НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ЦЕНТР ПРЕДПРИНИМАТЕЛЬСКИХ РИСКОВ»

ВЫЯВЛЕНИЕ СПЕЦИАЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ НЕГЛАСНОГО ПЕРЕХВАТА ИНФОРМАЦИИ

(КОНСПЕКТ)

Санкт-Петербург
2008

Содержание:

1. Методология комплексной информационной безопасности объектов. Информационные ресурсы, подлежащие защите.

Защита конфиденциальной информации на предприятии должна носить комплексный характер. Это обусловлено тем, что предприятие как информационный объект имеет каналы утечки информации различного проявления. Вследствие этого рассмотрим модель информационного объекта, затем рассмотрим различные каналы утечки информации, а также направления развития защиты информации и основные способы ее защиты.

Модель информационного объекта.

Защищаемый от утечки информации по техническим каналам информационный объект — сложные взаимодействующие между собой и внешней средой, информационные, предметные и энергетические системы. Модель информационного объекта (рис. 1) включает взаимосвязанные информационную, энергетическую и предметную системы.

Информационная система обменивается с внешней информационной системой входной и выходной информацией (вход 1.1, выход 2.1). Информационная система взаимодействует с энергетической системой и через нее - с внешней средой. Через энергетическую систему может формироваться канал утечки информации. Энергетическая система объекта, например турбина летательного аппарата, воздействует на внешнюю среду, создавая акустическое демаскирующее поле. Энергетическая система также взаимодействует с материальной системой, в результате чего генерируется вибрационное (механическое) поле. Вибрационное поле может модулировать сигналы информационной системы. Материальная система (например, планер, космический аппарат, летательный аппарат, надводный корабль, подводный корабль и др.) воздействует на окружающую среду и возбуждает в ней акустическое и вибрационное поля.

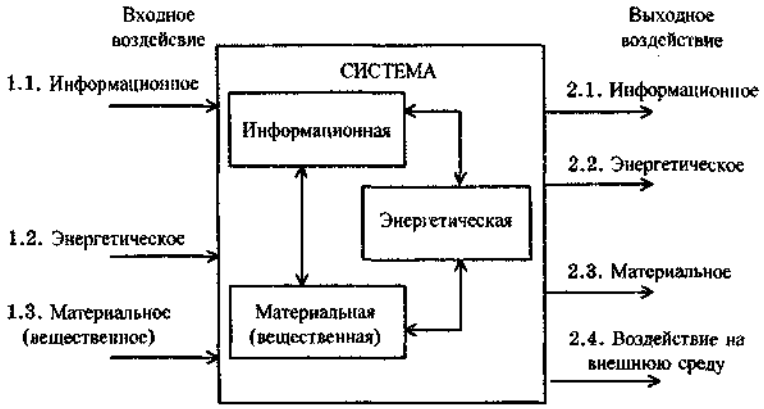

Рис. 1. Модель информационного объекта

Модель информационного объекта защиты формирует типовые объекты. Типовые объекты защиты, взаимодействуя с внешней средой (рис. 1), создают доля различной природы (тепловые, акустические, электромагнитные, включая поля оптического диапазона и др.), которые определяют информационное пространство. Информационное взаимодействие объектов обусловливает формирование информационных полей.

Исследования включают данные о признаковых (информационных) полях, возмущенных или излучаемых системами, извлекаемыми средствами перехвата и обработки.

Исследование явлений предполагает абстрагирование от многих свойств реальных носителей информации, несущественных для моделирования информационных процессов. Моделирование информационных процессов одной природы процессами другой физической природы, имеющими ту же самую информационную сущность, позволяет представить объект в виде взаимодействия информационных систем между собой и с окружающей средой (рис. 1).

Каждая система имеет свои элементы, свою внутреннюю структуру, связи, число переменных параметров, ограничения, связанные с ее взаимодействием в системе более высокого уровня через внешние связи, а также связи через окружающую среду и с окружающей средой.

Функционирование объектов скрывают от наблюдения и дезинформируют их истинные цели и назначение. Так, материальная и энергетическая системы

генерируют и излучают в окружающую среду акустические и вибрационные колебания.

Кроме того, подвижные объекты возмущают окружающую среду при движении в ней. Возмущенная окружающая среда (твердая, водная и воздушная) становится источником генерации и распространения в ней механических (акустических, вибрационных и виброакустических) колебаний. Например надводные и подводные корабли, взаимодействуют с водной и воздушной средами и создают такие же колебания. Информационная система генерирует колебания различной природы (магнитную и электрическую составляющие электромагнитного поля (ЭМП), акустическое поле — механические (вибрационные) колебания).

Система существует во взаимодействии с внешней средой и отличается внутренней структурой, связями и иерархией (см. рис. 1). Система обладает структурой, важнейшими частями которой являются подсистемы с явно выраженными локальными свойствами, которые по совокупности образуют систему более высокого уровня.

Системе присущи целенаправленность и управляемость, наличие общей цели и задач. Система высокого уровня имеет возможность корректирования подсистем, а также, не смотря на большую размерность, быть легко моделируемой (по числу элементов и разнородности функций). Каждый элемент системы связан с остальными таким образом, что изменение параметров этого элемента обусловливает изменение в остальных элементах и системе в целом. Системе присуща эмерджентность — наличие интегральных свойств, выводимых из известных свойств элементов системы и способов соединений.

Математическое моделирование позволяет при меньших затратах ресурсов решить задачу автоматизированного контроля канала утечки информации. Это, в первую очередь, относится к разработке новых перспективных информационных систем, их лабораторных и полигонных испытаний. Защита информации обеспечивает максимальную эффективность, если разрабатывается как подсистема определенной информационной системы.

Защита информации основана на согласовании информационной системы и системы защиты информации, на максимальной эффективности защищенности информационной системы. Защищенность обеспечивается маскированием сигналов в каналах утечки информации. Сведения о параметрах селекции, информационных параметрах сигналов, полях рассеивания и их наводках на неинформационные цепи, получены их оценкой (измерением). Сравнением измеренных параметров с нормированными значениями параметров устанавливают меру защищенности каналов от утечки информации.

Маскирование обеспечивает скрытие факта, места, времени, содержания, сведений о сигналах, снижение уровней сигналов и излучения полей рассеивания, исключающих извлечение информации и ее обработки. Дезинформация имитирует ложное представление об объекте защиты, информационных сигналах и полях, режимах функционирования объекта защиты.

Сосредоточенными и распределенными элементами информационной системы во взаимодействии с окружающей средой образуются каналы утечки информации, которые исследуются с учетом свойств и характеристик сообщений, сигналов, системы и окружающей среды.

Сообщение - форма представления информации для ее передачи, хранения, обработки или непосредственного использования.

Сигнал — изменяющаяся физическая величина, однозначно отображающая сообщение. В информационной системе сведения, содержащие информацию, составляют сообщение, которое преобразуется в сигналы.

Эффективность любой информационной системы оценивается совокупностью показателей, а если возможно, то обобщенным показателем, определяемым более высокого уровня системой. Одним из важных показателей является показатель безопасности информации. Этот показатель может определяться совокупностью частных показателей, в том числе и показателями защиты информации от утечки по техническим каналам различной физической природы.

В процессе моделирования каналов утечки информации и их элементов необходимо ввести частные и обобщенные показатели, характеризующие эф-