Тульской государственный университет

Курсы повышения квалификации

Техническая защита информации

Лекция:

Цели и задачи ТЗКИ.

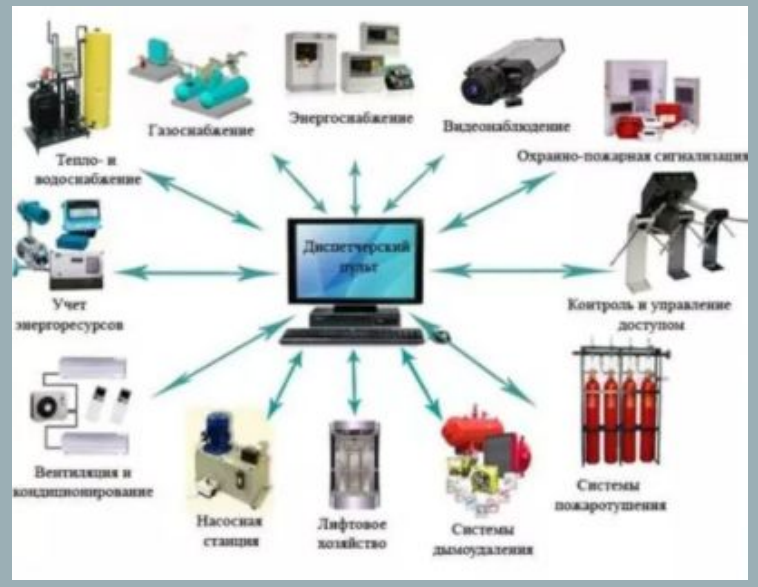
Защищаемая информация

и информационные ресурсы.

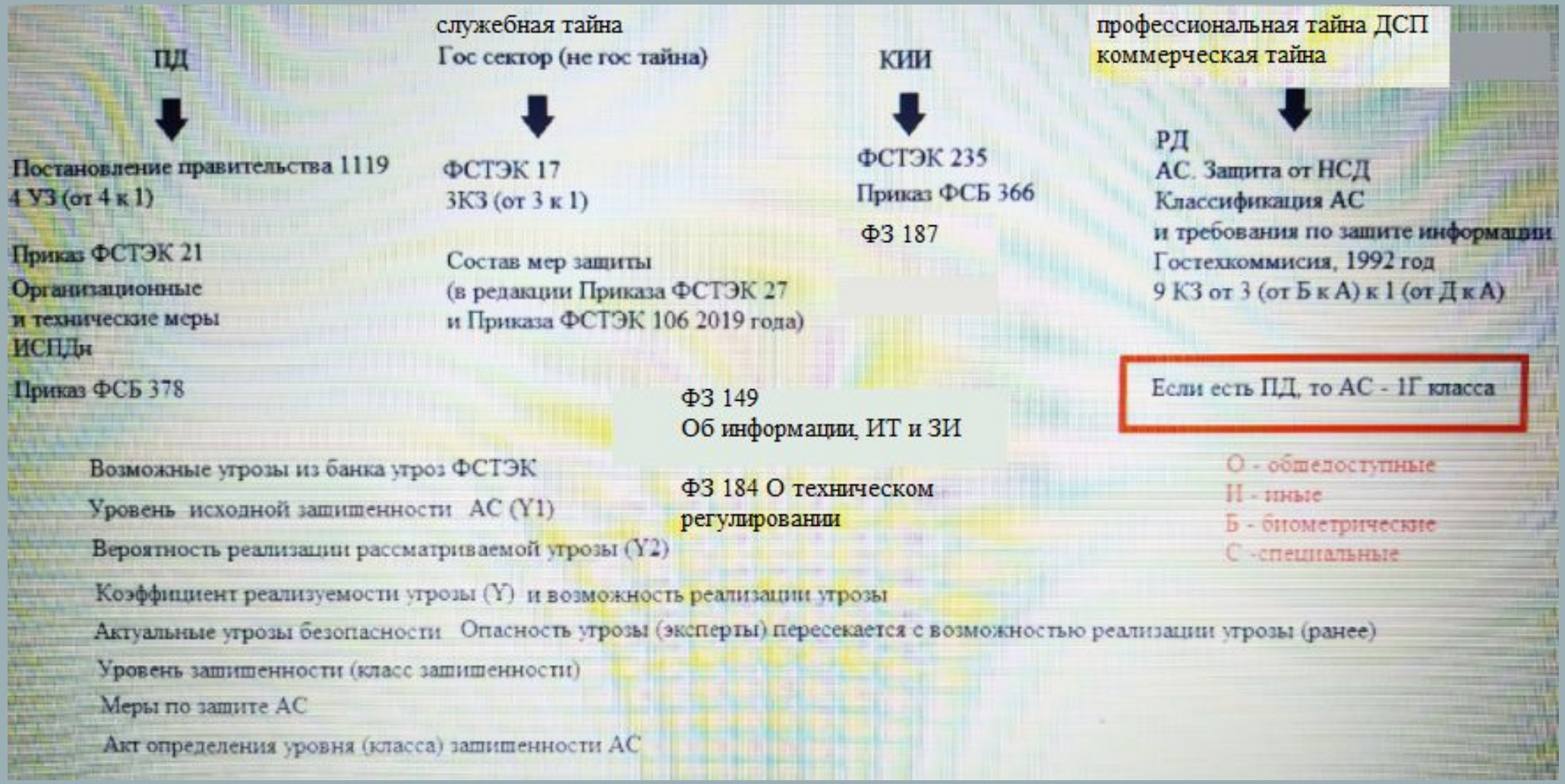
Объекты защиты.

Правовые и организационные основы

защиты информации ограниченного доступа



Техническая защита информации.
Виды защищаемой информации



Техническая защита информации. Виды защищаемой информации

Служебная тайна — это сведения, которые стали известны государственным органам и имеют ограниченный доступ. Это не то же самое, что коммерческая тайна: она может принадлежать и частным организациям, не только государственным. И это не то же, что профессиональная тайна: она тоже становится известна при исполнении профессиональных обязанностей, но может быть получена врачами, нотариусами, адвокатами, то есть не только госслужащими.

Необходимо отметить, что профессиональные тайны отличаются от других производных тайн тем, что, с одной стороны, в качестве субъекта – носителя тайны здесь выступает профессионал и именно по этой причине ему доверяется информация. С другой стороны, деятельность данного профессионала, как правило, характеризуется публичностью, соответственно, отношения по поводу профессиональной тайны имеют частно-публичный характер.

Техническая защита информации. Виды защищаемой информации

Примерный перечень сведений, составляющих коммерческую тайну, может выглядеть таким образом:

- Список клиентов и поставщиков.
- Информация об условиях заключенных договоров и о потенциальных сделках.
- Информация о ходе переговоров с контрагентами.
- Методика ценообразования.
- Финансовая информация о структуре себестоимости.
- Составляющие коммерческую тайну предприятия сведения о размерах, видах и условиях кредитов.
- Информация из управленческой отчетности.
- Стратегические и операционные планы, бюджеты, инвестиционные проекты, маркетинговые исследования, рекламные кампании.
- Информация о незапатентованных изобретениях.
- Информация о планируемых разработках или модернизациях.
- Информация о технологических характеристиках выпускаемой продукции.
- Информация о видах и состоянии используемого программного обеспечения.
- Информация, позволяющая получить доступ к программному обеспечению и компьютерной технике.
- Сведения о системах внутренней безопасности и охраны.
- Сведения о порядке и датах внутренних проверок.
- Сведения о результатах совещаний.
- Сведения о заработной плате сотрудников.
- Информация о методах управления и внутренней организации предприятия.
- Деловая переписка.

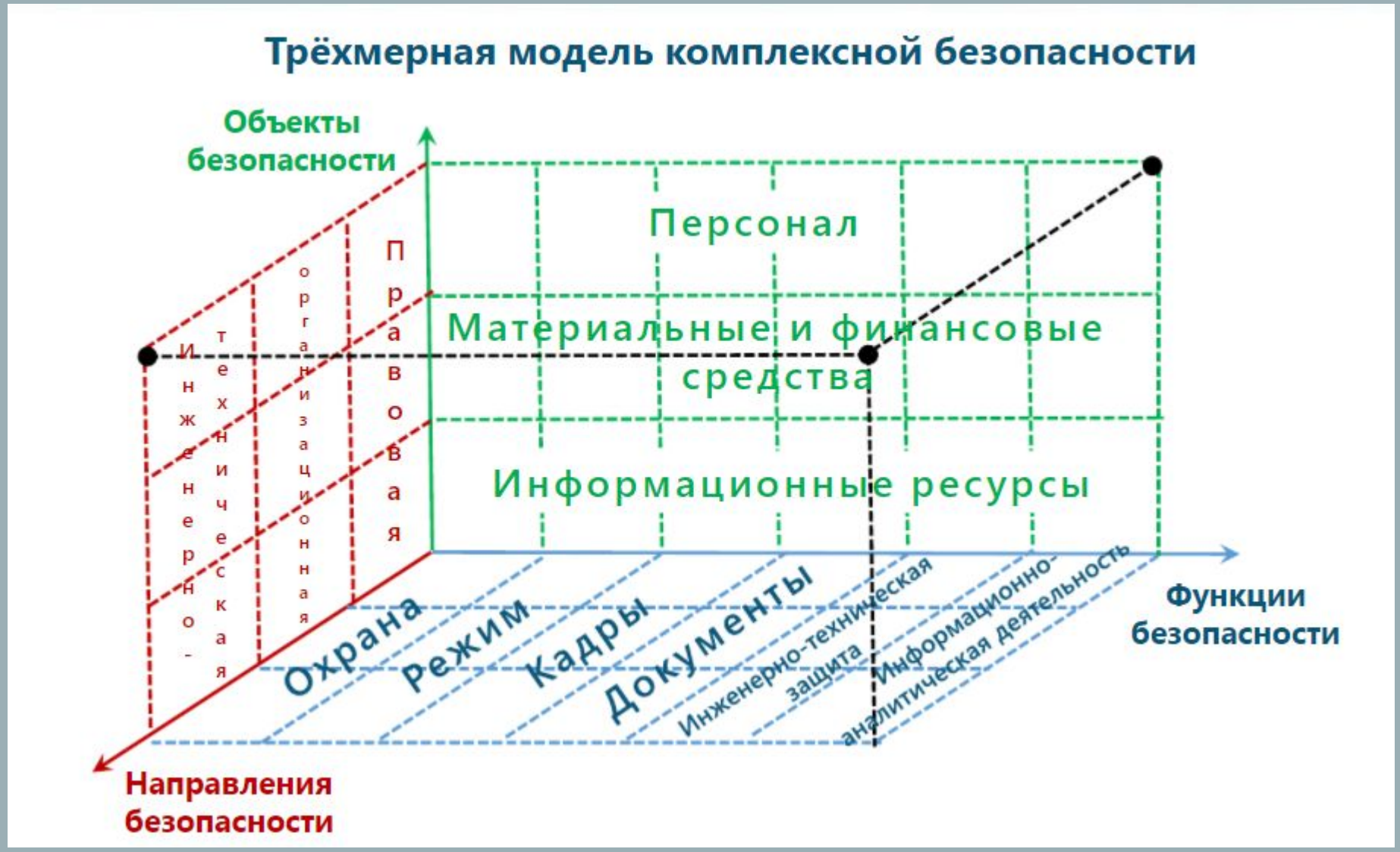
Техническая защита информации. Виды защищаемой информации

Что относится к сведениям, которые не могут составлять коммерческую тайну предприятия

Такие сведения оговорены в ст. 5 закона № 98-ФЗ и включают в себя информацию:

- указанную в учредительных документах и документах о регистрации юрлица или ИП в госорганах;
- указанную в разрешениях на коммерческую деятельность;
- об использовании бюджетных средств и об имуществе госучреждений и государственных (муниципальных) унитарных предприятий;
- влияющую на безопасность отдельных граждан или всего населения (о влиянии на окружающую среду, о соблюдении противопожарной, санитарной техники безопасности, безвредность пищевых продуктов и т. д.);
- относящуюся к кадровой (количество работников, их состав, система оплаты труда, условия и охрана труда, травматизм и проф. заболевания, имеющиеся вакансии, задолженность по зарплате и соцвыплатам);
- о противозаконных действиях и понесенных за это наказаниях;
- об условиях приватизации госсобственности;
- для некоммерческих организаций: о доходах, расходах, имуществе, о количестве сотрудников и их зарплате, об использовании бесплатного труда;
- о списке лиц, которые выступают от имени организации без доверенности;
- прочая информация, необходимость раскрытия которой указана в других законах.

Техническая защита информации. Основные аспекты



Технические (инженерно-технические) средства защиты информации

ИНЖЕНЕРНО–ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ

Под инженерно-техническими средствами защиты информации понимают физические объекты, механические, электрические и электронные устройства, элементы конструкции зданий, средства пожаротушения и другие средства, которые обеспечивают:

- защиту территории и помещений КС от проникновения нарушителей;
- защиту аппаратных средств КС и носителей информации от хищения;
- предотвращение возможности удаленного (из–за пределов охраняемой территории) видеонаблюдения (подслушивания) за работой персонала и функционированием технических средств КС;
- предотвращение возможности перехвата ПЭМИН (побочные электро-магнитные наводки), вызванных работающими техническими средствами КС и линиями передачи данных; организацию доступа в помещения КС сотрудников;
- контроль над режимом работы персонала КС; контроль над перемещением сотрудников КС в различных производственных зонах;
- противопожарную защиту помещений КС;
- минимизацию материального ущерба от потерь информации, возникших в результате стихийных бедствий и техногенных аварий.

Важнейшей составной частью инженерно-технических средств защиты информации являются технические средства охраны, которые образуют первый рубеж защиты КС и являются необходимым, но недостаточным условием сохранения конфиденциальности и целостности информации в КС.

Основные задачи организационно-технических требований по технической защите информации. Организационные основы ТЗИ

Основные цели

- организация и осуществление мер по обеспечению безопасности деятельности и защите информации всеми возможными в конкретных условиях способами и средствами;
- предупреждение проникновения в служебные помещения, в охраняемые зоны и на территорию фирма посторонних лиц;
- обеспечение порядка вноса (выноса), ввоза (вывоза) финансовых и материальных ценностей и входа (выхода) сотрудников и клиентов.

Примечание

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

Требования внутриобъектового режима

Внутриобъектовый режим - установленный порядок выполнения правил внутреннего трудового распорядка, направленных на обеспечение безопасности, сохранения материальных средств и защиты конфиденциальной информации.

Основные цели

- установление четкого распорядка рабочего времени;
- строгое соблюдение сотрудниками правил экономической и информационной безопасности, правил противопожарной и противоаварийной безопасности и техники безопасности;
- установление порядка приема и работы с посетителями сторонних организаций;
- оборудование фирмы техническими средствами обеспечения производственной деятельности (связь, автоматизация, охранная и пожарная сигнализация, замки, ограждения и др.);
- порядок сдачи и приема помещений под охрану;
- порядок ведения телефонных, факсовых и телекоммуникационных обменов информацией с соблюдением режима конфиденциальности.

Нарушения и возможные последствия

Требование (не определено или нарушается)

- ❑ установление четкого распорядка рабочего времени
  - бесконтрольное перемещение сотрудников;
  - отсутствие информации у руководства и службы безопасности о наличии и занятости персонала фирмы;
  - перегруженность системы контроля управления доступом;
  - подмена идентификаторов.

Возможные последствия

- кражи технических средств обработки и передачи информации;
- несанкционированное пребывание посторонних сотрудников в выделенных (защищаемых) помещениях;
- несанкционированный доступ к ОТСС и ВТСС автоматизированных систем;
- разглашение паролей.

Нарушения и возможные последствия

Требование (не соблюдается)

- ❑ строгое соблюдение сотрудниками правил экономической и информационной безопасности, правил противопожарной и противоаварийной безопасности и техники безопасности
- раскрытие паролей;
- модификация АС с целью последующего использования получаемых возможностей в преступных целях;
- установка технических средств несанкционированного съёма информации.

Возможные последствия

- разглашение конфиденциальной информации;
- физическое уничтожение средств ВТ и обеспечивающих сервисов;
- модификация конфиденциальной информации;
- отказ в обслуживании;
- заражение СВТ вирусами.

Нарушения и возможные последствия

Требование (не установлено или не соблюдается)

- ❑ установление порядка приема и работы с посетителями сторонних организаций
- бесконтрольное пребывание в помещениях фирмы посторонних;
- отвлечение сотрудников фирмы от планового исполнения служебных обязанностей;
- отвлечение сотрудников службы охраны.

Возможные последствия

- установка технических средств несанкционированного съёма информации;
- получение конфиденциальной информации через различные каналы утечки;
- ведение промышленного (коммерческого) шпионажа.

Нарушения и возможные последствия

Требование (недостаточно оборудован)

- ❑ оборудование техническими средствами обеспечения производственной деятельности (связь, автоматизация, охранная и пожарная сигнализация, замки, ограждения и др.)
- ▪ вынужденные простои ожидания *(1 принтер на всех)*;
- ▪ бесконтрольное пребывание сотрудников в различных помещениях *(зашёл, т.к. дверь была открыта)*;
- ▪ курение в неустановленных местах *(а кто узнает!?)*;
- ▪ отсутствие ответственности за средства обеспечения производственной деятельности.

Возможные последствия

- ▪ кратковременные оставления рабочих мест, способствующие кражам, съёму информации, установке вредоносных программ и т.д.;
- ▪ пожары, затопления;
- ▪ выход из строя средств обеспечения производственной деятельности.

Порядок работы со сторонними лицами

Основные действия

- принимающий специалист накануне делает заявку канцелярии на следующий день с указанием Ф.И.О. прибывающих, их места работы и времени предполагаемого прибытия;
- в день прибытия приглашенных канцелярия фиксирует их прибытие в журнале учета посетителей и приглашает специалиста фирмы;
- специалист встречает прибывших, получает в канцелярии ключи от комнаты переговоров и сопровождает туда посетителей. *Запрещается прием представителей сторонних организаций в других помещениях фирмы без специального на то разрешения директора или его заместителя;*
- в ходе работы необходимо плотно закрывать окна и шторы;
- по окончании работы с посетителями принимающий их специалист провожает их до выхода и делает в журнале учета посетителей соответствующие заметки о времени их ухода.

Примечание

Во время пребывания посетителей принимающий специалист обязан контролировать их пребывание и действия. После завершения встречи специалист фирмы закрывает комнату переговоров и сдает ключи от нее канцелярии.

Требования пропускного режима

Пропускной режим - это установленный в фирме порядок, при котором исключается возможность бесконтрольного прохода (проезда), вноса (выноса) финансовых и материальных ценностей.

- установление определенного порядка допуска на территорию объекта рабочих, служащих и посетителей;
- установление определенного порядка вывоза (выноса), ввоза (вноса) денежных и материальных ценностей;
- устройство ограждения, освещения, оборудование контрольно-проходных и проездных пунктов (постов) и бюро пропусков средствами сигнализации, связи и др. необходимой техникой, обеспечивающей осуществление пропускного режима, а также обеспечение их документацией и инвентарем;

- определение круга должностных лиц, имеющих право выдачи и подписи всех видов пропусков;
- оборудование камер хранения личных вещей и площадок для личного автотранспорта.

Система регулирования допуска в организацию стронных лиц

- объективное определение надежности лиц, допускаемых к работе;
- ограничение максимального количества лиц, допускаемых на объекты фирмы;
- установление для каждого работника (или посетителей) дифференцированного по времени, месту и виду деятельности права доступа;
- четкое определение порядка выдачи разрешений и оформления документов для входа (въезда) в фирму;
- определение объемов контрольно-пропускных функций на каждом пропускном и проездном пункте;

- оборудование контрольно-пропускных пунктов (постов) техническими средствами, обеспечивающими достоверный контроль проходящих, объективную регистрацию прохода и предотвращение несанкционированного (в том числе силового) проникновения посторонних лиц;
- высокую подготовленность и защищенность персонала контрольно-пропускных пунктов.

Требования к пропускным документам

Удостоверения и пропуска

постоянные, временные и разовые для сотрудников и посетителей, а также материальные для ввоза (вывоза) материальных ценностей.

- Проставляются печати, предусмотренные правилами режима, и цифровые знаки, определяющие зону доступности, период их действия, право проноса портфелей (кейсов, папок и др.).
- Образцы удостоверений и пропусков разрабатываются службой безопасности и утверждаются руководством фирма.
- Утвержденные образцы удостоверений личности, пропусков, оттисков цифровых знаков, печатей (штампов), проставляемых на удостоверениях и пропусках, списки с образцами подписей руководителей или уполномоченных лиц, имеющих право подписывать удостоверения и пропуска, передаются начальнику отдела режима и охраны под расписку.

Требования к пропускным документам

- Полная замена удостоверений и постоянных пропусков производится, как правило, через 3-5 лет. Через 2-3 года производится перерегистрация с проставлением соответствующей отметки.
- Для перерегистрации, замены или изменения пропускных документов ежегодно по состоянию на 1 января в службу безопасности отделом кадров направляются списки сотрудников с указанием должности, фамилии, имени, отчества и наименования документа с соответствующими пометками (круглосуточно, рабочее время с __ по __, с портфелем, в какую зону и т.п.).
- Удостоверения и постоянные пропуска выдаются указанным лицам на основании письменных ходатайств руководителей учреждений, где они состоят в штате.
- Удостоверения или постоянные пропуска выдаются сотрудникам при поступлении на работу на основании приказа о зачислении в штат.

Система управления доступом в организацию

Возможные угрозы:

- кражи средств обработки информации;
- кражи коммерческой информации;
- установка технических средств съёма информации;
- проникновение с целью грабежа;
- захват заложников;
- отключение системы сигнализации;
- ликвидация персонала охраны.

Организационно-режимные мероприятия

- ✓ составление перечня зон и помещений, куда необходимо ограничить доступ нежелательных лиц;
- ✓ категорирование зон и помещений по степени опасности;
- ✓ составление перечня лиц, которые имеют право санкционированного доступа в эти помещения;
- ✓ определенные процедур (правил) доступа.

Определяются руководством фирма совместно с ответственным за безопасность и могут быть различными в зависимости от условий и специфики работы фирмы.

Зоны доступа. Рекомендации по разделению

- вход в фирму (общий или раздельный для клиентов и сотрудников);
- вход в основные помещения;
- вход в хранилище;
- вход в центральное хранилище;
- вход в помещение архива документации;
- вход в зону дирекции;
- вход в помещение центрального пульта охраны;
- вход во вспомогательные помещения (трансформаторная подстанция, телефонные станции, система кондиционирования).

Угрозы

Устранение человеческого фактора:

- *нейтрализация охранника;*
- *подкуп;*
- *шантаж;*
- *быстрая утомляемость.*

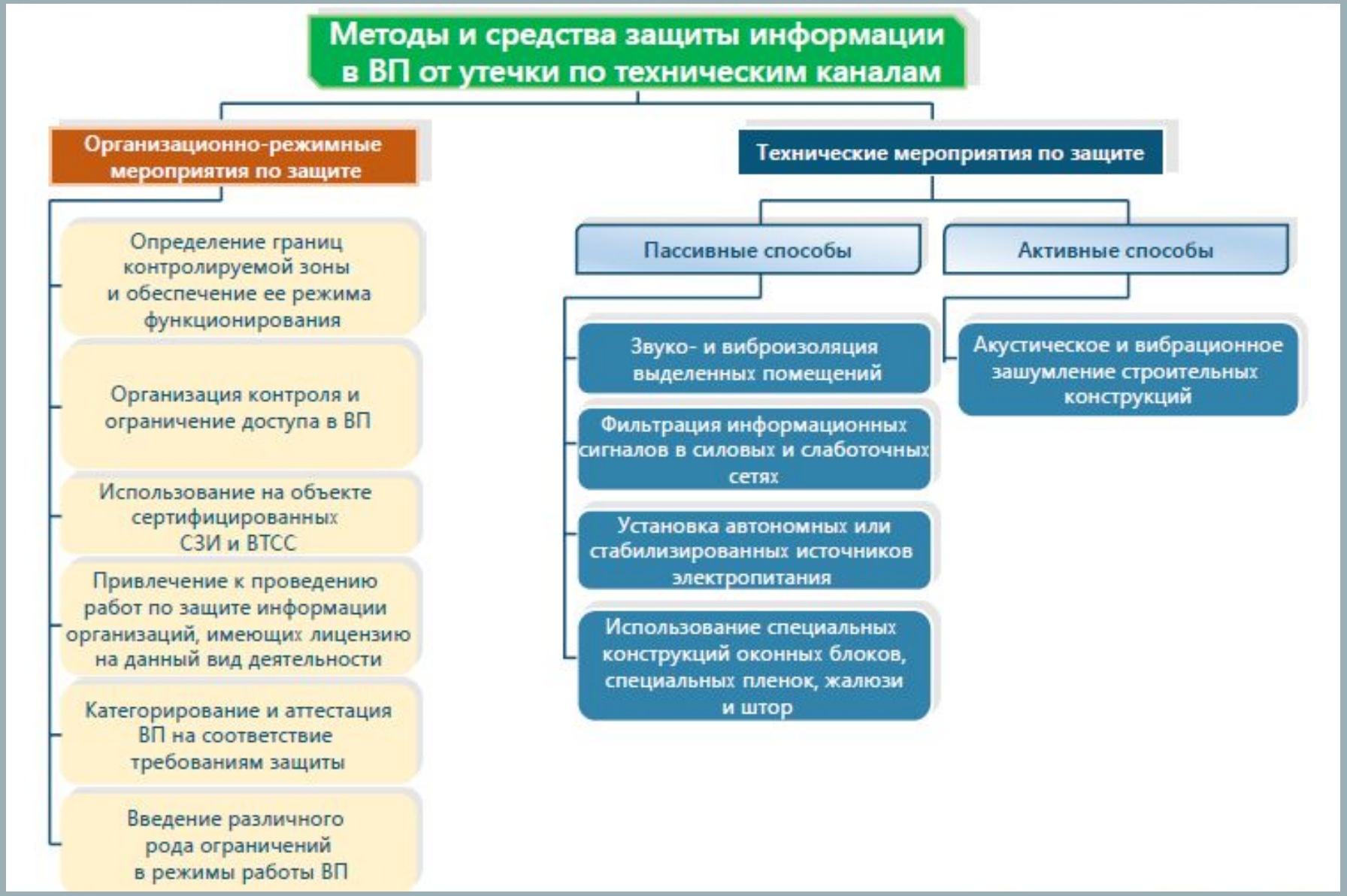
Автоматизация пропускного режима

- обеспечение санкционированного входа и выхода в заданные зоны и помещения строго определенных лиц в разрешенное время;
- учет, регистрация и документирование фактов входа/выхода и времени;
- представление информации дирекции фирмы о местонахождении сотрудников, а службе безопасности - о наличии людей в определенных зонах и состоянии запорных устройств (открыты или закрыты двери или замки);
- система должна подавать сигнал тревоги в центральный пульт управления при попытке несанкционированного прохода в помещение в неразрешенное время, а также в случаях фальсификации пропуска. *В особо уязвимых зонах должны использоваться способы нейтрализации действия нарушителя*
- *путем блокировки его в шлюзовой камере.*

Направления технической защиты конфиденциальной информации

- защита документированной КИ от несанкционированного ознакомления с ее содержанием, а также копирования, корректировки и уничтожения;
- защита речевой КИ, циркулирующей в служебных помещениях, от перехвата техническими средствами;
- защита КИ от несанкционированного снятия с телефонных линий связи общего пользования;
- защита КИ, обрабатываемой или хранящейся в средствах вычислительной техники, от несанкционированного доступа и снятия за счет побочных электромагнитных излучений и наводок.

Направления технической защиты конфиденциальной информации



ВТСС – вспомогательные технические средства и системы
ВП – выделенное помещение
СЗИ – средства защиты информации

Направления технической защиты конфиденциальной информации

Генератор шума Гном-3

Комплекс виброакустической защиты объектов информатизации "Барон-S1" Число помеховых каналов

Система пространственного зашумления Баррикада SEL SP 21

Генератор шума ГШ-1000М

Аппаратура защиты от акустической Разведки "Соната АВ" модель 3М

Система «Шторм-5» -система постановки виброакустических и акустических помех

Благодарим за внимание!!!