СЕКЦИЯ 6. ИНФОРМАТИЗАЦИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ И ЗАЩИТА ИНФОРМАЦИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ГОСУДАРСТВЕННОГО ЗЕМЕЛЬНОГО КАДАСТРА И УЧЕТА ОБЪЕКТОВ НЕДВИЖИМОСТИ НА ТЕРРИТОРИИ КРАСНОЯРСКОГО КРАЯ

В.И. Козырь, Е.Н. Марченко, А.В. Мальцев
Филиал ФГУП «Федеральный кадастровый центр «Земля» «Красноярский региональный кадастровый центр «Земля», г.Красноярск

1. Общая ситуация и подходы к созданию системы информационной безопасности региональных автоматизированных систем ведения государственного земельного кадастра и государственного учета объектов недвижимости.

КРКЦ «Земля» участвует в разработке Федеральной целевой программы (ФЦП) “Создание автоматизированной системы ведения государственного земельного кадастра и государственного учета объектов недвижимости (2002-2007)" утвержденной постановлением Правительства Российской Федерации от 25 октября 2001г. № 745 (далее по тексту – Программа), в зоне своей ответственности.

Для обеспечения информационной безопасности в автоматизированной системы ведения государственного земельного кадастра и государственного учета объектов недвижимости (далее по тексту – АС ГЗК и ГУОН) создается единая подсистема обеспечения информационной безопасности, а на каждом объекте информатизации развертывается или ведется работа по развертыванию комплексной системы защиты информации от несанкционированного доступа (далее по тексту – КСЗИ от НСД).

Разработчики и пользователи АС ГЗК и ГУОН определяют информационные ресурсы, подлежащие защите, в соответствии с новыми введенными приказом в январе 2003 г. Росземкадастром документами «Развернутыми перечнями сведений, подлежащих засекречиванию….» и «Перечнями сведений, отнесенных к служебной информации ограниченного распространения с пометкой «Для служебного пользования….».

В рамках проектирования развертывания АС ГЗК и ГУОН по территории России разработаны:

– «Концепция обеспечения информационной безопасности развития автоматизированной системы ведения государственного земельного кадастра и государственного учета недвижимости»;

– «Общесистемные решения по обеспечению информационной безопасности в системном проекте развития автоматизированной системы ведения государственного земельного кадастра и государственного учета недвижимости»;

– «Типовые технические решения по обеспечению информационной безопасности развития автоматизированной системы ведения государственного земельного кадастра и государственного учета недвижимости».

Аналогичные документы и решения по защите информации, определяющие направления работ по информационной безопасности применительно к АС ГЗК и УН Красноярского края, будут разработаны и представлены КРКЦ «Земля» в ноябре - декабре 2003г.

2. Организационная структура управления информационной безопасностью в системе Росземкадастра

В целях реализации положений "Доктрины информационной безопасности Российской Федерации" утвержденной Президентом Российской Федерации 09.09.2000г.,. Пр-1895 и выполнения Программы, в части **разработки подсистемы информационной безопасности в АС ГЗК и ГУОН,** в системе Росземкадастра создана следующая организационная структура управления информационной безопасности:

1) приказом Росземкадастра №П/211 от 29 декабря 2001г. создана Дирекция ФЦП АС ГЗК и ГУОН.

Директор Дирекции первый заместитель руководителя Росземкадастра В.С. Кислов, Главный конструктор автоматизированной системы государственного земельного кадастра (АС ГЗК), осуществляет курирование вопросов создания и функционирования системы обеспечения информационной безопасности и подготовки необходимых решений в рамках ФЦП АС ГЗК и ГУОН и отрасли;

2) приказом Росземкадастра №П/7 от 15 января 2002г. создан Наблюдательный совет Федеральной целевой программы, по реализации подпрограммы «Информационное обеспечение управления недвижимостью, реформирования и регулирования земельных и имущественных отношений»;

3) приказом Госкомзема России № 74 от 01 июня 1999г.:

– в центральном аппарате Росземкадастра создана и функционирует Постоянно действующая техническая комиссия (ПДТК), для руководства и координации работ по обеспечению информационной безопасности в отрасли;

– на ФГУП ФКЦ «Земля» возложены функции головной организации отрасли по обеспечению информационной безопасности при ведении ГЗК и автоматизированной обработки информации;

4) контроль за обеспечением информационной безопасности в отрасли осуществляют соответствующие управления центрального аппарата Росземкадастра, в пределах своей компетенции (Управление государственного земельного кадастра, Управление мониторинга земель, стандартизации и сертификации, Отдел гражданской обороны и специальной работы и ФГУП ФКЦ «Земля»);

5) приказом Росземкадастра №П/259 от 04 апреля 2002г. в территориальных органах субъектов РФ, подведомственных учреждениях и предприятиях Росземкадастра назначены ответственные за защиту государственной тайны и обеспечение информационной безопасности, замещающие должности не ниже заместителя руководителя (директора);

6) в большинстве территориальных органов, областных федеральных государственных учреждений «Земельная кадастровая палата», подведомственных организациях, предприятиях и учреждениях Росземкадастра, имеются (1-3 чел.) подготовленные (прошедшие отраслевое обучение) в т.ч. 15 чел. в Учебном центре КРКЦ «Земля» (для Красноярского края) специалисты по защите информации, или организована работа по обучению и назначению созданию групп специалистов или специализированных подразделений по защите информации. Этими специалистами проводятся работы по эксплуатации КСЗИ от НСД на объектах информатизации АС ГЗК и ГУОН.

Исходя из структуры управления безопасностью принятой в Росземкадастре предлагается следующая структура управления подсистемой обеспечения информационной безопасности АС ГЗК и УН Красноярского края:

1) Управление подсистемой обеспечения информационной безопасности АС ГЗК и УН Красноярского края осуществляет руководитель Комитета по земельным ресурсам и землеустройству Росземкадастра по Красноярскому краю.

2) Один из заместителей руководителя КЗРиЗ по Красноярскому краю осуществляет курирование оперативных вопросов функционирования, подсистемы обеспечения информационной безопасности АС ГЗК и УН КК и подготовки необходимых решений.

В АС ГЗК и УН КК реализуется следующая организационная структура управления подсистемой обеспечения информационной безопасности:

Первый уровень управления: управленческий аппарат КЗРиЗ по Красноярскому краю;

Второй уровень управления: головная организация по обеспечению информационной безопасности в АС ГЗК и УН КК – филиал Федерального государственного унитарного предприятия Федерального кадастрового центра "Земля" «Красноярский региональный кадастровый центр «Земля» (г.Красноярск);

Третий уровень управления: специализированные группы специалистов или отдельные специалисты по защите информации, в учреждениях и организациях Росземкадастра по Красноярскому краю.

В управленческом аппарате КЗРиЗ по Красноярскому краю создается постоянно действующая техническая комиссия – ПДТК, на которой рассматриваются вопросы разработки ПИБ АС ГЗК и УН КК. Контроль, за разработкой ПИБ АС ГЗК и УН КК осуществляют соответствующие управления аппарата КЗРиЗ по Красноярскому краю, в пределах своей компетенции.

В филиале ФГУП «ФКЦ «Земля» «Красноярский РКЦ «Земля» создается специализированное структурное научно-техническое подразделение – отдел информационной безопасности, который осуществляет работы по разработке ПИБ, в рамках АС ГЗК и УН КК, со следующими основными функциями:

– разработка нормативных документов по обеспечению информационной безопасности, применительно к АС ГЗК и УН КК;

– разработка рекомендаций по защите информации от НСД;

– анализ и выявление возможных внешних и внутренних угроз безопасности, возможных каналов утечки информации;

– разработка рекомендаций, выбор, приобретение и проверка на совместимость с общим и технологическим программным обеспечением современных сертифицированных систем и средств (программных, программно-аппаратных, технических, криптографических и т.п.) защиты информации;

– участие в разработке и поставке на объекты информатизации АС ГЗК и УН КК защищенных программно-технических комплексов, предназначенных для обработки секретной информации;

– разработка вопросов защиты конфиденциальной информации, с использованием криптографических средств защиты информации, в том числе при ее передаче по телекоммуникационным сетям связи и использовании электронной цифровой подписи;

– организация проведения подготовки и аттестации и контроля объектов информатизации по требованиям информационной безопасности;

– участие в разработке защищенных информационных технологий и ГИС-технологий;

– взаимодействие с Гостехкомиссией России, ФСБ России, отделом информационной безопасности ФГУП ФКЦ «Земля» (г.Москва) –Головной организации по обеспечению информационной безопасности в системе Росземкадастра, другими министерствами и ведомствами, предприятиями, организациями, сертификационными и аккредитованными центрами по вопросам информационной безопасности АС ГЗК и УН КК, в пределах своей компетенции;

– разработка предложений по совершенствованию защиты секретной и конфиденциальной информации;

– оказание консультативной и практической помощи по защите государственной тайны и конфиденциальной информации на объектах информатизации АС ГЗК и УН КК;

– участие в установке и отладке сертифицированных средств и систем защиты информации на объектах информатизации АС ГЗК и УН КК;

– организация специализированных курсов, проведение подготовки и обучение, специалистов по защите информации, для объектов информатизации АС ГЗК и УН КК, на базе имеющегося Учебного центра.

Отдел информационной безопасности филиала ФГУП «ФКЦ «Земля» «Красноярский РКЦ «Земля» в настоящее время дооснащается различными средствами защиты информации от несанкционированного доступа (СЗИ от НСД), нормативной документацией, измерительной техникой для проведения специсследований по каналу побочных электромагнитных излучений и наводок (ПЭМИН), используя при этом имеющиеся производственные ресурсы в ФГУП ФКЦ «Земля» и его филиалах в других субъектах Российской Федерации.

Внедрение и реализацию требований по обеспечению информационной безопасности на объектах информатизации АС ГЗК и УН КК в учреждениях Росземкадастра осуществляют специально подготовленные отдельные специалисты или группы специалистов по защите информации.

3. Разработка отраслевых «пакетов» нормативных документов по информационной безопасности

Для обеспечения всех объектов информатизации документами в области информационной безопасности, с учетом специфики создания АС ГЗК и ГУОН в отрасли проведены и ведутся работы по разработке отраслевых нормативных документов (НД) по обеспечению информационной безопасности, в соответствии с требованиями Законов Российской Федерации «О государственной тайне», «Об информации, информатизации и защите информации», «О международном информационном обмене», «О праве на информацию», «Доктрины информационной безопасности Российской Федерации», «Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», а также других документов, стандартов и иных НД по безопасности информации, утвержденных органами государственного управления в пределах их компетенции (Гостехкомиссии России, ФСБ России, ФАПСИ и Росземкадастр).

Разработанные или разрабатываемые отраслевые НД направлены на защиту информации с ограниченным доступом, конфиденциальной информации (включающей информацию ограниченного распространения с пометкой – "для служебного пользования", персональные данные и коммерческую тайну), открытой (общедоступной) информации (для защиты ее целостности, сохранности и достоверности), взаимоувязаны между собой, с единой терминологией.

Кроме этого, ряд НД направленные Гостехкомиссией России в адрес Росземкадастра, переданы в территориальные органы и областные ФГУ «ЗКП» и подведомственные организации, для руководства в работе.

С 01 марта 2000г., приказом № 01 с по Госкомзему России введены в действие шесть базовых отраслевых НД, в составе:

– «РД. Концепция обеспечения информационной безопасности в системе Государственного комитета Российской Федерации по земельной политике»;

– «РД. Типовое Руководство по защите информации, составляющей государственную тайну, от технических разведок и от ее утечки по техническим каналам в системе Госкомзема России»;

– «РД. Временное типовое Положение по защите информации, составляющей государственную тайну, при ее обработке в автоматизированных системах в системе Государственного комитета Российской Федерации по земельной политике»;

– «РД. Временная Инструкция о порядке обращения и обеспечения защиты конфиденциальной информации при ее обработке в системе Государственного комитета Российской Федерации по земельной политике»;

– «РД. Типовая программа и методика проведения аттестационных испытаний автоматизированных систем на соответствие требованиям по безопасности информации в системе Государственного комитета Российской Федерации по земельной политике»;

– «Терминология в области информационной безопасности. Справочник по терминам, понятиям и определениям».

К разработке НД, были привлечены ведущие организации и специалисты аккредитованных центров по защите информации в РФ, таких как “Атомзащитаинформ” при Минатоме России, Ассоциация «Конфидент», НТЦ «Атлас» ФАПСИ, при консультативном участии специалистов Гостехкомиссии России и ряда других организаций. Базовые отраслевые НД направлены в Комземы областного уровня.

Введение в действие базового «пакета» НД позволило обеспечить Комземы Росземкадастра необходимыми отраслевыми НД по обеспечению информационной безопасности, проводить работы по защите информации в соответствии с действующими требованиями и с учетом специфики создания АС ГЗК.

Завершена разработка новых (введены в действие марте 2003г.) 7-ми отраслевых НД по защите информации, в форме "Сборника Руководящих документов по обеспечению информационной безопасности в системе Федеральной службы земельного кадастра России", в составе следующих НД:

– «Руководящий документ. Типовое техническое задание по теме: «Разработка комплексной системы защиты информации автоматизированной системы»;

– «Руководящий документ. Временные требования и рекомендации по защите конфиденциальной информации при ее обработке в автоматизированных системах»;

– «Методическое пособие. Модель угроз безопасности конфиденциальной информации в автоматизированной системе»;

– «Руководящий документ. Типовое положение о подразделении по защите информации»;

– «Руководящий документ. Типовое положение об администраторе автоматизированной системы, ответственном за безопасность информации»;

– «Руководящий документ. Типовая Инструкция по организации антивирусной защиты в автоматизированной системе»;

– «Руководящий документ. Типовая памятка пользователю, при работе в автоматизированной системе».

Сборник Росземкадастром направлен во все ФГУ «ЗКП» и Комземы областного уровня.

Ведутся работы по разработке следующих НД:

– «Методические указания по резервированию баз данных при ведении государственного земельного кадастра и государственного учета объектов недвижимости»;

– «Рекомендации по проектированию помещений при размещении и эксплуатации средств вычислительной техники».

В связи с принятием Федерального Закона Российской Федерации «Об электронной цифровой подписи» и планируемыми работами по применению криптографических средств защиты конфиденциальной информации в АС ГЗК и ГУОН, проведены исследования и разработан (при участии лицензированных ФАПСИ предприятий) проект нового «Сборника Временных руководящих документов по организации

системы защищенного электронного документооборота, с использованием средств криптографической защиты информации в автоматизированной системе ведения государственного земельного кадастра и государственного учета объектов недвижимости при проведении опытной эксплуатации и внедрении VipNet -технологии в системе Федеральной службы земельного кадастра России», в составе следующих НД:

1) «Временный руководящий документ. Термины и определения в области криптографической защиты информации»;

2) «Руководящий документ. Временное положение о порядке применения средств криптографической защиты информации в автоматизированной системе ведения государственного земельного кадастра и государственного учета объектов недвижимости»;

3) «Руководящий документ. Временное положение об удостоверяющем центре в автоматизированной системе ведения государственного земельного кадастра и государственного учета объектов недвижимости»;

4) «Руководящий документ. Временная инструкция Администратора информационной безопасности при работе со средствами криптографической защиты информации в автоматизированной системе ведения государственного земельного кадастра и государственного учета объектов недвижимости»;

5) «Руководящий документ. Типовая временная инструкция Администратора информационной безопасности Абонентского пункта Клиента при работе со средствами криптографической защиты информации в автоматизированной системе ведения государственного земельного кадастра и государственного учета объектов недвижимости».

С учетом этих документов ведется разработка подсистемы ОБИ в АС ГЗК и УН Красноярского края, в частности планируется на базе Филиала КРКЦ «Земля» **развернуть подчиненный Удостоверяющий центр**, для применения электронной цифровой подписи в КЗРиЗ и всех ФГУ «ЗКП» по Красноярскому краю.

4. Несколько слов о технологическом (испытательном) стенде информационной безопасности АС ГЗК и ГУОН Росземкадастра

В связи с массовым оснащением территориальных органов и ФГУ «ЗКП» средствами вычислительной техники, внедрением **отечественных кадастровых информационных технологий** и развертыванием АС ГЗК и ГУОН в системе Росземкадастра, необходимо решение проблемы создания защищенных кадастровых информационных технологий реализованных в виде программных комплексов (ПК) Единого государственного реестра земель (ЕГРЗ) с использованием сертифицированных программно-аппаратных средств защиты информации (СЗИ) от несанкционированного доступа (НСД).

При этом необходимо решение следующих основных задач:

1) проверка наличия в составе разработанных ПК ЕГРЗ собственных СЗИ от НСД;

2) выбор и проверка совместимости функционирования ПК ЕГРЗ с сертифицированными программно-аппаратными СЗИ от НСД, для соответствующих операционных систем (сред);

3) проверка механизмов защиты, требуемых для обеспечения заданных классов защищенности при обработке секретной и конфиденциальной информации, контроля корректности их функционирования и полноты документирования в соответствии с требованиями РД Гостехкомиссии России;

4) настройка правил разграничения доступа (ПРД) и защитных механизмов совмещенных комплексов ПК ЕГРЗ с сертифицированными СЗИ от НСД для выполнения требований по обеспечению заданных классов защищенности;

5) проведение предварительных испытаний и проверка функциональных возможностей совмещенных комплексов ПК ЕГРЗ с сертифицированными СЗИ от НСД;

6) анализ результатов предварительных ведомственных испытаний, оценка показателей и определение реального класса защищенности совмещенных комплексов;

7) разработка рекомендаций и замечаний по доработке ПК ЕГРЗ (разработчикам ПК ЕГРЗ), для подготовки к прохождению сертификационных испытаний для заданных классов защищенности в сертификационной испытательной лаборатории Гостехкомиссии России;

8) доработка ПК ЕГРЗ и их передача в сертификационную испытательную лабораторию Гостехкомиссии России;

9) получение сертификатов соответствия Гостехкомиссии России на совмещенные комплексы ПК ЕГРЗ с сертифицированными СЗИ от НСД требованиям безопасности информации..

Решение перечисленных задач выполняется проведением специальных ведомственных предварительных испытаний ПК ЕГРЗ, для чего в ФГУП ФКЦ «Земля» в отделе ИБ установлен и введен в эксплуатацию технологический (испытательный) стенд информационной безопасности АС ГЗК.

На стенде, реализованном в виде ЛВС (файл-сервер, графическая и 6-ть рабочих станций, с большим парком периферийного оборудования) установлены следующие основные специальные программные средства:

1) кадастровые информационные технологии – ПК ЕГРЗ различных версий;

2) сертифицированные программные и программно-аппаратные СЗИ от НСД, различных версий (семейств, по различные операционные системы):

- системы защиты Secret Net,;
- системы защиты «Аккорд»;
- системы защиты “Dallas Lock”;
- анализаторы «НКВД»;

3) криптографические средства защиты информации, VIPNet-технологии (включая электронную цифровую подпись), проект **Корневого отраслевого Удостоверяющего центра (по системе Росземкадастра),**

и другие постоянно обновляемые СЗИ от НСД и СЗИ от утечки информации по техническим каналам.

5. Организация системы обучения специалистов Росземкадастра в области информационной безопасности

Для обеспечения подготовки специалистов по вводу и эксплуатации защищенных программно-технических комплексов в системе Росземкадастра организовано обучение специалистов территориальных органов, Федеральных государственных учреждений «Земельная кадастровая палата», подведомственных предприятий и учреждений по защите информации по курсу: “Применение методов и средств защиты информации в кадастровых автоматизированных системах и технологиях”.

Преподавателями курса являются ведущие специалисты Росземкадастра (Управление государственного земельного кадастра, Управление мониторинга земель, Отдел гражданской обороны и специальной работы и ФГУП ФКЦ “Земля”), Гостехкомиссии России, МРАЦ, ФАПСИ, ФСБ России, ОКБ «САПР», ЗАО НИП «Информзащита», ВНИИПВТИ, 29 НИИ МО.

Занятия проводятся на основе активных методов обучения, с использованием мультимедиа технологий, а также разработаны необходимые учебные и методические пособия. Аналогичные курсы ведутся в Учебном центре КРКЦ «Земля», в настоящее время обучено 45 чел. Планируется обучение и в 2004 году, в т.ч. и обучение электронной цифровой подписи.

Система обучения специалистов позволит иметь обученных специалистов по защите информации в Красноярском крае, по внедрению и эксплуатации СЗИ от НСД и защищенных объектов информатизации в ФГУ «ЗКП».

ПРОГРАММНАЯ СИСТЕМА АКТИВНОГО МОНИТОРИНГА РАБОТЫ УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ И ЕЕ ПРИМЕНЕНИЕ В УЧЕБНОМ ПРОЦЕССЕ ПО КОМПЬЮТЕРНОЙ И СЕТЕВОЙ БЕЗОПАСНОСТИ

Т.М.Пестунова, А.Ю.Ткаченко
Институт вычислительных технологий СО РАН,
Новосибирский государственный университет

Многие аспекты обеспечения компьютерной безопасности требуют знания технологий удаленного управления компьютером, которые, с одной стороны, используются при создании информационного оружия, а с другой – применяются администраторами безопасности для контроля работы пользователей в комплексе с другими методами анализа защищенности компьютерных систем.

Описание архитектуры и функций системы «Наблюдатель». Программная система «Наблюдатель» (рис.1) позволяет осуществлять автоматизированный контроль работы удаленных пользователей и ориентирована на поддержку некоторых функций администратора безопасности. В частности, система позволяет:

– автоматизировать процесса наблюдения администратора безопасности за действиями пользователей;

– обеспечить обратную связь с сотрудниками, например, для отправки предупреждений;

– производить удаленное управление рабочей станцией по протоколу telnet и осуществлять выполнение стандартных операций, например, выключение компьютера.

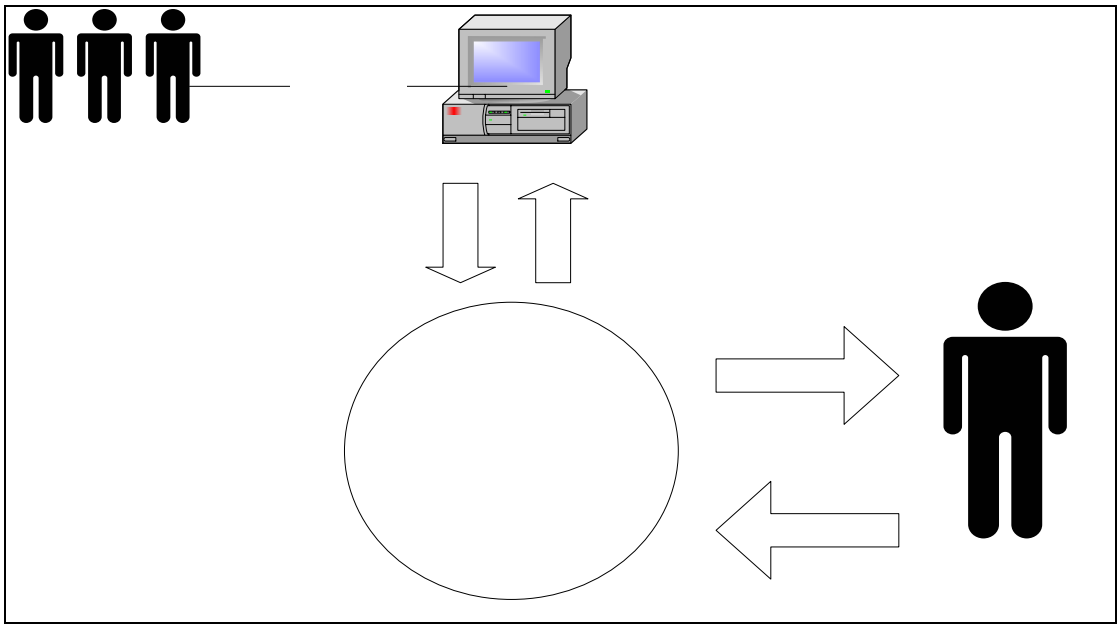

Рис.1. Взаимодействие администратора безопасности с пользователями посредством системы «Наблюдатель»

При разработке системы «Наблюдатель» использованы технологии объектно-ориентированного проектирования программного обеспечения (OOAD, RUP, UML, CASE Rational Rose) и программная реализация в среде Borland Delphi 7 и InterBase.

Текущая версия ориентирована на использование данных о взаимодействии с клавиатурой, однако, допускает расширение функций. Система разработана по технологии агент-менеджер и состоит из двух независимых частей. Администратор безо-

пасности взаимодействует с менеджерской частью программы (монитором), на которую поступает информация от агентской части, и может инициировать в удаленном режиме определенные управляющие действия.

Монитор представляет собой Windows-приложение с окнами для отображения данных и реализованным интерфейсом Drag&Drop для обеспечения коллективных операций над сущностями системы. Программа-агент устанавливается на рабочей станции, работу которой необходимо контролировать, реализуется в виде сервиса под ОС Windows и имеет возможность взаимодействовать с пользователем системы. Взаимодействие осуществляется либо посредством монитора, либо через протокол telnet. При этом пользовательский интерфейс агента - текстовый DOS-образный интерфейс: ввод команды в сеансе telnet и отображение результата на экране. Система может быть развернута локально или в сети и ориентирована на работу с операционными системами Windows 2000 и выше.

Агент функционирует в прозрачном для контролируемого сотрудника режиме, фиксирует всю информацию, касающуюся его взаимодействия с клавиатурой компьютера, оставаясь в рабочем состоянии на протяжении всего времени работы ОС. Статистические данные о работе сохраняются на текущей машине до момента передачи их монитору. Программа-менеджер в автоматическом режиме способна выполнять предустановленные действия на удаленной машине в случае получение текстовых данных, помеченных в системе, как «подозрительные». Все данные, такие как статистика сообщений клавиатуры, предупреждения сотруднику, нарушения, хранятся в базе данных системы для быстрого доступа к ним администратора безопасности.

Для администратора безопасности в системе предусмотрены следующие сервисы:

– запросить и просмотреть в любой момент статистику сообщений клавиатуры для конкретной рабочей станции и/или определенного сотрудника за некоторый период времени;

– потребовать фильтровать сообщения клавиатуры для их более подробного анализа;

– заблокировать или разблокировать учетную запись сотрудника;

– выключить или перезагрузить компьютер;

– принудительно завершить сеанс пользователя;

– послать текстовое сообщение сотруднику;

– выполнить на удаленной машине операции из числа предусмотренных в системе;

– сконфигурировать систему в автоматическом или ручном режиме;

– просмотреть информацию о работающих в сети сотрудниках (идентификационные данные, количество нарушений, предупреждений, сами предупреждения, информацию о сессиях);

– включить, или отключить сбор статистки на удаленной рабочей станции.

Система «Наблюдатель» может быть использована для организации лабораторного практикума по курсам компьютерной и сетевой безопасности для демонстрации некоторых возможностей удаленного доступа, а также как прототип системы анализа защищенности, на основе которого могут быть решаться некоторые задачи, связанные с отслеживанием и обработкой событий безопасности.

Лабораторный практикум на базе системы «Наблюдатель». При организации лабораторного практикума на базе системы «Наблюдатель» обязательно наличие методического обеспечения и четких инструкций для студентов (слушателей), преподавателя и администратора компьютерного класса. После установки изучаемого про-

граммного обеспечения программы-агенты начнут записывать всю информацию, вводимую с клавиатуры. Поэтому всю работу, касающуюся конфигурирования операционной системы рабочей станции, например, настройку учетных записей, необходимо проводить до установки программной системы «Наблюдатель». Перед установкой системы нужно настроить политику безопасности в операционной системе таким образом, чтобы группы контролируемых пользователей не могли получить доступ к программной системе и возможность ее использования не по назначению. Должны быть также отрегулированы вопросы, касающиеся предотвращения некорректного использования системы, которое может привести к утечке конфиденциальной информации (в т.ч. парольной), запуску вредоносных программ и.т.п. При этом надо иметь в виду, что в зависимости от сценария лабораторной работы функции управления монитором, могут в разные моменты передаваться администратору сети, преподавателю, обучаемым.

Лабораторная работа может проводиться в сетевом и локальном режимах. **В сетевом режиме** в компьютерном классе должны находиться не менее двух машин, объединенных в сеть. На одной устанавливается *программа-менеджер*, на остальных – *программы-агенты*. Для возможности установки системы необходимо, чтобы хотя бы одна из рабочих станций была оборудована дисководом компакт-дисков. В случае одноранговой сети выбор машины для установки менеджера не принципиален. Допускается возможность установки на один компьютер в сети сразу обеих частей системы. Если же сеть многоранговая, то рекомендуется устанавливать программу-менеджер на сервер, а программы-агенты – на клиентские станции. Для выполнения работы в условиях географически-разнесенной сети, т.е. состоящей из не менее, чем двух сегментов, необходимо применять сетевую версию системы клавиатурного мониторинга «Наблюдатель», менеджерскую часть которой после установки необходимо будет настроить, прописав адреса машин с агентами. **В локальном режиме** работа будет проводиться на одном или нескольких изолированных компьютерах, на каждом из которых будут установлены и программа-агент, и программа-менеджер. При этом можно использовать локальную версию системы «Наблюдатель», способную работать только в рамках одного сегмента сети, используя широковещательные передачи пакетов. Наличие дисковода компакт-дисков обязательно на каждой машине. Для безопасной работы системы необходимо, чтобы на каждом компьютере присутствовал дисковод флоппи-дисков. При установке системы целесообразно завести одного или нескольких тестовых пользователей для возможности просмотра результатов работы системы. Этим учетным записям назначаются минимальные права, ограничивающие возможность работы с данными чтением и записью только на дискету. После установки монитора при его запуске выполняются первоначальные настройки: пароль на доступ к агентам, порт соединения, адреса агентов, если используется сетевая версия, включение или отключение шифрования трафика, и др.

Сценарии лабораторной работы могут быть различными. Приведем пример одного из возможных сценариев.

1. Перед выполнением работы группа обучаемых разделяется на две подгруппы, одна из которых работает в качестве администратора безопасности, а другая – в режиме пользователей, за которыми ведется наблюдение. Впоследствии они меняются ролями. Учащиеся-пользователи получают у преподавателя данные тестовых учетных записей и дискету с «конфиденциальной» информацией (она может быть модифицирована в ходе выполнения работы) и заходят в систему.

2. Обучаемые, играющие роль контролируемых пользователей, выполняют с использованием клавиатуры ряд команд, которые могут быть интерпретированы, как «подозрительные». Для удобства выполнения работы можно заранее договориться о

множестве «запрещенных» команд и действий (например, модификация «конфиденциальной» информации на дискете, посещение «запрещенных» сайтов и т.п.)

3. В это время другая часть студентов под контролем администратора компьютерного класса или преподавателя наблюдает за всем происходящим через программу-менеджер (а именно, видит какие команды и какие слова набирают на клавиатуре на выбранной машине их товарищи) и, в случае «подозрительных» действий наблюдаемых, посылает им предупреждения, выполняет команду на машине с нарушителем или прекращает сессию «подозрительного» пользователя.

По окончании работы администратор класса выполняет удаление программной системы «Наблюдатель» и всех её данных (текстовые файлы с записанной информаций мониторинга), приостанавливает действие тестовых учетных записей или удаляет их.

Возможности практического применения системы. Применение системы для решения практических задач администратора безопасности (таких как периодическая проверка работы пользователей) требует предварительного решения ряда организационно-правовых аспектов, очерчивающих рамки применения системы – разработка режима использования системы и получение санкций на использование со стороны руководства, предотвращение несанкционированного использования системы, предупреждение сотрудников о принципиальной возможности такого контроля. Хотя система «Наблюдатель» не обладает многими функциями дорогостоящих профессиональных систем анализа защищенности, ее применение, как показывает опыт одного из авторов, позволяет существенно повысить дисциплину пользователей и предотвратить нежелательные виды деятельности на компьютеризированных рабочих местах. Достоинством системы является небольшой объем требуемых вычислительных ресурсов, простота в использовании и гибкость настройки, что позволяет оперативно адаптировать систему под конкретную среду и цели использования. Администратор безопасности создает модель исследуемой сети в системе, задавая состав компьютеров и сотрудников, при этом каждому компьютеру на схеме должен соответствовать IP-адрес и имя, которые используются данной машиной в реальной сети, а также данные о конкретных работающих в сети сотрудниках. Статистическая информация, накапливаемая в системе, может обрабатываться с применением алгоритмов обнаружения закономерностей и использоваться для формирования «типового поведенческого портрета» пользователя путем выявления специфических закономерностей работы конкретного пользователя и сопоставления их с ожидаемыми типичными для конкретного должностного лица сценариями работы.

РАБОТА С ПЕРСОНАЛОМ КАК АСПЕКТ ОРГАНИЗАЦИИ КОМПЛЕКСНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.Б. Туговиков
СБ ОАО "КрАЗ", г. Красноярск

Становится все более очевидной возрастающая ценность информации как важной составляющей экономической и физической безопасности хозяйствующих субъектов. По данным специалистов потеря лишь четверти информации, относимой к категории коммерческой тайны организации, в течение нескольких месяцев приводит к ее банкротству в 50% случаев. Крупным террористическим актам, ограблениям банков, преступлениям в экономической сфере также предшествует сбор информации.

Очевидно, что уровень конфиденциальности защищаемой информации определяется, в первую очередь, человеческим фактором. В работе Алексинцева А.И. "Понятие и структура угроз защищаемой информации" (сборник МИФИ Безопасность информационных технологий. №3 за 2000) приводится перечень усиливающих и разрушающих защиту внешних воздействий, при этом автор отмечает "Самым распространенным, многообразным и опасным источником дестабилизирующего воздействия на защищаемую информацию являются люди". Действительно, если мы рассматриваем технические средства защиты информации как отдельный фактор обеспечения информационной безопасности, очевидно, что он обеспечивают конфиденциальность информации настолько, насколько ответственно относится персонал к обслуживанию и эксплуатации технических средств. Кроме того, никакие, даже дорогостоящие средства защиты не смогут воспрепятствовать разглашению конфиденциальных сведений собственными сотрудниками организации. Западные специалисты по обеспечению экономической безопасности считают, что сохранность конфиденциальной информации на 80 % зависит от правильного подбора, расстановки и воспитания персонала. О. Генне в статье «Соглашения о намерениях» пишет, – «Причин, которые могут подвигнуть того или иного сотрудника на излишнюю откровенность, существует множество: от самых спонтанных и невинных, таких как чрезмерная болтливость, до вполне продуманных и злокозненных, например приобретения материальной выгоды или желания отомстить за нанесенную реальную или воображаемую обиду» (журнал «Защита информации. Конфидент», № 2, 2003).

В литературе по сетевой безопасности приведена формула, описывающая зависимость безопасности информации, размещенной в компьютерной сети от пяти основных факторов:

$$S = f(F*P*A*L*C) \quad (1)$$

где S - полная безопасность системы, F - физическая безопасность, P - персональная безопасность (ответственность, лояльность и сознательность), A - административный контроль, L - безопасность при передаче данных, C - безопасность компьютерной обработки данных. Каждый элемент может изменяться в интервале от 0 до 1. Очень хорошая защита находится в интервале от 0,8 до 0,9, значение, меньшее, чем 0,3 говорит о неудовлетворительном уровне безопасности информации. Эта формула по нашему мнению может быть распространена на безопасность традиционного бумажного конфиденциального документооборота.

В свете изложенного выше попробуем более детально рассмотреть параметр "персональной безопасности". Как нам кажется, для формального описания этого параметра можно использовать иллюстративную формулу следующего типа:

$$P_L = \mathrm{Min}\ \{p_i(\Theta_+,\Theta_-,\Sigma(\psi_1,\ldots,\ \psi_N,\psi_{N+1},\ \ldots,\ \psi_K),\ t)\}. \quad (2)$$

Здесь P_L –параметр безопасности L-го субъекта доступа (L=1,…M), характеризующий уровень защищенности информации от человеческого фактора;

N – количество персон, имеющих доступ к информационному объекту;

Σ –суммарное психологическое воздействие K персон на благонадежность i-й персоны;

p_i- уровень благонадежности i-й персоной, эти значения определены на отрезке [0,1), то есть уровень благонадёжности может изменяться в интервале от 0 – что означает полную невыполнимость сохранения конфиденциальности, до 1 - полная благонадежность, что в принципе не достижимо при $t > T_i \geq 0$, где T_i (μ_+,μ_-) – персональное время гарантии конфиденциальности;

Θ_+,Θ_-- совокупность усиливающих и, соответственно, понижающих персональную ответственность внешних воздействий ($\Theta = \theta_1,\ldots,\theta_J$);

ψ_j – воздействие j-й персоны на благонадежность i-й персоны. Воздействия ψ могли бы относиться к Θ_+,Θ_-, но выделены в отдельную категорию, так как, являясь субъективным фактором, могут оказывать как укрепляющее, так и разрушающее воздействие на персональную ответственность, (здесь для j = N+1,…K – персоны не являющиеся субъектами доступа, но связанные с i-й персоной дружескими, родственными и другими отношениями);

t – время. Параметр персональной благонадежности может существенно меняться во времени: это зависит от уровня зарплаты; уровня защиты информации; наличия наказаний за утечку информации; отношения руководства. На лояльность влияет возможность сделать карьеру; материальные потребности, возможности перехода на более перспективную работу в другую организацию и т.д.

Вычисление значения коэффициентов p_i требует отдельной проработки и дополнительных исследований в части получения количественной оценки благонадежности персоны как субъекта доступа к объектам конфиденциальной информации. Для получения количественных оценок, видимо, может быть использован программно-аппаратный комплекс «Полиграф», так называемый детектор лжи, естественно при специальном подборе и настройке системы вопросов и подготовке специалистов по тестированию. В настоящее время в сети Internet можно также найти описание программ, которые могли бы быть использованы для получения количественных оценок лояльности персонала (www.loyalty-expert.ru). Случаи практического использования подобных программ для оценки благонадежности персонала, имеющего или получающего доступ к конфиденциальной информации предприятия, автору не известны. Тем не менее, представляется очевидным то, что увеличение значения параметра P_L является вполне достижимым. Наработанные практикой пути повышения значения P_L следующие:

1) заключение индивидуальных соглашений о соблюдении конфиденциальности с каждым работником, допущенным к конфиденциальной информации, независимо от вида ее представления (к документам, к компьютерным системам, к присутствию на переговорах или просто в помещениях, где носители конфиденциальной информации присутствуют или она произносится);

2) установление доплаты за работу с конфиденциальной информацией, так как даже относительно небольшой процент надбавки воспринимается как факт, говорящий о важности выполнения режима конфиденциальности;

3) назначение из числа **N** работников, допущенных к объекту конфиденциальной информации как минимум одного ответственного за соблюдение установленных мер информационной безопасности из числа наиболее авторитетных и ответственных членов коллектива;

4) постоянное проведение разъяснительной работы, PR - акций с целью повышения лояльности к предприятию в целом, помощь в решении проблем в социальной сфере и т.п.;

5) проведение консультаций по проблемам защиты информации, разъяснений, что необходимо предпринять при подозрении на несанкционированный доступ, другие нарушения информационной безопасности;

6) по мере возможности, исключение из состава допущенных к конфиденциальной информации персон, обладающих устойчиво низким значением p_j, или оказывающих отрицательное влияние на уровень p_j других персон;

7) регулярный контроль выполнения установленных правил информационной безопасности;

8) регулярное проведение комплексного психологического тестирования и (или) контроля работников, в том числе на предмет изменения уровня благонадежности, в частности в статье «Использование полиграфа для проверки сотрудников» (Мир и безопасность № 3, 2003) С. Журин как один из факторов положительного воздействия на лояльность предлагает использование «Полиграфа».

Уменьшение риска падения значения параметра p_i связано, с уменьшением или полным исключением негативного воздействия различных факторов на лояльность каждого отдельно взятого работника, либо преобладание воздействия положительных факторов над воздействием отрицательных.

Практика показывает, что параметры F и A, описанные в формуле (1) стоит рассматривать как положительные воздействия, составляющие Θ_+ в формуле (2), сюда же необходимо отнести наличие средств контроля доступа. К ним относятся в части организационных мер обеспечения защиты информации – журналы учета передачи конфиденциальных документов, дисков и дискет, учет отправления сообщений по электронной почте, учет сдачи помещений под охрану и т.п. В части технических мер контроля доступа могут использоваться автоматические системы контроля доступа в помещения, системы видео – наблюдения, специальные программно – аппаратные средства типа ISS SAFEsuite, Symantec, которые регистрируют действия пользователей компьютерной сети, действия пользователей персональных компьютеров (Dallas Loc, SecreNet), либо используют для формирования отчетов файлы-журналы (Log-файлы), формируемые операционными системами.

Естественно, что работники должны быть предупреждены о контроле их действий со стороны соответствующих административных служб. При этом в качестве фактора положительно влияющего на персональную ответственность является сам факт наличия внешнего контроля. В то же время отсутствие внешнего контроля является фактором, который относится к Θ_-. Примером тому могут служить известные случаи нарушений информационной безопасности сетевыми администраторами, совершения экономических преступлений администраторами банковских информационных систем. Как правило, на эту категорию работников параллельно с обязанностями по разграничению доступа возлагаются обязанности по контролю доступа, то есть их действия с конфиденциальной информацией и критичными с точки зрения безопасности ресурсами никто не контролирует, что наряду с отсутствием регулярного психологического тестирования, значительно снижает уровень персональной ответственности. Что особо опасно, так как администраторы сетевых операционных систем, информационных систем, баз данных имеют доступ к подавляющему большинству субъектов доступа и их параметр p_i присутствует в P_L практически для всех L. Действительно, если сетевой администратор имеет $p_i = 0$, то в формуле (1),мы получаем P=0, в результате информационная безопасности всей системы S=0.

Таким образом, с развитием информационных компьютерных сетей и систем, с перемещением подавляющего объема информационных потоков в эту сферу наличие специальных служб, обеспечивающих информационную безопасность и грамотно работающих с персоналом, становится неотъемлемой и обязательной составляющей в построении системы безопасности каждого объекта информатизации.

ВЕРОЯТНОСТНЫЕ МЕТОДЫ МОДЕЛИРОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Г.А. Федоров, Е.Д. Карепова
Красноярский государственный технический университет,
Институт вычислительного моделирования СО РАН,Красноярск

До настоящего времени разработано множество формальных моделей безопасности. Однако большинство из них оценивает защищенность систем на логическом уровне. Такие важные вопросы, как топология вычислительной системы с точки зрения безопасности и применимость различных средств защиты для обеспечения сохранности или конфиденциальности информации не рассматриваются. В данной работе дается описание формальной модели безопасности как вероятностной. Это означает, что основные параметры модели представляют собой вероятности некоторых событий безопасности, интересующих разработчика. Особенностью данного подхода является автоматическое задание параметров модели либо доказательство невозможности ее построения при заданных ограничениях.

Построение формальной модели

Целью построения модели является создание системы обеспечения безопасности информации на основе некоторого набора имеющихся средств – подсистем различных типов и функционального назначения и тех ресурсов, которые расходуются на их установку. Объектом моделирования является вычислительная сеть, для которой разработчику желательно создать систему обеспечения безопасности обработки и обмена информации. Топография сети задается в виде гиперграфа G = <U,V>, где множество вершин U представляет собой множество участников информационного обмена (абонентов, узлов сети), а множество ребер V – множество связей между ними (линий связи, передачи данных). Граф G является взвешенным и раскрашенным. Каждой вершине и каждому ребру графа приписывается некоторый набор параметров. При задании системы параметров необходимо, чтобы они представляли собой реальные величины, значение которых можно получить либо вследствие испытаний, либо путем расчетов. Например, в качестве параметра узла может быть предложена надежность – вероятность того, что санкционированный запрос к узлу будет удовлетворен.

Наиболее простой является модель, которая оценивает работу вычислительной сети всего по двум параметрам: безопасность и работоспособность. Оценку связей в таком случае лучше всего проводить по критерию надежности передачи и пропускной способности.

Задается множество функций зависимости величины параметра элемента графа от затрат некоторого ресурса (ресурсов). Данные функции могут иметь как дискретный, так и непрерывный характер. Определяется количество доступного ресурса (в наиболее простом случае – сумма денег, затрачиваемых на создание системы обеспечения безопасности информации). Задается некоторая общая функция полезности системы, зависящая от параметров всех элементов системы. На последнем этапе моделирования формулируются требования к значениям параметров отдельных элементов системы или подсистем. Затем решается задача нахождения максимума функции по-

лезности при заданных ограничениях. На выходе будут получены значения параметров элементов системы и требуемые затраты ресурса.

Следует заметить, что построенная система является статической и будет описывать только начальный момент существования сети («запуск системы»). В дальнейшем, в ходе эксплуатации заданные параметры будут изменяться в зависимости от происходящих в системе событий безопасности (удачных или неудачных атак, сбоев, профилактических мероприятий). Впрочем, существует возможность описать в рамках данного вероятностного подхода и динамический случай.

Простейшая формальная модель и примеры ее реализации

Пусть конструируемая система представлена в виде графа G = <U,V>, где множество вершин U представляет собой множество участников информационного обмена, а множество ребер V – множество связей между ними. Каждой вершине из множества U будут приписаны два параметра: защищенность и работоспособность, а каждому ребру из V некоторая надежность и пропускная способность:

$\forall u \in U$, $u = (d, w)$, $0 \le d \le 1$, $0 \le w \le 1$, где d – защищенность, w – работоспособность;

$\forall v \in V$, $v = (q, m)$, $0 \le q \le 1$, $0 < m$, где q – надежность, m – пропускная способность.

Данные величины имеют определенный смысл:

d – вероятность того, что несанкционированный запрос к данному узлу будет каким-либо образом отклонен.

w – вероятность того, что санкционированный запрос к данному узлу будет удовлетворен.

q – вероятность того, что сообщение будет передано по каналу без утери или искажения.

m – количество информации, которое будет возможно передать по каналу за единицу времени.

Для данной системы будет задан параметр α - вероятность того, что очередной запрос к некоторому узлу окажется несанкционированным.

Функции полезности для узлов и связей определены следующим образом:

$Q_{ui} = Q(d, w \mid d, w \in u_i) = \alpha d + (1 - \alpha)w$

$R_{vj} = R(q \mid q \in v_j) = q$

Общая функция полезности будет определена в виде:

$$F = F(Q_{u1},\ldots,Q_{un},R_{v1},\ldots,R_{vk}) = (\sum_{i=1}^{n} Q_{ui})/n + (\sum_{i=1}^{k} R_{vj})/k$$

Здесь n и k – общее количество вершин и ребер соответственно.

Простую модель лучше всего ограничить одним ресурсом. Наиболее очевидными в данном случае представляются денежные расходы.

Функции зависимостей значений параметров от расхода ресурса будут дискретными следующего вида:

$f_s(r_{si}) = p_{si}$

где $s = (d,w,q)$, $0 \le p_{si} \le 1$, или $s = (m)$, $0 < p_{si}$.

Аргументы и значения функций следует определять в соответствии с доступным спектром средств и методик защиты, передачи информации, средств ее обработки. Для реальной системы в качестве материала можно использовать результаты тестирования систем, представляемые их разработчиками.

Как уже было сказано, значения параметров получаются в ходе решения задачи нахождения максимума функции полезности системы F при заданном количестве ресурса I. Кроме ограничения на количество ресурсов можно добавить множество ограничений вида $s_i \ R \ c_{si}$, где $s = \{d,w\}$, $i = 1…n$, или $s = \{q,m\}$, $i = 1…k$, $R = \{<, \le, \ge, >, =, \ne\}$, c_{si} – некоторая константа. Так как функции, определяющие зависимость значений параметров от количества ресурсов, имеют дискретный характер, то нахождение решения возможно полным или частичным перебором вариантов значений параметров.

Вычислительный эксперимент

Пусть имеется сеть из n узлов, построенная по топологии «кольцо». В этом случае все связи получаются равнозначными, следовательно, значения их параметров совпадают. Поэтому составляющая связей функции полезности системы F определяется как константа, и функция F имеет вид:

$$F = F(Q_{u1},…,Q_{un},R_{v1},…,R_{vk}) = \left(\sum_{i=1}^{n} Q_{ui}\right)/n + C$$

где C – некоторая константа, определяющая полезность всех связей. Рассмотрим несколько примеров:

Пример 1:

Пусть $n = 6$, $\alpha = 0.1$, $I = 700$, $C = 0.5$

Рассматривается простейшая формальная модель.

Функции зависимостей значений параметров от расхода ресурса будут следующими:

$f_d(r)$:

r_i	10	20	50
$f_d(r_i)$	0.1	0.5	0.9

$f_w(r)$:

r_i	30	50	110	120
$f_w(r_i)$	0.3	0.5	0.9	1.0

Ограничения на значения параметров не накладываются. В результате вычислений получается $F = 1.32$.

Пример 2:

Пусть $n = 6$, $\alpha = 0.5$, $I = 1000$, $C = 0.3$.

Рассматривается простейшая формальная модель.

Функции зависимостей значений параметров от расхода ресурса будут следующими:

$f_d(r)$:

r_i	10	50	110
$f_d(r_i)$	0.1	0.3	0.7

$f_w(r)$:

r_i	20	40	100	120
$f_w(r_i)$	0.3	0.4	0.8	0.9

Ограничения на значения параметров не накладываются. В результате вычислений получается F = 1.01.

Заключение

Предложенный подход к созданию моделей систем обеспечения безопасности информации обладает рядом преимуществ. Во-первых, алгоритм задания параметров системы достаточно прост – в дискретном случае требуемые значения могут быть получены простым перебором вариантов. Во-вторых, реальная интерпретация параметров позволяет легко перейти от формальной модели к построению реальной системы. В-третьих, формальная модель является масштабируемой и дает возможность достаточно просто добавлять или убирать параметры системы, что позволяет разработчику получить нужный ему уровень абстракции модели.

Литература

1. Сереченко В.В. Применение математических методов для оценки защищенности информационных систем согласно стандарту ISO/IEC 15408 // Материалы конференции МИФИ-2002. – Москва. – 2002. – с. 115-121.

2. Новиков Ф.А. Дискретная математика для программистов. – ПитерПресс, С.-Петербург, 2003 г.

3. Кормен Т., Лейерсон Ч., Ривест Р. Алгоритмы построения и анализ. – Москва, МЦНМО, 2000 г.