ГОСУДАРСТВЕННЫЙ КОМИТЕТ СВЯЗИ, ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

РЕФЕРАТ

По дисциплине: Комплексная система защиты информации

На тему: Организационные основы защиты информации на предприятии

Выполнил: Шазимов А.

Группа 233-12

Принял(а): _____

Ташкент – 2014

Организационные основы защиты информации на предприятии

Основные направления, принципы и условия организационной защиты информации

Из упоминавшихся ранее средств и методов обеспечения информационной безопасности особо были выделены организационные, которые в совокупности с другими элементами системы защиты информации на предприятии подробно описаны в последующих главах учебника. Для наиболее полного и глубокого анализа происходящих в сфере защиты конфиденциальной информации процессов, понимание сущности планируемых и проводимых в этих целях мероприятий прежде всего необходимо рассмотреть одно из важнейших направлений защиты конфиденциальной информации — организационную защиту информации.

Организационная защита информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации предприятия. От полноты и качества решения руководством предприятия и должностными лицами организационных задач зависит эффективность функционирования системы защиты информации в целом. Роль и место организационной защиты информации в общей системе мер, направленных на защиту конфиденциальной информации предприятия, определяются исключительной важностью принятия руководством своевременных и верных управленческих решений с учетом имеющихся в его распоряжении сил, средств, методов и способов защиты информации и на основе действующего нормативно-методического аппарата.

Среди основных направлений защиты информации наряду с организационной выделяют правовую и инженерно-техническую защиту информации.

Однако организационной защите информации среди этих направлений отводится особое место.

Организационная защита информации призвана посредством выбора конкретных сил и средств (включающие в себя правовые, инженерно-технические и инженерно-геологические) реализовать на практике спланированные руководством предприятия меры по защите информации. Эти меры принимаются в зависимости от конкретной обстановки на предприятии, связанной с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к ее утечке.

Роль руководства предприятия в решении задач по защите информации трудно переоценить. Основными направлениями деятельности, осуществляемой руководителем предприятия в этой области, являются: планирование мероприятий

по защите информации и персональный контроль за их выполнением, принятие решений о непосредственном доступе к конфиденциальной информации своих сотрудников и представителей других организаций, распределение обязанностей и задач между должностными лицами и структурными подразделениями, аналитическая работа и т.д. Цель принимаемых руководством предприятия и должностными лицами организационных мер — исключение утечки информации и, таким образом, уменьшение или полное исключение возможности нанесения предприятию ущерба, к которому эта утечка может привести.

Система мер по защите информации в широком смысле слова должна строиться исходя из тех начальных условий и факторов, которые, в свою очередь, определяются состоянием устремленности разведок противника либо действиями конкурента на рынке товаров и услуг, направленными на овладение информацией, подлежащей защите.

Это правило действует как на государственном уровне, так и на уровне конкретного предприятия.

Используются два примерно равнозначных определения организационной зашиты информации.

Организационная защита информации — составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Организационная защита информации на предприятии — регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

Первое из приведенных определений в большей степени показывает сущность организационной защиты информации. Второе — раскрывает ее структуру на уровне предприятия. Вместе с тем оба определения подчеркивают важность нормативно-правового регулирования вопросов защиты информации наряду с комплексным подходом к использованию в этих целях имеющихся сил и средств. Основные направления организационной защиты информации приведены ниже.

Организационная защита информации:

- Организация работы с персоналом;
- Организация внутриобъектового и пропускного режимов и охраны;
- Организация работы с носителями сведений;
- Комплексное планирование мероприятий по защите информации;
- Организация аналитической работы и контроля.

Основные принципы организационной защиты информации:

- принцип комплексного подхода — эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;

- принцип оперативности принятия управленческих решений (существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации);

- принцип персональной ответственности — наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения.

Среди основных условий организационной защиты информации можно выделить следующие:

- непрерывность всестороннего анализа функционирования системы защиты информации в целях принятия своевременных мер по повышению ее эффективности;
- неукоснительное соблюдение руководством и персоналом предприятия установленных норм и правил защиты конфиденциальной информации.

При соблюдении перечисленных условий обеспечивается наиболее полное и качественное решение задач по защите конфиденциальной информации на предприятии.

Основные подходы и требования к организации системы защиты информации

Успешное решение комплекса задач по защите информации не может быть достигнуто без создания единой основы, так называемого «активного кулака» предприятия, способного концентрировать все усилия и имеющиеся ресурсы для исключения утечки конфиденциальной информации и недопущения возможности нанесения ущерба предприятию. Таким «кулаком» призвана стать система защиты информации на предприятии, создаваемая на соответствующей нормативно-методической основе и отражающая все направления и специфику деятельности данного предприятия.

Под системой защиты информации понимают совокупность органов защиты информации (структурных подразделений или должностных лиц предприятия), используемых ими средств и методов защиты информации, а также мероприятий, планируемых и проводимых в этих целях.

Для решения организационных задач по созданию и обеспечению

функционирования системы защиты информации используются несколько основных подходов, которые вырабатываются на основе существующей нормативно-правовой базы и с учетом методических разработок по тем или иным направлениям защиты конфиденциальной информации.

Один из основных подходов к созданию системы защиты информации заключается во всестороннем анализе состояния защищенности информационных ресурсов предприятия с учетом устремленности конкурирующих организаций к овладению конфиденциальной информацией и, тем самым, нанесению ущерба предприятию. Важным элементом анализа является работа по определению перечня защищаемых информационных ресурсов с учетом особенностей их расположения (размещения) и доступа к ним различных категорий сотрудников (работников других предприятий).

Работу по проведению такого анализа непосредственно возглавляет руководитель предприятия и его заместители по направлениям деятельности. Изучение защищенности информационных ресурсов основывается на положительном и отрицательном опыте работы предприятия, накопленном в течение последних нескольких лет, а также на деловых связях и контактах предприятия с организациями, осуществляющими аналогичные виды деятельности.

При создании системы защиты информации, в первую очередь, учитываются наиболее важные, приоритетные направления деятельности предприятия, требующие особого внимания. Предпочтение также отдается новым, перспективным направлениям деятельности предприятия, которые связаны с научными исследованиями, новейшими технологиями, формирующими интеллектуальную собственность, а также развивающимся международным связям. В соответствии с названными приоритетами формируется перечень возможных угроз информации, подлежащей защите, и определяются конкретные силы, средства, способы и методы ее защиты.

К организации системы защиты информации с позиции системного подхода выдвигается ряд требований, определяющих ее целостность, стройность и эффективность.

Система защиты информации должна быть:

- централизованной — обеспечивающей эффективное управление системой со стороны руководителя и должностных лиц, отвечающих за различные направления деятельности предприятия;
- плановой — объединяющей усилия различных должностных лиц и структурных подразделений для выполнения стоящих перед предприятием задач в области защиты информации;
- конкретной и целенаправленной — рассчитанной на защиту абсолютно конкретных информационных ресурсов, представляющих интерес для конкурирующих организаций;
- активной — обеспечивающей защиту информации с достаточной степенью

настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия;
- надежной и универсальной — охватывающей всю деятельность предприятия, связанную с созданием и обменом информацией.

Основные методы, силы и средства, используемые для организации защиты информации

Один из важнейших факторов, влияющих на эффективность системы защиты конфиденциальной информации, — совокупность сил и средств предприятия, используемых для организации защиты информации.

Силы и средства различных предприятий отличаются по структуре, характеру и порядку использования. Предприятия, работающие с конфиденциальной информацией и решающие задачи по ее защите в рамках повседневной деятельности на постоянной основе, вынуждены с этой целью создавать самостоятельные структурные подразделения и использовать высокоэффективные средства защиты информации. Если предприятия лишь эпизодически работают с конфиденциальной информацией в силу ее небольших объемов, вместо создания подразделений они могут включать в свои штаты отдельные должности специалистов по защите информации. Данные подразделения и должности являются органами защиты информации.

Предприятия, работающие с незначительными объемами конфиденциальной информации, могут на договорной основе использовать потенциал более крупных предприятий, имеющих необходимое количество квалифицированных сотрудников, высокоэффективные средства защиты информации, а также большой опыт практической работы в данной области.

Ведущую роль в организации защиты информации на предприятии играют руководитель предприятия, а также его заместитель, непосредственно возглавляющий эту работу.

Руководитель предприятия несет персональную ответственность за организацию и проведение необходимых мероприятий, направленных на исключение утечки сведений, отнесенных к конфиденциальной информации, и утрат носителей информации. Он обязан:

- знать фактическое состояние дел в области защиты информации, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки конфиденциальной информации;
- определять обязанности и задачи должностным лицам и структурным подразделениям предприятия в этой области;
- проявлять высокую требовательность к персоналу предприятия в вопросах сохранности конфиденциальной информации;
- оценивать деятельность должностных лиц и эффективность мероприятий по защите информации.

Заместитель руководителя предприятия обязан постоянно изучать все стороны и направления деятельности предприятия для принятия своевременных мер по защите информации; руководить работой службы безопасности (иных структурных подразделений, решающих задачи по защите информации); выполнять другие функции по организации защиты информации в ходе проведения предприятием всех видов работ. Более подробно обязанности руководителя предприятия и его заместителя, отвечающего за защиту информации, рассмотрены в других статьях.

На предприятиях для организации работ по защите информации могут создаваться следующие основные виды структурных подразделений: режимно-секретные;
подразделения по технической защите информации и противодействию иностранным техническим разведкам;
подразделения криптографической защиты информации; мобилизационные;
подразделения охраны и пропускного режима.

Функции, возлагаемые на перечисленные подразделения, определяются решением (приказом) руководителя предприятия и отражаются в соответствующих положениях.

По решению руководителя предприятия данные подразделения организационно могут объединяться в службу безопасности, руководитель которой в некоторых случаях может быть наделен статусом заместителя руководителя предприятия и полномочиями должностного лица, осуществляющего руководство работой структурных подразделений предприятия, деятельность которых связана с использованием и защитой информации.

Режимно-секретное подразделение, мобилизационное подразделение и подразделение по технической защите информации и противодействию иностранным техническим разведкам создаются на предприятиях, выполняющих работы с использованием сведений, составляющих государственную тайну (вне зависимости от наличия на предприятии иной информации с ограниченным доступом).

Режимно-секретное подразделение является основным структурным подразделением предприятия и решает задачи организации, координации и контроля деятельности других структурных подразделений (персонала предприятия) по обеспечению защиты сведений, составляющих государственную тайну. На предприятиях, не выполняющих работы со сведениями, составляющими государственную тайну, для решения аналогичных задач в отношении других видов информации с ограниченным доступом создается и функционирует служба безопасности (служба защиты информации).

Подразделение по технической защите информации и противодействию иностранным техническим разведкам решает задачи организации и проведения

комплекса технических мероприятий, направленных на исключение или существенное затруднение добывания иностранными разведками с помощью технических средств сведений, отнесенных к конфиденциальной информации и подлежащих защите.

Подразделение криптографической защиты информации создается в целях предотвращения утечки конфиденциальной информации при ее передаче по открытым каналам (линиям) связи с помощью технических средств, а также при использовании локальных вычислительных сетей, имеющих выход за пределы территории предприятия.

Подразделение охраны и пропускного режима создается в целях предотвращения несанкционированного (бесконтрольного) пребывания на территории и объектах предприятия посторонних лиц и транспорта, нанесения ущерба предприятию путем краж (хищений) с территории предприятия материальных средств и иного имущества. В некоторых случаях для решения задач охраны и пропускного режима на предприятиях могут создаваться отдельные самостоятельные подразделения.

Мобилизационное подразделение решает задачи всесторонней подготовки предприятия к работе в условиях военного времени, призыва и поступления мобилизационных людских и материальных ресурсов.

Кроме перечисленных подразделений предприятия к работе по организации защиты информации могут привлекаться и иные структурные подразделения, для которых выполнение мероприятий по защите информации не является основной функцией.

К таким подразделениям относятся кадровый орган, орган юридической службы (юрисконсульт), орган психологической и воспитательной работы, пресс-служба предприятия и др. Особо необходимо отметить важность участия в организации защиты информации производственных, так называемых «тематических» структурных подразделений (отдельных должностных лиц), которые создают продукцию и товары или оказывают услуги (например, производство стрейч пленки), и в связи с этим самым непосредственным образом взаимодействуют с другими предприятиями и органами государственной власти.

Для проведения работ по организации защиты информации используются также возможности различных нештатных подразделений предприятия, в том числе коллегиальных органов (комиссий), создаваемых для решения специфических задач в этой области. В их числе — постоянно действующая техническая комиссия, экспертная комиссия, комиссия по рассекречиванию носителей конфиденциальной информации, комиссия по категорированию объектов информатизации и др. Функции, возлагаемые на данные комиссии, рассмотрены в других статьях.

Чтобы добиться максимальной эффективности при решении задач защиты

информации, наряду с возможностями упомянутых штатных и нештатных подразделений (должностных лиц) необходимо использовать имеющиеся на предприятии средства защиты информации.

Под средствами защиты информации понимают технические, криптографические, программные и другие средства и системы, разработанные и предназначенные для защиты конфиденциальной информации, а также средства, устройства и системы контроля эффективности защиты информации.

Технические средства защиты информации — устройства (приборы), предназначенные для обеспечения защиты информации, исключения ее утечки, создания помех (препятствий) техническим средствам доступа к информации, подлежащей защите.

Криптографические средства защиты информации — средства (устройства), обеспечивающие защиту конфиденциальной информации путем ее криптографического преобразования (шифрования).

Программные средства защиты информации — системы защиты средств автоматизации (персональных электронно-вычислительных машин и их комплексов) от внешнего (постороннего) воздействия или вторжения.

Эффективное решение задач организации защиты информации невозможно без применения комплекса имеющихся в распоряжении руководителя предприятия соответствующих сил и средств. Вместе с тем определяющую роль в вопросах организации защиты информации, применения в этих целях сил и средств предприятия играют методы защиты информации, определяющие порядок, алгоритм и особенности использования данных сил и средств в конкретной ситуации.

Методы защиты информации — применяемые в целях исключения утечки информации универсальные и специфические способы использования имеющихся сил и средств (приемы, меры, мероприятия), учитывающие специфику деятельности по защите информации.

Общие методы защиты информации подразделяются на правовые, организационные, технические и экономические.

Методы защиты информации с точки зрения их теоретической основы и практического использования взаимосвязаны. Правовые методы регламентируют и всесторонне нормативно регулируют деятельность по защите информации, выделяя, прежде всего, ее организационные направления. Тесную связь организационных и правовых методов защиты информации можно показать на примере решения задач по исключению утечки конфиденциальной информации, в частности относящейся к коммерческой тайне предприятия, при его взаимодействии с различными государственными и территориальными инспекторскими и надзорными органами. Эти органы в соответствии с

предоставленными им законом полномочиями осуществляют деятельность по получению (истребованию), обработке и хранению информации о предприятиях и гражданах (являющихся их сотрудниками).

Передача информации, в установленном порядке отнесенной к коммерческой тайне или содержащей персональные данные работника предприятия, должна осуществляться на основе договора, предусматривающего взаимные обязательства сторон по нераспространению (неразглашению) этой информации, а также необходимые меры по ее защите.

Организационные механизмы защиты информации определяют порядок и условия комплексного использования имеющихся сил и средств, эффективность которого зависит от применяемых методов технического и экономического характера.

Технические методы защиты информации, используемые в комплексе с организационными методами, играют большую роль в обеспечении защиты информации при ее 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.

Среди перечисленных методов защиты информации особо выделяются организационные методы, направленные на решение следующих задач:
реализация на предприятии эффективного механизма управления, обеспечивающего защиту конфиденциальной информации и недопущение ее утечки;
осуществление принципа персональной ответственности руководителей подразделений и персонала предприятия за защиту конфиденциальной информации;
определение перечней сведений, относимых на предприятии к различным категориям (видам) конфиденциальной информации;

ограничение круга лиц, имеющих право доступа к различным видам информации в зависимости от степени ее конфиденциальности;
подбор и изучение лиц, назначаемых на должности, связанные с конфиденциальной информацией, обучение и воспитание персонала предприятия, допущенного к конфиденциальной информации;
организация и ведение конфиденциального делопроизводства;
осуществление систематического контроля за соблюдением установленных требований по защите информации.

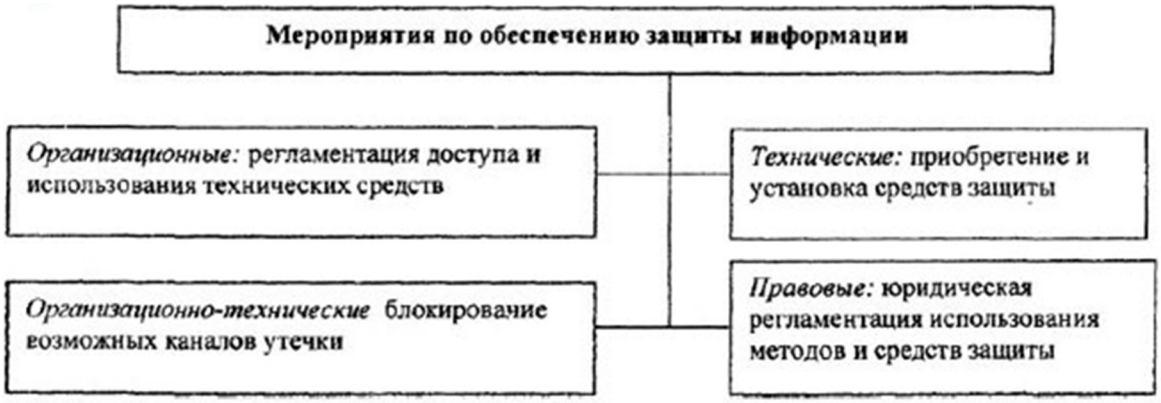
Приведенный перечень организационных методов не является исчерпывающим и, в зависимости от специфики деятельности предприятия, степени конфиденциальности используемой информации, объема выполняемых работ, а также опыта работы в области защиты информации, может быть дополнен иными методами.

Система организационных мер защиты информации в организации

Система защиты информации - это **рациональная совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, ее разглашении или утечке**. Структура системы защиты охватывает не только электронные информационные системы, а весь управленческий комплекс фирмы. При формировании системы безопасности необходимо четко уяснить, какие задачи перед ней стоят.

Задачи системы безопасности информации

Для решения этих задач используется комплекс мероприятий, в число которых входит **система организационных мер**.



Мероприятия по обеспечению защиты информации

Основная характеристика системы: ее комплексность, т.е. **наличие в ней обязательных элементов, охватывающих все направления защиты информации**. Соотношение элементов и их содержания обеспечивают индивидуальность построения системы защиты информации и гарантируют неповторимость системы, трудность ее преодоления - razgovorodele.ru. Элементами системы являются: правовой, организационный, инженерно-технический, программно - аппаратный и криптографический.

Организационный элемент системы защиты информации содержит меры управленческого, ограничительного и технологического характера, определяющие основы и содержание системы защиты, побуждающие персонал соблюдать правила защиты конфиденциальной информации фирмы. Элемент включает в себя регламентацию:

1) Формирования и организации деятельности службы безопасности и службы конфиденциальной документации, обеспечения деятельности этих служб нормативно-методическими документами по организации и технологии защиты информации.
2) Составления и регулярного обновления состава защищаемой информации фирмы, составления и ведения перечня защищаемых бумажных, машиночитаемых и электронных документов.
3) Разрешительной системы разграничения доступа персонала к защищаемой информации.
4) Методов отбора персонала для работы с защищаемой информацией, методики обучения и инструктирования сотрудников.
5) Направлений и методов воспитательной работы с персоналом, контроля соблюдения сотрудниками порядка защиты информации.
6) Технологии защиты, обработки и хранения бумажных, машиночитаемых и электронных документов; внемашинной технологии защиты электронных документов.
7) Порядка защиты ценной информации фирмы от случайных или умышленных несанкционированных действий персонала.
8) Ведения всех видов аналитической работы.
9) Порядка защиты информации при проведении совещаний, заседаний, переговоров, приеме посетителей, работе с представителями СМИ.
10) Оборудования и аттестации помещений и рабочих зон, выделенных для работы с конфиденциальной информацией.
11) Пропускного режима на территории, в здании, помещениях, идентификации транспорта и персонала фирмы.
12) Системы охраны территории.
13) Действий персонала в экстремальных ситуациях.
14) Организационных вопросов приобретения, установки и эксплуатации технических средств защиты информации и охраны.
15) Работы по управлению системой защиты информации.
16) Критериев и порядка проведения оценочных мероприятий по установлению степени эффективности системы защиты информации.

Система организационных мер по защите информации представляют собой **комплекс мероприятий**, включающих четыре основные компонента:

- *изучение обстановки на объекте;*
- *разработку программы защиты;*
- *деятельность по проведению указанной программы в жизнь;*

- контроль за ее действенностью и выполнением установленных правил.

К числу рассматриваемых **подсистем организационного плана** по защите информации можно отнести следующие мероприятия:

- ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;
- организация надежной охраны помещений и территории прохождения линии связи - razgovorodele.ru;
- организация, хранения и использования документов и носителей конфиденциальной информации, включая порядок учета, выдачи, исполнения и возвращения;
- создание штатных организационных структур по защите ценной информации или назначение ответственного за защиту информации на конкретных этапах ее обработки и передачи;
- создание особого порядка взаимоотношений со сторонними организациями и партнерами;
- организация секретного и КТ - делопроизводства.

1. Организационная защита в системе комплексной защиты информации

Лекции -> Концептуальные основы организационного обеспечения Информационной безопасности

Цели и задачи организационной защиты информации (ЗИ)

Организационные меры ЗИ — комплекс мероприятий по ЗИ, направленный на регламентацию деятельности персонала в процессе обработки информации

Основные цели организационных мер защиты:

- Обеспечение правильности функционирования механизмов защиты
- Регламентация автоматизированной обработки информации

Основные направления организационной защиты на объекте:

- Защита от НСД (от не санкционированного доступа)
- Защита информации от утечки по техническим каналам
- Защита информации от незадекларированных возможностей (Например, от вредоносного программного обеспечения)
- Защита информации от ИТР (от иностранных технических разведок)

Основные организационные мероприятия по созданию и обеспечению функционирования комплексной системы защиты информации

- Разовые мероприятия
  Мероприятия, однократно проводимые и повторяемые только при полном пересмотре принятых решений
- Эпизодические мероприятия
  Мероприятия, проводимые при осуществлении или возникновении определенных изменений в защищаемой системе или внешней среде
- Периодически проводимые мероприятия
- Постоянно проводимые мероприятия

К **разовым** мероприятиям относятся:

- Мероприятия по созданию научно-технической и методологической основы защиты системы, в том числе концепции и руководящие документы
- Мероприятия, осуществляемые при проектировании, строительстве и оборудовании объектом
- проведение специальных проверок всех технических средств

 разработка и утверждение функциональных обязанностей должностных лиц

 мероприятия по разработке правил управления доступом к ресурсам системы

 организация пропускного режима на предприятии и в отдельных помещениях

 создание подразделений по защите информации

К **эпизодическим** мероприятиям относятся:

 мероприятия, осуществляемые при кадровых изменениях в составе персонала

 мероприятия, осуществляемые при ремонте и модификации оборудования, ПО

 и т.д.

К **периодически проводимым** мероприятиям относятся:

 распределение / разграничение реквизитов разграничения доступа (раздача паролей)

 анализ системных журналов и принятие мер по обнаруженным недостаткам и проблемам

 анализ состояния и оценка эффективности мер защиты информации

 мероприятия по пересмотру состава и перестроению системы защиты

 и т.д.

К **постоянно проводимым** мероприятиям относятся:

 мероприятия по обеспечению достаточного уровня физической защиты всех элементов объекта (охрана, в том числе и противопожарная, сохранность съемных носителей)

 явный или скрытый контроль за работой персонала системы

 контроль за реализацией выбранных мер защиты

 постоянно осуществляемый анализ состояния системы защиты