие. Предотвращать возможность их реализации не обязательно

Характеристика информационных потоков программного модуля – модель нарушителей безопасности информации

Нарушитель – это лицо, осуществляющее несанкционированный доступ к информации, которое ошибочно (вследствие неосведомленности или неосторожности) или целенаправленно (по злому умыслу, или без него), используя различные возможности, методы и средства осуществило попытку выполнить операции, которые привели или могут привести к нарушению свойств информации, опреде-

ленных политикой безопасности [9]. Относительно АС нарушители подразделяются на внутренних нарушителей и внешних.

Внешний нарушитель – это нарушитель, который действует с внешней, относительно АС, стороны. К ним могут относиться посторонние лица или клиенты, пользующиеся системой, а также любые лица, которые находятся за пределами помещения и здания, где находится АС.

Внутренний нарушитель – это нарушитель, действующий с середины АС. Он рассматривается как лицо, имеющее доступ к помещениям, в которых расположены средства вычислительной техники АС. Внутренний нарушитель имеет возможность реализовать угрозу информации и может быть как авторизированным пользователем, так и не авторизированным. К ним могут относиться лица из числа персонала или пользователей системы.

Модель нарушителя – это абстрактный формализованное или неформализованное описание действий нарушителя, который отражает его практические и теоретические возможности, априорные знания, время, место, действия и др. [9]. Модель нарушителя отражает практические и теоретические возможности нарушителя, априорные знания, характер его возможных действий, время и место действия. Для достижения своих целей нарушитель должен приложить определенные усилия и затратить определенные ресурсы.

Модель нарушителя определяет:

1) предположения о категориях лиц, к которым может принадлежать нарушитель;

2) предположения о мотивах действия нарушителя и их градации по степени опасности для АС;

3) предположения о квалификации нарушителя и его технической обеспеченности;

4) ограничения и предположения о характере возможных действий нарушителя.

Кроме того, нарушители классифицируются по следующим характеристикам, а именно:

1) цели совершения нарушений;

2) мотив совершения нарушений;

3) уровень знаний нарушителя о системе;

4) уровень возможностей, предоставляемых нарушителю средствами АС;

5) место совершения действия (атаки);

6) время действия;

7) средства и методы преодоления системы защиты, которые может использовать нарушитель.

1. Целью совершения нарушений (умышленных действий внешних и внутренних нарушителей) могут быть:

(Ц1) получение необходимой информации в нужном объеме и составе;

(Ц2) получение возможности вносить изменения в информацию в соответствии со своими намерениями (интересами, планами);

(Ц3) причинение убытков собственнику и пользователям АС путем уничтожения (повреждения) материальных и информационных ценностей.

2. По мотивам совершения нарушений, нарушитель классифицируется согласно следующим категориям:

(М1) ошибочность действий;

(М2) безответственность;

(М3) самоутверждение;

(М4) корыстный интерес;

(М5) профессиональный долг.

3. По уровню знаний нарушителя о системе:

(Z1) владеют информацией о функциональных особенностях технических и программных средств компонентов АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеют пользоваться штатными средствами;

(Z2) обладают высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;

(Z3) обладают высоким уровнем знаний в области вычислительной техники

и программирования, проектирования и эксплуатации АС;

(Z4) обладают информацией о функциях и механизмах действия средств защиты АС.

4. По уровню возможностей, предоставляемых средствами АС, нарушитель характеризуется следующими иерархическими уровнями (каждый следующий уровень содержит функциональные возможности предыдущего):

(В1) первый уровень определяет самый низкий уровень возможностей ведения диалога с рабочими станциями, серверами, активным сетевым оборудованием АС – возможность запуска фиксированного набора задач (программ), которые реализуют заранее предусмотрены функции обработки информации;

(В2) второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями обработки информации;

(В3) третий уровень определяется возможностью управления функционированием компонентов АС, т. е. влиянием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования (возможно создание или использование специальных технических средств);

(В4) четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию, сопровождение программно-аппаратного обеспечения компонентов АС, которые могут включать в состав АС собственные средства с новыми функциями обработки информации.

5. По месту совершения действия:

(МД1) без получения доступа на контролируемую территорию АС;

(МД2) с получением доступа на контролируемую территорию, но без доступа к техническим средствам АС;

(МД3) с получением доступа к техническим средствам пользователей АС;

(МД4) с получением доступа к местам хранения данных (носителей, архивов и т. п.);

(МД5) с получением доступа к средствам администрирования АС и средствам управления КСЗ.

6. По времени действия нарушитель классифицируется согласно следующим категориям:

(ВД1) во время перерывов в работе компонентов системы (в нерабочее время, во время плановых перерывов в работе, перерывов для обслуживания и ремонта и т.п.);

(ВД2) во время функционирования АС (или компонентов системы);

(ВД3) при создании системы;

7. По методам и способам нарушений, которые могут использоваться:

(СН1) используются агентурные методы получения сведений;

(СН2) используются пассивные технические средства перехвата информации;

(СН3) используются штатные средства компонентов АС или недостатки проектирования КСЗИ для реализации попыток НСД;

(СН4) используются способы и средства активного воздействия на технические и программные средства компонентов АС, изменяющие конфигурацию системы (несанкционированное подключения дополнительных или модификация штатных технических средств, внедрение и использование специального программного обеспечения).

Характеристика информационных потоков программного модуля – модель безопасности объекта испытаний

Необходимо выделить следующие уровни информации, которая циркулирует в данном модуле функционирования ПО:

1) анализ политики безопасности и основных направлений защиты информации;

2) характеристики подкласса автоматизированной системы;

3) функциональный профиль защищенности.

Под политикой безопасности информации следует понимать совокупность законов, правил, ограничений, рекомендаций, инструкций и т.п., регламентирующих порядок обработки информации и направленные на защиту информации от возможных угроз.

Выделяют следующие основные направления, по которым обеспечивается защита информации:

1) нормативно-правовые меры защиты информации;

2) организационные меры защиты информации;

3) технические средства защиты информации.

Анализ и определение основных мер по защите информации объекта испытаний проводится на основе проведенного анализа угроз информации. В соответствии с моделью угроз информации пользователь выбирает наиболее целесообразные меры защиты от данных угроз.

В дальнейшем определение мер по защите информации объекта испытаний учитывается при выборе стандартного или построении не стандартного функционального профиля защищенности.

Информация, характеризующая **подкласс АС,** определяется в соответствии с [10]:

1) АС в которой повышенные требования к обеспечению конфиденциальности обрабатываемой информации;

2) АС в которой повышенные требования к обеспечению целостности обрабатываемой информации;

3) АС в которой повышенные требования к обеспечению доступности обрабатываемой информации;

4) АС в которой повышенные требования к обеспечению конфиденциальности и целостности обрабатываемой информации;

5) АС в которой повышенные требования к обеспечению конфиденциальности и доступности обрабатываемой информации;

6) АС в которой повышенные требования к обеспечению целостности и доступности обрабатываемой информации;

7) АС в которой повышенные требования к обеспечению конфиденциальности, целостности и доступности обрабатываемой информации;

Далее необходимо выбрать, какой профиль защищенности, должен быть реализован системой защиты информации – стандартный или не стандартный.

Если был выбран **стандартный функциональный профиль защищенности**, то необходимо из предложенного списка стандартных функциональный профилей защищенности, в соответствии с НД ТЗИ 2.5-005-99 выбрать необходимый. Представленные стандартные профили отвечают тем видам компьютерных систем потребность, в которых является наиболее актуальной.

Выбор стандартного функционального профиля защищенности должен проводиться на основе определенных ранее основных мер по защите информации объекта испытаний.

Всего определено 90 стандартных профилей, которые являются иерархичными, в том смысле, что их реализация обеспечивает повышение уровня защищенности от угроз соответствующего типа.

При выборе стандартного профиля должно быть реализовано предоставление справочной информации относительно подробного описания и характеристики тех функций, которые в него входят.

Также должна быть реализовано предоставление справочной информации относительно возможности и целесообразности выбора того или иного стандартного функционального профиля защищенности.

Если был выбран **не стандартный функциональный профиль защищенности**, необходимо провести его построение.

Для этого в соответствии с НД ТЗИ 2.5-004-99 нужно последовательно выбрать:

1) функциональные критерии защищенности;

2) виды услуг защищенности и их уровни;

3) набор функций защищенности.

Способность АС обеспечивать определенный уровень защищенности обрабатываемой информации определяется функциональными критериями, разбитыми на четыре группы:

1) конфиденциальность;
2) целостность;
3) доступность;
4) наблюдаемость.

Каждая из групп критериев описывает услуги, которые обеспечивают защиту в соответствии с угрозами одной из четырех основных групп. Так, в соответствии с НД ТЗИ 2.5-004-99 для каждого вида критериев определено конкретное количество услуг:

1) конфиденциальности – 5 (КД, КА, КО, КК, КВ);

2) целостности – 4 (ЦД, ЦА, ЦО, ЦВ);

3) доступности – 4 (ДР, ДС, ДЗ, ДВ);

4) наблюдаемости – 9 (НР, НК, НЦ, НТ, НА, НИ, НО, НВ, НП).

Каждая из вышеперечисленных услуг может включать несколько уровней. Чем выше уровень услуги, тем более полную она обеспечивает защиту, от определенного вида угроз. Уровни услуг имеют иерархическую структуру в соответствии с полнотой защиты, хотя не обязательно являют собой точные составляющие друг – друга.

Они начинаются с первого и повышаются до значения n., где n – уникально для каждого вида услуг. Если, для примера, взять такие виды услуг как, доверительная конфиденциальность – КД, то ее ранжирование по уровням выглядит таким образом:

- минимальная доверительная конфиденциальность;
- базовая доверительная конфиденциальность;
- полная доверительная конфиденциальность;
- абсолютная доверительная конфиденциальность.

Таким образом, n = 4, при этом, все последующие уровни включают предыдущие, т. е., например, возможности обеспечения абсолютной доверительной конфиденциальности автоматически покрывают возможности обеспечения полной, базовой и минимальной.

В НД ТЗІ 2.5-004-99 приводится перечень необходимых требований относительно механизмов и способов защиты для обеспечения каждой из функций, которая входит в состав каждой из услуг всех уровней. Например, для обеспечения абсолютной доверительной конфиденциальности необходимо выполнение таких условий как существование соответствующей политики безопасности, определенных правил разграничения доступа, определенных требований по наблюдаемости и т. д. Отметим, что выбор способов реализации условий (аппаратный, программный и т. д.) остается за разработчиком АС.

Для каждой выбранной услуги, соответствующего уровня пользователь выбирает из предложенного табличного списка те функции защиты, которые должны быть реализованы в соответствии с ТЗ.

Далее, пользователь выбирает те функции защиты, которые должны быть реализованы в соответствии с ТЗ, однако, не нашли отражения в предложенном списке функций защиты определенного уровня услуг.

Программа сравнивает полученные данные со своей базой знаний основанной на критериях НД ТЗИ 2.5-004-99. После чего предоставляет результаты совпадения по введенным требованиям и их соответствия с критериями.

Услуги различных видов и уровней определенным способом группируются в структуры, которые получили название функциональных профилей защищенности. **Профиль** – это минимально необходимый перечень услуг, который может обеспечить СЗИ, чтобы удовлетворить определенным требованиям относительно уровня защищенности информации в АС.

На основе сформированного функционального профиля защищенности программа дает развернутый анализ излишних

функций и недостающих для построения определенного профиля и достижения определенного уровня защищенности.

Характеристика информационных потоков программного модуля – определение механизмов защиты объекта испытаний

На данном этапе функционирования программного обеспечения, пользователю предоставляется возможность определить механизмы защиты, которые будут использоваться для защиты информации в объекте испытаний.

При определении механизмов защиты программа должна учитывать информацию, которая была обработана на прежних этапах функционирования программного обеспечения.

Программа должна предоставить возможность определения механизмов защиты на основе «Технического проекта» или «Технического задания», которые можно использовать в качестве входной информации.

Программа должна предоставить возможность определения механизмов защиты в соответствии с функциональными критериями защищенности. Для каждой функции, каждой услуги определенного уровня, определяются соответствующие механизмы защиты, которыми они будут реализовываться.

Целесообразность выбора и использования механизмов защиты должна учитывать информацию об объекте испытаний и модель угроз информации.

Характеристика механизмов защиты и построение модели защиты объекта испытаний должно происходить поэтапно, в соответствии с видами информации, которые характеризируют объект испытаний и указываются на этапе – характеристика объекта испытаний, а также сформированной моделью угроз информации и моделью безопасности объекта испытаний.

На основе характеристики объекта испытаний строится модель угроз информации, затем модель нарушителя информации и модель безопасности.

На основе указанных функций и услуг соответствующих уровней входящих в модель безопасности объекта испытаний, строится модель средств защиты информации, в которой должны быть указаны средства (технические, программные, организационные, нормативные), которые будут реализовывать функции защиты и устранять угрозы информации.

Необходимо выделить следующие уровни информации, которые характеризируют **модель механизмов защиты информации**:

1) свойства информации, которые необходимо обеспечить средствам защиты (конфиденциальность, целостность, доступность, наблюдаемость);

2) уровень аппаратного обеспечения средств защиты (АОСЗ) (поддержка управления памятью, поддержка управления процессами (задачами), поддержка взаимодействия между процессами, аппаратные модули, выполняющие определенные функции по защите информации, которые не относятся к поддержке ОС (аппаратные модули шифрования).);

3) уровень общесистемного программного обеспечения средств защиты (модули разграничения доступа, модули идентификации, автетнификации и авторизации пользователей и процессов, модули аудита, модули регистрации событий, модули реализации контроля целостности);

4) уровень прикладного программного обеспечения средств защиты;

5) уровень сетевого обеспечения средств защиты (отдельные аппаратные модули и их функции, программные модули и их функции);

6) уровень антивирусных средств защиты;

7) уровень управления системой защиты (наличие механизмов обеспечивающих управление средствами защиты информации);

8) уровень персонала (наличие персонала обеспечивающих управление и функционирование СЗИ, их функции и задачи);

9) уровень документации (наличие соответствующей документации по защите информации).

Выводы

Проведен анализ информации, циркулирующей в структурно-функциональных модулях программного обеспечения, определены уровни информационных потоков, а также, проанализирована методика информационного взаимодействия для модулей программного обеспечения, автоматизированной поддержки проведения испытаний КСЗИ.

В дальнейшем планируется провести более детальный анализ методики функционирования программного обеспечения для автоматизированной поддержки проведения испытаний КСЗИ. Также, планируется провести более детальную разработку требований для программного средства и формализованный анализ его структурно-функциональных модулей.

1. *Колтик М.А.* Методы и способы реализации автоматизированной поддержки проведения испытаний КСЗИ // Проблеми програмування «ИПС» НАН України. – 2013. – № 1. – С. 72 – 87.
2. *ДСТУ* 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
3. *НД* ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999. – № 22.
4. *НД* ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального призначення. Основні положення.
5. *НД* ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000. – № 53.
6. *НД* ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999. – № 22.
7. *НД* ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
8. *http*://www.anti-malware.ru/node/46
9. *НД* ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999. – № 22.
10. *НД* ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999. – № 22.

Получено 21.01.2013

Об авторах:

Боровская Елена Николаевна,
директор департамента,

Колтик Максим Анатолиевич,
аспирант.

Место работы авторов:

ООО НИИ Автоматизированных
компьютерных систем "Экотех",
03187, Киев-187,
Проспект Академика Глушкова, 40.
Тел.:044 526 1444.
E-mail: e.borovskaya@ekotex.ua,

Институт программных систем
НАН Украины,
Тел.: 067 218 2809.
E-mail: maxfaktor@ua.fm