Министерство образования и науки Российской Федерации

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

А.Ф. Супрун

КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ РЕАЛИЗАЦИИ УГРОЗ

УЧЕБНОЕ ПОСОБИЕ

ЧАСТЬ 1

Санкт-Петербург
Издательство СПб ГПУ
2012

ББК 32.97
УДК 681.3
О-75

Супрун А.Ф., Комплексное обеспечение информационной безопасности. Моделирование процессов реализации угроз. Часть 1.
Учеб. пособие. СПб. Изд-во СПбГПУ, 2012. 50 с.
ISBN 5-93517-292-5

Пособие соответствует государственному образовательному стандарту дисциплины " Комплексное обеспечение информационной безопасности автоматизированных систем" направления подготовки специалистов 090105.65 "Комплексное обеспечение информационной безопасности автоматизированных систем".

Рассмотрены проблемы комплексного обеспечения информационной безопасности автоматизированных систем, проектирование систем обеспечения безопасности путем создания математических моделей процессов утечки информации. Приведена методика оценки рисков в автоматизированных системах. Пособие окажет большую помощь в написании курсовой работы по курсу ."Комплексное обеспечение информационной безопасности автоматизированных систем".

Предназначено для студентов пятого курса факультета технической кибернетики, изучающих курс "Комплексное обеспечение информационной безопасности автоматизированных систем" в рамках подготовки специалиста.

Табл. 1. Ил. 13. Библиогр.: 31 назв.

Печатается по решению редакционно-издательского совета Санкт-Петербургского государственного политехнического университета.

Автор выражают признательность заведующему кафедрой ИБКС профессору П.Д. Зегжда за поддержку и финансовое обеспечение издания пособия.

СОДЕРЖАНИЕ

	Предисловие	4
1.	Постановка проблемы комплексного обеспечения информационной безопасности АС. Методология формирования задач защиты и выбор моделей	6
2.	Обоснование и методика выявления каналов утечки информации	16
	2.1. Структура технического канала утечки информации.	16
	2.2. Разработка модели нарушителя-злоумышленника	20
3.	Модель мониторинга возможных каналов утечки информации	27
4	Разработка моделей защиты	35
	4.1. Разработка структуры, графа и математической модели защиты технических каналов утечки информации	35
	4.2. Модель подавления технических каналов утечки информации	40
ЗАКЛЮЧЕНИЕ		46
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ		48

Предисловие

Проблема защиты государственной тайны в процессе служебной или иной деятельности с использованием автоматизированных систем стоит крайне остро.

Одним из основополагающих организационных принципов обеспечения защиты государственной тайны является ограничение и стабилизация состава допущенных лиц, их тщательная предварительная проверка и сохранение определенного контроля за их деятельностью после прекращения контакта с информацией, составляющей государственную тайну.

Однако не менее важным является вопрос обеспечение защиты помещений от утечки закрытой информации по различным каналам и недопущение угрозы конфиденциальности со стороны нарушителя-злоумышленника.

В РФ требования к системам комплексной защиты информации формируются, главным образом, на основе руководящих документов Государственной технической комиссии. Однако эти требования носят декларативный и обобщенный характер, изложенный, в основном, на качественном уровне.

Этого явно недостаточно для построения перспективных и оценки существующих систем защиты. Возникает настоятельная потребность в научно-обоснованных, объектно-ориентированных и, желательно, количественно измеримых методах технико-экономической оценки информационной защищенности автоматизированных систем.

На сегодняшний день элементы системы информационной безопасности выбираются путем сравнительного анализа технических и экономических показателей предлагаемых на рынке средств защиты, которые включаются в состав комплексной системы защиты информации (КСЗИ).

Общие затраты на обеспечение информационной безопасности объекта согласно предъявляемым требованиям по защищенности определяются в

спецификациях средств реализации плана защиты информации. Необходимо учитывать, что прямое сокращение рекомендуемых средств защиты неминуемо приведет к определенным брешам в системе безопасности.

Контроль за выполнение правил политики информационной безопасности возлагается на должностных лиц. Решение о достаточности проведения технических защитных мер принимается на основе данных мониторинга.

Анализ исследований показывает, что угрозы безопасности носят комплексный характер, поэтому системы мониторинга и защиты должны быть так же комплексными.

Для осуществления мер безопасности любая организация должна нести определенные затраты. Очевидно, что наиболее благоприятным для организаций является такое положение, когда уровень затрат на обеспечение информационной безопасности является рациональным, при котором необходимое состояние нормального функционирования системы защиты обеспечивается при минимальных затратах.

Срок службы системы обеспечения информационной безопасности достаточно продолжителен. На протяжении срока службы несколько раз может измениться состав её технических средств. Исходя из этого, одним из основных вопросов, решаемых лицами, принимающими управленческие решения, является задача рационализации состава технических средств (как варианта системы), обеспечивающих сохранение её эффективности на протяжении жизненного цикла.

Выполнение оценок достаточности мер защиты и экономической целесообразности выбранного варианта требует разработки и исследования моделей угроз и защиты. Этому посвящена часть 1 пособия.

1. Постановка проблемы комплексного обеспечения информационной безопасности АС. Методология формирования задач защиты и выбор моделей

При решении задачи разработки мер защиты требуется проведение научных исследований, связанных с выполнением тактико-экономических оценок её эффективности. Важнейший элемент сравнительных оценок – это модели системы защиты и угроз информационной безопасности.

По известному определению модель – это некоторая промежуточная вспомогательная система (естественная или искусственная, материальная или абстрактная), обладающая следующими основными свойствами:

а) находится в объективном соответствии с познаваемым объектом (системой);

б) способная замещать в определённом отношении данный объект (систему);

в) предназначенная для выдачи информации о данном объекте, получаемой на основе исследования данной модели и соответствующих правил перехода модель – объект (прототип).

Т.е. обобщенно, моделирование определяется как метод опосредованного познания, при котором изучаемый объект-оригинал находится в некотором соответствии с другим объектом-моделью, причем модель способна в том или ином отношении замещать оригинал на некоторых стадиях познавательного процесса. Стадии познания, на которых происходит такая замена, а также формы соответствия модели и оригинала могут быть различными.

В данном случае нас интересует моделирование, заключающееся в построении некоторой системы-модели, связанной определенными соотношениями подобия с системой-оригиналом, причем в этом случае отображение одной системы в другую является средством выявления зависимостей между

двумя системами, отраженными в соотношениях подобия, а не результатом непосредственного изучения поступающей информации.

Существует большое количество различных видов моделирования, начиная от наглядного и заканчивая физическим, когда в модели сохраняют природу явлений и процессов, протекающих в реальном объекте исследования. В основе всех видов лежит теория подобия, которая утверждает, что абсолютное подобие может иметь место лишь при замене одного объекта другим точно таким же. При моделировании абсолютное подобие не имеет места, и стремится к тому, чтобы модель достаточно хорошо отображала исследуемую сторону функционирования объекта. В этом случае говорят об адекватности модели.

Наиболее распространенным видом моделирования различных процессов является математическое моделирование – это процесс установления соответствия данному реальному объекту некоторого математического объекта, называемого математической моделью.

В принципе, для исследования характеристик процесса функционирования любой системы математическими методами, включая и машинные, должна быть обязательно проведена формализация этого процесса, т. е. построена математическая модель. Ее исследование позволяет получать характеристики рассматриваемого реального объекта. Вид математической модели зависит как от природы реального объекта, так и от задач исследования объекта, требуемой достоверности и точности решения задачи. Она, как и всякая другая, описывает реальный объект с некоторой степенью приближения.

Для аналитического моделирования характерно то, что процессы функционирования элементов системы записываются в виде некоторых функциональных соотношений (алгебраических, интегро-дифференциальных, конечно-разностных и т.д.) или логических условий.

При имитационном моделировании реализующий модель алгоритм воспроизводит процесс функционирования системы во времени, причем имити-

руются элементарные явления, составляющие процесс, с сохранением их логической структуры и последовательности протекания во времени, что позволяет по исходным данным получить сведения о состояниях процесса в определенные моменты времени, дающие возможность оценить характеристики системы.

Комбинированное (аналитико-имитационное) моделирование позволяет объединить достоинства аналитического и имитационного моделирования. При построении комбинированных моделей производится предварительная декомпозиция процесса функционирования объекта на составляющие подпроцессы, и для тех из них, где это возможно, используются аналитические модели, а для остальных подпроцессов строятся имитационные модели. Такой подход позволяет охватить качественно новые классы систем, которые не могут быть исследованы с использованием только аналитического или имитационного моделирования в отдельности.

Информационное моделирование (часто называемое кибернетическим) связано с исследованием моделей, в которых отсутствует непосредственное подобие физических процессов, происходящих в моделях, реальным процессам. В этом случае стремятся отобразить лишь некоторую функцию и рассматривают реальный объект как «черный ящик», имеющий ряд входов и выходов, и моделируются некоторые связи между выходами и входами. Таким образом, в основе информационных (кибернетических) моделей лежит отражение некоторых информационных процессов управления, что позволяет оценить поведение реального объекта. По своим основным свойствам информационное моделирование в определенной степени перекликается с имитационным, используя его сильные стороны.

Структурно-системное моделирование базируется на некоторых специфических особенностях структур определенного вида, используя их как средство исследования систем или разрабатывая на их основе с применением других методов формализованного представления систем (теоретико-

множественных, лингвистических и т. п.) специфические подходы к моделированию.

При создании систем, использующих различные методы моделирования следует предъявлять к методам различные требования. Среди основных можно назвать гибкость и информационную полноту.

Гибкость системы моделирования подразумевает возможность моделирования различных предметных областей при помощи одинаковых моделей. Это достигается путем использования наиболее универсальных методов. Информационная полнота – возможность моделирования максимально большого количества характеристик объектов предметной области.

В большинстве случаев для проведения моделирования выбирается метод математического моделирования: аналитическое, информационное и структурно-системное. Хотя это не отрицает использования и иных методов, более соответствующих поставленной задаче, и применения всевозможных их комбинаций.

Анализ показывает, что существуют общие требования, на которых должен базироваться процесс построения модельного ряда:

– адекватность;

– комплексность – ключевой параметр, обеспечивающий выполнение всех защитных функций в рамках единой системы;

– информационное единство – унификация способов представления объектов предметной области во всех элементах системы;

– открытость и развиваемость – возможность изменения или расширения модельного ряда.

Для моделирования ряда процессов очень часто приоритет отдается адекватности модели.

Особо актуальной при моделировании является проблема адекватности модели моделируемому процессу. В [4] отмечено, что качество любых моде-

лей оценивается, прежде всего, их полезностью для решения задачи, а не с точки зрения адекватности объектам моделирования.

Адекватность модели можно оценить, сравнивая её с эталоном, либо с результатами эксперимента. Деятельность человека создаёт и эксплуатирует сложные системы, экспериментальное применение которых весьма проблематично, также как и использование моделей – эталонов. Поэтому предложен следующий критерий адекватности: мера объективного соответствия модели познаваемому объекту характеризуется тем, насколько полно в модели отражены основные закономерности существования этого объекта.

Достоверность получаемых результатов, выводов и рекомендаций любого научного исследования, содержащего модель, определяется тремя факторами:

– обоснованной адекватностью модели;

– обоснованными исходными данными;

– логичным следованием выводов и рекомендаций из результатов исследования модели.

Такая структура исследований, обоснования их достоверности отвечает принципам системного подхода.

Необходимо отметить, что понятие адекватности существенно зависит от класса используемых моделей. Связано это с тем, что понятие «модель» имеет два смысловых уровня. В широком смысле модель включает описательную, формальную, алгоритмическую и программную формы её реализации, а в узком – не включает алгоритм и программу.

В плане решения инженерных задач с применением вероятностно-статистических моделей, при должной квалификации авторов по технологии соответствующего аппарата, в отношении выполнения требований по адекватности проблематичными не представляются.

Основная часть прикладных задач, проблематичных с точки зрения построения и использования вероятностных моделей, относится к системно

сложным объектам (ССО) к которым, безусловно, относятся системы обеспечения информационной безопасности.

Эти ССО имеют в своей структуре организационные, организационно-технические и технические составляющие.

Одним из важнейших атрибутов ССО является целенаправленное поведение.

В процессе достижения цели система защиты, так или иначе, взаимодействует с внешней средой, которая может быть нейтральной, а чаще всего - «враждебной».

Основное место в структуре адекватности занимает содержательная корректность, как необходимое условие адекватности. Для формальных моделей соблюдением ряда принципов, в качестве одного из которых выступает принцип иерархии.

Необходимо заметить, что поведенческие вероятностные модели способны давать более или менее надежные результаты только для массовых явлений, систем большой численности единичных актов.

Для описания поведенческих действий злоумышленников вероятностные модели малопригодны, но в отсутствии других исследователь вынужден остановить свой выбор на них.

Таким образом, можно констатировать, что для организационных и организационно-технических систем, участвующих в противоборстве, вероятностные модели способны привести к надежным оценкам только в отношении их обобщенных интегральных характеристик-потенциалов. Для этих оценок в вероятностной мере могут быть установлены критерии любых известных категорий для принятия решений по применению систем.

На рис. 1. приведена структура факторов адекватности, заимствованная из сборника научных докладов на семинарах по системному анализу, проводимых под руководством профессора И.Г. Захарова.

Содержательный аспект обеспечивается постановочной частью задачи. Аппаратный (инструментальный) аспект обеспечивается аппаратом моделирования с учетом постановочной части: существование, единственность, устойчивость решений (результатов).

Точность является инструментальным условием достаточности, а полезность и прагматичность – её содержательным условием.

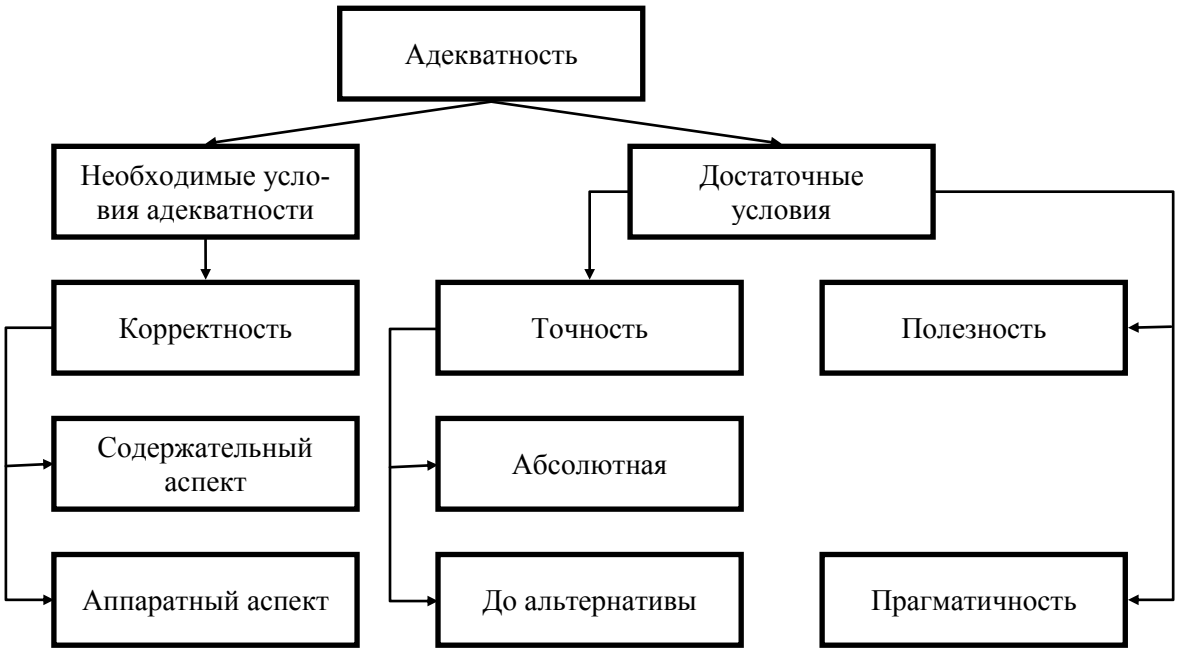


Рис. 1. Структура факторов (аспектов) адекватности

В основу модели системы информационной защиты в рамках данного исследования положена система моделирования предметной области, обладающая следующими свойствами:

– основным методом моделирования является математическое с использованием преимущественно аналитических моделей;

– моделируется как динамика процесса, так и его структура, т.е. отношения между составляющими его субъектами;

– моделируются не только количественные, но и качественные (смысловые) характеристики процессов и объектов их составляющих.

Выделяя состав задач, подлежащих решению в рамках данной работы, можно сформулировать следующий список:

– сбор информации о предметной области;

– моделирование процессов предметной области;

– анализ протекающих процессов;

– оценка состояния предметной области;

– прогнозирование развития рассматриваемых процессов;

– оптимизация процессов предметной области;

– мониторинг процессов, протекающих в предметной области.

Под сбором информации о предметной области понимается процесс, состоящий из сбора информации о составе предметной области (субъектах и ресурсах), структуре (схемы процессов преобразования ресурсов, характеризующие взаимоотношения между субъектами), качественных и количественных характеристиках элементов процессов. Иными словами его можно назвать ведением процессов предметной области. Для этого необходимо решить задачу классификации объектов, определить модель представления процессов и их составляющих. Наиболее соответствующим задаче является иерархическое представление, когда объекты предметной области, процессы, протекающие в ней, составлены из элементарных операций (унифицированных по своему характеру), декомпозированы до определенного уровня и упорядочены по соответствующим уровням. Манипулирование уровнем декомпозиции позволяет повысить глубину (детализацию) анализа, что приведет к повышению качества аналитической информации. Таким образом, в составе структуры модельного ряда в данной предметной области должны присутствовать:

– модули, позволяющие описывать объекты предметной области в виде иерархических моделей;

– схемы протекающих процессов;

– качественные и количественные характеристики объектов и элементов процессов.

Отметим, что физические поля, по которым происходит утечка конфиденциальной информации, продуцированные в ходе ведения служебной или

иной деятельности с использованием объекта информатизации, изменяются как во времени, так и в пространстве, то есть, являются функциями координат точки *x*, *y*, *z* относительно источника поля и времени.

При исследовании применительно к *i*-му каналу, данную физическую величину будем называть потенциалом поля излучения ($U_{\text{и}}^{i}$)

$$U_{\text{è}}^{i} = U_{\text{è}}^{i}(x, y, z) \tag{1}$$

где: *x*, *y*, *z* – координаты источника поля (с учетом этажности здания)

Совокупность значений полей в пространстве на заданный момент времени будем называть полем утечки конфиденциальной информации.

По аналогии, для организации активной защиты и оценки достаточности защитных мер введем понятие потенциала поля подавления (ПП).

$$U_{\text{п}}^{i} = U_{\text{п}}^{i}(x, y, z) \tag{2}$$

где: *x*, *y*, *z* – координаты установки источника подавления поля.

В дальнейшем координатам будут присваиваться соответствующие индексы.

Для характеристики пространственного распределения величин потенциалов в фиксированный момент времени вводится понятие эквискалярной поверхности, в каждой точке которой величина соответствующего поля сохраняет свое постоянное значение:

$$U_{\text{и}}^{i} = U_{\text{и}}^{i}(x, y, z) = C; \quad U_{\text{п}}^{i} = U_{\text{п}}^{i}(x, y, z) = C \tag{3}$$

где С – постоянная для заданной эквискалярной поверхности при фиксированном времени *t*.

Расчет численных значений потенциалов (или амплитуд) физических полей утечки и полей подавления различной природы производится с использованием известных методик (формул).

Кривые пересечения эквискалярной поверхности с любой другой поверхностью (как правило, параллельной поверхности земли) называются изолиниями величины потенциала поля. Описание изолиний имеет большое значение, так как позволяет в дальнейшем производить построение координатных законов подавления информативного сигнала (поля).

Следует заметить, что информативные поля и поля средств их подавления можно рассматривать с двух принципиально различных позиций: как детерминированные или случайные поля. Соответственно и результаты, получаемые на основе разных представлений полей будут носить детерминированный или вероятностный характер.

Задача заключается в проведении моделирования процессов предметной области, описанных в виде схем в соответствии с характеристиками объектов и процессов. При этом моделирование может проводиться по данным, описывающим реальные процессы (для получения недостающей информации), а также по модельным (игровым) данным. Это позволяет оценить различные варианты развития процессов.

Решение задач анализа процессов и оценки их состояния заключается в получении, на основе модельных данных, значений выбранных аналитических показателей и выработке качественного заключения о характере протекания процессов и состоянии предметной области.

Роль прогнозирования развития процессов, протекающих в предметной области, состоит в том, что, базируясь на вышеописанных средствах моделирования процессов, использовании современного математического аппарата прогнозирования, можно получить данные о состоянии предметной области в будущем.

Оптимизация процессов заключается в поиске схем процессов, количественных и качественных характеристик их составляющих, направленном на достижение заданного или наилучшего результатов.

Мониторинг процессов, протекающих в предметной области, заключается в проведении вышеописанных задач сбора информации, моделирования, анализа, оценки и прогнозирования в реальном времени (или модельном, в случае использования системы в режиме проигрывания различных вариантов развития процессов).

Создание систем информационной защиты на современном уровне развития средств нарушения политики безопасности является сложной задачей, но необходимая научно-методическая и технологическая базы уже имеются. Не менее сложной, но вполне выполнимой задачей является задача оценки достаточности мер защиты.

2. Обоснование и методика выявления каналов утечки информации.

2.1. Структура технического канала утечки информации.

Анализируемые виды угроз следует выбрать из соображений здравого смысла, но в пределах выбранных видов провести максимально полное рассмотрение.

Оценивая вероятность осуществления угроз, целесообразно учитывать не только среднестатистические данные, но и специфику конкретных информационных систем. Для проведения анализа уязвимости целесообразно иметь в распоряжении исследователя модели каналов утечки информации и НСД (несанкционированный доступ), методики определения вероятности информационного контакта, модель нарушителя, перечень возможностей информационных инфекций, способы применения и тактико-технические возможности технических средств ведения разведки, методику оценки информационной безопасности.

Наглядной иллюстрацией (моделью) связи объектов информатизации (защиты), каналов реализации угроз и способов защиты может служить «ку-

бик» безопасности применительно к учебному процессу (рис. 2.).

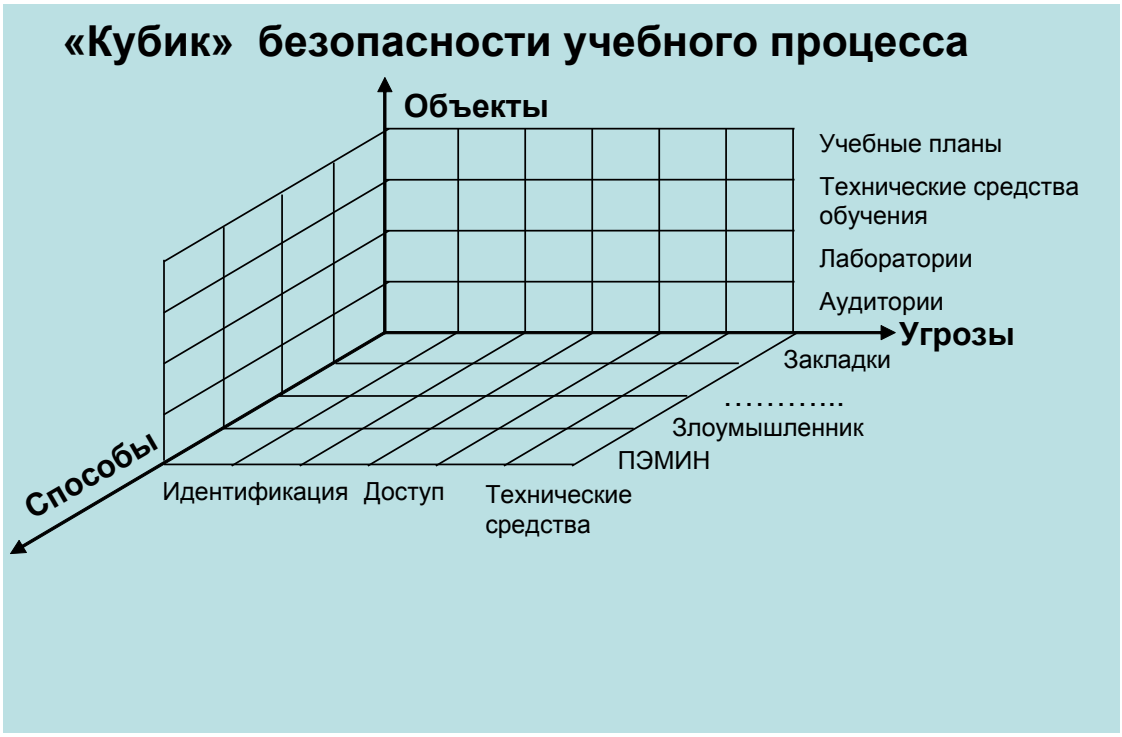


Рис. 2. Модель связи объектов, угроз и способов защиты

Анализ уязвимости начинается с выбора анализируемых объектов и определения степени детальности их рассмотрения. На этом этапе большую помощь может оказать разработанная инфологическая структура объекта. Для определения объектов защиты можно рассматривать АУТК как многоуровневую систему. На каждом уровне определяются уязвимые элементы АУТК.

Следующим шагом на пути анализа уязвимости АУТК является моделирование каналов утечки информации и НСД. Любые технические средства по своей природе потенциально обладают каналами утечки информации.

Под каналом утечки информации понимается физический путь от источника конфиденциальной информации, по которому возможна утечка охраняемых сведений, к злоумышленнику. Для возникновения (образования, установления) канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства приема и фиксации информации на стороне злоумышленника.

Основная задача моделирования каналов утечки информации и соответ-

ствующих способов несанкционированного доступа к источникам конфиденциальной информации на типовом объекте АУТК — выявление особенностей, характеристик, условий возникновения каналов и в результате получение новых знаний, необходимых для построения системы защиты информации.

Любая модель канала утечки информации должна показывать не только сам путь, но и возможность (вероятность) установления информационного контакта.

Структура технических каналов утечки конфиденциальной информации в процессе служебной деятельности с использованием охраняемых технических систем информатизации, разрабатываемых образцов и макетов, а также тренажеров-имитаторов представлены на рис. 3. [3]

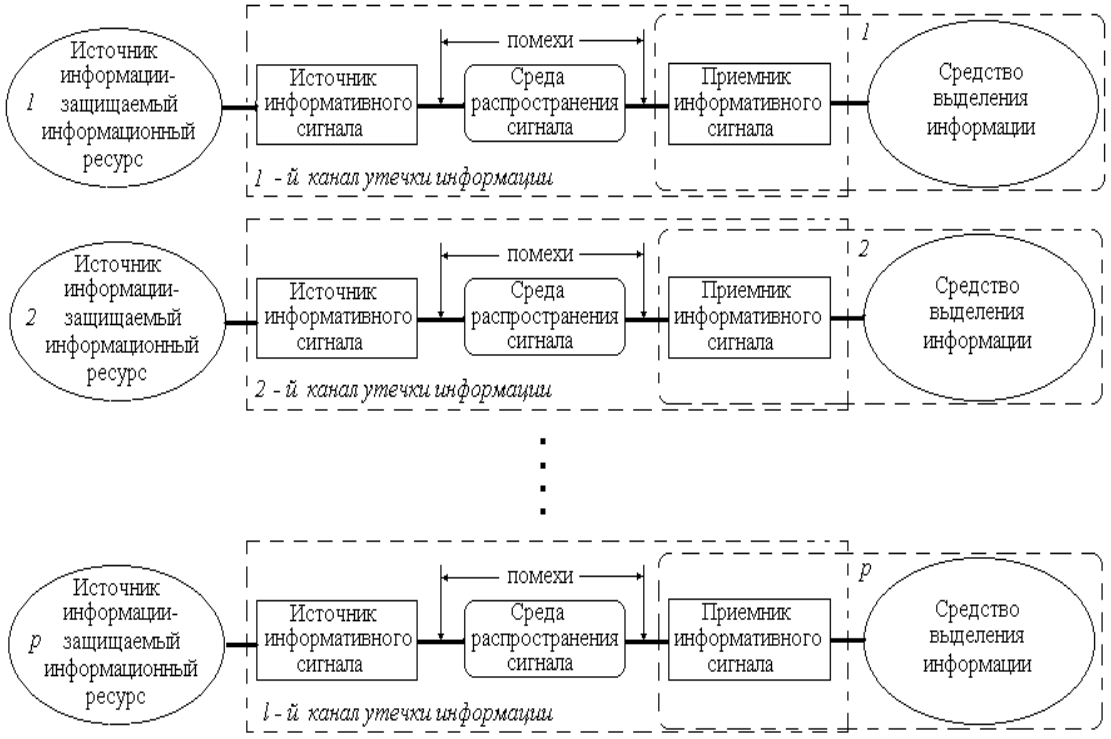


Рис. 3 Структура каналов утечки информации

Вероятность установления информационного контакта — численная величина, определяемая пространственными, временными и энергетическими условиями и характеристиками средства наблюдения.

Условия установления информационного контакта можно представить в

виде следующей обобщенной модели. Разнообразие источников конфиденциальной информации исследуемого объекта, способов несанкционированного доступа к ним и средств реализации несанкционированного доступа в конкретных условиях требует разработки частных моделей каждого варианта информационного контакта и оценки вероятности его возникновения. Имея определенные методики, можно рассчитать возможность такого контакта в конкретных условиях.

Главная ценность подобных методик заключается в возможности варьирования аргументами функции (мощность излучения, высота и коэффициент направленного действия антенны, технические характеристики средств информатизации и т.п.) в интересах достижения минимальных значений вероятности установления информационного контакта, а значит, и в поиске совокупности способов снижения ее значений.

Для анализа уязвимости информационных ресурсов объекта информатизации необходимо не только выявить каналы утечки информации, хорошо представлять облик нарушителя, вероятные способы его действий в условиях применения организационных и технических мер защиты, намерения, а также возможности технических средств получения информации по различным каналам. Только совокупность этих знаний позволит адекватно среагировать на возможные угрозы и, в конце концов, выбрать соответствующие средства защиты.

2.2. Разработка модели нарушителя-злоумышленника.

При разработке наиболее вероятного сценария осуществления противоправных действий по доступу к информации (нарушения) в конкретной системе, одной из важнейших составляющих является модель нарушителя. Наличие такого сценария, который должен постоянно корректироваться на основе новых знаний о возможностях нарушителя, после изменений в системе защиты и на основе анализа причин произошедших нарушений, позволит

повлиять на сами причины либо точнее определить требования к системе защиты от данного вида нарушений.

Основные контуры модели нарушителя определены в руководящем документе Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». В соответствии с этим документом в качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами объекта информатизации, являющийся специалистом высшей квалификации, знающий все об объекте и, в частности, о системе и средствах ее защиты.

Кроме уровня знаний нарушителя, его квалификации, подготовленности к реализации своих замыслов, для формирования наиболее полной модели нарушителя в АУТК необходимо определить:

– категорию лиц, к которым может принадлежать нарушитель:

– мотивы действий нарушителя (преследуемые нарушителем цели);

– техническую оснащенность и используемые для совершения нарушения методы и средства;

– предполагаемые место и время осуществления незаконных действий нарушителя;

– ограничения и предположения о характере возможных действий.

Вполне очевидно, что правильно построенная (адекватная реальности) модель нарушителя – та, в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия и т. п.

Характеристики – важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты. Модель должна постоянно корректироваться с учетом получения новых знаний о возможностях нарушителя и изменениях в системе защиты на основе анализа причин произошедших нарушений, что позволит повлиять на сами эти причины, а также точнее определить требования к системе защиты от данного вида нарушений.

Для того чтобы модель нарушителя приносила максимальную пользу, она должна быть сориентирована на конкретный объект защиты (модель не может быть универсальной), учитывать мотивы действий и социально-психологические аспекты нарушения, потенциальные возможности по доступу к информационным ресурсам различных категорий внешних и внутренних нарушителей на различных пространственно-временных срезах объекта защиты.

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно, поэтому модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика.

Нарушитель – злоумышленник представляет собой лицо, осознанно предпринявшее попытку выполнения запрещенных операций и использующее для этого различные возможности, методы и средства. Любой нарушитель для реализации своих замыслов руководствуется определенной мотивацией и намерениями, владеет совокупностью знаний, умений и навыков (способов) совершения противоправных действий с применением технических средств, обладающих соответствующим потенциалом. Только совокупность знаний обо всех элементах облика нарушителя позволит адекватно среагировать на возможные угрозы и, в конце концов, выбрать соответствующие средства защиты.

Кроме того, реальные возможности нарушителя во многом определяются и состоянием объекта защиты, наличием потенциальных каналов утечки информации, качеством средств защиты информации. От надежности системы защиты информации зависят и действия нарушителя, так как для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы.

Однако умения и навыки могут быть реализованы при условии нахождения в определенных точках (помещениях) объекта, из которых можно реализовать угрозу. Поэтому, кроме уровня знаний нарушителя, его квалификации, подготовленности к реализации своих замыслов, для формирования наиболее полной модели нарушителя необходимо определить категорию лиц, к которым может принадлежать нарушитель.

При формировании модели нарушителя необходимо дифференцировать всех сотрудников не только по их возможностям доступа к системе, но и по возможным потерям от действия персонала, то есть по потенциальному ущербу от каждой категории пользователей.

Для уточнения возможного сценария нарушений модель нарушителя должна быть конкретизирована и расширена. С этой целью каждая категория вероятных нарушителей должна быть проанализирована отдельно по следующим параметрам:

– техническая оснащенность и используемые для совершения нарушения методы и средства;

– предполагаемые места и время осуществления незаконных действий нарушителя;

– ограничения и предположения о характере возможных действий.

Учет места и времени действий злоумышленника также позволит конкретизировать его возможности по доступу к информационным ресурсам и учесть их для повышения качества системы защиты информации.

Ограничения и предположения о возможном характере действий нарушителя могут основываться на различного рода статистических данных, опыте других предприятий и организаций, а также своем собственном и в значительной степени сузят область поиска нарушителя.

Каждый элемент модели нарушителя должен иметь продолжение как в виде причинно-следственных связей между отдельными блоками, так и в виде детализации информации, содержащейся и каждом блоке. Такая детализация

предполагает построение цепочек предполагаемых последствий наступления тех или иных заключений относительно облика нарушителя.

На рис. 4. представлен алгоритм учета факторов, определяющих облик нарушителя и позволяющий получить впоследствии некую матрицу нарушений информационной безопасности, связывающую атакуемые точки информационной системы, тип воздействия, место и время обнаружения нарушения с категорией пользователя. Такая матрица в случае возникновения нарушения позволит локализовать возможные негативные последствия.

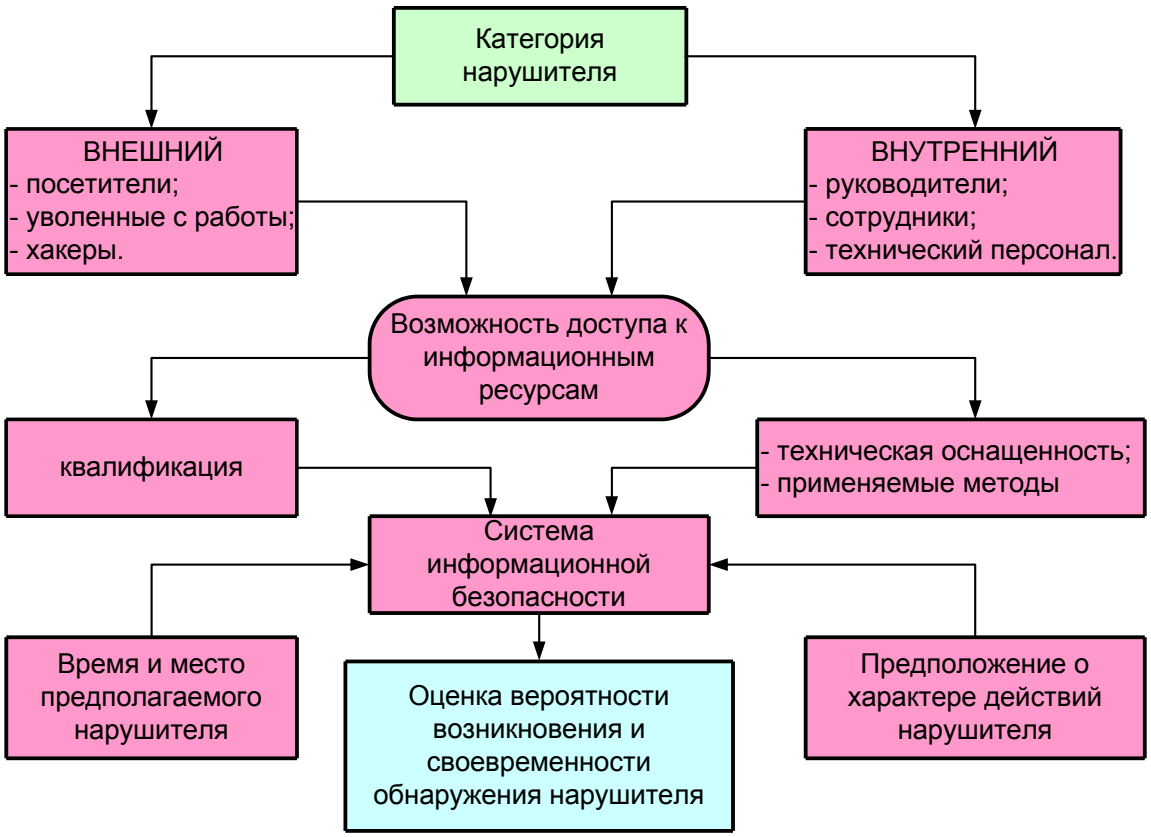


Рис. 4 Алгоритм учета факторов, определяющих облик нарушителя.

Ограничения и предположения о возможном характере действий нарушителя могут основываться на различного рода статистических данных, опыте других предприятий и организаций, а также своем собственном и в значительной степени сузят область поиска нарушителя.

В формализованном виде модель нарушителя-злоумышленника с раскрытием содержания соответствующих вероятностей представлена на рис. 5.

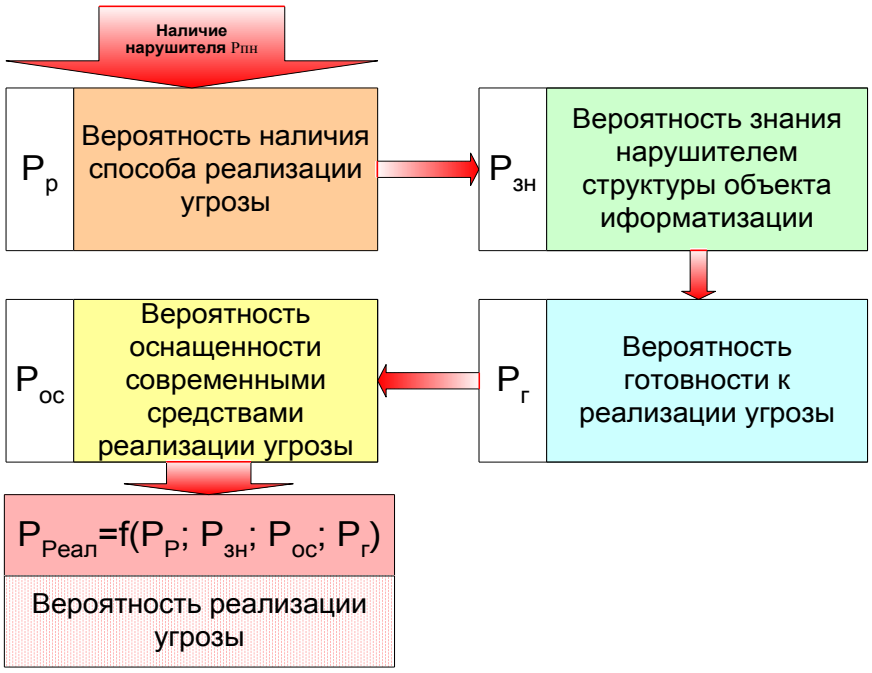


Рис. 5. Структура модели нарушителя-злоумышленника

В заключение необходимо еще раз подчеркнуть, что модель нарушителя является важной составляющей для качественного анализа риска и определения требований к составу и характеристикам системы защиты. Модель нарушителя – это не статическое образование. Она должна постоянно изменяться и корректироваться с учетом появления новых данных о возможностях нарушителя и изменениях в системе защиты. Кроме того, модель нарушителя может быть представлена в нескольких вариантах, так как наличие совокупности моделей нарушителя позволит прогнозировать возможные события по проникновению и систему во всем разнообразии складывающихся ситуаций и построить надежную систему зашиты информации, используя современные средства интеллектуальной поддержки для управления системой защиты.

В результате исследований причин нарушений установлено, что главный источник НСД может находится внутри самой структуры : до 85% нарушений совершаются самими служащими организации, имеющими до-

ступ к ее системе, и только 15-25% нарушений совершаются лицами со стороны.

При формировании модели нарушителя и оценке риска от действий персонала необходимо дифференцировать всех сотрудников организации по возможности доступа и, следовательно, по потенциальному ущербу от каждой категории пользователей. Кроме того, необходимо учитывать, что пользователи различных категорий различаются не только по степени риска, но и по тому, какому элементу системы они угрожают больше всего. В результате можно оценить степень риска данной категории пользователей относительно данного элемента системы и представить результаты анализа в виде таблицы соответствий.

Приведенный подход к категорированию персонала системы по степени риска должен использоваться для определения возможностей каждого типа нарушителя по незаконному доступу к информации, циркулирующей в организации.

При формировании модели нарушителя в организации следует уделять особое внимание личности нарушителя. Это поможет разобраться в побудительных мотивах и принять соответствующие меры для уменьшения вероятности совершения нарушений.

В целях овладения конфиденциальной информацией нарушители широко используют современные технические средства, обеспечивающие реализацию рассмотренных способов НСД к объектам и источникам охраняемых сведений.

Приведенная классификация предусматривает, прежде всего, постоянное обновление информации о характеристиках технических и программных средств ведения разведки и обеспечения доступа к информации. Учет места и времени действий злоумышленника также позволит конкретизировать его возможности и учесть их для повышения качества системы защиты информации.

Наличие совокупности моделей действий нарушителя может быть полезной с точки зрения прогнозирования возможных событий во всем разнообразии складывающихся ситуаций, предотвращения действий нарушителя, построения надежной системы защиты информации, использования современных средств интеллектуальной поддержки для управления системой защиты.

3. Модель мониторинга возможных каналов утечки информации

В общей системе мер по защите возможных каналов утечки информации приоритет должен быть отдан комплексу мероприятий, направленных на снижение риска нарушения конфиденциальности. Для управления риском осуществляется мониторинг состояния среды распространения информационных сигналов, анализ риска при реализации угрозы.

Под мониторингом [англ. monitoring от лат. Monitor – предостерегающий] понимается определенная система наблюдения (а также оценки и прогноза) состояния и развития различных процессов и явлений. Он заключается в слежении за состоянием определенных структур, объектов, явлений и процессов, а его результаты используются для предупреждения о создающихся опасностях, угрозах и критических ситуациях и обеспечения органов управления информационной поддержкой для подготовки и принятия управленческих решений по изменению в нужном направлении состояния и развития системы и процесса.

Применительно к объектам информатизации мониторинг – это постоянный сбор информации, наблюдение и контроль за объектом, включающий процедуры анализа риска, измерения параметров сигналов, способных нести конфиденциальную информацию.

Данные мониторинга служат основой для анализа риска и прогнозирования. Целью прогнозирования реализации угрозы конфиденциальности ин-

формации является выявление времени ее возникновения, возможного места, масштаба и последствий для безопасности государства.

Как правило, контроль за соблюдением правил политики информационной безопасности осуществляется специалистами Гостехкомиссии РФ. Однако, для разработки планов защиты организации, определения рационального состава средств защиты, поддержанию системы защиты в работоспособном состоянии руководству организации целесообразно иметь собственную систему контроля ИБ.

Существует большое число видов мониторинга, различающихся по учитываемым источникам и факторам, методам наблюдений и т.п. На рис. 6 приведена классификация видов мониторинга.

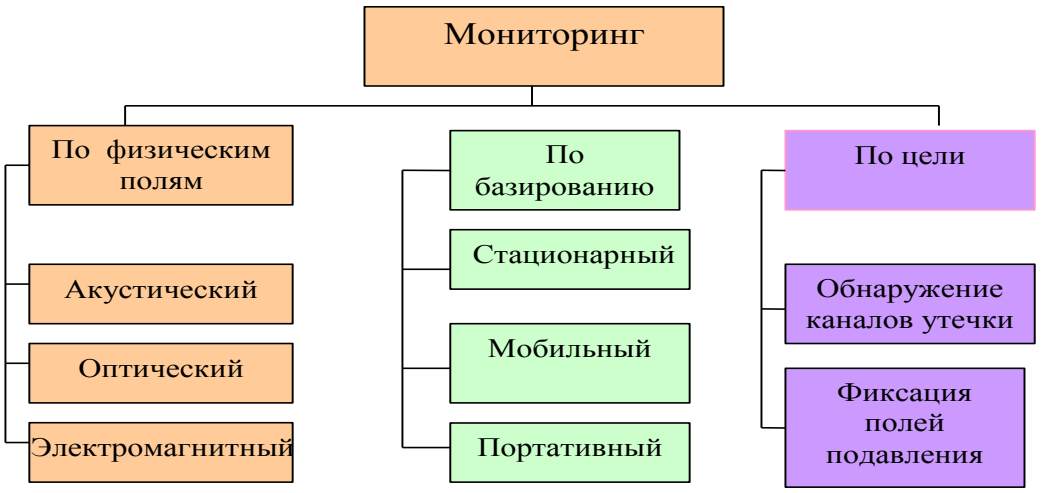


Рис. 6. Классификация видов мониторинга каналов утечки информации.

Целью контроля системы защиты информации аудиторных и лабораторных помещений также является установление соответствия требованиям стандартов и других нормативных документов по защите информации, применительно к следующим возможным каналам ее утечки:

– прямому акустическому перехвату информации с использованием направленных микрофонов;

– виброакустическому каналу перехвата информации с использованием разведывательных стетоскопов с ограждающих конструкций и инженерно-технических коммуникаций;

– оптикоакустическому каналу перехвата информации с использованием лазерных систем дистанционного прослушивания;

– каналу утечки информации за счет акустоэлектрических преобразований в вспомогательных технических средствах и системах (ВТСС);

– каналу утечки информации за счет высокочастотного навязывания;

– каналу утечки информации за счет ПЭМИН (побочное электромагнитное излучение наводки) звукоусилительной и звуковоспроизводящей аппаратуры;

– непреднамеренному подслушиванию с контролируемой территории;

– каналу утечки информации за счет внедренных радиоэлектронных устройств перехвата информации в импортных ВТСС.

Устройствами, предназначенными для выявления и локализации работающих подслушивающих устройств, радиомикрофонов являются индикаторы (детекторы) поля или излучений. Индикаторы поля по сути являются широкополосными высокочастотными усилителями и реагируют на любой сигнал в рабочем диапазоне частот. Модели индикаторов отличаются сервисными функциями: рабочим диапазоном частот, наличием акустозавязки, возможностью измерения частоты, видами индикации, конструктивным исполнением. Поиск с использованием индикаторов поля осуществляется следующим образом. При обходе помещения фиксируются места с повышенным уровнем электромагнитного поля, далее регулируя порог срабатывания индикатора (изменяя чувствительность), локализуют место нахождения источника излучения и производят физический поиск источника.

Скоростные поисковые приемные устройства ближней зоны предназначены для обнаружения работающих миниатюрных подслушивающих устройств и радиомикрофонов. Их отличительной особенностью является

высокая скорость перестройки в рабочем диапазоне частот. Скоростные поисковые приемники позволяют прослушивать принимаемые сигналы, что для моделей этого класса является основным признаком, помогающим оператору опознавать опасные сигналы. В некоторых моделях предусмотрена индикация уровня принимаемого сигнала.

Обнаружение устройств несанкционированного съема информации в автоматическом (без участия оператора) и в ручном режимах обеспечивают автоматизированные комплексы, работающие под управлением соответствующего программного обеспечения (ПО). Они предназначены для бесшумного автоматического контроля и обнаружения подслушивающих устройств: анализа радиодиапазона, инфракрасного диапазона, телефонных, проводных и силовых линий.

С целью получения конфиденциальной информации часто используются проводные коммуникации. Это может быть прослушивание телефонных переговоров с передачей информации по радиоканалу или по проводам, прослушивание помещений с помощью микрофонов подсоединенных к слаботочным коммуникациям или неиспользуемым (старым) проводам, а также прослушивание помещений через оконечные устройства методом высокочастотного навязывания (ВЧ-навязывания). Для обнаружения проводных подслушивающих устройств и оценки возможности их применения используются анализаторы проводных линий.

Существуют также универсальные поисковые устройства, предназначенные для выявления различных технических каналов утечки информации, в том числе обнаружения и определения местонахождения работающих радиомикрофонов, обнаружения сигналов, передаваемых по проводам (в том числе по электрической сети, находящейся под напряжением), обнаружения источников ИК-излучения, оценки акустической и виброакустической защищенности помещений, а также для контроля качества защиты информации.

Все перечисленные выше устройства предназначены для выявления только работающих устройств несанкционированного съема информации. Однако существуют устройства съема с дистанционным управлением, с накоплением информации или с источниками питания с законченным ресурсом, выявление которых также необходимо, т.к. их наличие указывает на проявляемый интерес. Такого рода устройства съема обнаруживаются приборами, называемыми нелинейными локаторами. Принципы, на которых основана работа нелинейных локаторов, позволяют производить поиск электронных устройств, независимо от их состояния, т.е. активизировано (включено) оно или нет, и в том числе позволяют обнаруживать отдельные *p-n* переходы, например, одиночные полупроводниковые диоды.

Антенна прибора создает в контролируемой зоне электромагнитное поле (зондирующий сигнал). При наличии в зоне контроля радиоэлектронного устройства любого назначения в нем происходит преобразование частоты зондирующего сигнала в высшие кратные гармоники с последующим их переизлучением в окружающее пространство.

Вторая и третья гармоники отраженного от устройства сигнала принимаются антенной и регистрируются приемником прибора. Максимальный отклик от полупроводниковых элементов наблюдается на второй гармонике зондирующего сигнала. При облучении окисных пленок, образованных естественным путем, максимальный отклик наблюдается на третьей гармонике зондирующего сигнала. Информация о факте обнаружения выдается: в виде звукового сигнала в головных телефонах или в виде световых сигналов на индикаторах уровня красного цвета при обнаружении электронного объекта или на индикаторах зеленого цвета при обнаружении контактной нелинейности (индикаторы размещены на антенном датчике).

Нелинейный локатор является одним из наиболее необходимых приборов для выявления технических каналов утечки информации, так как обнаружить неизлучающие устройства съема информации (например, радиомик-

рофоны с дистанционным управлением или с накоплением информации) другими методами или приборами невозможно.

При работе с нелинейным локаторам пользователь, "сканируя" антенной поверхности мебели и строительных конструкций, получает различные отклики. Наиболее сложной при этом является задача распознавания откликов от электронных устройств и коррозионных диодов. Для облегчения работы оператора по распознаванию сигналов от полупроводниковых устройств и коррозионных диодов используются: прием отраженных сигналов на 2-й и 3-й гармониках, т.к. уровень отраженного сигнала на 2-ой гармонике от электронного устройства как правило превышает уровень сигнала от коррозионных диодов, а на 3-ей гармонике наблюдается обратная картина; режим выделения огибающей 20 кГц (используется в локаторах с импульсным излучением) также облегчает распознавание отраженных сигналов; режим отключения модуляции зондирующего сигнала позволяет, прослушивая сигналы откликов, распознавать истинные или ложные сигналы, в том числе прослушивать работающие радиомикрофоны.

Отечественная промышленность выпускает достаточно большое число технических средств контроля уровней утечки информационного сигнала и контроля эффективности активных и пассивных средств защиты, имеющих сертификаты ГТК (Гостехкомиссия РФ) (табл. 1).

Технические средства контроля

Таблица 1.

Наименование измерительной аппаратуры	Назначение измерительной аппаратуры
Комплект селективного микровольтметра UNIPAN-233 в составе: селективный микровольтметр UNIPAN-233; Комплект антенн измерительных рамочных ШС2.090.000 … ШС2.090.008; Антенна электрическая АЭ-1	Для оценки защищенности от утечки информации за счет: - ПЭМИН; - наводок в сети электропитания и заземления, обусловленных паразитными связями и неравномерностью токопотребления
Комплект измерителя напряженности поля радиопомех FSM – 11 в составе: селективный микровольтметр SMV-11; антенна измерительная FMA-11; токосъемные клещи SMZ-11; пробник напряжения ТК-103	Для оценки защищенности от утечки информации за счет: - ПЭМИН; наводок в сети электропитания и заземления, обусловленных паразитными связями и неравномерностью токопотребления. Оценка реального затухания сигналов ПЭМИН на трассе: АУТК – граница контролируемой зоны
Комплект измерителя напряженности поля радиопомех FSM – 8,5 в составе: селективный микровольтметр SMV-8,5; антенна измерительная DP-1; - антенна измерительная DP-3	Для оценки защищенности от утечки информации за счет: - ПЭМИН; оценка реального затухания сигналов ПЭМИН на трассе: ТС (технические средства) – граница контролируемой зоны
Осциллограф	Для визуального наблюдения информативных сигналов
Комплект селективного транзисторного комплекта STV-301-2 в составе: Селективный транзисторный вольтметр STV-301-2; Антенна измерительная STA-101; Антенна измерительная FSA-101	Для оценки защищенности от утечки информации за счет наводок в сети электропитания и заземления, обусловленных паразитными связями и неравномерностью токопотребления
Генераторы высокочастотные Г4–107, Г4-102	Оценка реального затухания сигналов ПЭМИН на трассе: ТС – граница контролируемой зоны

Таким образом, можно констатировать, что оценка риска утечки конфиденциальной информации не может быть выполнена без мониторинга возможных технических каналов и обобщения полученных данных. Эта задача решается с использованием комплексной системы мониторинга. Структура модели системы приведена на рис. 7.

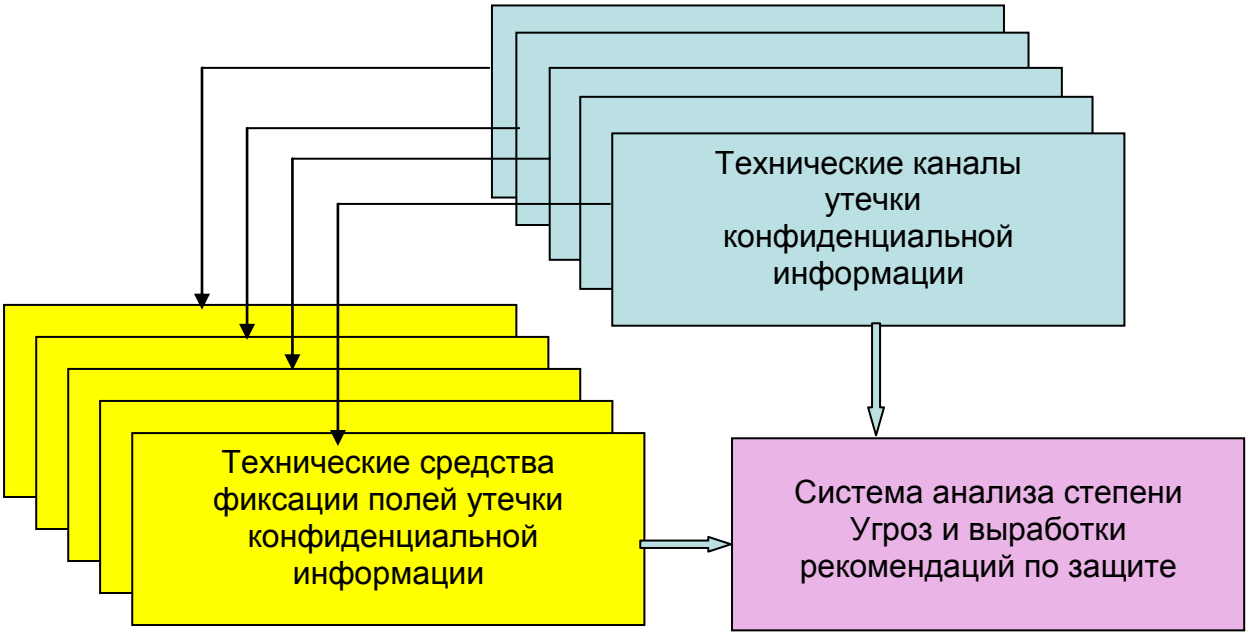


Рис. 7. Структура модели комплексной системы мониторинга.

В общем случае мониторинг должен обеспечить выявление «брешей» в системе защиты, позволить оценить вероятность утечки конфиденциальной информации по всей совокупности каналов и оценку достаточности (эффективности) защитных мероприятий.

Возможность утечки сигнала, несущего информацию конфиденциального характера (наличие «бреши» в системе защиты) предлагается оценивать с использованием математической модели вида:

$$D_{U_1} \vee D_{U_2} \vee \ldots \vee D_{U_j} \vee \ldots \vee D_{U_y} \rangle R_k \qquad (4)$$

где: D_{Uy} – дальность распространения информационного сигнала j-го канала;

R_k – радиус контролируемой (охраняемой) зоны.

Вероятность реализации угрозы конфиденциальности $P_{ут}$ может быть рассчитана по формуле:

$$P_{ут} = 1 - \prod_{j=1}^{y} \prod_{i=1}^{I} (1 - P_{j.i}) \quad (5)$$

где $P_{j.i}$ – вероятность утечки информации по *j*-му каналу в *i*-м диапазоне

Задача, стоящая перед комплексной системой защиты может считаться выполненной при выполнении условия:

$$\frac{U_n}{U_{n_1}}(R_k) \wedge \frac{U_n}{U_{n_2}}(R_k) \wedge \ldots \wedge \frac{U_n}{U_{n_j}}(R_{jk}) \wedge \frac{U_n}{U_{y_2}}(R_k) \rangle 1 \quad (6)$$

гдеU_n, U_{n_j} – потенциалы полей подавления и излучения соответственно.

Данный математический аппарат модели комплексной системы мониторинга позволит количественно оценить вероятность утечки информации по всей совокупности каналов и достаточность мер защиты.

4. Разработка моделей защиты

4.1. Разработка структуры, графа и математической модели защиты технических каналов утечки информации.

На основе анализа возможных каналов утечки конфиденциальной информации на рис. 8 приведена структурная схема защиты *j*-го канала с использованием технических средств,

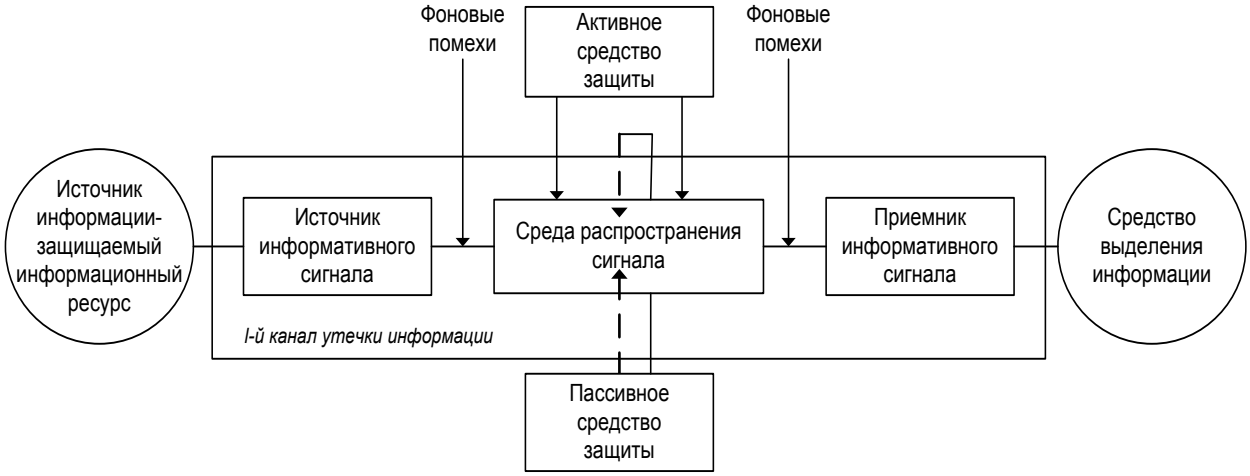


Рис. 8. Структурная схема защиты i-го канала.

а на рис. 9 - граф модели защиты технического канала утечки информации.

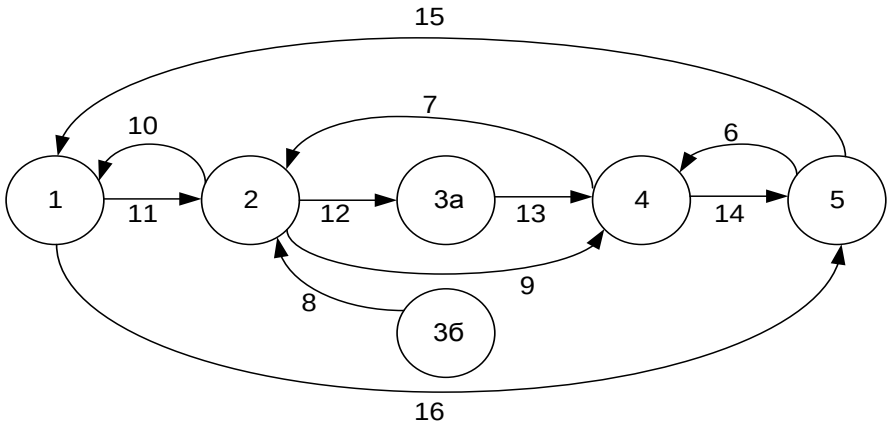


Рис. 9 Граф модели защиты технического канала утечки информации

На рисунке приняты следующие обозначения:

1 – защищаемый информационный ресурс;

2 – технический канал утечки информации;

3а – пассивное техническое средство защиты информации в канале;

3б – активное техническое средство защиты информации в канале;

4 – средство приема и выделения (перехвата) смеси информативного сигнала с помехой из среды их распространения;

5 – нарушитель;

6 – совокупность действий нарушителя по использованию средства перехвата для добывания информативного сигнала;

7 – активное воздействие средства перехвата информации на среду распространения смеси информативного сигнала и помехи от активного средства защиты;

8 – воздействие сигнала помехи от активного средства защиты на среду распространения информативного сигнала;

9 – пассивное воздействие средства перехвата информации на среду распространения смеси информативного сигнала и помехи от активного средства защиты;

10 или 11 – проникновение информативного сигнала в среду распространения за счет активного (10) или пассивного (11) воздействия среды распространения на защищаемый информационный ресурс;

12 – процесс распространения информативного сигнала до пассивного средства защиты;

13 – процесс распространения остаточного информативного сигнала от пассивного средства защиты до средства перехвата;

14 – совокупность действий нарушителя по использованию средства перехвата для выделения смысловой информации из информативного сигнала;

15 – активное получение нарушителем защищаемого информационного ресурса напрямую от владельца ресурса, минуя технические каналы утечки информации;

16 – передача владельцем защищаемого информационного ресурса напрямую нарушителю, минуя технические каналы утечки информации.

На рис. 10 представлен граф логики действий нарушителя по добыванию информации в каналах утечки информации при условии технической защиты.

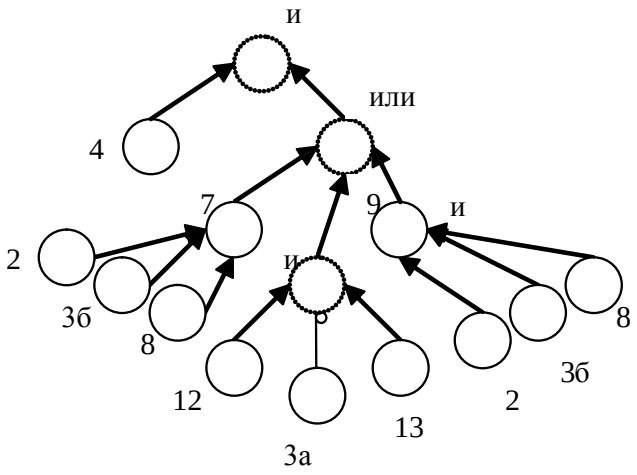


Рис. 10. Логика действий нарушителя по добыванию информации при условии использования средств технической защиты

Расчет вероятности добывания информации нарушителем за заданное время t при условии применения средств технической защиты производится по формуле:

$$P^t = P_4^t \cdot (1-(P_2^t \cdot P_{3б}^t \cdot P_7^t \cdot P_8^t) \cdot (P_2^t \cdot (1-P_{3б}^t) \cdot P_8^t \cdot P_9^t) \cdot (P_{12}^t \cdot (1-P_{3а}^t) \cdot P_{13}^t)) \quad (7)$$

Итоговая свертка вероятности добывания информации в l–м канале при условии применения средств технической защиты, исходя из графа добывания информации, структуры l–го канала и логики функционирования нарушителя за время t примет вид:

$$P^t = P_1^t \cdot P_2^t \cdot P_5^t \cdot P_4^t \cdot$$
$$\cdot (1-(P_2^t \cdot (1-P_{3б}^t) \cdot P_7^t \cdot P_8^t) \cdot (P_2^t \cdot (1-P_{3б}^t) \cdot P_8^t \cdot P_9^t) \cdot (P_{12}^t \cdot (1-P_{3а}^t) \cdot P_{13}^t)) \quad (8)$$

где

$$P_1^t = 1-(P_2^t - P_2^t \cdot P_{11}^t \cdot P_{14}^t) \cdot (P_5^t - P_5^t \cdot P_5^t \cdot P_{15}^t \cdot P_{16}^t) \quad (9)$$

Значение каждого элемента свертки вероятностей может варьироваться в зависимости от типа p средства перехвата, используемого нарушителем, типа средства защиты. Среднее время T_l^P добывания информации в l–м канале, исходя из графа добывания, структуры l–го канала и логики функционирования нарушителя при заданной вероятности P примет вид:

$$T_l^p = T_1^t \cdot T_2^t \cdot T_5^t \cdot T_4^t =$$
$$\max[(\max(T_2^p; \min(T_{11}^p; T_{14}^p)); (\max(T_{15}^p; \min(T_{15}^p; T_{16}^p)); \quad (10)$$
$$(\min(T_2^p; T_{3б}^p; T_7^p; T_8^p)); (\max(T_{12}^p; T_{13}^p; T_{14}^p; T_{3a}^p))]$$

Значение каждого элемента свертки времени может варьироваться в зависимости от типа p средства перехвата, используемого нарушителем и типа средства защиты информации в канале. Значения вероятностей отдельных событий по добыванию информации нарушителем получаются исходя из следующих соображений:

– энергетических зависимостей (соотношения чувствительности средств перехвата и уровней информативных сигналов в каждом канале);

– энергетических зависимостей (соотношения чувствительности средств перехвата, уровней информативных сигналов в каждом канале и уровня подавляющего шума при использовании активного средства защиты);

– энергетических зависимостей (соотношения чувствительности средств перехвата, уровней информативных сигналов в каждом канале и степени вносимого затухания при использовании пассивного средства защиты);

– возможностей доступа потенциального нарушителя со средствами перехвата к каналу утечки информации;

– наличия благоприятных условий для распространения информативных сигналов от источника сигнала к его приемнику;

– наличия защищаемого информационного ресурса в канале в момент доступа потенциального нарушителя к каналу (совпадение по времени событий).

4.2. Модель подавления технических каналов утечки информации

Анализ современных подходов к построению моделей защищенности позволяет выделить два основных метода, базирующихся на использовании детерминистических или стохастических математических моделей.

Детерминированный подход основывается на использовании моделей «нагрузка-стойкость», где в качестве исходных рассматриваются действующие нагрузки, создаваемые потенциалом поля подавления любой физической природы, и характеристики потенциала поля излучения (ПЭМИН) подавляемого канала. При этом параметры нагрузки и стойкости рассчитываются по формулам, в которых исходные данные, величины влияющих характеристик и коэффициентов носят строго определенный характер.

Так, для нагрузки, создаваемой мгновенным полем подавления

$$X_i^m = f(q, R, k), \tag{11}$$

где X_i^m – параметр *i*-го ПП;

q – мощность источника ПП;

R – расстояние от источника ПП до источника излучения;

k – коэффициент, учитывающий взаимодействие со средой.

Результат взаимодействия полей одной природы представляется в виде события, являющегося детерминированной функцией расчетной схемы величин X_i^m и соответствующей величины ПИ (поле излучения). Канал утечки считается подавленным, если нагрузка превышает его стойкость, и наоборот. В параметрической форме условие подавления:

$$X_i^m > X_{i\ \text{доп}}^m, \tag{12}$$

где $X_{i\ \text{доп}}^m$ – показатель стойкости канала при воздействии *i*-го ПП (поле подавления).

Этот показатель в дальнейшем будем называть показателем устойчивости канала утечки информации.

Показателями устойчивости канала утечки являются максимальные значения параметров действующих ПП, при которых техническим средством может быть выделен информативный сигнал, т.е. сохраняются «нормальное функционирование канала утечки».

Показатели устойчивости определяют на натурных испытаниях с применением средств подавления (генераторы шумов), на моделирующих установках, или путем теоретических расчетов с последующей экспериментальной проверкой.

В последнем случае исследуется обобщенная модель объекта в виде

$$\{Y_i\} = H\{X_i\}, \qquad (13)$$

где X_i – множество значений ПП, характеризующих внешнее воздействие;

Y_i – множество значений параметров, характеризующих «реакцию» канала на эти воздействия.

Оператор H характеризует структуру и свойства канала, при его помощи каждой реализации внешнего воздействия ставится в соответствие реализация «реакции» канала.

Несомненным достоинством детерминистского метода является его наглядность, так как результат доводится до физически ясно осмысливаемого правила определения ожидаемых последствий. По этой причине метод в параметрической форме широко используется при практических расчетах как для оценки стойкости каналов, так и для задания требований по потенциалу поля подавления.

На практике принято использовать показатели подавления и излучения в виде соответствующих радиусов (дальностей).

Основным недостатком рассмотренного метода является не учет случайного характера величин X и $X_{доп}$, причиной которого служит наличие неопределенностей, формирующих их значения на всех этапах взаимодействия ПП и ПИ.

Как правило, расчетные формулы для этих величин получены для некоторых усредненных исходных данных, приводящих к определенной идеализации физических моделей формирования ПП. Поэтому неопределенность аргументов, образующих основные расчетные формулы, как правило, устранить не представляется возможным. Это, в свою очередь, не позволяет оперировать точными значениями величин X и $X_{доп}$. В каждом конкретном случае они будут принимать случайное, заранее неизвестное, но какое-то одно значение. Для устранения влияния неопределенностей на результаты оценки используется вероятностный метод оценивания результатов воздействия ПП.

Этот метод удобен и для получения обобщенных вероятностных показателей подавления или сохранения канала, для того чтобы установить их взаимосвязь с более общими системными показателями.

Три тесно связанных идеи положены в основу вероятностного метода:

– условия формирования и распространения ПП, а также «реакция» канала на воздействие этих полей есть случайные события или процессы;

– понятие «подавление» трактуется как вероятность невыхода информативного сигнала за пределы контролируемой зоны (области допустимых значений);

– событие «подавление» происходит мгновенно после включения генератора.

В общем случае вероятностные показатели при оценке воздействия ПП представляются численными значениями вероятности того, что случайное значение воздействующего параметра $\hat{X}$ будет меньше его некоторого зна-

чения, т.е. Вер ($\hat{X} < x$), или не меньше этого значения Вер ($\hat{X} \geq x$), или находиться в определенных пределах Вер ($x_1 \leq \hat{X} \leq x_2$).

Наиболее общим и распространенным способом определения этих вероятностей является задание функции распределения

$$F(x) = P(\hat{X} < x), \tag{14}$$

$$1 - F(x) = (\hat{X} \geq x), \tag{15}$$

$$F(x_2) - F(x_1) = P(x_1 \leq \hat{X} \leq x_2). \tag{16}$$

Тогда выражение для вероятности подавления может быть записано в общем виде

$$P_{\text{п}} = P\{\hat{X} \geq \hat{X}_{\text{доп}}\} = P\{\hat{X} - \hat{X}_{\text{доп}} > 0\}. \tag{17}$$

Для конкретных ситуаций можно рассматривать три случая вычисления этого показателя:

а) параметр ПП есть величина случайная, задаваемая функцией плотности распределения $f(x)$, показатель стойкости – величина детерминированная. Тогда (рис. 11а)

$$P_{\text{п}} = P\{\hat{X} \geq X_{\text{доп}}\} = 1 - F(X_{\text{доп}}) = 1 - \int_0^{X_{доп}} f(x)\text{dx} = \int_{X_{доп}}^{\infty} f(x)\text{dx}, \tag{18}$$

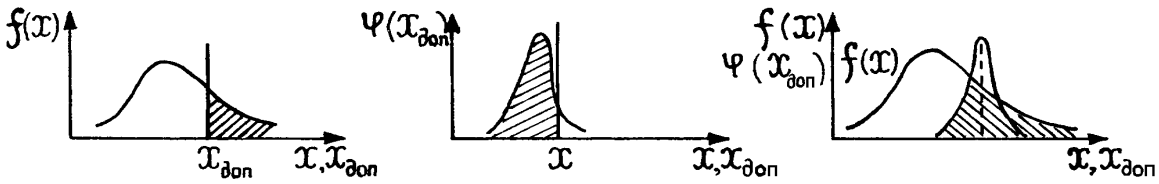
Вероятность сохранения канала $P_{\text{с}} = 1 - P_{\text{п}}$.

б) параметр ПП – величина детерминированная, показатель стойкости - случайная с плотностью распределения $\varphi(x_{\text{доп}})$, рис. 2.11б.

$$P_{\text{п}} = P\{\hat{X}_{\text{доп}} < x\} = \int_0^{X} \varphi(x_{\text{доп}})\text{dx}_{\text{доп}}, \tag{19}$$

в) параметр ПП и показатель стойкости величины случайные, рис. 11в. Тогда

$$P_{\text{п}} = P\{\hat{X} - \hat{X}_{\text{доп}} > 0\} = \int_0^{\infty}\int_X^{\infty} f(x_{\text{доп}})\cdot\varphi(x_{\text{доп}})\text{dxdx}_{\text{доп}}, \qquad (20)$$



а) б) в)

Рис. 11. Схема для определения вероятности подавления:

Таким образом, вероятностный подход не заменяет собой детерминистский. При его осуществлении так же необходимо рассчитывать величины X и $X_{\text{доп}}$, дополняя эти расчеты определением характеристик случайных величин, что приводит к возрастанию объема решаемой задачи.

Приведенные выражения устанавливают зависимость вероятности подавления от параметров ПП. Поэтому, вероятность $P_{\text{п}} = P\{\hat{X}_{\text{доп}} < x\}$ обозначим через $G(X)$ и назовем факторным (параметрическим) законом подавления (ФЗП). После интегрирования (20) получим

$$P_{\text{п}} = \int_0^{\infty} G(X)\cdot f(X)\text{dx}. \qquad (21)$$

Учитывая, что параметр X зависит от расстояния, получим координатный закон подавления (КЗП)

$$G(R) = \int_0^{\infty} G(X)\cdot f(X_R)\text{dx}, \qquad (22)$$

который устанавливает зависимость между вероятностью подавления и расстоянием от точки размещения источника поля подавления.

Здесь $f(X_R)$ – функция плотности распределения параметра ПП на расстоянии R.

Вид координатного закона подавления представлен на рис. 12. На расстояниях $R \le R_a$ $G(R) = 1$, что соответствует зоне безусловного подавления;

при $R_a < R \le R_{без}$ находится зона вероятного подавления, и при $R > R_{без}$ – «зона безопасности» подавляемого канала.

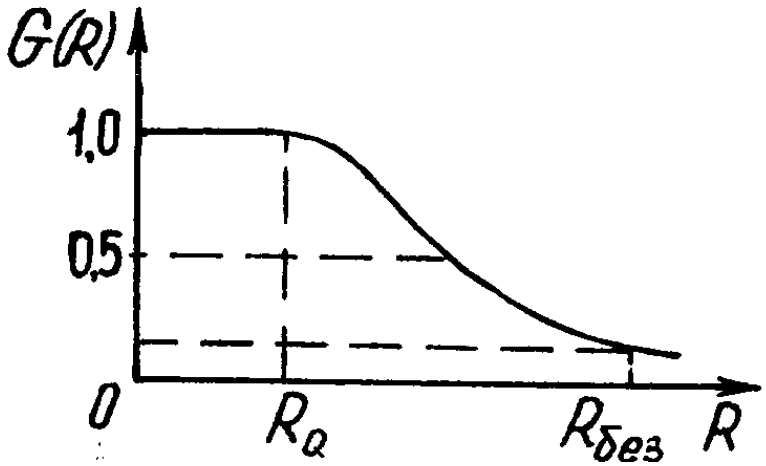


Рис. 12. Координатный закон подавления

Основными числовыми характеристиками координатного закона подавления (КЗП) являются площадь ($S_п$) и радиус приведенной зоны подавления, (рис. 13) т.е. зоны, в которой каналы утечки информации подавляются достоверно.

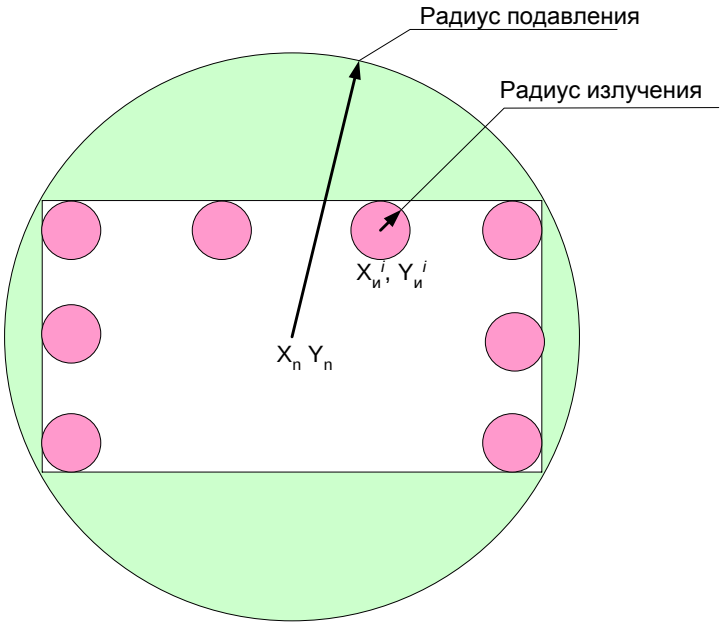


Рис. 13. Графическое представление модели подавления ПЭМИ.

На данном рисунке зона возможного перехвата информационного сигнала от совокупности технических средств – источников ПЭМИ аппроксимирована прямоугольником. В зависимости от степени компактности распо-

ложения таких средств, она может быть представлена в виде эллипса или равновеликого круга.

Вполне очевидно, что потенциал поля подавления должен быть таким, чтобы

$$dS_{П} = G(R)dS = 2\pi R \cdot G(R)dR, \quad (23)$$

$$S_{П} = 2\pi \int_{0}^{\infty} R\,G(R)dR, \quad (24)$$

$$R_{П} = \sqrt{2\int_{0}^{\infty} RG(R)dR} \quad (25)$$

Радиус приведенной зоны с точностью 2...3% равен расстоянию, на котором $G(R) = 0{,}5$. Это расстояние принимается за радиус подавления.

Практическое значение КЗП заключается в том, что расчет вероятности подавления сводится к расчету вероятности накрытия зоной подавления приведенную зону распространения информативного сигнала.

Заключение

1. На основе общего методического подхода к разработке и выбору моделей при проведении исследований в данной предметной области формализованы структура и предложен математический аппарат моделей каналов утечки конфиденциальной информации, используемой в процессе деятельности организации, имеющей средства информатизации и способов её защиты.

2. С использованием информационно-логической схемы функционирования типового объекта информатизации произведена «увязка» понятий «объект— угроза — способы защиты».

3. Разработаны алгоритм учета факторов, определяющих облик нарушителя-злоумышленника, формализованы его вероятностная модель, логика

действий и математическая модель реализации угрозы конфиденциальности с учетом преодоления систем защиты.

4. Обоснована необходимость наличия на типовом объекте комплексной системы мониторинга, разработаны структура и математическая модель для оценки вероятности утечки информативного сигнала и действенности мер защиты.

5. С использованием методического аппарата методов исследования операций разработана математическая модель для оценки эффективности подавления технического канала утечки информативного сигнала и её графическое представление.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Ададуров С.Е., Корниенко А.А. Методы обнаружения и оценивания аномалий информационных систем.//Материалы 10-й Международной конференции «ИнфоТранс-2005»СПб, ПГУПС, 2005.

2. Бабиков В.Н. Диссертация на соискание ученой степени кандидата технических наук. СПб, СПбГПУ, 2006.

3. Бабиков В.Н., Кляхин В.Н. Алгоритм формализованной постановки задачи защиты информации. //Сб. трудов 9-й Всероссийской научно-практической конференции «Актуальные проблемы защиты и безопасности». Т.4, РАРАН, СПб., 2006.

4. Бабиков В.Н., Кляхин В.Н. Угрозы безопасности автоматизированной системе ОСОДУ.// Материалы 2-й научно-практической конференции «Реализация государственной жилищной политики в Ленинградской области». СПбГПУ, 2005.

5. Барсуков В.С., Водолазкий В.В. Современные технологии безопасности: интегральный подход.– М.: «Нолидж», 2000.

6. Бухарцев Ю.А., Ильин В.Е., Кудрявцев А.И., Куликов В.А. и др. Автоматизированные информационные системы.– Л.: ВАС, 1988.

7. ГОСТ 34.003-90 Автоматизированные системы.

8. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от НСД к информации. Общие технические требования.

9. ГОСТ Р 50922-96. Защита информации. Основные требования и определения.

10. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

11. ГОСТ Р 51583-2000. Порядок создания автоматизированных систем в защищенном исполнении.

12. ГОСТ РВ 50934-96. Защита информации. Организация и содержание работ по защите информации об образцах военной техники от технических разведок.

13. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации

14. Гостехкомиссия России. Руководящий документ. Временное положение по организации изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.

15. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения

16. Гостехкомиссия России. Руководящий документ. Концепция активного противодействия.

17. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

18. Гостехкомиссия России. Руководящий документ. Специальные требования и рекомендации по защите информации.

19. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.

20. Гусев В.С. О некоторых подходах к обеспечению комплексной безопасности хозяйствующих субъектов.– СПб.: 1999.

21. Захаров С.Г., Супрун А.Ф. Человек и его безопасность в условиях электромагнитных излучений. Техника безопасности при эксплуатации передвижных электроустановок. – СПб.;- 1996.

22. Зегжда П.Д., Ивашко А.М. Как построить защищенную информационную систему. СПб: Мир и семья-95, Интерлайн, 1998.

23. Каторин Ю.Ф. и др. Большая энциклопедия промышленного шпионажа. – СПб.: Полигон, 2000.-896 с.

24. Матвеев В.В. Организационные, технические и методические аспекты обеспечения безопасности особо важных и потенциально опасных объектов Монография. СПб, СПбГПУ, 2005.

25. Матвеев В.В., Супрун А.Ф. Новый вызов политике информационной безопасности. Материалы VIII Всероссийской конференции по проблемам науки и высшей школы. Фундаментальные исследования в технических университетах. Национальная безопасность. 26-27 мая 2004. Т. 2. Часть 1. СПб.: СПбГПУ, 2004.

26. Матвеев В.В., Супрун А.Ф. Обоснование моделей каналов утечки информации. Материалы конференции в рамках XXXV Недели науки СПбГПУ, 2006г.

27. Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам (Постановление Совета Министров - Правительства РФ от 15.09.93 г. № 912-51).

28. ПросихинВ.П., Зегжда П.Д. Обеспечение безопасности управления системами передачи данных в электроэнергетике.// Проблемы информационной безопасности, № 1, 2005.

29. Саенко И.Б. и др. Активный аудит действий пользователей в защищенной сети.//Защита информации. Конфидент.2002, №4-5.

30. Симонов С. М. Методология анализа рисков в информационных системах. Защита информации. Конфидент, №1, 2001. С 72-76.

31. Староверов Д. Оценка угроз воздействия конкурента на ресурсы организации. Защита информации. Конфидент, №2, 2000 г., с. 58-62.

32. Технические системы и средства защиты информации. Информационные материалы. - М.: ЗАО «Научно-производственный центр «НЕЛК»», 2004.

33. Хомоненко А.Д. Численные методы анализа систем и сетей массового обслуживания. – М.: МО СССР, 1991.

34. Шпак В.Ф. Методологические основы обеспечения информационной безопасности объекта / Конфидент, 2000, № 1.– С. 72 - 86.

Супрун Александр Федорович

КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ РЕАЛИЗАЦИИ УГРОЗ

УЧЕБНОЕ ПОСОБИЕ

ЧАСТЬ 1

Лицензия лр № 020593 от 07.08.97
Налоговая льгота – Общероссийский классификатор продукции
ОК 005-93, т. 2; 95 3005 – учебная литература

Подписано в печать . Формат 60x84/116. Печать цифровая.

Усл. Печ л. 3,25. Уч.-изд. л. 3,25. Тираж 50. Заказ .

Отпечатано с готового оригинал-макета, предоставленного автором в Цифровом типографском центре Издательства Политехнического университета. 195251, Санкт-Петербург, Политехническая ул., 29.

Тел.: (812) 550-40-14

Тел./факс: (812) 297-57-76