ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 002.56(075.8)

МОДЕЛЬ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

В.Я. ИЩЕЙНОВ
С.М. ЧУДИНОВ

Российский государственный гуманитарный университет, г. Москва

e-mail: pr_dmitr@mail.ru
e-mail: chud35@yandex.ru

Излагаются научно-технические материалы по разработке и использованию модели безопасности конфиденциальной информации в информационной системе.

Ключевые слова: информационная безопасность, модель безопасности конфиденциальной информации, использование модели в информационной системе.

Безопасность конфиденциальной информации при ее обработке в информационных системах обеспечивается с помощью системы защиты, включающей организационные меры и средства защиты (технические) информации, в том числе шифровальные (криптографические средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки конфиденциальной информации, а также используемые в информационной системе информационных технологий.

Технические и программные средства должны удовлетворять установленным, в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту конфиденциальной информации.

Техническими средствами, позволяющими осуществлять обработку конфиденциальной информации на объектах информатизации являются: средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки конфиденциальной информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео-и буквенно-цифровой информации), программные средства защиты информации, применяемые в информационных системах.

Для обеспечения безопасности конфиденциальной информации при ее обработке в информационных системах на объектах информатизации необходима защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнито-оптической и иной основе.

Организация работ по обеспечению безопасности конфиденциальной информации при ее обработке в информационных системах включает следующие этапы:

1. Определение угроз безопасности конфиденциальной информации при ее обработке и формирование на их основе модели угроз.

2. Разработку на основе модели угроз системы защиты конфиденциальной информации, обеспечивающей нейтрализацию предполагаемых угроз с использование методов и способов защиты конфиденциальной информации.

3. Проверку готовности средств защиты конфиденциальной информации к использованию.

4. Обеспечение лиц, использующих средства защиты конфиденциальной информации, правилам работы.

5. Учет лиц, допущенных к работе с конфиденциальной информацией в информационной системе.

При разработке модели безопасности конфиденциальной информации необходимо учитывать следующие исходные данные:

- характеристики безопасности конфиденциальной информации, обрабатываемой в информационной системе;
- структуру информационной системы;
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
- режим обработки конфиденциальной информации;
- режим разграничения прав доступа пользователей информационной системы;
- месторасположение технических средств информационной системы.

По заданным характеристикам безопасности конфиденциальной информации, обрабатываемой в информационной системе, информационные системы подразделяются на типовые и специальные.

Типовые информационные системы – системы, в которых требуется обеспечение только конфиденциальности информации.

Специальные информационные системы – системы, в которых вне зависимости от необходимости обеспечения конфиденциальности информации требуется обеспечить хотя бы одну из характеристик безопасности конфиденциальной информации (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

Структурно информационные системы могут быть:

-автономными (не подключенными к иным информационным системам) комплексами технических и программных средств, предназначенных для обработки конфиденциальной информации – автоматизированные рабочие места (АРМ);

-комплексами АРМ, объединенными в единую информационную систему средствами связи без использования технологии удаленного доступа – локальные информационные системы (ЛИС);

-комплексами АРМ и (или) ЛИС, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа – распределительные информационные системы (РИС).

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы – однопользовательские и многопользовательские.

По разграничению прав доступа пользователей информационные системы подразделяются на системы – без разграничения прав доступа и с разграничением прав доступа.

Местонахождение технических средств подразделяется на системы все технические средства которых находятся в пределах контролируемой зоны и системы, технические средства которых частично или полностью находятся за пределами контролируемой зоны.

Структурная модель информационной системы представлена на рисунке 1.

Учитывая вышеизложенное и характер угроз структурная модель угроз безопасности конфиденциальной информации может быть представлена в виде, рисунок 2.

Исходя из рассмотрения структурной модели информационной системы, рис.1 функциональная модель информационной системы запишется в виде:

Fuc= f(Fc1;Fq2;Fn3;Ft4;Fp5;Fd6),

где: Fc1,Fq2,Fn3,Ft4,Fp5,Fd6 – функции характеристик информационной системы.

В свою очередь функции характеристик информационной системы могут быть представлены в виде:

-функции характеристик структурной ИС,

Fc1=f(z1,z2,z3), где:

z1 – автономная автоматизированная система (автоматизированное рабочее место – АРМ);

z2 – локальная автоматизированная система (ЛИС);

z3 – распределительная информационная система (РИС).

-функции характеристик безопасности ИС,

Fq2=f(k1,k2), где:

k1 – типовая информационная система;

k2 – специальная информационная система.

-функции характеристик подключения к каналам связи ИС,

Fn3=f(p1,p2), где:

p1- подключение к сети общего пользования;

p2 – подключение к сетям Internet.

-функции характеристик местонахождения технических средств,

Ft4=f(ρ1,ρ2), где:

ρ1 – информационная система в пределах контролируемой зоны;

ρ2 – информационная система частично или полностью за пределами контролируемой зоны.

-функции характеристик режима обработки,

Fp5=f(x1,x2), где:

x1 – обработка информации однопользовательская;

x2 – обработка информации многопользовательская.

-функции характеристик разграничения прав доступа,

Fd6=f(δ1,δ2), где:

δ1 – обработка информации без разграничения прав доступа;

δ2 – обработка информации с разграничением прав доступа.

Функциональную модель угроз безопасности информационной системы исходя из рис.2 представим в виде:

Fy(t)=f{((F1(t),F2(t),F3(t),F4(t),F5(t),F6(t))},

Рис. 1. Структурная модель информационной системы

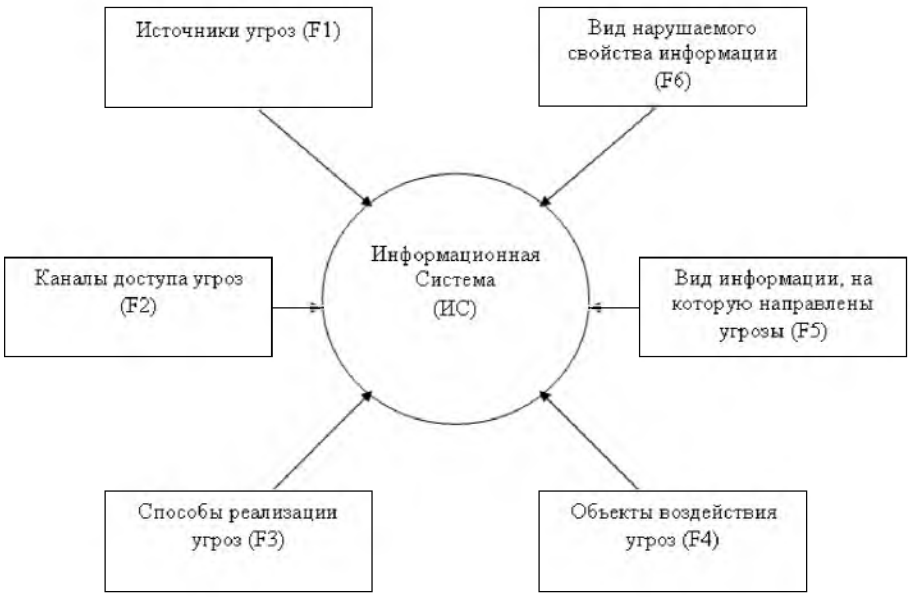

Рис. 2. Структурная модель угроз безопасности конфиденциальной информации в информационной системе

где: F1(t),F2(t),F3(t),F4(t),F5(t),F6(t) – функции угроз информационной системе.

В свою очередь:

-функция источника угроз,

F1(t)=f(α1,α2,α3), где:

α1 – угрозы, создаваемые нарушителем (физическим лицом);
α2 – угрозы, создаваемые аппаратными закладками;
α3 – угрозы, создаваемые программными средствами.

-функция угроз через каналы доступа,

F2(t)=f(β1,β2,β3,β4,β5,β6), где:

β1 – наличие в автоматизированной системе (АС) вредоносной программы;
β2 – наличие в АС аппаратных закладок;
β3 – действие при реализации протоколов сетевого взаимодействия и каналов передачи данных;
β4 – недостаточность технической защиты информации;
β5 – уязвимость средств защиты информации;
β6 – уязвимость системы при внештатных ситуациях.

-функция угроз по способам реализации,

F3(t)=f(γ1,γ2), где :

γ1 – угрозы от специальных воздействий;
γ2 – угрозы по техническим каналам.

-функция угроз через объекты воздействия,

F4(t)=f(υ1,υ2,υ3), где:

υ1 – угрозы информации в базах данных;
υ2 – угрозы информации в составе файловой системы;
υ3 – угрозы системным программным компонентам.

-функция угроз по виду информации,

F5(t)=f(τ1,τ2,τ3,τ4), где:

τ1 – угрозы речевой информации;
τ2 – угрозы визуальной информации;
τ3 – угрозы в технических средствах обработки информации;
τ4 – угрозы информации, обрабатываемой в АС

-функция угроз по виду нарушаемого свойства информации,

F6(t)=f(ξ1,ξ2,ξ3), где:

ξ1 – угрозы конфиденциальности;
ξ2 – угрозы целостности системного программного обеспечения;

ξ3 – угрозы доступности программных средств защиты информации.

Окончательно функциональную модель безопасности конфиденциальной информации в информационной системе можно представить в виде:

Fб(t)=f{(Fuc;Fy(t)}

Разработка функциональной модели безопасности конфиденциальной информации в информационной системе позволит смоделировать предполагаемые угрозы в системе защиты для обеспечения их нейтрализации.

Список литературы

1. Ищейнов В.Я., Мечатунян М.В. Основные положения информационной безопасности. Изд-во «МАРТИТ», Москва 2012 г. С.211

2. Ищейнов В.Я. Программно-аппаратные средства защиты информации в сетях передачи данных. Компьютерные науки и технологии, КниТ 2011, Сборник трудов Второй Международной научно-технической конференции, Белгород.

MODEL OF SAFETY CONFIDENTIAL INFORMATION IN INFORMATION SYSTEM

V.J. ISCHEYNOV
S.M. CHUDINOV

Russian State University for the Humanities, Moscow

e-mail: pr_dmitr@mail.ru
e-mail: chud35@yandex.ru

Scientific and technical materials on development and use of model of safety of confidential information in information system are stated

Keywords: information security, model of safety of confidential information, model use in information system