МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА
Колледж программирования и кибербезопасности

Техническая защита информации

Лекция 3

Тема лекции: Системный подход к технической защите информации. Основные положения концепции

Преподаватель ПЦК Информационной безопасности
Дмитренко Павел Сергеевич

Список сокращений

АС – автоматизированная система;

АОИ – Аттестация объекта информатизации;

БД – база данных;

ВИ – владелец информации;

ВТСС – вспомогательные технические средства и системы;

ЗИ – защита информации;

ЗУ – закладное устройство;

ИБ – информационная безопасность;

ИК – инфракрасное (излучение);

КЗ – контролируемая зона;

МП – магнитное поле;

ОТСС – основные технические средства и системы;

ОИ – объект информатизации;

Список сокращений

ППФ – помехоподавляющие фильтры;

ПЭМИ(Н) – побочные электромагнитные излучения (наводки);

РЭС(У) – радиоэлектронные системы (устройства); **(Т)КУИ –** технический (канал утечки информации); **СЗИ –** система защиты информации;

СрЗИ – средства защиты информации;

СП – силовое поле;

ТЗИ – техническая защита информации;

УФ – ультрафиолетовое (излучение);

ЭВМ – электронная вычислительная машина;

Э(М)П – электрическое (магнитное) поле.

ЭЗ – элемент защиты;

ЭМВ – электромагнитная волна;

Рекомендуемая литература:

Основная:

1.Торокин А.А. Инженерно-техническая защита информации: учеб. пособие для студ. /А.А. Торокин. - М.: Гелиос АРВ, 2005. – 960 с.: ил.

2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т 1. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. – 636 с.

3. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. - М.: Горячая линия-Телеком, 2015. – 586 с.: ил.

4. Ворона В.А., Тихонов В.А., Митрякова Л.В. Теоретические основы обеспечения безопасности объектов информатизации: учебное пособие. - М.:

Рекомендуемая литература:

Дополнительная:

5. Дураковский А.П., Куницын И.В., Лаврухин Ю.Н. Контроль защищенности речевой информации в помещениях. Аттестационные испытания ВТСС по требованиям безопасности информации: Учебное пособие. – М.: НИЯУ МИФИ, 2015. – 152 с.

6. Малюк А.А., Горбатов В.С, Королев В.И., Фомичев В.М., Дураковский А.П. и др. Введение в информационную безопасность: учебное пособие. /под ред. В.С. Горбатова - М.: Горячая линия-Телеком, 2011. – 288 с.: ил.

7.Савельев И.В. Курс общей физики, т.1-3. М.: «Лань», 2006 и др. издания, гриф Министерства образования Российской Федерации.

8.Литвинов О.С., Горелик В.С. Электромагнитные волны и оптика: учебное пособие. - М.: Изд-во МГТУ имени Н.Э. Баумана, 2006. – 448 с.: ил.

Дисциплина **«техническая защита информации»** является основополагающей при изучении технических средств защиты информации, технических средств разведки, а также комплексной системы технических средств охраны.

Цель курса - *изучение источников, носителей и принципов технической защиты информации, а также принципов построения технических средств охраны объектов; подготовка к разработке технических систем защиты информации, содержащейся в речевых, аудио и видео сигналах и текстовых документах.*

Раздел 1. Концепция и теоретические основы технической защиты информации

Тема 1.1. Системный подход к технической защите информации

1. Основные положения системного подхода к технической защите информации.
2. Цели,задачи и ресурсы системы технической защиты информации.
3. Угрозы безопасности информации и мерыпо их предотвращению.

4.Принципы технической защиты информации. 5. Принципыпостроения системы технической защиты информации.

Концепция технической защиты информации. Системный подход

Концепция технической защиты информации — это система взглядов на защиту информации с помощью технических средств.

Основа концепции *технической защиты информации* - постановка задачи защиты информации с помощью технических (инженерных) средств и определение принципов ее решения.

Задачи технической защиты информации - задачи противоборства органов и специалистов по информационной безопасности, с одной стороны, и злоумышленников, с другой стороны. Данные задачи являются слабоформализуемыми – т.к. не имеют формальных методов решения, и основу методологии их решения составляютсистемный подход и системный анализ.

Сущность системного подхода

Системный подход - это исследование объекта или процесса с помощью модели, называемой системой:

- совокупность сил и средств, обеспечивающих решение задачи, представляется в виде модели, называемой системой;
- система описывается совокупностью параметров;
- любая система рассматривается как подсистема более сложной системы, влияющей на структуру и функционирование рассматриваемой;
- любая система имеет иерархическую структуру;
- при анализе системы необходим учет внешних и внутренних влияющих факторов;
- свойства системы превышают сумму свойств ее элементов.

Сущность системного подхода

Системное мышление *– это форма мышления, характеризующая способность человека на бессознательном уровне решать задачи дедуктивным методом. Эти методы применительно к технической ЗИ предусматривают:*

-четкую постановку задачи, включающую определение вопросов защищаемой информации и её источников как объектов защиты, выявление угроз этой информации и формулирование целей и задач ЗИ;

- разработку принципов и путей решения задачи;

- разработку методов решения задач;

-создание программного, технического и методического обеспечения решения задачи.

Сущность системного подхода

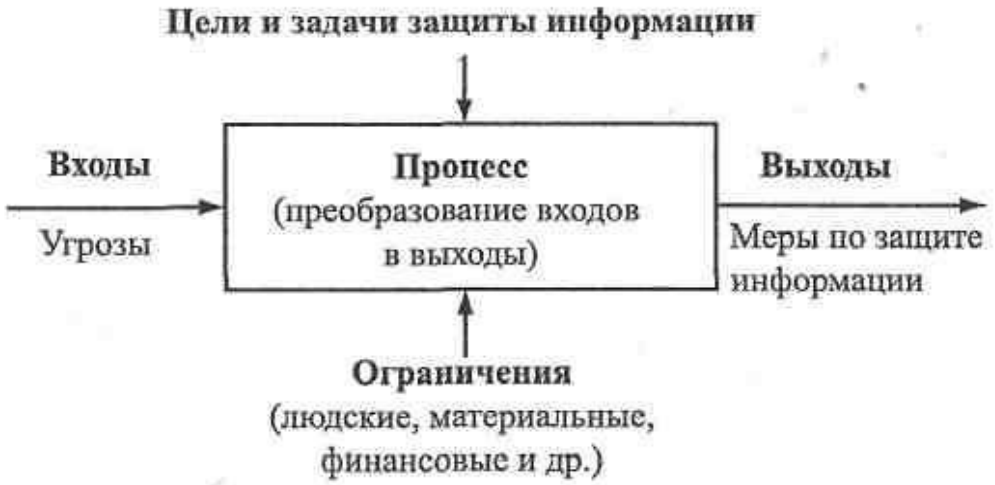
Системный анализ предусматривает *применение комплекса методов, методик и процедур, позволяющих выработать в результате анализа модели системы рациональные рекомендации по решению проблем.*

Математическим обеспечением системного анализа является аппарат исследования операций.

Система *защиты информации* – это модель системы, объединяющей ресурсы организации, обеспечивающие ЗИ.

Следовательно, система защиты информации представляет собой модель системы, объединяющей силы и средства организации, обеспечивающие защиту информации.

Сущность системного подхода



Параметры системы:

-цели и задачи (конкретизированные в пространстве и во времени);

-входы и выходы системы;

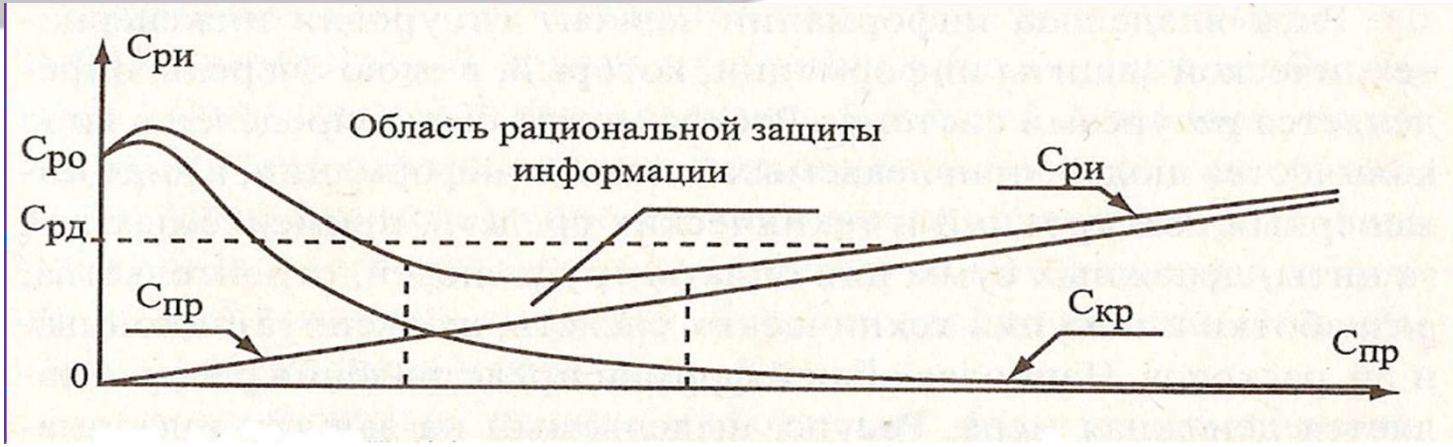
-ограничения, которые необходимо учитывать при построении (оптимизации) системы;

-процессы внутри системы, обеспечивающие преобразование входов в выходы

Сущность системного подхода

Цели представляют собой ожидаемые результаты функционирования *системы защиты информации*, а ***задачи*** то, что надо сделать для того, чтобы система могла обеспечить движение поставленных целей. Возможность решения задач зависит от ***ресурса***, выделяемого на защиту информации. Ресурс включает в себя людей, решающих задачи защиты информации, финансовые, технические и др. средства, расходуемые на *защиту информации (ЗИ)*. ***Входами*** системы защиты информации являются угрозы информации, а выходами – меры, которые надо применить для предотвращения угроз или снизив их до допустимого уровня. Так для слабоформализуемых задач нет методов их точного решения, то процесс представляет собой выбор для

Сущность системного подхода



Чем больше ресурс на защиту информации, тем более высокий уровень безопасности информации может он обеспечить. В принципе, при неограниченном ресурсе можно получить сколь угодно малую вероятность реализации угрозы. Если обозначить через $C_и$ и $P_у$ цену информации и вероятность реализации угрозы соответственно, то ущерб от реализации угрозы можно оценить величиной $C_у = C_и P_у$. Величину ущерба можно рассматривать как возможные (потенциальные) косвенные расходы, а ресурс — как прямые (учитываемые бухгалтерией) расходы $C_{пр}$ на защиту информации. Следовательно, владелец (пользователь) информации объективно вынужден нести расходы на нее, равные сумме прямых и косвенных расходов: $C_{ри} = C_{пр} + C_{кр}$. Между этими слагаемыми существует тесная связь — косвенные расходы обратно пропорциональны прямым расходам. Эта связь позволяет оценить на качественном уровне зависимость суммарных расходов на информацию от прямых расходов, качественно отображенной на рис. 1.2.

Сущность системного подхода

Рост суммарных расходов на информацию при малых прямых расходах вызван тем обстоятельством, что эффект защиты начинает проявляться, когда прямые расходы превышают некоторую критическую массу.

Из рисунка выше следует, что при некоторых прямых расходах наблюдается область с минимальными суммарными расходами на информацию. Эта область является **областью рациональной защиты информации**.

Зависимость суммарных расходов на информацию ($C_{ри}$) от прямых расходов($C_{пр}$)

$C_и$ – цена информации,

$P_у$ - вероятность реализации угрозы, $C_у = C_и P_у$ – величина ущерба, или косвенные расходы($C_{кр}$), обратно пропорциональны $C_{пр}$.

$$C_{ри} = C_{пр} + C_{кр}$$

Сущность системного подхода

Основная цель защиты информации – обеспечение заданного уровня ее безопасности.

Заданный уровень ***безопасности информации*** – такое состояние защищенности информации от угроз, при котором обеспечивается допустимый риск ее уничтожения, изменения и хищения.

Угрозы безопасности информации

Угрозы безопасности информации — состояния и действия субъектов и материальных объектов, которые могут привести к изменению, уничтожению и хищению информации.

Изменение, уничтожение, хищение и блокирование информации — это результаты реализации угроз или свершившиеся угрозы.

Наибольшую угрозу для информации, содержащей государственную тайну, создает зарубежная разведка.

Угрозы безопасности информации

Основной интерес зарубежной разведки:

- О состоянии и прогнозах развития военного, научно-технического и экономического потенциалов государств;
- О достижениях науки и техники, содержании научно-исследовательских, опытно-конструкторских, проектных работ и технологий, имеющих важное оборонное и экономическое значение;
- О тактико-технических характеристиках и возможностях боевого применения образцов вооружения и боевой техники;
- О дислокации, составе, вооружении войск и состоянии их боевого обеспечения;
- Об объемах запасов, добычи, поставки потребления стратегических видов и сырья, и полезных ископаемых; материалов
- О выполнении условий международных договоров, прежде всего, об ограничении вооружений и др.

Угрозы безопасности информации

Каждая угроза влечёт за собой определённый ущерб – моральный или *материальный*, а защита и противодействие угрозе призвано снизить его величину, *в идеале* – полностью, реально – значительно или хотя бы частично. Но и это удаётся далеко не всегда.

С учётом этого ***угрозы*** могут быть *классифицированы по следующим кластерам:*

1) по величине принесённого ущерба:

-предельный, после которого фирма может стать банкротом;

- значительный, но не приводящий к банкротству;

-незначительный, который фирма может компенсировать и др.;

Угрозы безопасности информации

С учётом этого ***угрозы*** могут быть *классифицированы по следующим кластерам (продолжение):*

2) по вероятности возникновения:
- весьма вероятная угроза;
- вероятная угроза;
- маловероятная угроза;

3) по причинам появления:
- стихийные бедствия;
- преднамеренные действия;

4) по характеру нанесённого ущерба:
- материальный;
- моральный;

5) по характеру воздействия:
- активные;
- пассивные;

6) по отношению к объекту:
- внутренние;
- внешние.

Угрозы безопасности информации

Источниками внешних угроз являются:

- недобросовестные конкуренты;
- преступные группировки и формирования;
- отдельные лица и организации административно-управленческого аппарата.

Источниками внутренних угроз могут быть:

- администрация предприятия;
- персонал;
- технические средства обеспечения производственной и трудовой деятельности.

Соотношение внешних и внутренних угроз на усреднённом уровне можно охарактеризовать примерно так:

- 82% угроз совершается собственными сотрудниками фирмы либо при их прямом или опосредованном участии;
- 17% угроз совершается извне – внешние угрозы;
- 1% угроз совершается случайными лицами.

Модель нарушителей ИБ на объекте

Каждый собственник имущества (субъект, в объёме реализующий полномочия владения, пользования, распоряжения указанным имуществом) сталкивается с задачей обеспечения его охраны от различного типа угроз, начиная от банальной кражи до его полного уничтожения. Особую озабоченность при этом у него вызывает построение системы охраны объекта (предприятия), имеющего рассредоточенные на какой-то площади складские и/или производственные помещения и т.д.

Отличительной чертой предприятия является такого протяжённый трудноконтролируемый периметр, имеющий, как правило, несколько точек прохода (проезда) персонала (служебного транспорта).

Модель нарушителей ИБ на объекте

Нарушитель – это лицо, предпринявшее попытку выполнения запрещённых операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, в целях самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

Модель нарушителей ИБ на объекте

При разработке модели нарушителя определяются:

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
- предположения о квалификации нарушителя и его технической оснащённости (об используемых для совершения нарушения методах и средствах);
- ограничения и предположения о характере возможных действий нарушителей.

Нарушители могут быть *внутренними* (из числа персонала) или *внешними* (посторонними лицами).

Модель нарушителей ИБ на объекте

Можно выделить несколько основных мотивов нарушений:

- безответственность;
- самоутверждение;
- вандализм;
- принуждение;
- месть;
- корыстный интерес;
- идейные соображения.

При нарушениях, вызванных безответственностью, пользователь производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности.

Модель нарушителей ИБ на объекте

Основная цель нарушителя в рассматриваемом варианте заключается в скрытном преодолении зоны периметра предприятия для получения несанкционированного доступа к охраняемому имуществу собственника.

Способ и время, затраченное им на преодоление зоны периметра, прямо зависят от его осведомлённости о возможностях *системы охраны периметра* предприятия, технической и физической подготовленности, а также от конечных целей вторжения.

Модель нарушителей ИБ на объекте

Для определения требуемого уровня защищённости периметра предприятия (его способности противостоять действиям нарушителя) необходимо формирование базовой модели нарушителя, на способности и возможности которого должна ориентироваться создаваемая *система охраны периметра.*

Под моделью нарушителя понимается его описательная характеристика, отражающая его возможный моральный облик, уровень физической подготовленности, знаний, обученности и оснащённости, которые дают возможность оценить степень его способности и заинтересованности в преодолении зоны периметра предприятия, с одной стороны, а с другой – определить допустимый *уровень технической подготовленности рубежейохраны зоны периметра*.

Модель угроз ИБ на объекте

Модель угроз представляет собой перечень возможных действий (целей и способов их достижения) нарушителя по преодолению зоны периметра предприятия (распределённого объекта охраны).

Под целью вторжения понимается конечная цель нарушителя, реализуемая им после преодоления зоны периметра. Их возможный спектр достаточно широк – от простой кражи до террористических действий, он прямо зависит от типа охраняемого имущества. *Определение целей вторжения* на территорию предприятия, облика возможного нарушителя и наиболее вероятных сценариев его действий даёт возможность сформировать требования к техническим средствам системы охраны периметра, при реализации которых

Модель угроз ИБ на объекте

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определённые ресурсы. При формировании модели угроз в рассматриваемом случае необходимо учитывать только те угрозы охраняемому имуществу предприятия, которые включают несанкционированное преодоление зоны его периметра нарушителем, обладающим возможностями сформировавшей его базовой модели. Здесь полезными могут быть натурные испытания по количественной оценке возможностей нарушителя, например, времени преодоления внешнего ограждения заданной конструкции или зоны отчуждения, оборудованной инженерными средствами задержания, и т.п.

Модель угроз ИБ на объекте

При этом, как правило, исходят из принципа *«хуже быть не может»*, т.е. если созданная система обнаружения в состоянии противостоять (обнаружить) нарушителю базовой модели, то она сможет противостоять всем типам нарушителей, обладающих меньшим уровнем подготовленности по какому-нибудь параметру.

Область интересов для коммерческой разведки:

- Коммерческая философия и деловая стратегия руководителей фирм-конкурентов, их личные и деловые качества
- Научно-исследовательские и конструкторские работы
- Финансовые операции фирм
- Организация производства, в том числе данные о вводе в строй новых, расширении и модернизации существующих производственных мощностей, объединение с другими фирмами
- Технологические процессы при производстве новой продукции, результаты ее испытаний
- Маркетинг фирмы, в том числе режимы поставок, сведения о заказчиках и заключаемых сделках, показатели реализации продукции
- Сведения об организациях, потенциально являющихся союзниками или конкурентами
- Сведения о деятельности потенциальных и реальных конкурентов
- Учет и анализ попыток несанкционированного получения коммерческих секретов конкурентами
- Оценка реальных отношений между сотрудничающими и конкурирующими организациями;
- Анализ возможных каналов утечки конфиденциальной информац[3]и[1]и.

Методы коммерческой разведки:

-промышленный шпионаж

Цель - добывание данных о разрабатываемой продукции.

-**бизнес-разведка** (деловая, конкурентная, экономическая).

Цель - получение информации для руководства, необходимой для принятия им обоснованных управленческих решений, т.е. сведения о глобальных процессах в экономике, политике, технологии производства, партнерах и конкурентах, тенденциях рынка и других вопросах.

Основу конкурентной разведки составляют процессы поиска информации в открытых источниках и ее анализ с целью получения необходимых сведений.

Эффективность защиты безопасности информации

Многообразие угроз безопасности информации порождает многообразие мер ее защиты.

Эффективность каждой меры защиты безопасности информации оценивается своими локальными (частными) показателями эффективности. Их можно разделить на **функциональные (оперативные)** и **экономические**.

Функциональные показатели характеризуют уровень безопасности информации, **экономические** — расходы на ее обеспечение.

Локальный функциональный показатель эффективности защиты информации - показатель количества и качества информации, которая может попасть к злоумышленнику, и характеристики реально возникающих угроз безопасности информации.

Эффективность системы защиты информации в целом

определяется глобальными функциональным и экономическим критериями или показателями. В качестве функционального глобального критерия часто используется «взвешенная» сумма функциональных локальных показателей.

- Если обозначить через ω_i значение i-го локального показателя, то глобальный показатель(критерий) определяется как

$$W_r = \Sigma \alpha_i \omega_i, \text{ причем } \Sigma \alpha_i = 1.$$

Коэффициент α_i характеризует «вес» локального показателя. Физического смысла такой показатель не имеет.

- **Глобальный экономический показатель представляет собой меру суммарных расходов на информацию.**

Эффективность тем выше, чем ниже расходы при одинаковом уровне безопасности информации или чем больше уровень ее безопасности при одинаковых расходах. Первый подход к оценке эффективности используется при отсутствии жестких ограничений на ресурс, выделяемый для защиты информации, второй — при заданном ресурсе.

Базовые принципы технической защиты информации

Возможность защиты должна соответствовать возможностям нападения!!!

- **надежность;**
- **непрерывность;**
- **скрытность;**
- **целеустремленность;**
- **рациональность;**
- **активность;**
- **гибкость;**
- **многообразие способов защиты;**
- **многозональность;**
- **многорубежность;**
- **комплексное использование различных способов и средств;**
- **экономичность.**

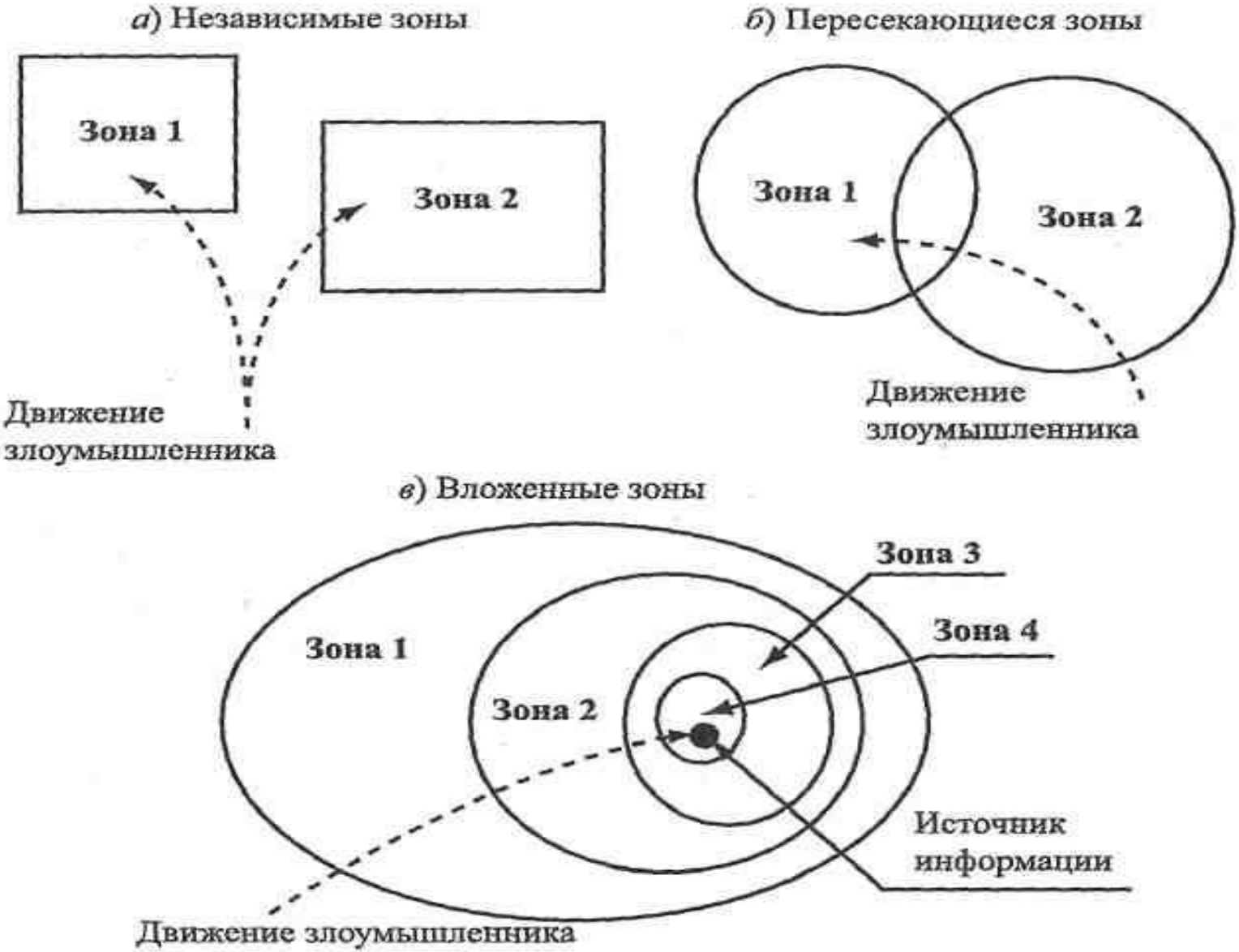
Система защиты информации должна содержать:

- рубежи вокруг источников информации, преграждающих распространение сил воздействия к источникам информации и ее носителей от источников;
- силы достоверного прогнозирования и обнаружения угроз;
- средства достоверного прогнозирования и обнаружения угроз;
- методы и способы принятия решения о мерах по предотвращению или нейтрализации угроз;
- силы нейтрализации угроз, преодолевших рубежи защиты;
- средства нейтрализации угроз, преодолевших рубежи защиты.

Основные принципы построения системы защиты информации

- многозональность пространства, контролируемого системой инженерно-технической защиты информации;
- многорубежность системы инженерно-технической защиты информации;
- равнопрочность рубежа контролируемой зоны;
- надежность технических средств системы защиты информации;
- ограниченный контролируемый доступ к элементам системы защиты информации;
- адаптируемость (приспособляемость) системы к новым угрозам;
- согласованность системы защиты информации с другими системами организации.

Виды контролируемых зон



Виды контролируемых зон

Контролируемая зона (КЗ) – это территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа. *Контролируемая зона* может ограничиваться периметром охраняемой территорией частично, охраняемой территорией, охватывающей здания и сооружения, в которых проводятся закрытые мероприятия, частью зданий, комнаты, кабинетом, в которых проводятся закрытые мероприятия.

Контролируемая зона может устанавливаться больше чем охраняемая территория, при этом обеспечивающая постоянный контроль за не охраняемой частью территории. В *контролируемой зоне* посредством проведения технических и режимных мероприятий должны быть созданы условия, предотвращающие возможность утечки из неё информации (конфиденциальной).

Постоянная контролируемая зона – это зона, границы которой устанавливаются на длительный срок.

Виды контролируемых зон

Временная зона – это зона, устанавливаемая для проведения закрытых мероприятий разового характера. Согласно требованиям нормативных документов технической защиты информации (НДТЗИ) должна обеспечиваться *контролируемая зона* следующих размеров:

-первой категории универсального объекта требуется 50 м контролируемой зоны;

- второй категории объекта требуется 30 м;

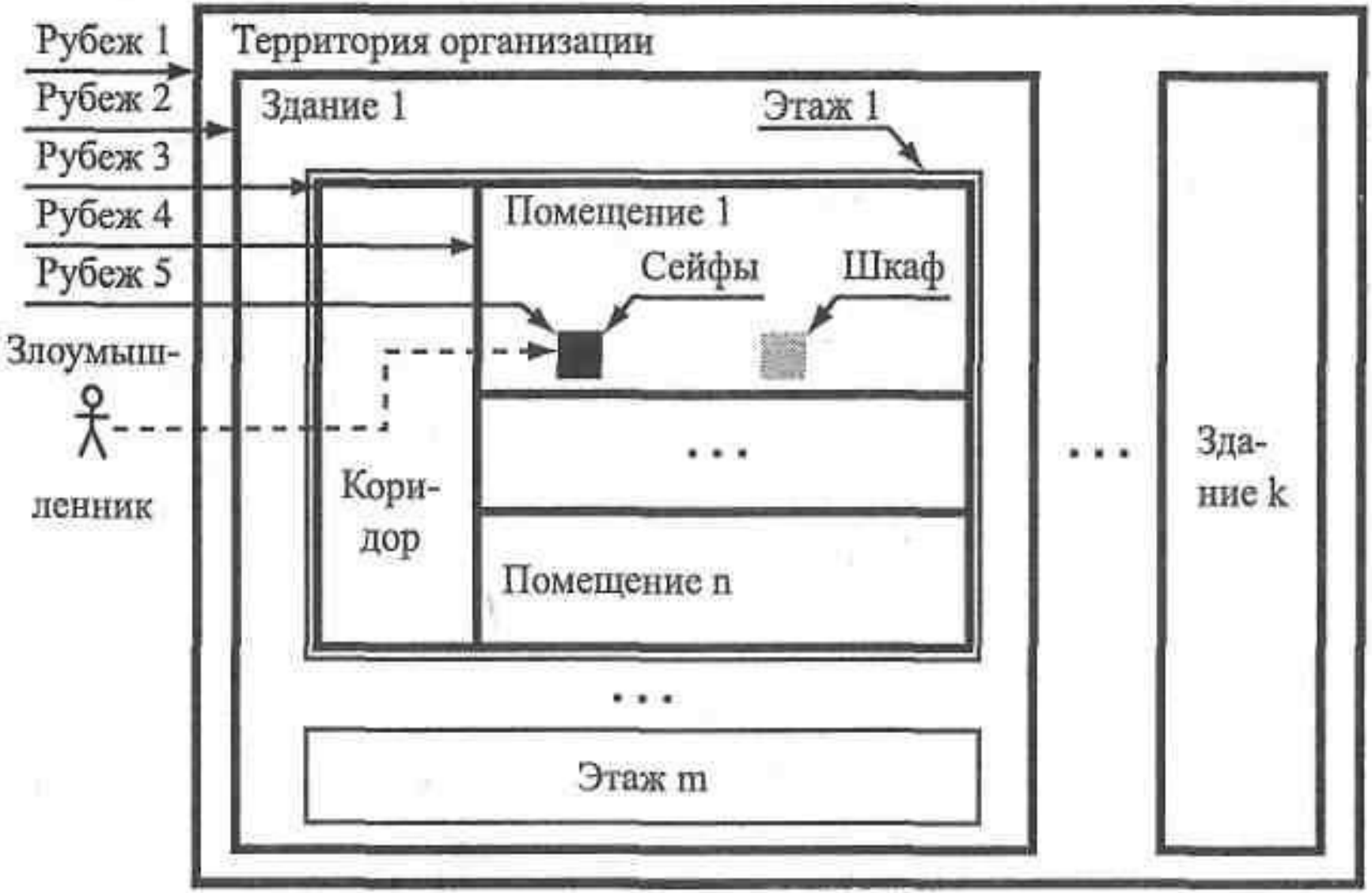
-третьей категории объектов требуется 15 м контролируемой зоны.

Также требуется определённый размер контролируемой зоны для разных типов специализированных объектов (СО).

Классификация зон по условиям доступа

Категория зоны	*Наименование зоны*	*Функциональное назначение зоны*	*Условия доступа сотрудников*	*Условия доступа посетителей*
0	Свободная	Места свободного посещения	Свободный	Свободный
I	Наблюдаемая	Комнаты приема посетителей	Свободный	Свободный
II	Регистрационная	Кабинеты сотрудников	Свободный	По удостоверению личности с регистрацией
III	Режимная	Секретариат, компьютерные залы, архивы	По идентификационным картам	По разовым пропускам
IV	Усиленной защиты	Кассовые операционные залы, материальные склады	По спецдокументам	По спецпропускам
V	Высшей защиты	Кабинеты высших руководителей, комнаты для ведения переговоров, специальные хранилища	По спецдокументам	По спецпропускам

Типовые зоны и рубежи организации



Требования к защищаемым помещениям, где циркулирует конфиденциальная информации

*Помещение, в котором циркулирует защищаемая инфор*мация, должно находиться в контролируемой зоне. Помещение должно
быть оборудовано надёжными автоматическими замками, средствами сигнализации и контроля доступа, постоянно находящимися под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (ПЭВМ, документов, реквизитов доступа и т.п.).

Уборка помещений с установленными в них ПЭВМ должна производиться с разрешения ответственного, за которым закреплены данные технические средства, или дежурного по подразделению с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

Категорирование помещений

Все помещения фирмы в зависимости от назначения и характера совершаемых в них актов, действий или операций *разделяются на несколько зон доступности* (*классов безопасности*), которые учитывают степень важности различных частей объекта с точки зрения возможного ущерба от криминальных угроз.

Зоны безопасности располагаются последовательно, от забора на территории объекта до хранилища ценностей и информации, создавая цепь чередующихся препятствий, которые придётся преодолевать злоумышленнику.

Для определения категории помещения создаётся комиссия, состоящая из председателя и не менее трёх членов. В результате действия комиссии создаётся Акт категорирования помещения. *Повторные категорирования помещения проводят ежегодно.*

Категорирование помещений

Акт категорирования помещения содержит следующие пункты:

-высший гриф секретности информации, циркулирующей в защищаемом помещении;

-объём циркулирующей в помещении информации с высшим грифом секретности;

- основание для категорирования;

- ранее установленная категория;

- установленная категория.

На основании вышеуказанных классов определяются категории помещений в условиях конкретной организации.

Обеспечение режима в защищаемых помещениях

Обеспечение режима в ЗП сводится в основном к регламентации доступа и использования ТСО производственной и трудовой деятельности и обработки конфиденциальной информации в традиционных или автоматизированных режимах. Она, как правило, проводится *силами службы безопасности* путём использования простейших организационных мер и доступных для этого *технических средств (ТС).*

Обеспечение режима предусматривает:

- определение категорий помещений;
- определение границ контролируемой зоны;
- определение технических средств, используемых для обработки конфиденциальной информации в пределах контролируемой зоны;
- определение опасных с точки зрения возможности образования каналов утечки информации или способов несанкционированного доступа (НСД) к ней через технические средства;

Обеспечение режима в защищаемых помещениях

Обеспечение режима предусматривает (*продолжение*):

-реализацию мер локализации или воспрещения возможных каналов утечки конфиденциальной информации или способов НСД к ней;

-организацию контроля (поиска и обнаружения) возможного неконтролируемого излучения опасных сигналов за счёт побочных электромагнитных излучений и наводок (ПЭМИН) или специально используемых для этого сигналов;

-организацию системы допуска персонала в контролируемую зону;

- организацию строгого контроля прохода и проноса каких-либо предметов, устройств, средств, механизмов в контролируемую зону, способных представлять собой технические средства получения и передачи конфиденциальной информации

Организация защиты информации

Основные методы технической защиты информации

В организациях работа по технической защите информации, как правило, состоит из двух этапов:

- построение или модернизация системы защиты:
- поддержание защиты информации на требуемом уровне.

Построение системы защиты информации проводится во вновь создаваемых организациях, в остальных - модернизация существующей.

В зависимости от целей, порядка проведения и применяемого оборудования методы и способы защиты информации от утечки по техническим каналам можно разделить на организационные, правовые и технические [1].

Организация защиты информации

Организационные способы защиты

Эти мерыосуществляются без применения специальной техники и предполагают следующее:

-установление контролируемой зоны вокруг объекта;

- введение частотных, энергетических, временных и пространственных ограничений в режимы работы технических средств приема, обработки, хранения и передачи информации (ТСПИ);

- отключение на период проведения закрытых совещаний вспомогательных технических средств и систем (ВТСС), обладающих качествами электроакустических преобразователей (телефон, факс и т.п.), от соединительных линий;

ВТСС[1];

- применение только сертифицированных ТСПИ и

Организация защиты информации

Организационные способы защиты

Эти мероприятия осуществляются без применения специальной техники и предполагают (*продолжение*):

- привлечение к строительству и реконструкции защищенных помещений, монтажу аппаратуры ТСПИ, а также к работам по защите информации исключительно организаций, лицензированных соответствующими службами на деятельность в данной области;
- категорирование и аттестование объектов информатизации (ОИ) и защищаемых помещений на соответствие требованиям обеспечения ЗИ при проведении работ со сведениями различной степени;
- режимное ограничение доступа на объекты размещения ТСПИ и в выделенные помещения

Организация защиты информации

Поисковые мероприятия

Портативные подслушивающие (закладные) устройства (ЗУ) выявляют в ходе проведения специальных обследований и проверок. Обследование объектов размещения ТСПИ и защищаемых помещений выполняется без применения техники путем визуального осмотра. В ходе спецпроверки, выполняемой с применением пассивных (приемных) и активных поисковых средств, осуществляется:

- контроль радиоспектра и ПЭМИ ТСПИ;
- выявление с помощью сканеров, интерсепторов, индикаторов ЭМП, частотомеров или программно-аппаратных комплексов контроля негласно установленных ЗУ;
- специальная проверка защищаемых помещений, ТСПИ и ВТСС с использованием нелинейных локаторов и мобильных рентгеновских установок [1]

Организация защиты информации

Техническая защита

Подобные мероприятия проводятся с применением как пассивных, так и активных защитных приемов и средств. Нейтрализация каналов утечки достигается путем ослабления уровня информационных сигналов или снижения соотношения сигнал/шум в тракте передачи до величин, исключающих возможность перехвата за пределами контролируемой зоны.

К *пассивным техническим способам защиты* относят:

- установку систем ограничения и контроля доступа на объектах размещения ТСПИ и в выделенных помещениях;
- экранирование ТСПИ и соединительных линий средств;
- заземление ТСПИ и экранов соединительных линий приборов;
- встраивание в ВТСС, обладающие «микрофонным» эффектом и имеющие выходы за пределы контролируемой зоны, специальных фильтров;
- звукоизоляция выделенных помещений;
- ввод автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ и др. [1].

Организация защиты информации

Техническая защита

Активное воздействие на каналы утечки осуществляют путем реализации:

- пространственного зашумления, создаваемого генераторами электромагнитного шума;
- прицельных помех, генерируемых на рабочих частотах радиоканалов подслушивающих устройств специальными передатчиками;
- акустических и вибрационных помех, генерируемых приборами виброакустической защиты;
- подавления диктофонов устройствами направленного высокочастотного радиоизлучения;
- зашумления электросетей, посторонних проводников и соединительных линий ВТСС, имеющих выход за устройств [1].

Обеспечение защиты информации в чрезвычайных ситуациях

Защита информации в чрезвычайных ситуациях

- порядок формирования, задачи и основные направления деятельности нештатного подразделения предприятия – специальной комиссии, создаваемой приказом руководителя предприятия в целях выработки мер по предупреждению чрезвычайных ситуаций на предприятии, а также мер по защите информации при возникновении чрезвычайных ситуаций;
- практические меры, направленные на недопущение нанесения ущерба информационной безопасности предприятия вследствие возникновения чрезвычайной ситуаций, в том числе на предотвращение утечки защищаемой информации, утраты, хищения или уничтожения носителей конфиденциальной информации;

Обеспечение защиты информации в чрезвычайных ситуациях

Защита информации в чрезвычайных ситуациях

(продолжение)

– анализ возможных угроз и различных факторов, приводящих к возникновению на предприятии чрезвычайных ситуаций.

Особое внимание уделяется вопросам координации действий всех структурных подразделений, участвующих в решении задач защиты информации.

Пропускной режим и охрана объектов организации (предприятия)

Пропускной режим и охрана объектов предприятия – организационные мероприятия по созданию и совершенствованию системы пропускного режима и охраны, такие как:

- подготовка приказов о вводе в действие или о выводе из действия всех видов пропусков, о назначении ответственных должностных лиц;
- разработка и переработка инструкций и положений, мероприятия по материально-техническому обеспечению, установке и эксплуатации технических средств охраны и др.

Обеспечение защиты информации в чрезвычайных ситуациях

При планировании мероприятий по защите информации учитываются все возможные виды и способы проявления чрезвычайных ситуаций, мероприятия по защите информации при возникновении чрезвычайных ситуаций отражаются в соответствующих планах (его структурных подразделений) работы предприятия на календарный месяц.

В данном разделе плана (либо в отдельном приложении к плану) указываются также:

- фамилия, имя, отчество, домашний адрес и контактные телефоны (в том числе мобильной связи) каждого сотрудника, принимающего участие в ликвидации последствий чрезвычайной ситуации на объектах предприятия;
- очерёдность и порядок вызова (оповещения) всех сотрудников, участвующих в выполнении работ по ликвидации последствий чрезвычайной ситуации, в зависимости от её вида, сроки прибытия этих сотрудников на объекты

Обеспечение защиты информации в чрезвычайных ситуациях

В данном разделе плана (либо в отдельном приложении к плану) указываются также (*продолжение*):

- обязанности каждого сотрудника предприятия и последовательность выполнения им мероприятий (работ) в соответствии с конкретным планом действий;
- перечень сил и средств (в том числе транспортных средств и средств связи), привлекаемых к решению задач ликвидации последствий чрезвычайных ситуаций;
- места стоянки и маршруты движения транспортных средств, эвакуирующих носители конфиденциальной информации (в том числе крупногабаритные);
- маршруты эвакуации носителей конфиденциальной информации, места их сосредоточения, способы и порядок охраны эвакуированных носителей (крупногабаритных изделий), привлекаемые для охраны силы и средства (в том числе штатных подразделений охраны).

Организация защиты информации

Техническая защита

Технические методы защиты информации, используемые в комплексе с организационными методами, играют большую роль в обеспечении защиты информации при её хранении, накоплении и обработке с использованием средств автоматизации. Технические методы необходимы для эффективного применения имеющихся в распоряжении предприятия средств защиты информации, основанных на новых информационных технологиях.

Контрольные вопросы

- Почему для слабоформализуемых задач сложно найти оптимальное решение?
- Чем отличается система от совокупности ее элементов?
- Особенности системы технической защиты по сравнению с системой в виде структурного подразделения, организации и т. д.
- Параметры системы защиты.
- Что представляет собой процесс системы инженерно-технической защиты информации?
- Особенности системного мышления.
- Что надо априори знать для формулирования целей и задач инженерно-технической защиты информации?
- Что представляет собой ресурс системы защиты информации?
- Чему равны суммарные расходы на информацию?
- Физический смысл рациональной области защиты информации.
- Что надо определить перед выбором мер защиты информации?
- Что представляют собой локальные и глобальный показатели эффективности защиты информации?