ГБПОУ СПТ им. Б.Г.Музрукова

МДК.03.01. Технические методы и средства , технологии защиты информации
Раздел 4. Организационные основы инженерно-технической защиты информации

Лекция 38

Типовые меры по инженерно-технической защите информации

Разработчик: Столяров И.В.,
преподаватель ГБПОУ СПТ им. Б.Г.Музрукова

г. Саров
2017

План лекции

1. **Основные организационные и технические меры по обеспечению инженерно-технической защиты информации.**
2. **Контроль эффективности инженерно-технической защиты информации.**

Построение (модернизация) системы защиты информации и поддержание на требуемом уровне ее защиты в организации предусматривают проведение следующих основных работ:

- уточнение перечня защищаемых сведений в организации, определение источников и носителей информации, выявление и оценка угроз ее безопасности;
- определение мер по защите информации, вызванных изменениями целей и задач защиты, перечня защищаемых сведений, угроз безопасности информации;
- контроль эффективности мер по инженерно-технической защите информации в организации.

Меры по защите информации целесообразно разделить на две группы: организационные и технические.

Классификация **организационных мер** ИТЗИ приведена на рис. 26.1.

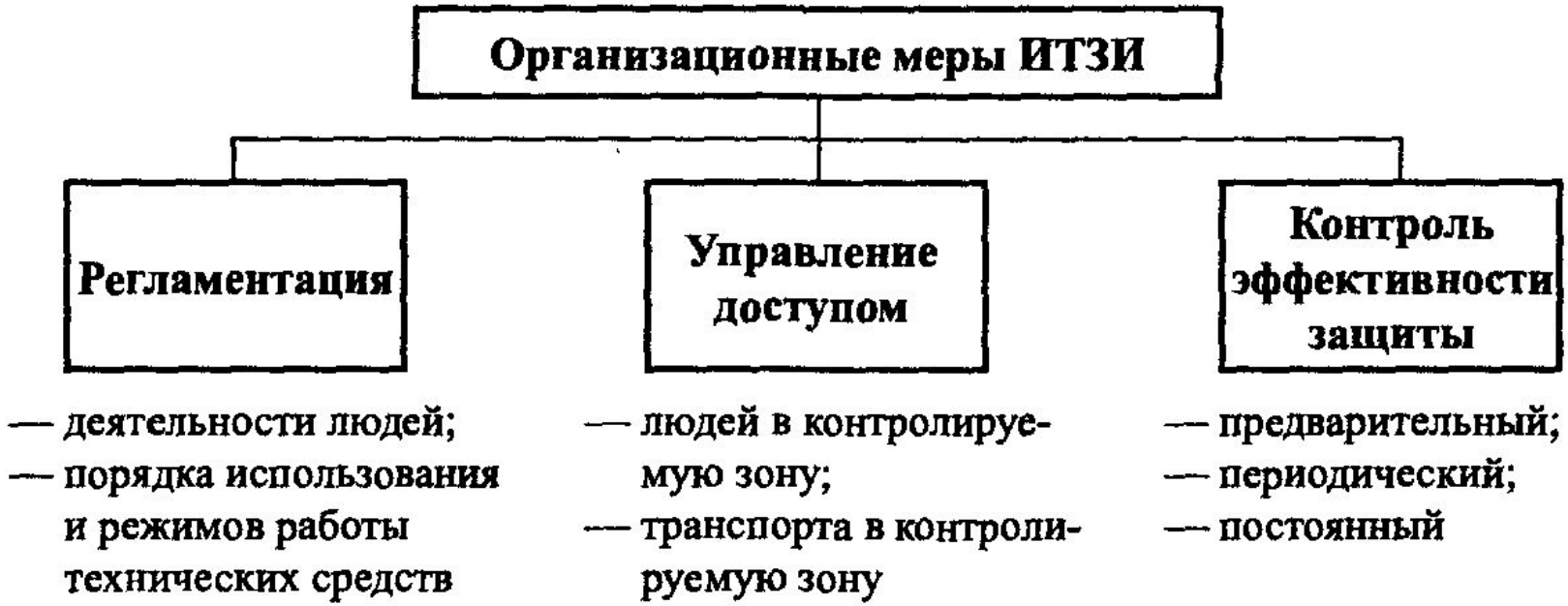

Рис. 26.1. Структура организационных мер

Регламентация — это установление временных, территориальных и режимных ограничений в деятельности сотрудников организации и работе технических средств, направленных на обеспечение безопасности информации.

Регламентация предусматривает:

- установление границ контролируемых и охраняемых зон;
- определение уровней защиты информации в зонах;
- регламентация деятельности сотрудников и посетителей (разработка распорядка дня, правил поведения сотрудников в организации и вне ее и т. д.);
- определение режимов работы технических средств, в том числе сбора, обработки и хранения защищаемой информации на ПЭВМ, передачи документов, порядка складирования продукции и т. д.

Управление доступом к информации включает мероприятия, обеспечивающие санкционированный доступ к ней людей, средств и сигналов. Оно предусматривает:

- идентификацию лиц и обращений;
- проверку полномочий лиц и обращений;
- регистрацию обращений к защищаемой информации;
- реагирование на обращения к информации.

Идентификация пользователей, сотрудников, посетителей, обращений по каналам телекоммуникаций проводится с целью их надежного опознавания.

Проверка полномочий заключается в определении прав лиц и обращений по каналам связи на доступ к защищаемой информации. Для доступа к информации уровень полномочий обращения не может быть ниже разрешенного. С целью обеспечения контроля над прохождением носителей с закрытой информацией производится регистрация (протоколирование) обращений к ним путем записи в карточках, журналах, на магнитных носителях.

К **техническим** относятся меры, реализуемые путем установки новых или модернизации используемых инженерных конструкций и технических средств защиты информации. Технические меры предусматривают применение методов, способов и средств, типовой перечень которых приведен в табл. 26.1.

Меры, определяющие порядок использования этих средств, составляют основу организационных мер инженерно-технической защиты информации.

Таблица 26.1

№ п/п	Вид угрозы	Методы защиты	Средства инженерно-технической защиты
1	2	3	4
1	Преднамеренные воздействия злоумышленников на источники информации	Укрепление механической прочности рубежей	Инженерные конструкции: бетонные заборы, колючая проволока, толстые стены и перекрытия, решетки и пленки на окнах, металлические двери, хранилища и сейфы
		Обнаружение злоумышленников	Охранные извещатели, телевизионные средства наблюдения
		Нейтрализация преднамеренных воздействий	Средства тревожной сигнализации, оружие, средства пожаротушения, средства резервного электропитания
2	Пожар	Уменьшение теплопроводности среды	Огнеупорные сейфы помещения
		Обнаружение пожара	Пожарные извещатели
		Нейтрализация пожара	Огнетушители, автоматические системы пожаротушения
3	Наблюдение	Пространственное скрытие объектов наблюдения	Тайники
		Временное скрытие объектов наблюдения	Чехлы, естественные и искусственные маски во время работы средств наблюдения
		Маскировка объектов наблюдения	Естественные и искусственные маски, краски для маскировочного окрашивания, ложные объекты, пеиы, дымы, уголковые отражатели, линзы Люнеберга, средства уменьшения ЭПР объекта радиолокационного наблюдения (маски, поглощающие материалы)

1	2	3	4
		Засветка и ослепление	Яркие источники света, дипольные отражатели, генераторы помех радиолокационным станциям
4	Подслушивание	Кодирование слов речевого сообщения. Кодирование символов сообщения	Шифраторы
		Частотно-временное преобразование сигналов	Скремблеры
		Цифровое шифрование медленно изменяющихся характеристик речевых сигналов	Вокодеры
		Звукоизоляция и звукопоглощение	Ограждения, акустические экраны, кабины, кожухи, глушители, звукопоглощающие материалы
		Снижение уровня опасных электрических и радиосигналов	Средства отключения радиоэлектронных средств, фильтры опасных сигналов, ограничители малых амплитуд, буферы, экраны, конденсаторы для симметрирования кабелей, генераторы линейного и пространственного зашумления
		Обнаружение, локализация и изъятие закладных устройств	Обнаружители поля, интерсепторы, бытовые радиоприемники с конверторами,специальныерадиоприемники, анализаторы спектра, сканирующие радиоприемники, автоматизированные комплексы радиомониторинга, металлодетек-

1	2	3	4
			торы, нелинейные локаторы, обнаружители пустот, средства интерскопии, средства контроля напряжения и тока телефонных линий, измерители электрических параметров телефонных линий, кабельные радары, средства обнаружения скрытно работающих диктофонов, средства нарушения работы и уничтожения закладных устройств, генераторы прицельной и заградительной помехи
5	Перехват		Экраны, средства передачи информации широкополосными сигналами и сигналами с псевдослучайным изменением частоты, генераторы помех
6	Сбор и анализ отходов производства		Шредеры, устройства магнитного стирания, механические прессы, средства очистки демаскирующих веществ

Важнейшее и необходимое направление работ по защите информации — **контроль эффективности защиты информации**. Контроль проводится силами службы безопасности, руководителями организации и структурных подразделений, всеми сотрудниками организации, допущенными к закрытой информации.

Применяют следующие виды контроля:

- предварительный;
- периодический;
- постоянный.

Предварительный контроль проводится при любых изменениях состава, структуры и алгоритма функционирования системы защиты информации, в том числе:

- после установки нового технического средства защиты или изменения организационных мер;
- после проведения профилактических и ремонтных работ средств защиты;
- после устранения выявленных нарушений в системе защиты.

Периодический контроль осуществляется с целью обеспечения систематического наблюдения за уровнем защиты. Он проводится выборочно (применительно к отдельным темам работ, структурным подразделениям или всей организации) по планам, утвержденным руководителем организации, а также вышестоящими органами.

Наиболее часто должен проводиться периодический контроль на химических предприятиях, так как незначительные нарушения в технологическом процессе могут привести к утечке демаскирующих веществ. Для определения концентрации демаскирующих веществ регулярно берутся возле предприятия пробы воздуха, воды, почвы, снега, растительности.

Периодичность и места взятия проб определяются характером производства с учетом условий возможного распространения демаскирующих веществ, например розы ветров и скорости воздушных потоков, видов водоемов (искусственный, озеро, болото, река и др.), характера окружающей местности и т. д. Пробы воздуха рекомендуется брать с учетом направлений ветра на высоте примерно 1,5 м в непосредственной близости от границ территории (50–100 м) и в зоне максимальной концентрации демаскирующих веществ, выбрасываемых в атмосферу через трубы. Пробы воды берутся в местах слива в водоемы в поверхностном слое и на глубине 30–50 см с последующим смешиванием. Берутся также пробы почвы и пыли на растительности. С этой целью собирают листья с нескольких деревьев и кустов на уровне 1,5–2 м от поверхности и не ранее недели после дождя.

Периодический (ежедневный, еженедельный, ежемесячный) контроль должен проводиться также сотрудниками организации в части источников информации, с которыми они работают.

Общий (в рамках всей организации) периодический контроль проводится временными внутренними и внешними комиссиями обычно 2 раза в год. Целью его является тщательная проверка работоспособности всех элементов и системы защиты информации в целом. Так как о времени работы комиссии сотрудникам организации (предприятия) заранее известно, то эти проверки выявляет в основном недостатки, не устраненные перед началом работы комиссии.

Постоянный контроль осуществляется выборочно силами службы безопасности и привлекаемых сотрудников организации с целью объективной оценки уровня защиты информации и, прежде всего, выявления слабых мест в системе защиты организации. Так как объекты и время такого контроля сотрудникам не известны, то такой контроль, кроме того, оказывает психологическое воздействие на сотрудников организации, вынуждая их более тщательно и постоянно выполнять требования по обеспечению защиты информации.

Следует также отметить, что добросовестное и постоянное выполнение сотрудниками организации требований по защите информации основывается на рациональном сочетании способов принуждения и побуждения.

Принуждение — способ, при котором сотрудники организации вынуждены соблюдать правила обращения с источниками и носителями конфиденциальной информации под угрозой административной или уголовной ответственности.

Побуждение предусматривает создание у сотрудников установки на осознанное выполнение требований по защите информации, формирование моральных, этических, психологических и других нравственных мотивов. Воспитание побудительных мотивов у сотрудников организации является одной из задач службы безопасности, но ее усилия найдут благодатную почву у тех сотрудников, которые доброжелательно относятся к руководству организации и рассматривают организацию как долговременное место работы. Создание условий и традиций, при которых место работы воспринимается как второй дом, является, по мнению компетентных аналитиков, одним из факторов экономического роста Японии. Поэтому на строгость и точность выполнения сотрудниками требований по защите информации в значительной степени влияет климат в организации, который формируется ее руководством.

Эффективность защиты информации от технической разведки оценивается методами **технического контроля**. В ходе его производится определение технических параметров носителей информации. В результате сравнения их с нормативными значениями принимается решение об уровне безопасности защищаемой информации.

Технические меры контроля проводятся с использованием технических средств радио- и электрических измерений, физического и химического анализа и обеспечивают проверку:

- напряженности полей с информацией на границах контролируемых зон;
- уровней опасных сигналов и помех в проводах и экранах кабелей, выходящих за пределы контролируемой зоны;
- степени защумления генераторами помех структурных звуков в ограждениях;
- концентрации демаскирующих веществ в отходах производства.

Для измерения напряженности электрических полей используются селективные вольтметры, анализаторы спектра, панорамные приемники.

Различают три вида технического контроля:

- инструментальный;
- инструментально-расчетный;
- расчетный.

Инструментальные методы контроля обеспечивают наиболее точные результаты, так как они реализуются с помощью средств измерительной техники в местах контроля, прежде всего на границе контролируемой зоны. Так как измеряемые уровни опасных сигналов сравнимы с уровнями шумов, то для инструментального контроля необходимы высокочувствительные дорогостоящие измерительные приборы. Это обстоятельство существенно затрудняет реальные возможности проведения контроля.

Наибольшие проблемы возникают при инструментальном контроле ПЭМИН, так как частоты побочных излучений охватывают практически весь радиодиапазон, а их уровни соизмеримы с электромагнитным фоном. Стандартная контрольно-измерительная аппаратура не обеспечивает проведение исследований ПЭМИН в необходимом объеме. Поэтому для этих целей используются дорогостоящие специальные приборы и приборы для физических научных исследований. Для измерений сигналов ПЭМИН применяются измерительные приемники, селективные микровольтметры и анализаторы спектра с техническими характеристиками:

- диапазон частот — десятки Гц–десятки ГГц;
- чувствительность — десятки–сотни нВ;
- динамический диапазон — 100–150 дБ;
- избирательность — единицы Гц–единицы МГц;
- точность измерения уровня сигнала — 1–2 дБ.

Так как многие сигналы ПЭМИН имеют импульсный характер и согласно требованиям нормативно-методических документов, эти приборы должны оснащаться пиковыми и квазипиковыми детекторами. Очень полезно для возможности автоматизации измерений наличие у измерительных приборов программно-аппаратного интерфейса с ПЭВМ. С целью комплексного решения проблем исследований ПЭМИН ведущие организации в области производства технических средств защиты информации «Нелк», «Иркос», «Маском», «Элерон» и др. выпускают постоянно совершенствуемые автоматизированные комплексы для измерений излучений ПЭМИН.

Инструментально-расчетный технический контроль позволяет снизить требования к параметрам измерительной техники. Эти методы предполагают проведение измерений не на границе контролируемой зоны, а вблизи возможных источников сигналов (ОТТС). Возле источников сигналов уровни сигналов выше и, соответственно, требования к чувствительности измерительных приборов ниже. Уровни же сигналов в местах проведения контроля рассчитываются по соответствующим методикам расчета. Так как в качестве исходных данных для расчета применяются результаты измерений, то точность контроля будет определяться точностью измерений и используемого математического аппарата.

Наконец, если отсутствуют требуемые для инструментального или инструментально-расчетного контроля измерительные приборы, то осуществляется **расчетный** технический контроль путем проведения расчетов по априорным или справочным исходным данным. Существующие методы расчетного технического контроля обеспечивают приемлемые для практики результаты при оценке угроз подслушивания и наблюдения. Для оценки этих угроз существует достаточно большой выбор данных в справочниках по акустике и оптике. Например, в справочнике по акустике приводятся данные об уровне громкости речи в помещении, величины звукоизоляции для различных ограждений, уровни акустических шумов для различных видов деятельности, по которым легко рассчитывается отношение сигнал/шум в точке контроля, например в коридоре или соседнем помещении.

Меры контроля, так же как и защиты, представляют совокупность организационных и технических мероприятий, проводимых с целью проверки выполнения установленных требований и норм по защите информации. Организационные меры контроля включают:

- проверку выполнения сотрудниками требований руководящих документов по защите информации;
- проверку работоспособности средств охраны и защиты информации от наблюдения, подслушивания, перехвата и утечки информации по материально-вещественному каналу (наличие занавесок, штор, жалюзей на окнах, чехлов на разрабатываемых изделиях, состояние звукоизоляции, экранов, средств подавления опасных сигналов и зашумления, емкостей для сбора отходов с демаскирующими веществами и т. д.);
- контроль за выполнением инструкций по защите информации о разрабатываемой продукции;
- оценку эффективности применяемых способов и средств защиты информации.

Вопросы для самопроверки

1. Основные организационные меры по инженерно-технической защите информации.
2. Основные методы и средства инженерно-технической защиты информации от различных видов угроз.
3. Виды контроля эффективности инженерно-технической защиты информации.
4. Сущность постоянного контроля и его формы.
5. Виды технического контроля и когда они применяются?

Литература

1. *Гарсиа М.* Проектирование и оценка систем физической защиты. Пер. с англ. — М.: АСТ, 2002.
2. *Каторин Ю. Ф., Куренков Е. В., Лысов А. В., Остапенко А. Н.* Энциклопедия промышленного шпионажа. — СПб.: Полигон, 2000.
3. *Меньшаков Ю. К.* Защита информации от технических средств разведки. — М.: РГГУ, 2002.
4. *Петраков А. В., Дорошенко П. С., Савлуков Н. В.* Охрана и защита современного предприятия. — М.: Энергоатомиздат, 1999.
5. Специальная техника и информационная безопасность: Учебник. Т. 1 / Под ред. *В. И. Кирина.* — М.: Академия управления МВД России, 2000.
6. *Торокин А. А.* Инженерно-техническая защита информации. — М.: Гелиос АРВ, 2005.
7. *Хорев А. А.* Способы и средства защиты информации. — М.: МО РФ, 1998.
8. *Хорев А. А.* Теоретические основы оценки возможностей технических средств разведки. — М.: МО РФ, 2000.