сотрудников предприятия по организационно-правовым вопросам обеспечения экономической безопасности и способам защиты охраняемой информации.

С привлечением специалистов предприятия изучает все виды деятельности подразделений в целях выявления и закрытия возможных каналов утечки охраняемой информации и нанесения экономического ущерба.

Организует служебные расследования по фактам разглашения охраняемой информации, утраты документов или изделий, содержащих такие сведения, нарушений внутриобъектового и пропускного режима предприятия.

Осуществляет связь с правоохранительными и другими государственными органами по вопросам защиты коммерческой тайны и обеспечения экономической безопасности предприятия.

4. СТРУКТУРА

Исходя из задач и функций в СБ предприятия входят:

Подразделение защиты информации

Подразделение технических средств связи и противодействия техническим средствам разведки

Подразделение охраны.

Задачи, функции, права, ответственность структурных звеньев СБ определяются отдельными положениями и должностными инструкциями сотрудников.

Лабораторное занятие №7.
Тема: Организация службы безопасности предприятия

Содержание занятия

Введение
Вопрос 1. Положение о структуре службы безопасности предприятия.
1.1. Общие положения.
1.2. Правовые основы деятельности службы безопасности.
1.3. Основные задачи службы безопасности.
1.4 Общие функции службы безопасности.
1.5. Состав службы безопасности.
1.6. Права, обязанности и ответственность сотрудников службы безопасности.
1.7. Нештатные структуры службы безопасности.
Вопрос 2. Положение о подразделениях.
2.1. Положение об отделе режима и охраны.
2.2. Положение о секторе режима.
2.3. Положение о секторе охраны.
2.4. Положение о специальном отделе.
2.5. Положение о секторе обработки документов с грифом «коммерческая тайна».
2.6. Положение о группе инженерно-технической защиты.
2.7. Положение о группе безопасности внешней деятельности.

Введение.

В условиях формирования общего экономического пространства перед предприятиями особо остро встает задача сохранения коммерческой тайны. Можно сказать определенно: в период становления рынка недобросовестная конкуренция представляет собой серьезную угрозу этому процессу. Стало почти массовым процессом беззастенчивое заимствование интеллектуальной и промышленной собственности (методик, программ, знания и технологии) сотрудниками предприятий, работающими одновременно в кооперативах, малый предприятиях и других коммерческих структурах. К этому следует добавить целенаправленные действия по сманиванию или подкупу рабочих и служащих предприятий конкурента, чтобы завладеть секретами их коммерческой и производственной деятельности.
Современный промышленный шпионаж предполагает использование новейших достижений электроники, непосредственное тайное наблюдение, кражи со взломом, подкуп и шантаж. Речь идет о настоящей «тайной войне». Вот один из показательных примеров, приведенных в статье «Космический товар по минимальным ценам». Американское космическое ведомство весьма заинтересовано в приобретении у России целого ряда образцов космической техники и технологии по ее созданию, которые «в настоящее время предлагаются русскими по минимальным ценам». «Еще несколько лет назад мы намеревались выкрасть кое-что из этого», — заявило одно, пожелавшее остаться неизвестным, должностное лицо администрации США.
Урон американскому бизнесу от краж торговых секретов превышает по их оценкам 4 млрд. долларов ежегодно. То, что в мировой практике именуется промышленным шпионажем, мы даже не можем юридически классифицировать. С переходом на рыночные отношения в условия самостоятельности предприятий перед нами встали вопросы сохранности своих коммерческих секретов и безопасности предприятия.
Отечественный и зарубежный опыт свидетельствует, что основную роль в обеспечении

сохранности коммерческой тайны играют сами предприятия, а не государственные органы. Для защиты коммерческих секретов предприятия создают собственные службы безопасности. Важной предпосылкой создания службы безопасности предприятия является разработка ее структуры, состава, положений о подразделениях, и должностных инструкций для руководящего состава и сотрудников. Настоящее издание содержит справочный материал для специалистов, занятых разработкой защитных мероприятий, созданием систем безопасности, и для руководителей предприятий, поставивших перед собой задачу обеспечения безопасности производства и коммерческих секретов.

Вопрос 1. Положение о структуре службы безопасности предприятия.

Многогранность сферы обеспечения безопасности и защиты информации требует создания специальной службы, осуществляющей реализацию специальных защитных мероприятий.

Структура, численность и состав службы безопасности предприятия (фирмы, компании и т.д.) за рубежом определяются реальными потребностями предприятия и степенью конфиденциальности ее информации. В зависимости от масштабов и мощности организации деятельность по обеспечению безопасности предприятия и защиты информации может быть реализована от абонентного обслуживания силами специальных центров безопасности до полномасштабной службы компании с развитой штатной численностью. В зарубежных источниках, например, рассматривается следующая структура службы безопасности фирмы (рис. 1). Она возглавляется начальником службы безопасности, которому подчинены служба охраны, инспектор безопасности, консультант по безопасности и служба противопожарной охраны.

С учетом накопленного зарубежного и отечественного опыта и особенностей рыночной экономики предлагается рабочий вариант службы безопасности предприятия среднего масштаба производства, ее структура и должностные инструкции (рис. 2).

1.1. Общие положения.

Основными задачами службы безопасности предприятия являются обеспечение безопасности предприятия, производства, продукции и защита коммерческой, промышленной, финансовой, деловой и другой информации, независимо от ее назначения и форм при всем многообразии возможных каналов ее утечки и различных злонамеренных действий со стороны конкурентов.

1.2. Правовые основы деятельности службы безопасности.

Основные положения, состав и организация службы безопасности имеют юридическую силу в том случае, если они зафиксированы в основополагающих правовых, юридических и организационных документах предприятия.

В основу деятельности службы безопасности положены: Закон Российской Федерации «О безопасности";

Законы и регламенты России, обеспечивающие безопасность деятельности и сохранность коммерческой тайны;

Закон о предприятиях и предпринимательской деятельности; Кодекс законов о труде (КЗОТ);

Устав предприятия, коллективный договор, трудовые договоры, правила внутреннего трудового распорядка сотрудников, должностные обязанности руководителей, специалистов, рабочих и служащих.

1.3. Основные задачи службы безопасности.

Основными задачами службы безопасности предприятия являются: обеспечение безопасности производственно-торговой деятельности и

защиты информации и сведений, являющихся коммерческой тайной; организация работы по правовой, организационной и инженерно-

технической (физической, аппаратной, программной и математической) защите коммерческой тайны;

организация правильного делопроизводства, исключающего несанкционированное

получение сведений, являющихся коммерческой тайной;
предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну;
выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;
обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, заседания, связанные с деловым сотрудничеством как на национальном, так и на международном уровне;
обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;
обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;
оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

1.4 Общие функции службы безопасности.

Служба безопасности предприятия выполняет следующие общие функции:
организует и обеспечивает пропускной и внутри объектовый режим в зданиях и помещениях, порядок несения службы охраны, контролирует соблюдение требований режима сотрудниками, смежниками, партнерами и посетителями;
руководит работами по правовому и организационному регулированию отношений по защите коммерческой тайны;
участвует в разработке основополагающих документов с целью закрепления в них требований обеспечение безопасности и защиты коммерческой тайны, в частности, Устава, Коллективного договора, Правил внутреннего трудового распорядка, Положений о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;
разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ, организует и контролирует выполнение требований «ИНСТРУКЦИИ по защите коммерческой тайны";
изучает все стороны коммерческой, производственной, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций о деятельности предприятия и его клиентов, партнеров, смежников;
организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия;
разрабатывает, ведет, обновляет и пополняет «Перечень сведений, составляющих коммерческую тайну» и другие
нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;
обеспечивает строгое выполнение требований нормативных документов по защите коммерческой тайны;
осуществляет руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и других в части оговоренных в договорах условиях по защите коммерческой тайны;
организует и регулярно проводит учебу сотрудников предприятия и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к защите коммерческих секретов был глубоко осознанный подход;
ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;

ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;
поддерживает контакты с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне).

1.5. Состав службы безопасности.

Служба безопасности является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю предприятия.
Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности.
Организационно служба безопасности состоит из следующих структурных единиц:
отдела режима и охраны, в составе сектора режима и сектора охраны; специального отдела в составе сектора обработки секретных документов
и сектора обработки документов с грифом «Коммерческая тайна"; инженерно-технической группы;
группы безопасности внешней деятельности.

1.6. Права, обязанности и ответственность сотрудников службы безопасности.

Сотрудники подразделений службы безопасности в целях обеспечения защиты сведений, составляющих коммерческую тайну, имеют право:
требовать от всех сотрудников предприятия, партнеров, клиентов строгого и неукоснительного выполнения требований нормативных документов или договорных обязательств по защите коммерческой тайны;
вносить предложения по совершенствованию правовых, организационных и инженерно-технических мероприятий по защите коммерческой тайны.
Сотрудники службы безопасности обязаны:
осуществлять контроль за соблюдением «инструкции по защите коммерческой тайны";
докладывать руководству о фактах нарушения требований нормативных документов по защите коммерческой тайны и других действий, могущих привести к утечке конфиденциальной информации или утрате документов или изделий;
не допускать неправомерного ознакомления с документами и материалами с грифом «Коммерческая тайна» посторонних лиц.
Сотрудники службы безопасности несут ответственность за личное нарушение безопасности коммерческой тайны и за не использование своих прав при выполнении функциональных обязанностей по защите конфиденциальных сведений сотрудниками предприятия.

1.7. Нештатные структуры службы безопасности.

С целью более широкого охвата и качественного исполнения требований защиты коммерческой тайны решением руководства предприятия и службы безопасности могут создаваться отдельные комиссии, решающие определенные контрольно-ревизионные функции на временной или постоянной основе, такие как:
квартальные или годовые комиссии по проверке наличия, состояния и учета документов (материалов, сведений, ценностей);
комиссия по оценке возможностей публикации периодических документов, объявлений, проспектов, интервью и других выступлений в печати, на радио и телевидении, семинарах, симпозиумах, конференциях и т.п.;
периодические проверочные комиссии для проверки знаний и умений выполнять требования нормативных документов по защите коммерческой тайны, а также по оценке эффективности и надежности защитных мероприятий по обеспечению безопасности предприятия.

Вопрос 2. Положение о подразделениях.

Состав и функции подразделений службы безопасности определяются соответствующими Положениями.

Положение о структурном подразделении — документ, предназначенный для

нормативно-правовой регламентации деятельности каждого структурного подразделения. Положение определяет статус подразделения, отражает его место в составе службы безопасности, показывает его внутреннюю организацию. На основе Положения составляется штатное расписание подразделения, определяется степень ответственности за выполнение возложенных на него задач.

2.1. Положение об отделе режима и охраны.

2.1.1. Общие положения.

Отдел режима и охраны является самостоятельным структурным подразделением службы безопасности и подчиняется начальнику службы безопасности.

В своей деятельности отдел руководствуется требованиями «Инструкции по организации режима и охране».

2.1.2. Задачи.

Организация и осуществление мер по обеспечению безопасности деятельности и защите сведений, составляющих государственную и коммерческую тайну.

Разработка и совершенствование системы предотвращения несанкционированного допуска и доступа к сведениям, составляющим коммерческую тайну.

Организация и поддержание пропускного и внутри объектного режима.

Организация охраны арестованных по режиму конфиденциальных помещений.

Организация личной охраны руководителей и ведущих сотрудников.

Организация и установление мер физической и технической защиты зданий и помещений.

Организация, разработка и контроль системы безопасности в повседневных и в особых условиях (стихийные бедствия, поломки, аварии, беспорядки и т.п.).

2.1.3. Структура.

В составе отдела режима и охраны имеются следующие структурные единицы:

Сектор режима.

Сектор охраны.

2.1.4. Функции.

В соответствии с основными задачами отдел режима и охраны выполняет следующие функции:

Организует работу по выполнению решений, приказов и распоряжений руководства предприятия по обеспечению защиты коммерческих секретов и обеспечению безопасности деятельности.

Определяет единство действий и организует защиту, безопасность, сохранность документов и ценностей в обычных и особых условиях.

Разрабатывает, обновляет и дополняет инструкции, положения и иные нормативные материалы по режиму и охране.

Осуществляет руководство работой по установлению степени конфиденциальности сведений, содержащихся в документах. Совместно с основными подразделениями проводит работу по анализу практики применения «Перечня сведений, составляющих коммерческую тайну», по подготовке и внесению в него в установленном порядке необходимых изменений и дополнений, а также организует его переработку и переиздание.

Организует разработку и контроль за эффективностью действующей разрешительной системы допуска сотрудников, компаньонов и клиентов к ознакомлению и работе с документами конфиденциального характера, с целью исключения возможности ознакомления со сведениями, не относящимися к выполняемой ими работе.

Разрабатывает и рассматривает совместно со специальным отделом и подразделениями предложения по рационализированию делопроизводства с грифом «Коммерческая тайна», предотвращению факторов включения в документы секретного и несекретного характера излишнего объема сведений, являющихся коммерческой тайной, сокращению издаваемых и разрабатываемых документов конфиденциального характера, неоправданной из

рассылки.
Организует и обеспечивает систему контролируемого доступа и специального пропускного режима в здания и помещения.
Организует, обеспечивает и контролирует выполнение требований внутри объектного режима.
Определяет систему охраны и участвует в ее организации и обеспечении работы выделенных помещений.
Организует разработку тактических принципов использования средств автоматизации, сигнализации, связи и охраны.
Организует охрану, пропускной, допускной и внутри объектный режим и осуществляет оперативно-методическое руководство работами по защите выделенных помещений и информации, обрабатываемой и передаваемой с использованием технических средств.
Осуществляет руководство и режим защиты коммерческих сведений в работе по отбору, хранению и использованию архивных материалов.
Осуществляет методическое руководство и принимает непосредственное участие в проведении предупредительно-профилактической работы с исполнителями работ и документов конфиденциального характера.
Организует проведение служебных расследований по фактам утраты документов конфиденциального характера, разглашения охраняемых сведений, нарушения охраны и пропускного режима, необоснованного ознакомления сотрудников и командированных лиц со сведениями, составляющими государственную и коммерческую тайну и по другим фактам, которые привели или создавали условия, способствующие утечке конфиденциальной информации.
Обеспечивает личную охрану руководства и сотрудников.

2.1.5. Права начальника отдела.

На основе единоличия руководит деятельностью отдела режима и охраны по выполнению возложенных на отдел задач и функций.
Назначает проведение проверок состояния и эффективности работы по обеспечению сохранения коммерческих секретов, режима безопасности, охраны и технического ее обеспечения.
Требует от сотрудников представления объяснений по фактам, которые привели или могли привести к утечке информации, составляющей коммерческую тайну.
Ходатайствует о поощрении сотрудников, активно участвующих в работе по предупреждению утечки охраняемых сведений, выполнении требований режима и охраны.

2.2. Положение о секторе режима.

2.2.1. Общие положения.

Сектор режима является подразделением отдела режима и охраны службы безопасности и подчиняется непосредственно начальнику отдела.
В своей деятельности сектор руководствуется требованиями «Инструкции по режиму и охране» в части режима.

2.2.2. Задачи.

Организация пропускного и внутри объектного режима.
Разработка разрешительной системы и обеспечение допуска сотрудников к документам, материалам и сведениям, составляющим коммерческую тайну.
Контроль за соблюдением режима допуска к сведениям и документам.
Совершенствование системы пропускного и внутри объектного режима.
Участие в разработке «Перечня сведений, составляющих коммерческую тайну».

2.2.3. Структура.

В составе сектора режима выделяются следующие штатные должности: заведующий сектором режима;
старший инспектор по режиму — начальник бюро пропусков; инспектор по режиму;

инспектор по работе с персоналом, допущенным к сведениям, составляющим коммерческую тайну.

2.2.4. Функции.

В части обеспечения режима основными функциями сектора являются разработка, реализация и осуществление основных положений системы получения разрешений на доступ к информации, составляющей коммерческую тайну, в том числе:

права, обязанности и ответственность сотрудников, допущенных к работе с документами, содержащими коммерческую тайну;

схема выдачи разрешений на доступ сотрудников к сведениям, составляющим коммерческую тайну;

порядок доступа на совещания по вопросам, содержащим сведения, составляющие коммерческую тайну;

порядок и контроль доступа к сведениям, составляющим коммерческую тайну, представителей других предприятий и государственных органов;

ведение, уточнение и изменение «Перечня сведений, составляющих коммерческую тайну";

учет сотрудников, допущенных к работе с документами и материалами, содержащими сведения, составляющие коммерческую тайну;

учет и анализ нарушений режима работы с документами, содержащими коммерческую тайну, различного рода попыток несанкционированного доступа к конфиденциальным документам традиционного и автоматизированного исполнения (базы данных, персональные файлы и др.), случаев телефонных переговоров, содержащих конфиденциальную информацию;

организация и проведение деловых совещаний, переговоров и встреч с обсуждением вопросов, связанных с коммерческой тайной;

организация и обеспечение пропускного и внутри объектного режима: выдача пропусков (постоянных, временных, разовых), порядок посещения, учет посетителей;

определение выделенных помещений, проведение их паспортизации, обеспечение их защиты совместно с группой Инженерно-технической защиты информации.

В части работы с персоналом учитывается, что сотрудники — главный источник утечки конфиденциальной информации. С учетом этого функции группы составляют:

беседы с поступающими на работу в подразделения, работа которых связанна с коммерческой тайной, с целью установления их пригодности для этой работы;

изучение поступающего на работу в части его прошлой трудовой деятельности;

оформление обязательств о неразглашении сведений, составляющих коммерческую тайну;

анализ служебной осведомленности сотрудников;

анализ и учет трудовой удовлетворенности с целью предупреждения увольнения сотрудников, допущенных к сведениям, составляющим коммерческую тайну;

ведение досье на сотрудников, допущенных к документам с коммерческой тайной;

организация обучения сотрудников по вопросам защиты коммерческой тайны;

беседы с увольняющимися и оформление контракта (обязательства) не разглашать коммерческие секреты.

Кроме того, сектор в тесном взаимодействии с отделом кадров: разрабатывает планы комплектования кадрами;

оформляет прием, перевод и увольнение сотрудников, допущенных к коммерческой тайне;

готовит материалы для преставления сотрудников к поощрениям и должностным перемещениям.

2.2.5. Прав

Проводить беседы с поступающими на работу и увольняющимися и оформлять обязательства о неразглашении коммерческие секреты.

Требовать от сотрудников и клиентов строгого выполнения установленного пропускного

и внутриобъектового режима;
Проводить проверку состояния и организации работы по обеспечению режима работы с документами составляющими коммерческую тайну.
Требовать от сотрудников письменных объяснений по фактам нарушения пропускного и внутриобъектового режима;
Возбуждать ходатайства перед руководством о привлечении к дисциплинарной ответственности лиц, допустивших нарушения режима.
Представлять к поощрениям сотрудников, добросовестно выполняющих обязанности по сохранению в тайне охраняемых сведений.

2.2.6. Ответственность.

Всю полноту ответственности за выполнение задач и функций по режиму и работе с персоналом несет заведующий сектором режима.
Степень ответственности других сотрудников сектора устанавливается должностными инструкциями.

2.3. Положение о секторе охраны.

2.3.1. Общие положения.

Сектор охраны является подразделением отдела режима и охраны службы безопасности и подчиняется непосредственно начальнику отдела.
В своей деятельности сектор руководствуется требованиями «Инструкции по режиму и охране» в части охраны.

2.3.2. Задачи.

Обеспечение надежной защиты зданий, помещений, оборудования, валютных и материальных ценностей, а также личной охраны руководящего состава в обычных и экстремальных условиях.

2.3.3. Структура.

Сектор охраны состоит из:
комендантской службы;
группы личной охраны руководства.
Комендантская служба может состоять из коменданта здания, дежурного мастера по вневедомственной и объектовой технической охране и дежурного мастера по противопожарной охране.

2.3.4. Функции.

Сектор охраны осуществляет охрану зданий, помещений, оборудования, линий связи и перевозок, пожарную охрану, а также личную охрану руководящего состава.
Сектор охраны обеспечивает необходимые условия, исключающие несанкционированный доступ в охраняемые здания, помещения, отдельные конфиденциальные участки и зоны территории и служебных помещений. Особое внимание уделяется критическим условиям, связанным со стихийными бедствиями, поломками, авариями.
Сектор охраны:
реализует учет, контроль и наблюдение за охраняемыми зонами, помещениями, хранилищами;
обеспечивает установку и работу на местах технических средств охраны, охранной и пожарной сигнализации;
осуществляет прием под охрану и сдачу в эксплуатацию охраняемых помещений, проверяя при этом надежное срабатывание средств охраны, делая соответствующую запись в журнале приема и сдачи под охрану;
принимает меры по ликвидации возможных пожаров и других аварийных ситуаций.
В части личной охраны руководящего состава сектор руководствуется отдельным положением, разрабатываемым службой безопасности с учетом конкретных условий ее [illegible]

2.3.5. Права.

Проверять наличие, состояние и функционирование технических средств охраны

охранной и пожарной сигнализации.
Требовать строгого соблюдения установленного внутриобъектового режима и правил трудового распорядка
Участвовать в разработке мероприятий по усилению безопасности и сохранности имущества, средств, зданий и помещений.
Не допускать случаев использования неисправного оборудования, охранной и пожарной техники.
Принимать меры воздействия к сотрудникам, допускающим порчу или неправильную эксплуатацию охранно-пожарной техники.
Требовать своевременного ремонта и профилактики технических средств охраны и пожарной сигнализации.

2.3.6. Ответственность.

Всю полноту ответственности за качество и своевременное выполнение возложенных на сектор настоящим Положением задач и функций несет заведующий сектором.

2.4. Положение о специальном отделе.

2.4.1. общие положения.

Специальный отдел является самостоятельным структурным подразделением службы безопасности и подчиняется непосредственно начальнику службы.
В своей деятельности отдел руководствуется требованиями «Инструкции по режиму и охране» в части коммерческих секретов.

2.4.2. Задачи.

Организация и руководство делопроизводством секретных документов и документов с грифом «Коммерческая тайна».

2.4.3. Структура.

Специальный отдел состоит из следующих структурных единиц: сектор обработки секретных документов;
сектор обработки документов с грифом «Коммерческая тайна"; машинописное бюро оформления специальных документов; экспедиция.

2.4.4. Функции.

Обработка поступающей и отправляемой корреспонденции, доставка ее по назначению.
Осуществление контроля за сроками исполнения документов.
Организация работы по регистрации, учету и хранению документальных материалов текущего пользования.
Разработка номенклатуры дел, осуществление контроля за правильным формированием дел в подразделениях и подготовкой материалов к своевременной сдаче в архив.
Разработка и внедрение предложений по совершенствованию системы делопроизводства.
Печатание и размножение секретных документов и документов с грифом «Коммерческая тайна».
Участие в подготовке созываемых и проводимых руководством закрытых совещаний и организация их технического обслуживания.
Специальный отдел в части обеспечения обработки секретных документов руководствуется соответствующими документами, в части ведения делопроизводства с грифом «Коммерческая тайна» выполняет требование «Инструкции по защите коммерческой тайны».

2.4.5. Права.

Требовать от руководителей подразделений и исполнителей четкого и своевременного выполнения нормативных документов по организации и ведению специального делопроизводства.
Регулярно проверять правильность ведения делопроизводства в подразделениях, указывать руководителям подразделений на выявленные недостатки и требовать их устранения.

Возвращать исполнителям документы, оформленные с нарушением установленных правил делопроизводства.
Указания специального отдела в пределах его функций, предусмотренных Положением, являются обязательными к руководству и исполнению подразделениями предприятия.

2.4.6. Ответственность.

Всю полноту ответственности за качество и своевременное выполнение возложенных настоящим Положением задач и функций несет заведующий отделом.
Степень ответственности других сотрудников отдела устанавливается должностными инструкциями.

2.5. Положение о секторе обработки документов с грифом «коммерческая тайна».

2.5.1. Общие положения.

Сектор обработки документов с грифом «Коммерческая тайна» является структурным подразделением специального отдела службы безопасности и подчиняется непосредственно заведующему отделом. В своей работе сектор руководствуется «Инструкцией по защите коммерческой тайны».

2.5.2. Задачи.

Организация и руководство делопроизводством документов с грифом «Коммерческая тайна».

2.5.3. Структура.

В составе вектора устанавливаются следующие должности: заведующий сектором; делопроизводитель; машинистка.

2.5.4. Функции.

Получение, учет, исполнение и документирование поступающих и разрабатываемых документов, организация оптимального документооборота, обеспечение отправки, размножения и надежного хранения документов, их сохранности и своевременного уничтожения, а также проверка их наличия и контроль своевременного и правильного их исполнения.
Разработка нормативных документов, направленных на обеспечение сохранности коммерческой тайны.
Участие в разработке, пополнении и обновлении «Перечня сведений, составляющих коммерческую тайну».
Участие в процессе обучения персонала работе с документами, содержащими коммерческую тайну.

2.5.5. Права.

Требовать от подразделений, руководителей, сотрудников соблюдения требования по ведению делопроизводства с грифом «Коммерческая тайна».
Проверять правильность ведения делопроизводства в подразделениях, указывать руководителям подразделений на выявленные недостатки и требовать их устранения.
Представлять к поощрению сотрудников, четко выполняющих требования по сохранению коммерческой тайны. Принимать меры воздействия к лицам, допускающим нарушения в работе с документами, содержащими сведения, составляющие коммерческую тайну.

2.5.6. Ответственность.

Всю полноту ответственности за качество и своевременное выполнение возложенных настоящим Положением на сектор задач и функций несет заведующий сектором.
Степень ответственности других сотрудников сектора устанавливается должностными инструкциями.

2.6. Положение о группе инженерно-технической защиты.

2.6.1. Общие положения.

Группа инженерно-технической защиты информации является структурным подразделением службы безопасности и подчиняется непосредственно начальнику службы.

В своей деятельности группа руководствуется требованиями «Инструкции по Инженерно-технической защите».

2.6.2. Задачи.

Обследование выделенных помещений с целью установления потенциально возможных каналов утечки конфиденциальной информации через технические средства, конструкции зданий и оборудования.

Выявление и оценка степени опасности технических каналов утечки информации.

Разработка мероприятий по ликвидации (локализации) установленных каналов утечки информации организационными, организационно- техническими или техническими мерами, используя для этого физические, аппаратные и программные средства и математические методы защиты.

Организация контроля (в том числе и инструментального) за эффективностью принятых защитных мероприятий. Проведение обобщения и анализа результатов контроля и разработка предложений по повышению надежности и эффективности мер защиты.

Обеспечение приобретения, установки, эксплуатации и контроля состояния технических средств защиты информации.

2.6.3. Структура.

Структура и штатный состав группы Инженерно-технической защиты информации разрабатывается и утверждается руководством службы безопасности исходя из конкретных условий и технической оснащенности подразделений предприятия.

Возможно состав группы установить в следующем составе: руководитель группы — старший инженер;

Инженер (техник) группы по спец измерениям.

2.6.4. Функции.

Определение границ охраняемой (контролируемой) территории (зоны) с учетом возможностей технических средств, наблюдения злоумышленников.

Определение технических средств, используемых для передачи, приема и обработки конфиденциальной информации в пределах охраняемой территории (зоны).

Определение опасных, с точки зрения возможности образования каналов утечки, технических средств.

Локализация возможных каналов утечки информационно- организационными, организационно-техническими или техническими средствами и мероприятиями.

Организация наблюдения за возможным неконтролируемым излучением за счет ПЭМИН (побочных электромагнитных излучений и наводок).

Организация контроля наличия, проноса каких-либо предметов (устройств, средств, механизмов) в контролируемую зону, способных представлять собой технические средства несанкционированного получения конфиденциальной информации.

2.6.5. Права.

Группа Инженерно-технической защиты информации имеет право: проверять наличие технических средств обеспечения производственной

Деятельности в выделенных помещениях, измерять их параметры на соответствие требованиям безопасности;

устанавливать технические средства защиты каналов утечки информации через технические средства обеспечения производственной деятельности;

запрещать использование технических средств, не обеспечивающих требования безопасности.

2.6.6. Ответственность.

Всю полноту ответственности за инженерно-техническую защиту информации несет руководитель группы.

2.7. Подчинение группы службе безопасности внешней деятельности.

2.7.1. Общие положения.

Группа безопасности внешней деятельности является самостоятельным структурным подразделением службы безопасности и подчиняется непосредственно начальнику службы.

Группа организует работу в тесном взаимодействии с основными структурными подразделениями службы безопасности и предприятия.

2.7.2. Задачи.

Изучение и выявление предприятий и организаций, потенциально являющихся союзниками и конкурентами.

Добывание, сбор и обработка сведений о деятельности потенциальных и реальных конкурентов для выявления возможных злонамеренных действий по добыванию охраняемых сведений.

Учет и анализ попыток несанкционированного получения коммерческих секретов конкурентами.

Оценка степени реальных конкурентных отношений между сотрудничающими (конкурирующими) организациями.

Анализ возможных каналов утечки конфиденциальной информации.

2.7.3. Структура. Структура и штатное расписание определяется с учетом объемов и особенностей обстановки.

2.7.4. Функции.

Изучение торгово-конъюнктурных ситуаций в пространстве деятельности учредителей, партнеров, клиентов и потенциально возможных конкурентов.

Ситуационный анализ текущего состояния финансово-торговой деятельности с точки зрения прогнозирования возможных последствий, могущих привести к неправомерным действиям со стороны конкурирующих организаций и предприятий.

Выявление платежеспособности юридических и физических лиц, их возможности по своевременному выполнению платежных обязательств.

Установление антагонистических конкурентов, выявление их методов ведения конкурентной борьбы и способов достижения своих целей.

Определение возможных направлений и характера злоумышленных действий со стороны специальных служб промышленного шпионажа против предприятия, его партнеров и клиентов.

2.7.5. Права.

Требовать от соответствующих служб и подразделений необходимые для анализа сведения о деятельности партнеров и клиентов.

Осуществлять сбор и обработку необходимых сведений для выявления злоумышленных действий со стороны конкурирующих организаций.

2.7.6. Ответственность.

Вся полнота ответственности за полноту и своевременность оценки степени опасности действий со стороны конкурентов и злоумышленников по отношению к охраняемым сведениям и безопасности руководства и сотрудников лежит на группе безопасности внешней деятельности.

Лабораторное занятие №8.
Тема: Системный подход к разработке концепции обеспечения безопасности информационного объекта

СОДЕРЖАНИЕ ЗАНЯТИЯ

Обеспечение безопасности объектов (важных, особо важных, особого риска, режимных, особо режимных, не режимных, но содержащих значительные материальные ценности и т.д.) представляет собой столь широкую и многогранную область деятельности, что она в той или иной мере осуществляется практически многими предприятиями и организациями других министерств и ведомств самостоятельно, сообразуя с характерными или специфическими только для этих предприятий и организаций условиями деятельности, например: Федеральная служба безопасности, Министерство обороны, Министерство внутренних дел, Министерство по связи и информатизации и т.д.
Основными направлениями деятельности СБ (О) по обеспечению комплексной безопасности (в части, не касающейся пожарной безопасности) являются:

- инженерная и техническая защита территорий, зданий и помещений;
- организация контроля доступа сотрудников и командированных (посетителей);
- организация охраны особо важных помещений (жизненно важных центров);
- создание систем охранной сигнализации и телевизионного наблюдения;
- разработка рекомендаций по режиму охраны объектов и выработка предложений по работе СБ (О);
- защита объектов от угроз утечки информации, создание защищенных зон;
- контроль проноса технических средств в особо важные помещения (жизненно важные центры);
- выявление закладных средств подслушивания и видеонаблюдения в помещениях;
- проверка технических устройств обработки информации на наличие каналов утечки и разработка рекомендаций по их защите;
- организация непрерывного технического контроля опасных сигналов в каналах утечки;
- защита объектов от применения диверсионно - террористических средств;
- обеспечение безопасности автоматизированных систем обработки информации от несанкционированного доступа (НСД), несанкционированного копирования (ИСК), вирусной диверсии и других угроз;
- обеспечение применения специальных технических средств контроля особо важных помещений;
- организация контроля телефонных переговоров с их регистрацией.

Создание надежной системы защиты ДТА предполагает реализацию определенного типового порядка при проведении специальных работ, как то:

- анализ объекта и условий его расположения;
- рассмотрение возможных угроз воздействия на объект;
- специальный анализ ситуации для строящихся и реконструируемых объектов;
- разработка концепции безопасности от всех видов негативных воздействий;
- выработка предложений по техническому оснащению средствами безопасности на основе разработанной концепции и разработка проекта на оборудование инженерно-технических средствами;
- приобретение и монтаж специальных технических средств и комплексов (в соответствии с разработанным проектом);
- обучение персонала приемам и способам использования специальных технических

средств, постоянный контроль за эксплуатацией поставленных средств.
Ряд блоков задач может быть реализован на основе определенной типизации, исходя (опять-таки) из анализа параметров, характеризующих объект, условий его функционирования, потенциальных угроз, объема и свойств имеющихся (хранимых) энергоемких материалов и т.д. В каждом случае должна быть осуществлена классификация по структуре, качеству и свойствам применяемых технических средств защиты. Таким путем конкретизируется вопрос разработки рациональных схем защиты по каждому блоку задач на основе выбора конкретных технических средств из предлагаемых на рынке.
Пример. Для решения задач оборудования периметра какого-либо объекта техническими средствами охранной сигнализации предварительно следует знать ответы на вопросы:

1. Какова протяженность периметра.
2. Вид имеющегося заграждения (его параметры, материал).
3. Количество имеющихся ворот, калиток, их размеры, материал.
4. Ближайшее расстояние от охраняемого рубежа до помещения охраны, до ближайшего к периметру здания.
5. Наличие закладных (трубы, кабели).
6. Размер зоны отчуждения внутри периметра, наличие кустов и/или деревьев в зоне отчуждения.
7. Необходимость скрытности средств обнаружения (или отсутствие такой необходимости).
8. Требуемая точность обнаружения нарушителя на контуре периметра (3м, 10м, ...).
9. Требуемое количество рубежей охраны (периметр, подходы к зданиям), режимы охраны: круглосуточный, по мере необходимости, М-часовой.
10. Необходимость блокирования: перелаза через ограждения, разрушения ограждения, подкопа под ограждения.

Примечание. Здесь рассматривается лишь модель физического проникновения. Если же требуется информационная защита - задача охраны многократно усложняется.

11. Наличие в настоящее время (т.е. на момент предварительного анализа объекта охраны) каких-либо средств обнаружения, станционной аппаратуры в помещении службы охраны - системы сбора и обработки информации.
12. Какие затраты может позволить себе Заказчик на решение задач оборудования объекта (в частности периметра) техническими средствами охранной сигнализации и системой сбора и обработки информации.
13. В какие сроки требуется проведение такой работы. 14.Необходимы план объекта (эскиз), параметры по высоте зданий.

Примечания.

- Следует описать пожелания службы охраны (реальные с позиций затрат) для выбора ТСОС и ССОИ.
- Уровень полноты решения задач7,8,9,10 существенно влияет на размеры затрат.

Приведенный перечень вопросов - минимально необходимый с позиций предварительного анализа, но далеко не полный с позиций системного подхода.
Объективная необходимость построения высоко эффективных систем безопасности объектов в условиях резкого обострения криминогенной обстановки привела к разработке наукоемких интегрированных систем безопасности (ИСБ). ИСБ по существу нацелена на реализацию идей системной концепции обеспечения комплексной безопасности объекта с параллельным решением задач, не связанных непосредственно с задачами обеспечения безопасности) решением задач автоматизации управления широкой гаммой систем жизнеобеспечения объекта, как то: энергоснабжением, вентиляцией, отоплением, водоснабжением, лифтовым оборудованием, кондиционированием и т.д.

Среди функций, обязательных для исполнения в контуре ИСБ, следует считать:

- контроль за большим количеством помещений с созданием нескольких рубежей защиты (ИСБ разрабатывается только для больших объектов и зданий);
- иерархический доступ сотрудников и посетителей в помещения с четким разграничением полномочий по праву доступа в помещения по времени суток и по дням недели;
- идентификацию и аутентификацию личности человека, пересекающего рубеж контроля;
- предупреждение утечки информации;
- предупреждение попадания на объект запрещенных материалов и оборудования;
- накопление документальных материалов для использования их при рассмотрении и анализе происшествий;
- оперативный (автоматизированный) инструктаж работников охраны о порядке действий в различных штатных и нештатных ситуациях путем автоматического вывода на экран монитора инструкций в нужный момент;
- обеспечение полной интеграции систем видеонаблюдения, сигнализации, мониторинга доступа, оповещения, связи между персоналом СБ (О), персоналом службы пожарной безопасности, персоналом служб жизнеобеспечения объекта и т.д.;
- обеспечение взаимодействия постов охраны и органов правопорядка при несении охраны и в случае происшествий;
- слежение за точным исполнением персоналом охраны своих служебных обязанностей.

Исходя из изложенного ранее ясно, что составными частями ИСБ (укрупненно) должны быть:

- сеть датчиков, обеспечивающих получение максимально полной информации со всего пространства, находящегося в поле зрения службы безопасности и позволяющая воссоздавать на центральном пульте наблюдения и управления всестороннюю объективную картину состояния помещений, всей территории объекта и работоспособности всей аппаратуры и оборудования, включенного в контур ИСБ;
- исполнительные устройства, способные при необходимости действовать автоматически или по команде оператора;
- пункты контроля и управления системой отображения информации, через которые операторы могут следить за работой всей системы в пределах своих полномочий;
- ССОИ, наглядно представляющая информацию с датчиков и накапливающая ее для последующей обработки;
- коммуникации, по которым осуществляется обмен информацией между элементами системы и операторами.

При этом важно наличие возможности оперативного программирования (перепрограммирования) функций ИСБ. Это позволяет противодействовать эффективно таким ухищрениям злоумышленника как:

1. Исходные положения для разработки системной концепции обеспечения безопасности объектов охраны

В данном разделе излагаются основные направления деятельности по обеспечению безопасности объектов охраны (ОО), привлекательных для преступников с различных точек зрения. Преступные посягательства могут преследовать различные цели, например:

- кражи материальных или информационных ценностей;
- имеющие в виду решение террористические действия, направленные на решение политических или идеологических задач, как то: разрушение объекта (вывод его из строя); захват управления функционированием объекта (например, если это объекты

радиовещания, телевидения, связи, то захват осуществляется для решения задач дезинформации, пропаганды, информационной блокады населения); информационная разведка; ограбление; внедрение членов организованных преступных формирований (ОФП) или групп (ОПГ) в управленческие структуры и т.д.

Актуальность системного решения проблем и задач охранной деятельности особенно возросла в последние годы, что диктуется многими факторами, например:

- в современных условиях становления новых общественных, экономических, политических, производственных и иных отношений при недостатке механизмов их правового регулирования происходит закономерный взрыв криминогенной обстановки. Резко активизируется деятельность организованных преступных структур, происходит их количественный рост, качественная техническая и методическая оснащенность, проникновение в коммерческие, государственные, в том числе и в правоохранительные органы. По информационно- аналитическим обзорам специалистов (экспертов) уровень преступности в ближайшие годы будет сохраняться;
- преступные действия организованных структур, направленные на захват и ограбление учреждений, на получение конфиденциальной (секретной) информации о деятельности предприятий и т.д., все в большей степени подготавливаются как глубоко продуманные, технически хорошо оснащенные, смоделированные на достаточно высоком интеллектуальном и психологическом уровне акции;
- по данным экспертов подготовка и проведение преступных акций в большинстве случаев осуществляются на высоком профессиональном уровне, характеризуются системным решением (в том числе и в плане сокрытия следов) и часто отличаются жестокостью исполнения.

Исходя из изложенного, разработчики системной концепции обеспечения безопасности объектов в максимальной степени должны учитывать мировой и отечественный опыт, касающийся всей многогранной деятельности, организуемой по защите объектов.

Практика охранной деятельности показывает что необходим научнообоснованный подход к решению проблем и задач охраны объектов, в особенности, если это особо важные, особо опасные объекты, объекты особого риска или объекты, содержащие большие материальные ценности (например, банки, хранилища драгоценных камней и металлов и т.д.).

В связи с тем, что наиболее высоким уровнем разработки систем защиты характеризуются особо опасные, особо важные, особо режимные объекты и банки, и этот опыт, безусловно, полезен для объектов многих отраслей
народного хозяйства, где возможно придется работать сегодняшним студентам, в списке литературы приведены наименования соответствующих источников, опубликованных в открытой печати.

Очевидно, коль скоро действия преступников часто носят не просто ухищренный, а системно продуманный профессионалами характер, им следует противопоставить организацию и оснащение, выполненные на более высоком уровне профессионализма. Этим и объясняется необходимость разработки обобщенной системной концепции по обеспечению безопасности объектов, которая в каждом случае должна быть адаптирована к конкретному объекту, исходя из условий его функционирования, расположения, характера деятельности, географического положения, особенностей окружающей среды и обстановки и т.д. Таким образом, для каждого конкретного объекта должна разрабатываться на основе общей своя собственная концепция безопасности, исходя из положений которой разрабатывается проект оснащения объекта инженерно-
технических, специальных и программно-аппаратными средствами защиты.
Технические средства охраны (ТОО), установленные на объектах охраны, должны в комплексе с силами физической охраны и системой инженерных сооружений удовлетворять современным (исходя из сложившейся криминогенной обстановки) требованиям защиты ТОО от устремлений потенциального нарушителя.

Учитывая изложенное, разработчики технических средств охранной сигнализации (ТСОС) и комплексов технических средств охраны (КТСО) при анализе исходных положений для определения "моделей нарушителей" должны рассматривать и такие факторы, характерные для современной жизни, как:

- наличие в свободной продаже зарубежных и отечественных изделий спецтехники;
- возможность приобретения современного вооружения;
- возможность рекрутирования организованными преступными формированиями подготовленных в силовых структурах людей;
- наличие значительных финансовых ресурсов в криминальных структурах и т.д., т.е. факторов, расширяющих возможность преступных формирований организовывать против объектов охраны преступные действия с высоким уровнем их предварительной подготовки.

Одной из центральных подсистем в системе обеспечения безопасности ОО является автоматизированная система охраны (АСО), с помощью которой реализуются практические меры по предупреждению недозволенного доступа к технике, оборудованию, материалам, документам и охране их от шпионажа в пользу конкурентов, диверсий, повреждений, хищений и других незаконных или преступных действий.

На практике действия АСО (рис. 1) складываются из двух основных фаз: обнаружение нарушителя (в возможно короткий период времени с момента его появления в охраняемой зоне) и его задержание.

Задачи обнаружения нарушителя и определения места его проникновения могут быть решены как с помощью патрулей из личного состава службы охраны, так и с помощью технических средств охраны. Задачи обнаружения нарушителя и контроля за состоянием безопасности охраняемых объектов решаются, главным образом, с помощью технических средств охраны и телевизионного наблюдения. Применение этих средств позволяет в разумных пределах (с точки зрения реализации определенной тактики охраны) снизить численность личного состава охраны, но при этом повысить надежность защиты объекта, увеличить оперативность в принятии мер к задержанию нарушителя.

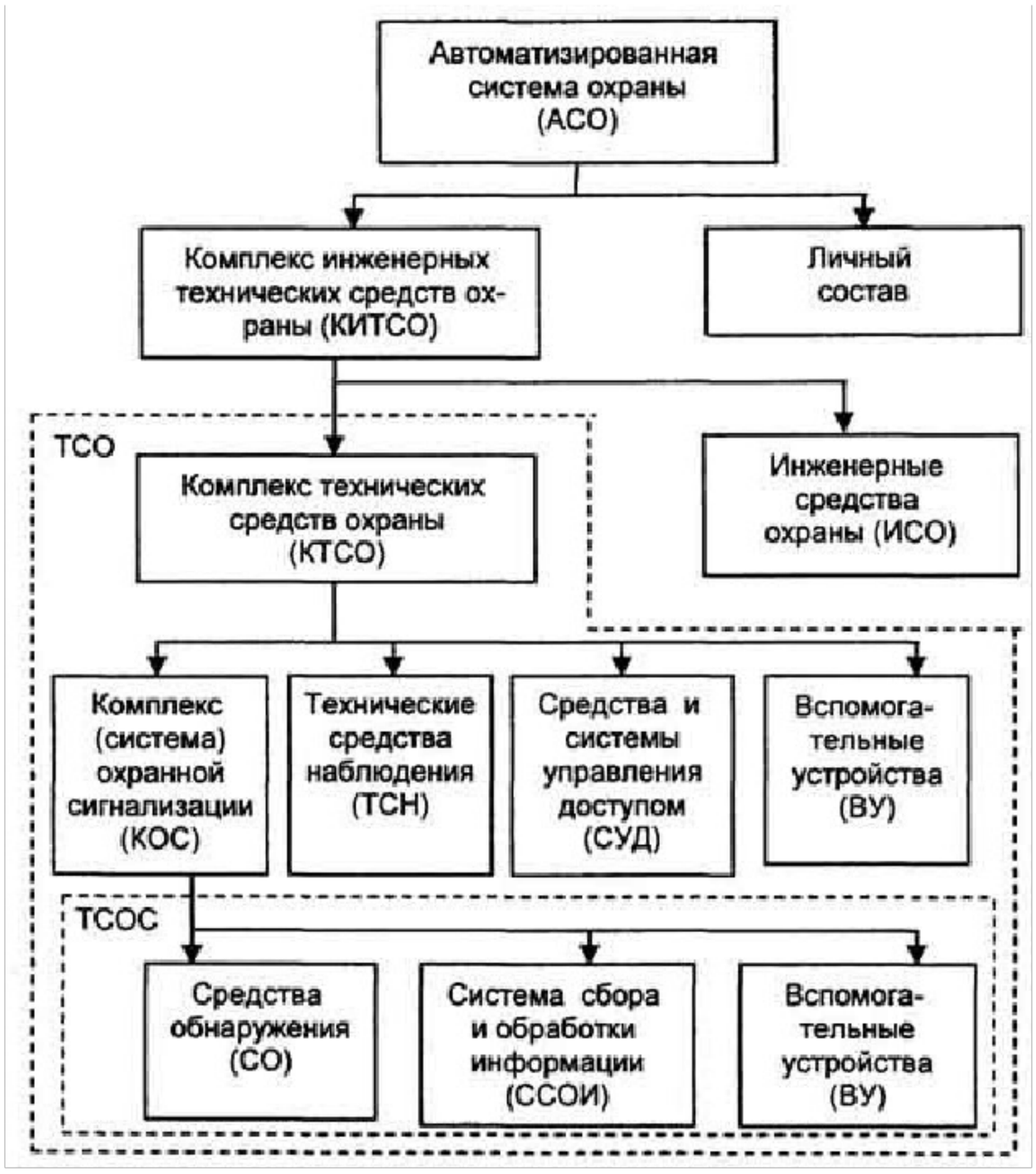

Рис. 1. Структура автоматизированной системы охраны

В общем случае **в состав комплекса технических средств обеспечения безопасности объекта входят:** технические средства охранной сигнализации (ТСОС); технические средства наблюдения (ТСН); система контроля доступа (СКД), в литературе применяются также понятия-синонимы - система управления доступом (СУД) и система контроля и управления доступом (СКУД); технические средства пожарной сигнализации (вопросы пожарной безопасности здесь не рассматриваются); технические средства обнаружения диверсионно-террористических средств и технические средства обнаружения (предотвращения) утечки информации. В состав ТСОС входят: средства обнаружения (СО); система сбора, обработки, отображения и документирования информации (ССОИ); вспомогательные устройства (ВУ) - системы электропитания, охранного освещения, оповещения и т.д.

Для решения задач и проблем выбора структуры и состава комплекса технических средств охраны необходимо, во-первых, проанализировать возможные варианты действий злоумышленника. Далее, для определенности, будем применять термин "нарушитель", имея в виду кого угодно, несанкционированным образом проникающего на охраняемую территорию и в его помещения, а именно: случайного, не имеющего определенных целей, человека; вора; грабителя; террориста или группы людей, вторгающихся с преступной целью. Исходя из анализа возможных действий нарушителя, составляются варианты его моделей, которые и принимаются за основополагающий фактор выбора тактики защиты объекта. Во-вторых, более углубленный или менее углубленный учет параметров моделей нарушителей осуществляется, исходя из значимости, ценности, важности объекта, т.е. требуемой категории его защиты (безопасности).

Важное влияние на выбор параметров нарушителя оказывают его стартовые позиции. Условно их можно разбить на четыре группы:

- нарушитель не имеет доступа на территорию объекта и, соответственно, преодолевает все рубежи охраны;

- нарушитель имеет доступ на объект, но не имеет доступа в режимную зону;
- нарушитель имеет доступ на объект и режимную зону, но не имеет доступа к конкретным охраняемым сведениям или материальным ценностям;
- нарушитель имеет доступ на объект, в режимную зону и к конкретным охраняемым сведениям или материальным ценностям.

Следует отметить, что при более простой (сложной) структуре объекта число стартовых позиций соответственно может уменьшаться (увеличиваться).

Очевидно, что для первой группы вероятность обнаружения и сложность проникновения на объект для совершения противоправных деяний в основном определяется КТСО, а для четвертой -уровнем всей системы обеспечения безопасности, включая и состояние режимной и кадровой работы, проводимой на объекте.

По каждой из возможных угроз необходимо определять территории, подлежащие контролю, и временные интервалы их контроля.

Структурную схему передачи оператору КТСО информации о наличии нарушителя можно представить в виде, приведенном на рис. 2.

Рис. 2. Структурная схема передачи информации о наличии нарушителя

Наиболее опасным, с точки зрения службы безопасности (охраны) объекта (СБ (О)) является подготовленный и технически оснащенный нарушитель, способный применить для обхода ТСОС множество способов. Очевидно, модель защиты должна строиться, исходя из моделирования всех возможных действий злоумышленника.

Вероятность обезвреживания (обнаружения и задержания) нарушителя силами физической охраны существенно зависит от характеристик ТСОС. Первая фаза обнаружение нарушителя - определяется вероятностью обнаружения нарушителя ТСОС, периодом наработки на отказ и временем восстановления ТСОС; вторая фаза - задержание нарушителя - зависит от времени обнаружения нарушителя техническими средствами охранной сигнализации с момента его появления на объекте и периода наработки на ложное срабатывание. Последнее объясняется тем, что при ложном срабатывании силы физической охраны отвлекаются на время проверки сигнала "Тревога" и не способны провести проверку двух и более фактов обработки ТСОС одновременно. Кроме того, ложное срабатывание создает с неизбежностью (объективно по законам психологии) стрессовую ситуацию, снижающую боеготовность сотрудников сил физической охраны на некоторый период времени, необходимый для восстановления гормонального баланса человеческого организма, а также порождает снижение бдительности из-за привыкания к факту появления ложных срабатываний.

Таким образом, при разработке проекта оборудования ОО техническими средствами охранной [illegible] гаммы технических факторов необходимо учитывать факторы, определяющие [illegible] нарушителя.

Рассмотрим, какие требования к проекту оборудования объекта ТСОС порождаются возможными действиями нарушителя.

Возможность нарушителя найти маршрут, не блокированный СО, должна быть

исключена. Для предотвращения прохода нарушителя должны быть блокированы все возможные маршруты движения нарушителя. Состояние физических преград (инженерных сооружений), имеющих большую стойкость и в связи с этим не блокированных СО, должно периодически контролироваться патрулями из личного состава охраны (обходно-дозорной службы) либо - с использованием телевизионных средств наблюдения.

Для увеличения вероятности обнаружения подготовленного и технически оснащенного нарушителя комплексом технических средств охраны объекта могут организовываться полностью скрытные (маскируемые) рубежи охраны.

С целью повышения устойчивости рубежей охраны к преодолению они должны оборудоваться СО, работающими на разных физических принципах действия (радиоволновые, ИК, сейсмические и т.д.), а также должна быть реализована функция дистанционного контроля. Комбинирование данных СО должно производиться по схеме М из N (например, при М=2, N=3, если сработали не менее двух из трех установленных СО, то принимается решение о выдаче сигнала "Тревога"). Числа М и N определяются в ходе проектирования КТСО индивидуально для каждого рубежа охраны объекта.

Для предотвращения обхода нарушителем рубежа охраны путем использования ухищренных способов передвижения необходимо устанавливать несколько СО, как правило, различных физических принципов действия, рассчитанных на блокирование участка при разных способах передвижения нарушителя. Для открытых пространств скорость движения может изменяться от 0,1 до 8 м/с, способы перемещения - от движения "ползком" до движения "в рост"; для физических преград (например, двери и ставни) способами преодоления могут быть открывание и разрушение (полное или частичное). Аналогично рассматриваются способы преодоления замкнутых пространств, а также стен, перекрытий и т.п.

Для предотвращения возможности имитации работы СО нарушителем соединительные линии системы сбора, обработки, отображения и документирования информации (ССОИ) должны иметь физическую и сигнализационную защиту коммутационных шкафов, коробок и т.п. При прокладке кабелей предпочтение следует отдавать скрытой проводке в закладных устройствах (трубах), обеспечивающих дополнительное экранирование и инженерную защиту.

В настоящее время выпускается большое число ССОИ, различающихся числом подключаемых СО, структурой соединительных линий - радиальная (лучевая), шлейфовал (магистральная), древовидная, петлевая (кольцевая) и другими характеристиками. Это позволяет оборудовать объект любого размера наперед заданной группы важности и/или категории защиты. Учет возможности вывода из строя ТСОС подготовленным и технически оснащенным нарушителем проводится при анализе возможных структурных схем построения ТСОС и КТСО в целом. При этом из рассмотрения должны быть исключены варианты, позволяющие замыканием (коротким замыканием) шин питания или информационно-адресных шин КТСО вывести его из строя. Для современных КТСО характерно использование лучевой или древовидной структуры информационно-адресных шин, раздельного управления и автономных защитных цепей электропитания каждого канала.

Ниже рассмотрим некоторые основные требования к выбору аппаратуры ССОИ, определяемые возможностью появления подготовленного и технически оснащенного нарушителя и степенью его подготовки и оснащенности. Возможность обхода ССОИ подготовленным и технически оснащенным нарушителем учитывается при выборе способа передачи информации в ССОИ. Различают три типа аппаратно-программной реализации АСОИ:

1. тип - с низкой устойчивостью к обходу;
2. тип - со средней устойчивостью к обходу;
3. тип - с высокой устойчивостью к обходу.

Под низкой устойчивостью ССОИ к обходу понимают такую организацию опроса СО в АСО, при которой при снятии участка (СО) с охраны состояние соединительной линии и датчика вскрытия СО со стороны АСО не контролируются (отсутствует режим "деблокирование").

Под средней устойчивостью понимают такую организацию опроса СО в АСО, при которой при снятии участка (СО) с охраны состояние соединительной линии и датчика вскрытия СО остаются под контролем АСО (имеется режим "деблокирование").

Под высокой устойчивостью понимают организацию опроса СО, аналогичную средней, но сообщения шифруются с использованием кода, гарантированная стойкость которого к обходу (дешифрации) составляет десятки тысяч часов.

Для предотвращения преодоления ТСО путем оказания воздействия на оператора системы охраны или использования его негативных качеств ССОИ должна иметь режим документирования и иерархическую систему управления, т.е. оператор не должен иметь полного контроля над ССОИ, необходимого лишь при ее настройке, а в системе охраны больших объектов оператор не должен обладать и возможностью снятия (постановки) некоторых участков охраны.

Для того чтобы оперативно обнаружить выход из строя составных частей КТСО, в том числе и в случае преднамеренных действий (саботажа), применяется дистанционный контроль (автоматизированный или автоматический), обеспечивающий проверку работоспособности СО, соединительной линии и приемной аппаратуры ССОИ, а также повышающий устойчивость ТСОС к обходу соединительных линий и имитации работы СО.

2. Системный подход-основа методологии разработки концепции комплексного обеспечения безопасности объектов охраны

Как показали результаты многих исследований, для выработки системного решения, удовлетворяющего необходимым и достаточным условиям обеспечения надежной защиты ОО от подготовленного и технически оснащенного нарушителя, требуется полный учет не только перечисленных выше факторов, но и многих других, как то: состояние инженерных сооружений объекта, состав и уровень подготовки сил физической охраны объекта, окружение объекта, характер объекта (легендируемый, нелегендируемый), расположение и количество сил поддержки, состояние сетей электропитания объекта и т.д.

Многолетний опыт по созданию систем защиты объектов убеждает в безусловной необходимости разрабатывать в каждом случае **системную концепцию обеспечения безопасности** конкретного объекта, которая на практике предполагает комплексное взаимоувязанное решение руководством предприятия и службой безопасности (охраны) ряда крупных блоков задач (часть из которых могут решаться лишь с помощью спецслужб при строгом соблюдении соответствующих законов РФ), как то:

1. **Определение стратегии комплексной безопасности.** Здесь решаются проблемы классификации, систематизации и дифференциации угроз; определяются структура и задачи служб безопасности; разрабатываются (определяются) нормативно-правовые документы, регламентирующие с позиций юриспруденции деятельность служб безопасности (СБ); на основе анализа ресурсов, технико-экономических показателей и социальных аспектов безопасности разрабатываются планы мероприятий по обеспечению безопасности объектов.
2. **Обеспечение безопасности от физического проникновения на территорию и в помещения объекта.** В этом блоке задач на основе анализа доступности объекта моделируются стратегия и тактика поведения потенциального нарушителя (по всем возможным маршрутам движений); дифференцируются зоны безопасности; на основе определения ключевых жизненно важных центров объектов разрабатываются принципы и схемы оборудования техническими средствами охранной сигнализации и телевизионного наблюдения, средствами инженерной, технической и специальной защиты рубежей

охраны (периметра, территории, зданий, помещений, хранилищ, сейфов, транспортных коммуникаций, средств связи, компьютерных сетей и т.д.). Соответственно, на основе расчета тактико- технических требований выбирается состав и номенклатура технических средств.

3. Защита информации. Решение задач данного блока обеспечивается специальными методами защиты. На основе разработки принципов проверки, классификации источников информации и каналов ее утечки разрабатываются концептуальные модели защиты от утечки информации, проводятся их оценки на предмет эффективности предлагаемых этими моделями решений. Здесь решается широкая гамма задач разработки методов защиты по всем возможным каналам утечки (речевой, визуальный, виброакустический, электромагнитный, проводной, за счет паразитных связей и наводок и др.). Разрабатывается нормативная база по защите от утечки информации. На основе моделирования возможных способов приема информации потенциальным нарушителем за пределами помещений посредством применения направленных микрофонов, лазерных средств и т.п. вырабатываются методы пассивной и активной защиты.

4. Защита от прогнозируемых к применению средств внегласного контроля. Эти задачи ориентированы на модель нарушителя - сотрудника учреждения, либо на проведение контрразведывательных мероприятий, если по оперативным каналам получена информация о заинтересованности, которую проявили организованные преступные формирования к данному объекту. Здесь решается ряд специфических задач от выбора и установки средств негласного контроля до выбора организационно-режимных мер защиты от негласного контроля со стороны потенциального нарушителя. Большое внимание здесь уделяется техническим средствам дефектоскопии, автоматизации средств контроля трактов передачи информации, анализу системы демаскирующих признаков и ряду других [*].

5. Защита от диверсионно-террористических средств (ДТС). Задачи данной предметной области также решаются специальными методами защиты. На основе исследования, классификации и моделирования вариантов активных действий террористов, прогнозирования возможных способов доставки ДТС на территорию объекта, изучения каналов управления диверсиями и технических способов их осуществления (например, с использованием радиовзрывателей) выбирается аппаратура обнаружения ДТС, разрабатываются организационно-технические мероприятия по созданию контрольных пунктов, постов проверки, использованию меточной техники и ряд других. Разрабатываются рекомендации по выбору техники обнаружения.

6. Обеспечение безопасности (защита информации) в локальных вычислительных сетях (ЛВС) и ПЭВМ, т.е. в автоматизированных системах обработки информации (АСОИ). Здесь на основе анализа моделей нарушителей, классификации видов угроз и видов компрометации информации разрабатывается комплексный подход к защите информации в автоматизированных информационных системах, ЛВС, серверах и ПЭВМ, соответствующая нормативно- правовая база защиты, регламентирующие документы; разрабатываются методы и способы программно-аппаратной защиты от несанкционированного доступа и копирования (НСД, ИСК). Особое место занимают разработка и внедрение специальных математических и программных методов защиты операционных систем, баз данных и серверов, методов идентификации пользователей и ЭВМ, паролей, ключей и антивирусных программ. На основе определения и анализа задач СБ разрабатываются организационные меры защиты.

Этот блок задач достаточно подробно рассмотрен в книге [100].

7. Защита [illegible] точки зрения проведения разведывательных операций со стороны [illegible] необходимость тщательной разработки данного блока задач является чрезвычайно актуальной, ибо наиболее доступными для перехвата нарушителем информации, безусловно, являются каналы связи.

Здесь на основе классификации сетей связи разрабатываются методы оптимизации связи, криптографической защиты, защиты телефонных сетей связи. Наряду с решением проблем стандартизации защиты, создаются специальные методы и способы, обеспечивающие конфиденциальную связь.

8. Человеческий фактор в системе обеспечения безопасности. Здесь рассматривается блок задач, решаемый детективной группой службы безопасности, как то:

- разработка и реализация мероприятий по изучению лиц из числа персонала и иных лиц, в действиях которых содержатся угрозы безопасности деятельности учреждения посредством воздействия на его сотрудников, их близких и родственников;
- проверка кандидатов для приема на работу;
- разработка и реализация мероприятий по обеспечению "чистоты рук";
- организация взаимодействия и поддержание контактов с силами поддержки и/или правоохранительными органами по вопросам обеспечения безопасности и многое другое.

9. Исследование средств отечественного и зарубежного вооружения, которые могут применяться для поражения объектов. В данном блоке задач должны быть рассмотрены возможные способы и применяемые организованными преступными формированиями (или исполнителями - одиночками) виды вооружения, взрывчатых или иных поражающих веществ для осуществления вооруженной акции.

Здесь на основе анализа тактико-технических характеристик традиционных и нетрадиционных средств поражения объектов должна быть дана классификация этих средств, описаны характерные признаки их поражающего действия, методы и способы их обнаружения, локализации, обезвреживания или уничтожения, а также проведена оценка эффективности систем охраны и обороны объектов.

10. Организация системы контроля доступа. Этот блок задач направлен на эффективную реализацию процедур проверки человека, пытающегося открыто ("законным образом") проникнуть на территорию объекта, в отдельные его помещения и режимные зоны. Здесь решаются задачи идентификации - это установление тождества (опознание личности) по совокупности общих и частных признаков и аутентификации - это установление подлинности личности (см. например [5, 55, 168]).

Кроме 10 перечисленных (которые напрямую связаны с оперативной охранной деятельностью) существуют иные блоки задач, рассматривающих как общесистемные проблемы, например, определение приоритетов (иерархий) во взаимодействии элементов системы безопасности, так и специальные, например обеспечение пожарной безопасности. Области охранной деятельности, связанные с реализацией названных задач, чрезвычайно многогранны. В данной книге рассматриваются лишь основы теории создания технических средств охраны, с помощью которых обеспечивается защита объекта охраны от физического проникновения нарушителя, т.е. решение второго блока задач (в американской литературе в данном случае применяется понятие "система физической защиты", см., например, М. Гарсия. Проектирование и оценка систем физической защиты / Пер. с англ.; Под ред. Р.Г. Магауенова. - М.: "Мир", 2002.).

Взаимоувязанное решение перечисленных блоков задач **системной концепции обеспечения безопасности объекта,** в каждом из которых существуют свои подходы, методы и способы решения, должно обеспечить непротиворечивость и полноту принимаемых мер защиты. Только в этом случае можно говорить о выполнении **необходимых и достаточных условий** в деле защиты объекта от подготовленных и технически оснащенных нарушителей.

Реализация каждого из блоков задач осуществляется посредством разработки проекта, который будет индивидуальный для учреждения и объекта (территории, здания, этажа, помещения). В зависимости от категории важности объекта этот проект должен обладать соответствующими грифами секретности. Однако и для нежимных объектов охраны такой проект должен носить строго конфиденциальный характер, т.е. быть

доступным строго ограниченному кругу лиц из числа сотрудников СБ(0) и руководства.
Необходимость комплексного решения (на основе системного подхода) перечисленных основных (типовых) блоков задач проистекает из того, что профессионализму ОПФ (Г), безусловно, следует противопоставить организацию и оснащение, выполненные на более высоком уровне профессионализма. Однако, коль скоро абсолютной защищенности быть не может, в каждом случае проводятся сравнительные оценки затрат на защиту и возможные потери при сознательном отказе от применения несоизмеримо дорогостоящих (относительно потерь) методов и технических средств защиты.
В мировой практике уже давно используется такое понятие как система защиты, под которой подразумевается комплекс организационных и технических мероприятий, направленных на выявление и противодействие различным видам угроз деятельности объекта.
Рассмотрение возможных угроз проводится по следующим основным направлениям:

- безопасность персонала: неэффективная защита может привести к ущербу здоровью или даже угрозе жизни сотрудников;
- угрозы материальным ценностям, имуществу и оборудованию;
- безопасность информации.

Существенным при оценке угроз и выборе приоритетов в системе защиты является учет международного опыта по организации охранной деятельности применительно к объектам конкретного вида, например, банков, предприятий, крупных офисов и т.д. Этот опыт берется за основу и при подготовке современных нормативов защиты. Так, например, западно-европейские фирмы

- производители оборудования для систем банковской защиты придерживаются единых критериев оценки угроз, согласно которым для сейфовых комнат - хранилищ ценностей и компьютерной информации приоритеты направлений защиты следующие (более подробно см. Концепция комплексной защиты банковских объектов. - М.: Росси Секьюрити, 1998.):
- терроризм, стихийные бедствия и аварии, пожары, наводнения, механическое разрушение;
- несанкционированный (неразрешенный) съем информации из компьютерного банка данных;
- несанкционированное проникновение в сейфовую комнату как с целью кражи ценностей, так и с целью кражи информации.

Несмотря на существенные различия в природе угроз, создание защиты от каждой из них должно идти в комплексе со всей системой. Например, несанкционированный съем информации может осуществляться дистанционно путем контроля из соседнего здания излучений от средств обработки банка данных, в котором может содержаться информация конфиденциального характера. Защитой от такого вида угрозы является экранирование аппаратуры и коммуникаций, применение специальной аппаратуры, искажающей картину электромагнитного поля излучения. Но съем информации можно проводить и с помощью специально внедренных в помещение подслушивающих устройств, как то: микрофоны, радиозакладки и т.п. (см. примечание на с. 22). Защитой в этом случае будет поиск техники подслушивания с привлечением компетентных органов, а также строгое соблюдение режима доступа в помещение или в здание, что является защитой и от несанкционированного проникновения.
В основе разработки системы защиты объекта и организации ее функционирования лежит принцип создания последовательных рубежей, в которых угрозы должны быть своевременно обнаружены, а их распространению будут препятствовать надежные преграды. Такие рубежи (зоны безопасности) должны располагаться последовательно от ограждения вокруг территории объекта до главного особо важного помещения, такого как хранилище материальных и информационных ценностей.

Защита объекта должна состоять из различного рода ограждений его периметра и специально оборудованных въездов и проходов, решеток на окнах и в дверных проемах, резервных выходов из здания, охранной сигнализации, охранного освещения и охранного теленаблюдения.

Элементы защиты всех участков объекта должны взаимодополнять друг друга. Эффективность всей системы защиты от несанкционированного проникновения будет оцениваться по максимуму времени, которое злоумышленник затратит на преодоление всех зон безопасности. За это же время должна сработать сигнализация, сотрудники охраны установят причину тревоги, примут меры к задержанию злоумышленника и вызовут подкрепление из ближайшего отделения милиции или из сил поддержки.

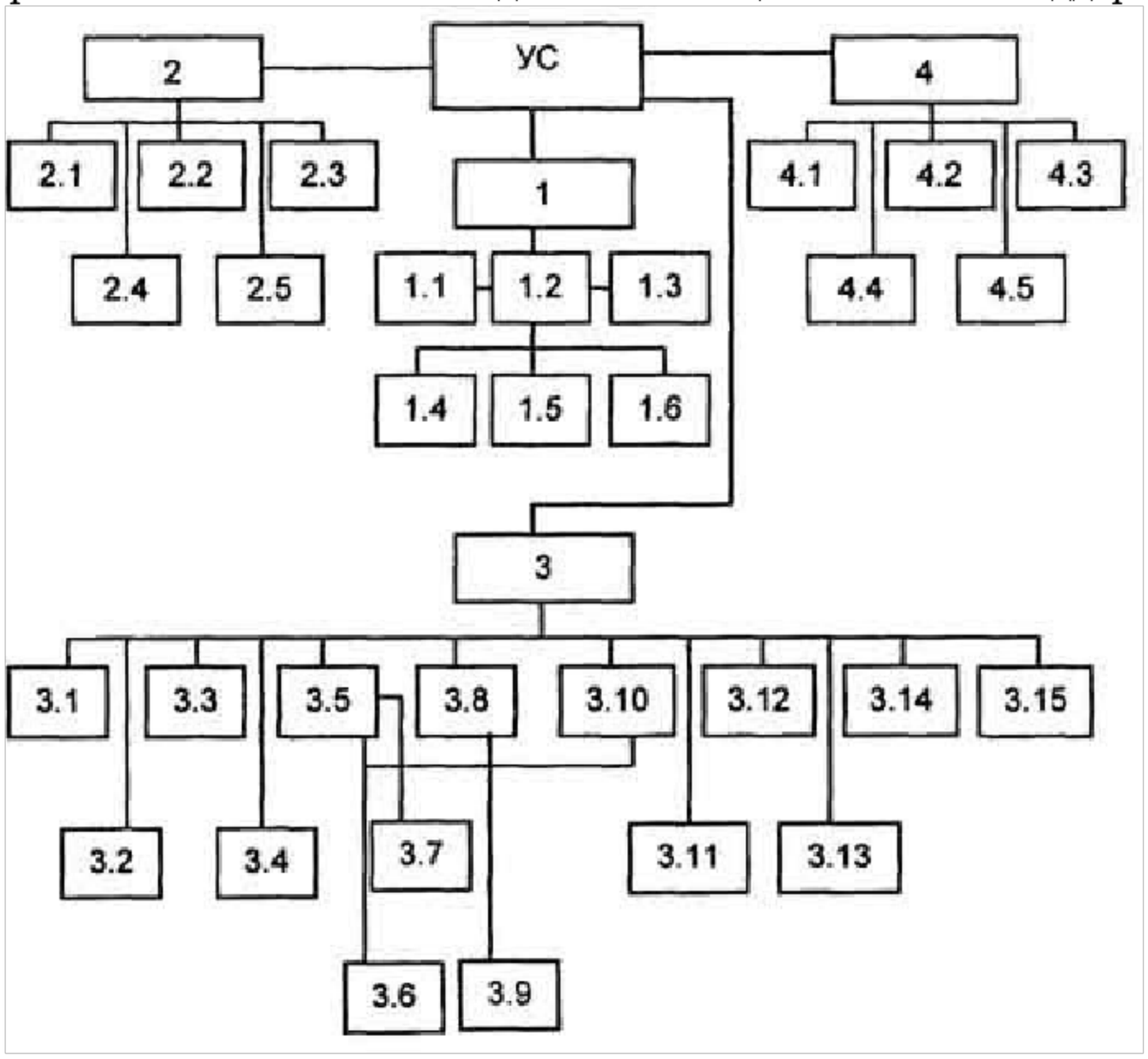

Рис. 3. Укрупненная структурная схема системы обеспечения безопасности объекта

Таким образом, эффективность системы защиты оценивается величиной времени с момента возникновения угрозы до начала противодействия или ликвидации ее. Чем более сложная и разветвленная система защиты, тем больше времени потребуется на ее преодоление и тем больше вероятность того, что угроза будет своевременно обнаружена, определена и отражена.

Современные системы безопасности основываются на реализации комплекса мероприятий по организации физической, инженерной, технической и специальной защиты.

В общем виде укрупненная структурная схема системы обеспечения безопасности объекта представлена на рис. 3. На рис. 3 приняты следующие обозначения:

УС - укрупненная структурная схема системы обеспечения безопасности объекта

- 1 - физическая защита
- 1.1 - объектовая и/или городская пожарная команда
- 1.2 - служба охраны
- 1.3 - караульный и/или силы поддержки
- 1.4 - работники контрольно-пропускного поста
- 1.5 - операторы технических средств охраны
- 1.6 - дежурная группа и подвижные посты

- 2 - инженерная защита
- 2.1 - усиленные ограждающие конструкции
- 2.2 - усиленные двери и дверные коробки
- 2.3 - металлические решетки и жалюзи
- 2.4 - спецзамки, усиленные запоры
- 2.5 - сейфы повышенной стойкости
- 3 - техническая защита
- 3.1 - средства обнаружения радиоактивных средств
- 3.2 - средства обнаружения оружия
- 3.3 - система пожарной сигнализации
- 3.4 - система тревожного оповещения
- 3.5 - система контроля доступа
- 3.6 - охранное освещение
- 3.7 - переговорные устройства
- 3.8 - система охранной сигнализации
- 3.9 - источник резервного электропитания
- 3.10 - система телевизионного наблюдения
- 3.11 - средства связи
- 3.12 - средства проверки почтовой корреспонденции
- 3.13 - средства обнаружения взрывчатых веществ
- 3.14 - система защиты средств ВТ и ЛВС
- 3.15 - средства обнаружения и защиты от технических средств проникновения через инженерные коммуникации, отверстия, проёмы и т.д.
- 4 - специальная защита (см. примечание на с. 22)
- 4.1 - обеспечение требований безопасности на этапе строительства
- 4.2 - проведение обследования помещений на наличие устройств съема информации
- 4.3 – спецпроверка технических средств передачи, обработки, накопления и хранения информации
- 4.4 - специальные защищенные помещения для переговоров
- 4.5 - средства спецзащиты сетей коммуникации

Физическая защита обеспечивается службой охраны, основной задачей которой является предупреждение несанкционированного физического проникновения на территорию, в здания и помещения объекта злоумышленников и их сдерживание в течение расчетного времени (до прибытия милиции или сил поддержки).

Инженерная защита предусматривает использование усиленных дверей и дверных коробок, металлических решеток, усиленных ограждающих конструкций, усиленных запоров, сейфов повышенной стойкости.

Техническая защита включает систему охранной сигнализации, систему телевизионного наблюдения, систему тревожного оповещения, автоматизированную систему контроля доступа, переговорные устройства, средства связи, пожарной сигнализации, средства проверки почтовой корреспонденции, охранного освещения, резервного (аварийного) электропитания, систему дежурного и тревожного освещения.

Не лишним может оказаться и установка детекторов оружия (металлоискателей) и средств контроля радиационной обстановки на входе здания для предотвращения возможности проведения терактов.

Специальная защита обеспечивает защиту от утечки информации, представляющей особую ценность, а также проверку надежности (лояльности) персонала службы охраны, материально ответственных лиц и некоторых других категорий служащих.

Специальная защита состоит из комплекса организационно-технических и специальных мероприятий, направленных на:

- обеспечение требований безопасности на этапах проектирования, строительства

(реконструкции) и эксплуатации зданий;

- периодическое проведение специальных обследований отдельных помещений для выявления возможно установленных в них подслушивающих устройств;
- сооружение специальных технически защищенных помещений для ведения конфиденциальных переговоров и контроль работоспособности специальных средств защиты;
- проверку и защиту технических средств, используемых для передачи, обработки, накопления и хранения конфиденциальной информации;
- оборудование средствами защиты электросети, внутренней и городской телефонной связи и других коммуникаций систем жизнеобеспечения;
- осуществление специальных проверочных мероприятий по выявлению неблагонадежных сотрудников и лиц с психическими отклонениями (автоматизированные системы психологического тестирования).

Как показывает опыт зарубежных фирм и отечественных организаций и предприятий, нормальное, безущербное функционирование возможно лишь при системном, взаимоувязанном использовании всех вышеназванных видов защиты и четко спланированных действиях сил службы охраны по сигнальной информации, получаемой от средств системы технической защиты.

Таким образом, мы вкратце рассмотрели основные положения обобщенной системной концепции обеспечения безопасности ОО.

3. Общий подход к категорированию объектов охраны

Основополагающими, определяющими выбор уровня защиты объекта, признаками являются категория важности объекта и модель нарушителя, от проникновения которого данный объект должен быть защищен.

Система охраны объекта, т.е. его периметра, территории, зданий, помещений - это сложный, многорубежный комплекс, включающий в себя физическую защиту (личный состав охраны), инженерные сооружения (решетки, стальные двери, сложные замки, замки - защелки, сейфы и т.п.), технические средства охранной сигнализации, системы телевизионного наблюдения (СТН), системы контроля доступа (турникеты, шлагбаумы, управляемые ворота и т.д.) и многое другое, что было рассмотрено в структурной схеме системы обеспечения безопасности объекта (см. рис. 3).

Создание технически высокооснащенной системы охраны чрезвычайно дорогостоящее дело, поэтому разработчики КТСО и СБ (О) (исполнители и заказчики) выбирают такую конфигурацию и архитектуру КТСО, которая была бы экономически разумной. Это означает, что затраты на создание, внедрение и эксплуатацию КТСО должны быть существенно ниже, чем стоимость того, что охраняется. По некоторым оценкам эти затраты составляют около 5% основных фондов и до 25% оборотных средств в расчете на один финансовый год.

Существуют определенные методики технико-экономических обоснований выбора того или иного варианта оборудования объекта ТСОС, например [187]. Однако очевидно, что для объектов особого риска, как например, ядерноопасных объектов, на которых проведение диверсионно- террористических актов может повлечь за собой неисчислимые бедствия, гибель людей, разрушение экологической системы целых регионов, требуются достаточные для их надежной защиты затраты.

Таким образом, абстрактно-типизированный подход к категорированию важности объектов (далее для краткости - категорированию объектов) необходим лишь для приближенной оценки возможных затрат на их оснащение инженерно-техническими, специальными и программными средствами защиты.

Второй аспект, влияющий на уровень затрат, т.е. в конце концов на выбор уровней защиты, это модель нарушителя. Например, очевидно, чем выше должностной статус злоумышленника, работающего на охраняемом объекте (например, им может быть

"директор", "главный инженер" и т.д.), тем выше будут затраты на создание системы безопасности, адекватной их "моделям". Поэтому следует понимать, что абсолютной защищенности объекта быть не может. Но это уже проблемы, выходящие далеко за рамки категорирования объектов, создания и применения КТСО, хотя и в определенной мере связанные с ними.

Итак, в данном изложении определение необходимых уровней защиты мы будем связывать с понятием классификации объектов по категориям важности, полагая априори, что злоумышленник является человеком "со стороны".

В первом приближении при выборе уровня защиты следует учитывать возможность обоснованного отнесения объекта к одной из четырех категорий:

- 1-я категория - особо важный объект;
- 2-я категория - особо режимный объект;
- 3-я категория - режимный объект;
- 4-я категория - нережимный объект.

Отнесение конкретных объектов к той или иной категории важности регламентируется специальным перечнем, утвержденным правительством РФ.

В относительно самостоятельных (национальных, областных, краевых) территориальных образованиях могут создаваться свои перечни объектов, дополняющие общий, исходя из требований местных условий и возможностей самостоятельного финансирования расходов по их оснащению КТСО.

Очевидно, что выбор уровня оснащения КТСО названных категорий объектов будет зависеть от многих конкретных факторов, как то: конфигурация территории, рельеф местности, географическое положение, структура расположения жизненно важных центров объекта, характер угроз и т.д.

Априори следует полагать:

- - *1-я и 2-я категории объектов* требуют высокого уровня оснащения КТСО, включения в него разнообразных ТСОС, телевизионных средств наблюдения (ТСН), наличия развитой ССОИ, СКД, создания многих рубежей защиты (зон безопасности), реализации функций автоматического определения направления движения нарушителя, состояния СО, анализа характера разрушающего действия нарушителя на КТСО и т.д.;
- - *3-я категория объектов* требует меньшего, но достаточно высокого уровня оснащения. Здесь выборочно исключается исполнение ряда функций охраны (защиты), затраты на реализацию которых заведомо выше возможных потерь от злоумышленных действий;
- - *4-я категория объектов* оснащается КТСО ограниченной структуры, предполагает наличие меньшего числа зон безопасности, реализацию меньшего количества функций в ССОИ.

Следует отметить, что наряду с категорированием объектов должно применяться и категорирование помещений с организацией соответствующих "зон безопасности". Это позволит минимизировать затраты на оснащение КТСО и организацию системы защиты в целом. Выбор категории (уровня защиты) должен осуществляться исходя из значимости объекта, характера потенциальных угроз и, соответственно, "моделей" вероятных нарушителей и моделей их вероятных действий.

Приведенная классификация категорий важности объектов представляет по существу лишь укрупненно-базисный подход. В специальных разработках по этой проблеме выделяются множества подклассов, на основе чего разрабатываются идеи типизации объектов и решения соответствующих задач типизации их оснащения КТСО.

Наиболее опасной угрозой для любого объекта является угроза проведения диверсионно-террористическими актами (ДТА) с применением диверсионно- террористических средств (ДТС).

Коль скоро невозможно ставить задачу защиты всех без исключения или абсолютного большинства объектов, ибо это непосильно из-за невероятно больших затрат финансовых,

материальных и людских ресурсов, принят подход, в рамках которого решаются задачи определения перечня типовых особо важных объектов народного хозяйства, МО и иных (требующих охраны) объектов. Этому подходу характерна разработка рациональных (типовых) схем защиты объектов, входящих в группу риска, исходя из вероятности использования на них ДТС или их привлекательности для преступных посягательств.

Исходя из международного опыта следует, что противодействие преступности, особенно ОПФ, может осуществляться лишь на основе государственной программы борьбы с преступностью. При этом приоритетный выбор объектов для организации системной защиты определяется, исходя из оценки возможного использования на них ДТС.

Типовые особо важные объекты, как правило, принадлежат таким отраслям как энергетика, транспорт, химические и нефтехимические, наука и техника, оборонная промышленность, оборона, связь и информатизация, а также Министерствам финансов, здравоохранения, культуры и силовым структурам страны. Эти отрасли являются ключевыми для жизнеобеспечения общества и от их действенной защиты зависит жизнь, спокойствие и морально- психологическое состояние всего народа, прогрессивность движения общества, результативность экономических преобразований.

Лабораторное занятие №9.
Тема: Аналитический подход к классификации угроз безопасности информационного объекта на основе моделирования нарушителей и их действи

СОДЕРЖАНИЕ ЗАНЯТИЯ

"Модель" нарушителя, возможные пути и способы его проникновения на охраняемый объект. Вопросы классификации нарушителей и угроз информационной безопасности
Характеристика нарушителя, степень его подготовки и оснащенности, общие рекомендации по применению технических способов защиты. В начале данной главы достаточно подробно говорилось о том, что охрана объекта является сложным интегрированным процессом. В широком смысле под охраной понимается комплекс организационных, контрольных, инженерно-технических и иных мероприятий, направленных на обеспечение полной, частичной или выборочной защиты информации, материальных ценностей и безопасности персонала объекта.
В узком смысле задача системы охраны заключается в обнаружении и пресечении действий людей, пытающихся тайно или открыто (но несанкционированно) проникнуть на охраняемую территорию объекта или в его зоны безопасности.
Как показывает опыт работы, нормальное безущербное функционирование системы защиты возможно при комплексном использовании всех видов защиты (изложенных в системной концепции) и четко спланированных действиях сил службы охраны по сигналам, получаемым от технических средств охранной сигнализации.
Охрана учреждения, как правило, является достаточно дорогостоящим мероприятием, поэтому при выборе уровня защиты целесообразно оценить возможные потери от "беспрепятственного" действия нарушителя и сравнить их с затратами на организацию охраны. Этот показатель является индивидуальным для каждого объекта и может быть оценен, как правило, весьма приближенно. Практика создания и эксплуатации комплексов технических средств охранной сигнализации показала, что в большинстве случаев для построения эффективной охраны требуется наличие комбинированных ТСОС, учитывающих возможность дублирования функций обнаружения на основе использования различных физических принципов действия средств обнаружения (близкие понятия - синонимы: датчиков, детекторов, извещателей).
В основе эффективного противодействия угрозе проникновения нарушителя в охраняемые помещения (сейфовые комнаты, переговорные помещения, архивы конструкторско-технологической документации, хранилища информационных баз данных и т.п.) лежит проведение априорных оценок:

- - приоритетов в системе защиты (т.е. следует определить, что может представлять наибольший интерес для нарушителя и должно защищаться в первую очередь);
- - путей возможного проникновения нарушителей;
- - информации, которой может располагать нарушитель об организации системы защиты предприятия;
- - технических возможностей нарушителя (его технической вооруженности) и т.д., т.е. оценок совокупности количественных и качественных характеристик вероятного нарушителя.

Такая совокупность полученных оценок называется "моделью" нарушителя. Эта модель, наряду с категорией объекта, служит основой для выбора методов организации охраны объекта, определяет сложность и скрытность применяемых технических средств охранной сигнализации и телевизионного наблюдения, варианты инженерно-технической защиты, кадровый состав службы охраны и т.д.
По уровню возможной технической оснащенности "нарушителя" условно можно разделить на следующие типы:

- - случайные (не знающие, что объект охраняется и не имеющие специальной цели

проникновения на объект);

- - неподготовленные (проникающие на объект со специальной целью и предполагающие возможность охраны объекта, но не имеющие информации о структуре и принципах действия системы охраны);
- - подготовленные (имеющие информацию о возможных методах обхода ТСО и прошедшие соответствующую подготовку);
- - обладающие специальной подготовкой и оснащенные специальными средствами обхода;
- - сотрудники предприятия (последние два типа нарушителей можно объединить термином "квалифицированный").

Наиболее распространенной "моделью" нарушителя является "неподготовленный нарушитель", т.е. человек, пытающийся проникнуть на охраняемый объект, надеясь на удачу, свою осторожность, опыт или случайно ставший обладателем конфиденциальной информации об особенностях охраны. "Неподготовленный нарушитель" не располагает специальными инструментами для проникновения в закрытые помещения и тем более техническими средствами для обхода охранной сигнализации. Для защиты от "неподготовленного нарушителя" часто оказывается достаточным оборудование объекта простейшими средствами охранной сигнализации (лучевые средства обнаружения на периметре, кнопки или магнитоуправляемые контакты на дверях в помещения) и организация службы невооруженной охраны (имеющей пульт охранной сигнализации и телефонную связь с милицией).

Более сложная "модель" нарушителя предполагает осуществление им целенаправленных действий, например, проникновение в охраняемые помещения с целью захвата материальных ценностей или получения информации. Для крупного учреждения наиболее вероятной "моделью" является хорошо подготовленный нарушитель, возможно действующий в сговоре с сотрудником или охранником. При этом возможны такие варианты проникновения, как:

- - негласное проникновение одиночного постороннего нарушителя с целью кражи ценностей, для установки специальной аппаратуры или для съема информации;
- - негласное проникновение нарушителя-сотрудника предприятия с целью доступа к закрытой информации;
- - проникновение группы нарушителей в охраняемые помещения в нерабочее время путем разрушения инженерной защиты объекта и обхода средств охранной сигнализации;
- - проникновение одного или группы вооруженных нарушителей под видом посетителей (в рабочее время, когда не введены в действие все средства инженерной и технической защиты) с целью силового захвата ценностей;
- - вооруженное нападение на объект с целью захвата заложников, ценностей, получения важной информации или организации собственного управления.

Очевидно, "модель" нарушителя может предполагать и сразу несколько вариантов исполнения целей проникновения на ОО.

Среди путей негласного проникновения нарушителя прежде всего могут быть естественные проемы в помещениях: двери, окна, канализационные коммуникации, кроме того непрочные, легко поддающиеся разрушению стены, полы, потолки. Поэтому при организации охранной сигнализации в охраняемом помещении в первую очередь должны быть установлены средства обнаружения для защиты окон и дверей. Обнаружение проникновения через стены, полы и потолки выполняют, как правило, СО, предназначенные для защиты объема помещения. Для усиления защиты окон и дверей широко используются металлические решетки и защитные жалюзи. Установка достаточно надежных решеток может иногда позволить отказаться от установки на них средств охранной сигнализации. Однако часто наблюдалось, что неправильная конструкция решеток открывает дополнительные возможности для проникновения в здание. Например, защищая окна первого этажа, решетки могут облегчить доступ к окнам

второго этажа.
Возможность проникновения на объект вооруженных нарушителей требует не только усиления вооруженной охраны, но и установки на входах обнаружителей оружия, оборудование особо ответственных (важных) рабочих мест сотрудников кнопками и педалями тревожного оповещения, а в ряде случаев и установки скрытых телекамер для наблюдения за работой сотрудников. Входы в хранилища ценностей должны оборудоваться специальными сейфовыми дверями с дистанционно управляемыми замками и переговорными устройствами.
Уровни технической оснащенности нарушителя и его знаний о физических принципах работы СО, установленных на объекте, определяют возможность и время, необходимое ему на преодоление средств инженерной защиты и обход сигнализационной техники. Наиболее эффективны СО, физический принцип действия и способ обхода которых нарушитель не знает. В этом случае вероятность его обнаружения приближается к единице (что определяется только техническими параметрами самого СО).
В конечном счете, поскольку задачей системы охраны является оказание противодействий нарушителю в достижении его целей, при построении системы охраны в ее структуру закладывается принцип создания последовательных рубежей на пути движения нарушителя. Угроза проникновения обнаруживается на каждом рубеже и ее распространению создается соответствующая преграда. Такие рубежи (зоны безопасности) располагаются последовательно от прилегающей к зданию территории до охраняемого помещения, сейфа. Эффективность всей системы защиты от несанкционированного проникновения будет оцениваться по минимальному значению времени, которое нарушитель затратит на преодоление всех зон безопасности. За это время, с вероятностью близкой к 1, должна сработать система охранной сигнализации. Сотрудники охраны установят причину тревоги (например, с помощью телевизионной системы наблюдения или путем выдвижения на место тревожной группы) и примут необходимые меры.
Если "модель" нарушителя рассматривает негласное проникновение в охраняемое помещение нарушителя-сотрудника (в том числе из службы охраны), в состав средств охранной сигнализации необходимо включить устройства документирования работы средств обнаружения, чтобы фиксировать несанкционированные отключения каналов сигнализации. Обычно указывается время постановки и снятия с охраны помещения. Аппаратура документирования должна устанавливаться в специальном помещении, куда имеют доступ только начальник охраны или ответственный сотрудник службы безопасности.
Итак, сложность системы охраны, ее насыщенность средствами инженерной и технической защиты определяются "моделью" нарушителя, категорией и особенностями объекта охраны. Количество необходимых зон безопасности определяется, исходя из состава материальных и информационных ценностей, а также специфических особенностей самого объекта. Если объект расположен в здании с прилегающей к нему территорией, то ограждение и периметральная охранная сигнализация образуют первую зону безопасности объекта. Последней зоной безопасности, например сейфовой комнаты, будет специальный сейф с кодовым запирающим устройством и сигнализационным средством, передающим информацию о попытках его вскрытия.
Очевидно, что для разработки "модели" нарушителя применительно к некоторому ОО необходимо обобщение большого опыта как отечественной, так и зарубежной практики построения систем охраны объектов, аналогичных рассматриваемому. С течением времени "модель" нарушителя, а следовательно, и вся концепция
охраны могут меняться. Отсюда следует вывод о необходимости периодического дополнения концепции охраны объекта, обновления системы инженерной защиты, системы охранной сигнализации, телевизионного наблюдения, системы контроля доступа и всех иных систем, рассматриваемых системной концепцией обеспечения безопасности.

Способы получения "нарушителем" информации об объекте и технических способах защиты объекта, вероятные пути проникновения. Целями "нарушителя" или "нарушителей", проникающих на объект, как отмечалось выше, могут быть: кража материальных и/или информационных ценностей, установка закладных устройств, разрушение объекта, захват заложников, а возможно и захват управления функционированием объекта. Злоумышленник будет искать наиболее оптимальные (менее опасные для себя) пути проникновения в нужное ему помещение для осуществления поставленной противозаконной (преступной) цели, будет стараться оставить как можно меньше следов своих действий, разрушений. С этой целью он будет изучать обстановку на объекте, алгоритм охраны, неохраняемые переходы, помещения, способы и условия хранения ценностей.

Применение систем охранной сигнализации с высокими тактико-техническими характеристиками на всех возможных путях движения "нарушителя" совместно с инженерной и физической защитой позволит достаточно надежно защитить объект на требуемом (заданном априори) уровне.

Таким образом, неоспорима важность принятия мер, максимально затрудняющих получение "нарушителем" сведений об основных характеристиках технических средств охраны, их принципе действия, режимах работы.

В то же время некамуфлируемость средств охранной сигнализации в местах скопления посетителей, распространение слухов об их сложности, уникальности и невозможности их "обойти" будет способствовать отпугиванию некоторых потенциальных "нарушителей".

Наиболее вероятными путями физического проникновения "нарушителя" в здание являются:

- через двери и окна первого этажа;
- по коммуникационным и техническим проемам подвала или цокольного этажа;
- с крыши через окна или другие проемы верхних этажей;
- путем разрушения ограждений (разбивание стекол, пролом дверей, решеток, стен, крыши, внутренних перегородок, пола и т.п.);
- имеются и иные способы, связанные с применением нарушителем специальных технических средств (все эти сведения легко почерпнуть из телефильмов, телепередач на криминальные темы, детективов и т.д.).

Необходимо максимально предусмотреть физические преграды перед нарушителем на пути его движения к материальным и информационным ценностям.

Внутренние переходы, подходы к наиболее важным помещениям должны быть оснащены не только средствами охранной сигнализации и телевизионного наблюдения, но и иметь надежную инженерную защиту в виде тамбуров с дистанционно управляемыми дверями, решетками, а сами хранилища ценностей - укрепленными перегородками.

Готовясь к преступлению, "нарушитель", используя легальную возможность посетить учреждение, ходит по некоторым его помещениям, может тщательно изучить наименее охраняемые места, расположение постов охраны, действия охранников при проходе сотрудников в различные режимные зоны. В этом случае очень важно разделять потоки клиентов учреждения от сотрудников. Проходы, помещения, где клиенты не обслуживаются, должны иметь кодовые замки или средства контроля доступа.

Некоторые подробности режима охраны преступник может получить, "разговорив" кого-либо из сотрудников учреждения или охраны.

Наибольшую опасность представляют сотрудники охраны, вступившие в преступную связь с "нарушителем". От них можно получить информацию и о принципах работы аппаратуры охранной сигнализации, ее режимах, "слабых" местах, оптимальных путях проникновения в требуемые помещения, а в решающий момент они могут отключить отдельные каналы охранной сигнализации. В связи с этим станционная аппаратура охранной сигнализации должна иметь систему документирования, должны протоколироваться дата и время включения/выключения каналов сигнализации, режимы

проверки неисправности аппаратуры с фиксацией даты и времени происшедшего сбоя, отключения на профилактику и т.д.

Информация о состоянии охраны на объекте, оптимальных путях движения к требуемому помещению и путях отхода нужна любому "нарушителю", как стремящемуся похитить какой-либо документ, установить подслушивающее устройство, так и "нарушителю", осуществляющему разбойное нападение или преследующего иные цели.

Исходя из анализа возможных "моделей" нарушителя, способов получения им информации, конкретной архитектуры здания, характеристик территории, прилегающих зданий, рельефа местности

и т.д., вырабатываются требования к инженерной защите, системе охранной сигнализации и размещению постов. Последнее означает, что для каждого конкретного объекта, здания, помещения должен разрабатываться конкретный проект его оснащения ТСОС-ТСН, СКД с учетом требований "Системной концепции...", дабы не допустить пробелов в системе защиты, которые раньше или позже но будут обнаружены грамотным злоумышленником.

Классификация нарушителей на основе моделей их действий (способов реализации угроз). Разработка моделей нарушителей осуществляется на основе исследования возможных видов угроз объекту и способов их реализации.

Угрозы могут носить общий или локальный характер и исходить:

- от людей (персонала, сторонних нарушителей или социальные, например: общественные беспорядки, забастовки и т.д.);
- от природных факторов (наводнение, засуха, землетрясение, снегопад, проливные дожди и т.д.);
- от нарушения систем жизнеобеспечения из-за техногенных факторов (отключение электропитания, пожар, утечка газов, радиоактивные осадки и т.д.), а также угрозы могут носить случайный характер.

При рассмотрении вопросов классификации нарушителей нас интересуют способы реализации угроз, исходящих от людей (злоумышленников).

Рассматривают три типа нарушителей - неподготовленный, подготовленный, квалифицированный и две группы способов реализации угроз (враждебных действий) - контактные, бесконтактные.

Способы проникновения на объект, в его здания и помещения могут быть самые различные (это описано во многих литературных источниках), например:

- разбитие окна, витрины, остекленной двери или других остекленных проемов;
- взлом (отжатие) двери, перепиливание (перекус) дужек замка и другие способы проникновения через дверь;
- пролом потолка, подлежащего блокировке;
- пролом капитального потолка, не подлежащего блокировке;
- пролом стены, подлежащей блокировке;
- пролом капитальной стены, не подлежащей блокировке;
- пролом (подкоп) капитального пола, не подлежащего блокировке;
- пролом (подкоп) пола, подлежащего блокировке;
- проникновение через разгрузочный люк;
- проникновение через вентиляционное отверстие, дымоход или другие строительные коммуникации;
- проникновение подбором ключей;
- оставление нарушителя на объекте до его закрытия;
- свободный доступ нарушителя на объект в связи с временным нарушением целостности здания из-за влияния природно-техногенных факторов или в период проведения ремонта.

проникновение через ограждение (забор, сетку, решетку), используя подкоп, перелаз, разрушение, прыжок с высоты и т.д.

Очевидно, что каждый тип нарушителей (неподготовленный, подготовленный,

квалифицированный) будет осуществлять проникновение на объект по разному - менее грамотно или более грамотно (ухищренно), используя различные условия, способствующие проникновению, как то:

- взрыв;
- пожар (поджог);
- разбойное нападение;
- наводнение;
- химическое заражение;
- общественные беспорядки;
- отключение электроэнергии на объекте, в районе, городе;
- постановка нарушителем помех ТСО на объекте;
- постановка нарушителем помех в канале связи объекта с охраной;
- предварительный вывод из строя ТСО на объекте;
- предварительный вывод из строя канала связи объекта с охраной;
- предварительный сговор нарушителя с персоналом объекта;
- предварительный сговор нарушителя с персоналом службы охраны объекта;
- создание и использование многих и многих других условий для проникновения на охраняемый объект, например: использование дрессированных животных и птиц, специальных технических средств обхода ТСО, специальных технических средств для предварительного изучения объекта и т.д.

Ряд моделей действий нарушителей достаточно широко представлены в художественной литературе, кинофильмах, в телепередачах с криминальными сюжетами, в научно-технических изданиях в открытой печати. Таким образом, потенциальному злоумышленнику вполне доступно повышение квалификации на материалах открытой печати, телепередач и кино. Этот неоспоримый факт, безусловно, должна в своей деятельности учитывать СБ(О) и соответственно строить тактику охраны учреждения. Очевидно, информация о тактике охраны (способах и методах противодействия любым из возможных действий злоумышленника) является строго конфиденциальной, секретной и совершенно секретной.

В зависимости от поставленных целей злоумышленник создает те или иные условия для проникновения на объект и в его помещения, пользуясь теми или иными контактными или бесконтактными способами проникновения.

К контактным способам совершения враждебных действий относятся:

1. Контактное проникновение на объект охраны (ОО): несанкционированное проникновение на территорию ОО;
- проход на основе маскировки (под сотрудника ОО, посетителя и т.п.);
- установка (занос на ОО) средств негласного слухового, визуального, электромагнитного и др. наблюдения.

2. Контактное нарушение целостности или характера функционирования объекта:
- нарушение линий жизнеобеспечения ОО;
- физическая ликвидация потенциала (ресурсов) ОО (взрыв, разрушение и др.);
- затруднение штатного режима функционирования объекта.

К бесконтактным способам совершения враждебных действий относятся:

1. Бесконтактные проникновения на объект охраны:
- перехват физических полей;
- контроль радио- и телефонных переговоров;
- визуальное и слуховое наблюдение;

2. Вывод объекта из строя без проникновения на него, как то:
- нарушение целостности объекта посредством использования направленного взрыва или дистанционного оружия;
- отключение линий жизнеобеспечения объекта.

Нарушителем считается лицо, нарушающее контрольно-пропускной режим, случайно

или преднамеренно нарушающее режим безопасности объекта охраны.
Для описания моделей нарушителей в качестве критериев классификации рассматриваются:
1. Цели и задачи вероятного нарушителя:
- проникновение на охраняемый объект без причинения объекту видимого ущерба (для решения задач разведки объекта, установки техники, закладки других устройств и т.п.);
- причинение ущерба объекту (при этом проникновение - только промежуточная задача действий вероятного нарушителя);
- освобождение спецконтингента (арестованных);
- преднамеренное проникновение при отсутствии враждебных намерений (любопытство, проникновение при решении посторонней задачи и др.);
- случайное проникновение.
2. Степень принадлежности вероятного нарушителя к объекту:
- вероятный нарушитель - сотрудник охраны;
- вероятный нарушитель - сотрудник учреждения;
- вероятный нарушитель - постороннее лицо.
3. Степень осведомленности вероятного нарушителя об объекте:
- детальное знание объекта;
- осведомленность о назначении объекта, его внешних признаках и чертах;
- неосведомленный вероятный нарушитель.
4. Степень осведомленности вероятного нарушителя о системе охраны объекта:
- полная информация о системе охраны объекта;
- информация о системе охраны вообще и о системе охраны конкретного объекта охраны;
- информация о системе охраны вообще, но не о системе охраны конкретного объекта;
- неосведомленный вероятный нарушитель.
5. Степень профессиональной подготовленности вероятного нарушителя:
- специальная подготовка по преодолению систем охраны;
- вероятный нарушитель не имеет специальной подготовки по преодолению систем охраны.
6. Степень физической подготовленности вероятного нарушителя:
- специальная физическая подготовка;
- низкая физическая подготовка.
7. Владение вероятным нарушителем способами маскировки:
- вероятный нарушитель владеет способами маскировки;
- вероятный нарушитель не владеет способами маскировки.
8. Степень технической оснащенности вероятного нарушителя:
- оснащен специальной техникой для преодоления системы охраны;
- оснащен стандартной техникой;
- не оснащен техническими приспособлениями.
9. Способ проникновения вероятного нарушителя на объект:
- использование негативных качеств личного состава охраны объекта;
- "обход" технических средств охраны;
- движение над поверхностью земли;
- движение по поверхности земли (в том числе подкоп).

На основе изложенных критериев можно выделить четыре категории нарушителя:
- нарушитель первой категории - специально подготовленный по широкой программе, имеющий достаточный опыт нарушитель- профессионал с враждебными намерениями, обладающий специальными знаниями и средствами для преодоления различных систем защиты объекта (организованный нарушитель);
- нарушитель второй категории - непрофессиональный нарушитель с враждебными

намерениями, действующий под руководством другого субъекта, имеющий определенную подготовку для проникновения на конкретный объект (подготовленный нарушитель);
- нарушитель третьей категории - нарушитель без враждебных намерений, совершающий нарушение безопасности объекта из любопытства или из каких-то иных личных намерений;
- нарушитель четвертой категории - нарушитель без враждебных намерений, случайно нарушающий безопасность объекта.

В принципе под моделью нарушителя понимается совокупность количественных (вес, скорость перемещения, рост и т.п.) и качественных (цели и способы действия, степень осведомленности и подготовленности и т.п.) характеристик нарушителя, с учетом которых определяются требования к комплексу инженерно-технических средств охраны (КИТСО) и/ или его составным частям.

Существуют определенные методики количественной оценки вероятностей обнаружения нарушителя, пытающегося проникнуть на объект охраны. Здесь учитываются гамма параметров, характеризующих категорию важности объекта, конфигурацию, архитектуру и тактико-технические характеристики применяемых в КТСО ТСОС, ТСН, СКД, а также количественных и качественных характеристик нарушителя и возможных моделей его действия.

Вопросы классификации угроз информационной безопасности. В системе обеспечения безопасности объектов одно из ведущих мест занимает обеспечение информационной безопасности. Действительно, любой (не случайный) потенциальный нарушитель до проникновения на объект и проведения преступных действий проводит в зависимости от поставленных им конечных целей более или менее глубокую разведку с тем, чтобы обезопасить себя и выполнить поставленную преступную задачу. Поэтому защита от посторонних лиц жизненно важной информации об объекте (количество и виды ресурсов, планы, уникальные технологии, места расположения жизненно важных центров обеспечения деятельности, например серверов баз данных, конструкторско-технологической документации и т.д.), а также информации о системе обеспечения охранной деятельности (структура, состав и режимы работы служб безопасности; структура, состав и принципы действия ТСО, СКД и т.д.; схемы размещения и принципы действия специальных технических средств обнаружения каналов утечки информации, обнаружения ДТС и т.д.) является наиболее приоритетной задачей, от успешного решения которой зависит уровень эффективности защиты объекта в целом.

Проблемы защиты информации решаются в каждом из блоков задач, рассматриваемых системной концепцией обеспечения комплексной безопасности объекта, и в каждом блоке эти проблемы решаются своими способами и методами, хотя имеются и некоторые общие особенности.

В каждом случае работа СБ(О) начинается с моделирования потенциальных угроз безопасности информации, их классификации и выбора (разработки) адекватных угрозам мер информационной защиты.

Рассмотрим для примера вопросы классификации угроз при решении проблем обеспечения безопасности автоматизированных систем обработки информации (АСОИ), т.е. ПЭВМ, ЛВС, серверов баз данных и т.д. и их информационного и программного обеспечения.

В большинстве случаев (например, в банковской деятельности около 80%) нарушения по НСД к АСОИ исходят от самих сотрудников учреждений. Потери в денежном выражении составляют от них около 70%, остальные потери приходятся на хакеров, террористов и т.п.

Можно выделить три основные причины внутренних нарушений: безответственность, самоутверждение и корыстный интерес пользователей (персонала) АСОИ [49]. Кроме того ущерб могут нанести и другие нарушители извне.

Есть опасность нанесения ущерба и не по злому умыслу, когда сотрудник учреждения,

имеющий доступ к базам данных ЛВС или ПЭВМ обладает малой квалификацией, невнимателен, недисциплинирован, неряшлив в соблюдении технологии обработки информации или в пользовании программными продуктами, либо просто утомлен, омрачен какими-то личными переживаниями, что также приводит к невнимательности. При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности. Предусмотреть все такие ситуации маловероятно. Более того, во многих случаях система в принципе не может предотвратить подобные нарушения (например, случайное уничтожение своего собственного набора данных). Иногда ошибки поддержки адекватной защищенной среды могут поощрять такого рода нарушения. Система защиты может быть также неправильно настроена. Эти категории "нарушителей" в излагаемой книге специально не рассматриваются.

О самоутверждении. Некоторые пользователи считают получение доступа к системным наборам данных крупным успехом, ведя своего рода игру "пользователь - против системы" ради самоутверждения либо в собственных глазах, либо в глазах коллег. Хотя при этом намерения могут быть и безвредными, эксплуатация ресурсов АСОИ считается нарушением политики безопасности. Пользователи с "более криминальными намерениями" могут найти конфиденциальные данные, попытаться испортить или уничтожить их. Такой вид нарушений называется зондированием системы. Большинство систем имеет ряд средств противодействия подобным "шалостям".

Нарушение безопасности АСОИ может быть вызвано и корыстным "злоумышленником". Под "злоумышленником" понимается человек (извне или сотрудник), обладающий достаточными знаниями в вопросах автоматизированной обработки информации, преследующий цели сознательного воздействия, направленного на кражу секретной информации о деятельности учреждения, его планах, процедурах проведения операций, организации системы охраны и т.д., т.е. той информации, которая позволит злоумышленнику в конце концов осуществить кражу средств, материальных или финансовых, или дезорганизовать деятельность учреждения. В этом случае он целенаправленно пытается преодолеть систему защиты от несанкционированного доступа к хранимой, передаваемой и обрабатываемой в АСОИ информации. Полностью защититься от таких проникновений практически невозможно. В какой-то мере утешает лишь то, что опаснейшие нарушения встречаются крайне редко, ибо требуют необычайного мастерства и упорства от злоумышленника, и его злонамеренное действие при грамотно организованной системе контроля может быть обнаружено, т.е. вероятность проведения таких акций против АСОИ может быть существенно снижена.

Приведем некоторые данные о количестве и объеме угроз для безопасности со стороны корыстных злоумышленников.

Итальянские психологи утверждают, что из всех служащих любой фирмы 25% - это честные люди, 25% - ожидают удобного случая для разглашения секретов и 50% будут действовать в зависимости от обстоятельств [141].

В 1994 г. трое репортеров лондонской газеты "Санди Тайме" провели эксперимент. Представляясь бизнесменами, они вышли на двадцать депутатов британского парламента с предложением направить в правительство запрос, в котором они заинтересованы, и получить за это наличными или чеком тысячу фунтов стерлингов. Из двадцати 17 сразу отказались, трое согласились. Аналогичные эксперименты проводила ФБР в начале 80-х гг.: агенты ФБР под видом арабских шейхов обращались к членам американского конгресса, предлагая им вознаграждение в десятки тысяч долларов за то, чтобы "шейхам" были устроены всякие поблажки [183].

Если эти закономерности перенести, например, на банковских служащих, то более чем от 10% вероятных злоумышленников ожидать неприятностей, связанных с продажей секретной информации.

Очевидно, ущерб от каждого вида нарушений зависит от частоты их появления и ценности информации. Чаще всего встречаются нарушения, вызванные халатностью и безответственностью, но ущерб от них обычно незначителен и легко восполняется. Например, во многих системах существуют средства, позволяющие восстанавливать случайно уничтоженные наборы данных при условии, что ошибка сразу же обнаружена. Регулярное архивирование рабочих файлов данных, имеющих важное значение, позволяет существенно уменьшить ущерб от их потери.

Ущерб от зондирования системы может быть гораздо больше, но и вероятность его во много раз ниже, ибо для таких действий необходимы достаточно высокая квалификация, отличное знание системы защиты и определенные психологические особенности. Наиболее характерным результатом зондирования системы является блокировка: пользователь вводит АСОИ в состояние неразрешимого противоречия (например, ввести задачу - софизм или вирус), после чего операторы и системные программисты тратят много времени для восстановления работоспособности системы. К примеру, в скандальной истории с вирусом Морриса в сети Internet, бывшей результатом зондирования системы, ущерб исчислялся миллионами долларов.

Отличительной чертой проникновений, наиболее редких, но и наиболее опасных нарушений, обычно является определенная цель: доступ (чтение, модификация, уничтожение) к определенной информации, влияние на работоспособность системы, слежение за действиями других пользователей и др. Для осуществления подобных действий нарушитель должен обладать теми же качествами, что и для зондирования системы, только в усиленном варианте, а также иметь точно сформулированную цель. Ущерб от проникновений может оказаться в принципе невосполнимым. Например, для банков это может быть полная или частичная модификация счетов с уничтожением журнала транзакций (полностью законченная операция с деньгами), т.е. если с какого-то счета сняты деньги, то они должны быть записаны в другом счете (не теряться и не быть излишками).

Причины, побуждающие пользователя совершать нарушения или даже преступления, различны. Наиболее серьезный ущерб системе угрожает в случае умышленного воздействия из-за обиды, неудовлетворенности своим служебным и/или материальным положением, или по указанию других лиц, под угрозой шантажа. Шантаж, как одно из средств нелегального доступа к ценной информации, используется преступными организациями, проводящими для этого специальные мероприятия по дискредитации ответственных работников учреждения. Ущерб при этом тем больше, чем выше положение пользователя в служебной иерархии.

Способы предотвращения ущерба в этом случае вытекают из природы причин (побудительных мотивов) нарушений и преступлений. Это - соответствующая подготовка пользователей, поддержание здорового рабочего климата в коллективе, подбор персонала, своевременное обнаружение потенциальных злоумышленников и принятие соответствующих мер. Ясно, что это не только задачи администрации и детективной группы, но и коллектива в целом. Сочетание этих мер способно предотвратить сами причины нарушений и преступлений.

Таким образом, наиболее уязвимым с позиции обеспечения безопасности может стать "человеческий фактор", т.е. недисциплинированность сотрудников, недостаточный профессионализм, возможность подкупа, шантажа, угроз насилия, обиды по поводу неадекватной оценки труда и многое другое. Более детальное описание методов противодействия такого рода угрозам изложены, например, в [27]. Отметим лишь, что коль скоро такие угрозы существуют, следует рекомендовать проведение соответствующих специальных исследований детективной группой, отделом кадров и администрацией с привлечением профессиональных психологов, психоаналитиков, кадагогов, а также использование технических средств (например, многофункциональных детекторов лжи).

Очевидно, что для выбора оптимального варианта нейтрализации действий злоумышленника из известных методов, способов и средств противодействия нужно знать (либо предполагать), что собой представляют (либо могут представлять) возможные нарушения и злоумышленник, т.е. нужны модели нарушений, "модель" нарушителя или "модель" его возможных действий. Исследование моделей нарушителей является отправной идеей в разработке стратегии и тактики обеспечения безопасности АСОИ. В самом деле, для выбора средств защиты нужно ясно представлять, от кого защищать АСОИ.

Например, возможен такой подход: на основе доступности компонентов программного и информационного обеспечения в табл. 1.1 представлены типы угроз и лица, которые могли бы вызвать такие угрозы.

При создании модели нарушителя и оценке риска потерь от действий персонала (необходимых этапов выработки политики безопасности) дифференцируют всех сотрудников по их возможностям доступа к системе и, следовательно, по потенциальному ущербу от каждой категории пользователей. Например, оператор или программист автоматизированной банковской системы может нанести несравненно больший ущерб, чем обычный пользователь, тем более непрофессионал.

Таблица 1.1. **Типы угроз и возможных нарушителей**

Тип угрозы	Нарушитель				
	Оператор	Сотрудник из управления	Программист	Инженер по техническому обслуживанию	Пользователь
Изменение кодов	+		+		
Копирование файлов	+		+		
Уничтожение файлов	+	+	+		+
Присвоение программ			+		
Шпионаж	+	+	+	+	
Установка подслушивания			+	+	
Саботаж	+		+		
Продажа данных	+	+	+		+
Воровство			+	+	+

Приведем примерный список персонала типичной АСОИ и соответствующую степень риска от каждого из них [46; 49]:

1. Наибольший риск:
- системный контролер;
- администратор безопасности.
2. Повышенный риск:
- оператор системы;
- оператор ввода и подготовки данных;
- менеджер обработки;
- системный программист.
3. Средний риск:
- инженер системы;
- менеджер программного обеспечения.
4. Ограниченный риск:
- прикладной программист;

- инженер или оператор по связи;
- администратор баз данных;
- инженер по оборудованию;
- оператор периферийного оборудования;
- библиотекарь системных магнитных носителей;
- пользователь-программист;
- пользователь-операционист.

5. Низкий риск:

- инженер по периферийному оборудованию;
- библиотекарь магнитных носителей пользователей.

Итак, при проектировании системы защиты АСОИ следует уделять внимание не только возможным объектам нарушений, но и вероятным нарушителям как личностям. Многолетний опыт функционирования тысяч АСОИ свидетельствует, что совершаемые без причины, а в силу случайных обстоятельств преступления очень редки.

На основе изложенных пояснений сути рассматриваемой проблемы моделирования угроз, нарушителей и их действий можно предложить следующий подход к классификации угроз безопасности АСОИ.

Отметим, что попытки дать исчерпывающую классификацию угроз безопасности АСОИ предпринимались неоднократно, однако список их постоянно расширяется, и потому в данном учебном пособии выделим лишь основные их типы.

Проводимая ниже классификация охватывает только умышленные угрозы безопасности АСОИ, оставляя в стороне такие воздействия как стихийные бедствия, сбои и отказы оборудования и др. Реализацию угрозы принято называть атакой.

Угрозы безопасности можно классифицировать по следующим признакам (выделим 9 групп) [27]:

1. **По цели реализации угрозы.** Атака может преследовать следующие цели:

- нарушение конфиденциальности информации;
- нарушение целостности информации (ущерб от уничтожения или несанкционированной модификации информации может быть много больше, чем при нарушении конфиденциальности);
- нарушение (полное или частичное) работоспособности АСОИ (нарушение доступности). Такие нарушения могут повлечь за собой неверные результаты, отказы от обработки потока информации или отказы при обслуживании.

2. **По принципу воздействия на АСОИ:**

- с использованием доступа субъекта системы (пользователя, процесса) к объекту (файлу данных, каналу связи и т.д.);
- с использованием скрытых каналов.

Субъектом доступа называется лицо или процесс, действия которого регламентируются правилами разграничения доступа, а объектом доступа - единица информационного ресурса АСОИ, доступ к которой регламентируется правилами разграничения доступа.

Под доступом понимается взаимодействие между субъектом и объектом (выполнение первым некоторой операции над вторым), приводящее к возникновению информационного потока от второго к первому.

Под скрытым каналом понимается путь передачи информации, позволяющий двум взаимосвязанным процессам обмениваться информацией таким способом, который нарушает системную политику безопасности (способ управления доступом). Скрытые каналы бывают двух видов:

- скрытые каналы с памятью, позволяющие осуществлять чтение или запись информации другого процесса непосредственно или с помощью промежуточных объектов для хранения информации (временной памяти);
- скрытые временные каналы, при которых один процесс может получать информацию о действиях другого, используя интервалы между какими-либо событиями (например,

анализ временного интервала между запросом на ввод-вывод и сообщением об окончании операции, что позволяет судить о размере вводимой или выводимой информации).

3. **По характеру воздействия на АСОИ.** Различают активное и пассивное воздействие. Первое всегда связано с выполнением пользователем каких-либо действий, выходящих за рамки его обязанностей и нарушающих существующую политику безопасности. Это может быть доступ к наборам данных, программам, вскрытие пароля и т.д.

Пассивное воздействие осуществляется путем наблюдения пользователем каких-либо побочных эффектов (от работы программы, например) и их анализа. Пример - прослушивание линии связи между двумя узлами сети. Пассивное воздействие всегда связано только с нарушением конфиденциальности информации в АСОИ, так как при нем никаких действий с объектами и субъектами не производится.

4. **По факту наличия возможной для использования ошибки защиты.** Реализация любой угрозы возможна только в том случае, если в данной конкретной системе есть какая-либо ошибка или брешь защиты.

Такая ошибка может быть обусловлена одной из следующих причин:

- неадекватностью (несоответствием) политики безопасности реальной АСОИ. В той или иной степени несоответствия такого рода имеют все системы, но в одних случаях это может привести к нарушениям, а в других - нет. Если выявлена опасность такого несоответствия, необходимо усовершенствовать политику безопасности, изменив соответственно средства защиты;
- ошибками административного управления, под которыми понимают некорректную реализацию или поддержку принятой политики безопасности в данной АСОИ. Пусть, например, согласно политике безопасности в АСОИ должен быть запрещен доступ пользователей к некоторому определенному набору данных, а на самом деле (по невнимательности администратора безопасности) этот набор данных доступен всем пользователям. Обнаружение и исправление такой ошибки требуют обычно небольшого времени, тогда как ущерб от нее может быть огромен;

ошибками в алгоритмах программ, в связях между ними и т.д., которые возникают на этапе проектирования программ или комплекса программ и из-за которых эти программы могут быть использованы совсем не так, как описано в документации. Такие ошибки могут быть очень опасны, к тому же их трудно найти, а для устранения надо менять программу или комплекс программ;

- ошибками реализации алгоритмов программ (ошибки кодирования), связей между ними и т.д., которые возникают на этапах реализации, отладки и могут служить источником недокументированных свойств.

5. **По способу воздействия на объект атаки (при активном воздействии):**

- непосредственное воздействие на объект атаки (в том числе с использованием привилегий), например, непосредственный доступ к набору данных, программе, службе, каналу связи и т.д., воспользовавшись какой-либо ошибкой. Такие действия обычно легко предотвратить с помощью средств контроля доступа;
- воздействие на систему разрешений (в том числе захват привилегий). При этом несанкционированные действия выполняются относительно прав пользователей на объект атаки, а сам доступ к объекту осуществляется потом законным образом;
- опосредованное воздействие (через других пользователей):
- "маскарад". В этом случае пользователь присваивает себе каким-либо образом полномочия другого пользователя, выдавая себя за него;
- "использование вслепую". При таком способе один пользователь заставляет другого выполнить необходимые действия (для системы защиты они не выглядят несанкционированными, ибо их выполняет пользователь, имеющий на это право), причем последний о нем может и не подозревать. Для реализации этой угрозы может использоваться троян (программа выполняет необходимые действия и сообщает о их результате тому, кто его внедрил).

Два последних способа очень опасны. Для предотвращения подобных действий требуется постоянный контроль как со стороны администраторов и операторов за работой АСОИ в целом, так и со стороны пользователей за своими собственными наборами данных.

6. **По способу воздействия на АСОИ:**

- в интерактивном режиме;
- в пакетном режиме.

Работая с системой, пользователь всегда имеет дело с какой-либо ее программой. Одни программы составлены так, что пользователь может оперативно воздействовать на ход их выполнения, вводя различные команды или данные, а другие так, что всю информацию приходится задавать заранее. К первым относятся, например, некоторые утилиты, управляющие программы баз данных, в основном - это программы, ориентированные на работу с пользователем. Ко вторым относятся в основном системные и прикладные программы, ориентированные на выполнение каких-либо строго определенных действий без участия пользователя.

При использовании программ первого класса воздействие оказывается более длительным по времени и, следовательно, имеет более высокую вероятность обнаружения, но более гибким, позволяющим оперативно менять порядок действий. Воздействие с помощью программ второго класса (например, с помощью вирусов) является кратковременным, трудно диагностируемым, гораздо более опасным, но требует большой предварительной подготовки для того, чтобы заранее предусмотреть все возможные последствия вмешательства.

7. **По объекту атаки.** Объект атаки - это тот компонент АСОИ, который подвергается воздействию со стороны злоумышленника. Воздействию могут подвергаться следующие компоненты АСОИ:

- АСОИ в целом: злоумышленник пытается проникнуть в систему для последующего выполнения каких-либо несанкционированных действий. Используют обычно "маскарад", перехват или подделку пароля, взлом или доступ к АСОИ через сеть;

объекты АСОИ - данные или программы в оперативной памяти или на внешних носителях, сами устройства системы, как внешние (дисководы, сетевые устройства, терминалы), так и внутренние (оперативная память, процессор), каналы передачи данных. Воздействие на объекты системы обычно имеет целью доступ к их содержимому (нарушение конфиденциальности или целостности обрабатываемой или хранимой информации) или нарушение их функциональности (например, заполнение всей оперативной памяти компьютера бессмысленной информацией или загрузка процессора компьютера задачей с неограниченным временем исполнения (нарушение доступности АСОИ);

- субъекты АСОИ - процессы и подпроцессы пользователей. Целью таких атак является либо прямое воздействие на работу процессора - его приостановка, изменение характеристик (например, приоритета), либо обратное воздействие - использование злоумышленником привилегий, характеристик другого процесса в своих целях. Воздействие может оказываться на процессы пользователей, системы, сети;
- каналы передачи данных. Воздействие на пакеты данных, передаваемые по каналу связи, может рассматриваться как атака на объекты сети, а воздействие на сами каналы - как специфический род атак, характерный для сети. К последним относятся: прослушивание канала и анализ графика (потока сообщений); подмена или модификация сообщений в каналах связи и на узлах- ретрансляторах; изменение топологии и характеристик сети, правил коммутации и адресации.

8. **По используемым средствам атаки.** Для воздействия на систему злоумышленник может использовать стандартное программное обеспечение или специально разработанные программы. В первом случае результаты воздействия обычно предсказуемы, так как большинство стандартных программ АСОИ хорошо изучены. Использование специально разработанных программ связано с большими трудностями, но

может быть более опасным, поэтому в защищенных системах рекомендуется не допускать добавления программ в АСОИ без разрешения администратора безопасности системы.

9. **По состоянию объекта атаки.** Состояние объекта в момент атаки весьма существенно для результатов атаки и содержания работы по ликвидации ее последствий. Объект атаки может находиться в одном из трех состояний:

- хранения на диске, магнитной ленте, в оперативной памяти или в любом другом месте в пассивном состоянии. При этом воздействие на объект обычно осуществляется с использованием доступа;
- передачи по линии связи между узлами сети или внутри узла, Воздействие предполагает либо доступ к фрагментам передаваемой информации (например, перехват пакетов на ретрансляторе сети), либо просто прослушивание с использованием скрытых каналов;
- обработки в тех ситуациях, когда объектом атаки является процесс пользователя.

Приведенная классификация показывает сложность определения возможных угроз и способов их реализации.

Более подробно распространенные угрозы безопасности АСОИ рассмотрены, например, в [18].

В связи с тем, что универсального способа защиты, который мог бы предотвратить любую угрозу, не существует, для обеспечения безопасности АСОИ в целом создают защитную систему, объединяя в ней различные меры защиты.

Изложенный далеко не полно пример решения проблемы классификации угроз информационной безопасности АСОИ убеждает в необходимости проведения глубоких исследований при решении аналогичных проблем в контуре всех иных блоков задач "Системной концепции..." [100].

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению самостоятельной работы по дисциплине «**Гуманитарные проблемы обеспечения информационной безопасности**»
для студентов направления подготовки 10.03.01 Информационная безопасность

направленность (профиль) Безопасность компьютерных систем

Пятигорск, 2022

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

– формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

– написание докладов;

– подготовка к семинарам, практическим и лабораторным работам, их оформление;

– составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);

– выполнение учебно-исследовательских работ, проектная деятельность;

– подготовка практических разработок и рекомендаций по решению проблемной ситуации;

– выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;

– компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;

– выполнение курсовых работ (проектов) в рамках дисциплин;

– выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

● подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);

● основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);

● заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Гуманитарные проблемы обеспечения компьютерной безопасности» направлена на формирование следующих **компетенций**:

Код	Формулировка:
ОПК-2	Способен применять роль информации, информационных технологий и информационной безопасности в современной обществе, их значения для обеспечения объективных потребностей и личности, общества и

	государства
ПК-3	Способность администрировать подсистемы информационной безопасности объекта защиты

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и специальных компетенций будущего бакалавра по соответствующему направлению подготовки

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе (астр.)		
			СРС	Контактная работа с преподавателем	Всего
3 семестр					
ОПК-1,ПК-3	Самостоятельное изучение литературы	Собеседование	37,17	4,13	41,3
ОПК-1,ПК-3	Подготовка к практическим	Опрос	2,43	0,27	2,7

	занятиям				
ОПК-1,ПК-3	Написание реферата/доклада	Доклад	9	1	10
Итого за 3 семестр			**48,6**	**5,4**	**54**

4. Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить сведения, излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;

2. Выделите главное, составьте план;

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;

4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим и лабораторным занятиям

Для того чтобы практические и лабораторные занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на практических занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных задач и примеров. При этом студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала - умение решать задачи или пройти тестирование по пройденному материалу. Однако следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

4.4. Методические рекомендации по написанию научных текстов (докладов, докладовов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного). Во-вторых, научиться организовывать свое время, ведь, как известно, свободное (от всяких глупостей) время – важнейшее условие настоящего творчества, для него наконец-то появляется время. Иногда именно на организацию такого времени уходит немалая часть сил и талантов.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст. Каждый раз надо представлять, что ваш текст будет кто-то читать и ему захочется сориентироваться в нем, быстро находить ответы на интересующие вопросы (заодно представьте себя на месте такого человека). Понятно, что работа, написанная «сплошным текстом» (без заголовков, без выделения крупным шрифтом, наиболее важных мест и т. п.), у культурного читателя должна вызывать брезгливость (для любого автора (исключения составляют некоторые древние тексты, когда и жанр был иной и к текстам относились иначе, да и самих текстов было

гораздо меньше – не то, что в эпоху «информационного взрыва» и соответствующего «информационного мусора»).

Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Доклад - это самостоятельное исследование студентом определенной проблемы, комплекса взаимосвязанных вопросов.

Доклад не должна составляться из фрагментов статей, монографий, пособий. Кроме простого изложения фактов и цитат, в доклад е должно проявляться авторское видение проблемы и ее решения.

Рассмотрим основные этапы подготовки студентом.

Выполнение доклада начинается с выбора темы.

Затем студент приходит на первую консультацию к руководителю, которая предусматривает:

- обсуждение цели и задач работы, основных моментов избранной темы;
- консультирование по вопросам подбора литературы;
- составление предварительного плана.

Следующим этапом является работа с литературой. Необходимая литература подбирается студентом самостоятельно.

После подбора литературы целесообразно сделать рабочий вариант плана работы. В нем нужно выделить основные вопросы темы и параграфы, раскрывающие их содержание.

Составленный список литературы и предварительный вариант плана уточняются, согласуются на очередной консультации с руководителем.

Затем начинается следующий этап работы - изучение литературы. Только внимательно читая и конспектируя литературу, можно разобраться в основных вопросах темы и подготовиться к самостоятельному (авторскому) изложению содержания доклада. Конспектируя первоисточники, необходимо отразить основную идею автора и его позицию по исследуемому вопросу, выявить проблемы и наметить задачи для дальнейшего изучения данных проблем.

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление. После доработки доклад сдается на кафедру для его оценивания руководителем.

Требования к написанию доклада

Написание 1 доклада является обязательным условием выполнения плана СРС по любой дисциплине профессионального цикла.

Тема доклада может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Доклад должен быть написан научным языком.

Объем доклада должен составлять 20-25 стр.

Структура доклада:

● Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.

● Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету исследования, в которой дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению.

Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.

● Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса

● Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.

● Приложение (при необходимости).

Требования к оформлению:

● текст с одной стороны листа;
● шрифт Times New Roman;
● кегль шрифта 14;
● межстрочное расстояние 1,5;
● поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;
● доклад должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

Защита доклада проводится на практических занятиях, после окончания работы студента над ним и исправления всех недочетов, выявленных преподавателем в ходе консультаций. На защиту доклада отводится 5-7 минут времени, в ходе которого студент должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Оценка доклада

Доклад оценивается по следующим критериям:

• соблюдение требований к его оформлению;

• необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации;

• умение студента свободно излагать основные идеи, отраженные в докладе;

• способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности и ошибки при защите доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него

не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.5. Методические рекомендации по выполнению исследовательских проектов

Исследовательская проектная работа – это групповая работа, для выполнения которой необходим выбор и приложение научной методики к поставленной задаче, получение собственного теоретического или экспериментального материала, на основании которого необходимо провести анализ и сделать выводы об исследуемом явлении. Выполнение проекта – это всегда коллективная, творческая практическая работа, предназначенная для получения определенного продукта или научно-технического результата. Такая работа подразумевает четкое, однозначное формирование поставленной задачи, определение сроков выполнения намеченного, определение требований к разрабатываемому объекту.

Выполнение 1 группового проекта является обязательным условием выполнения самостоятельной работы по любой дисциплине профессионального цикла. Тема проектного задания может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Требования по выполнению и оформлению проекта

При выполнении проекта приветствуется работа в группе (2-3 человека). Проект – это исследовательская работа, в ходе которой студенты должны продемонстрировать владение навыками научного исследования, умения проводить анализ, обобщать информацию, делать выводы, предлагать свои решения проблемы, рассматриваемой в проекте.

При подготовке материалов проекта студенты должны продемонстрировать владение современными методами компьютерной обработки данных.

Критерии оценки работы участника проекта.

Для каждого из участников проекта оцениваются:

• профессиональные теоретические знания в соответствующей области;

• умение работать со справочной и научной литературой, осуществлять поиск необходимой информации в Интернет;

• умение работать с техническими средствами;

• умение пользоваться соответствующими выполняемому проекту информационными технологиями;

• умение готовить материалы проекта для презентации: составлять и редактировать тексты, формировать презентацию проекта;

• умение работать в команде;

• умение грамотно представлять результаты собственной деятельности;

• коммуникабельность, инициативность, творческие способности.

Критерии выставления оценки участникам проекта

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
«Отлично»	Работа выполнена на высоком профессиональном уровне. Представленный материал в основном фактически верен, допускаются негрубые фактические неточности. Студент свободно отвечает на вопросы, связанные с проектом.	Технические средства и информационные технологии освоены и использованы для реализации проекта полностью	Студент проявил инициативу, творческий подход, способность к выполнению сложных заданий, навыки работы в коллективе, организационные способности.	Проект представлен полностью и в срок.
«Хорошо»	Работа выполнена на достаточно высоком профессиональном уровне. Допущено до 4–5 фактических ошибок. Студент отвечает на вопросы, связанные с проектом, но недостаточно полно.	Обнаруживаются некоторые ошибки в использовании соответствующих технических средств и информационных технологий	Студент достаточно полно, но без инициативы и творческих находок выполнил возложенные на него задачи.	Проект представлен достаточно полно и в срок, но с некоторыми недоработками.
«Удовлетворительно»	Уровень недостаточно высок. Допущено до 8 фактических ошибок. Студент может ответить лишь на некоторые из заданных вопросов, связанных с проектом.	Обнаруживает недостаточное владение навыками работы с техническими средствами и соответствующими и информационными технологиями	Студент выполнил большую часть возложенной на него работы.	Проект сдан со значительным опозданием (более недели) и не полностью
«Неудовлетворительно»	Работа не выполнена или выполнена на низком уровне. Допущено более 8 фактических ошибок. Ответы на вопросы, связанные с	Навыков работы с техническими средствами нет, информационные технологии не освоены	Студент практически не работал, не выполнил свои задачи или выполнил лишь отдельные не	Проект не сдан.

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
	проектом вопросы обнаруживают непонимание предмета и отсутствие ориентации в материале проекта.		существенные поручения в групповом проекте.	

Студенты должны: защитить проект в режиме презентации, предъявить файлы выполненного проекта, уметь рассказать о технологиях, использованных ими при выполнении проекта, дать оценку работы каждого члена группы (*если проект групповой*).

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.6. Методические рекомендации по подготовке к экзаменам и зачетам

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Экзаменационная сессия - это серия экзаменов, установленных учебным планом. Между экзаменами интервал 3-4 дня. Не следует думать, что 3-4 дня достаточно для успешной подготовки к экзаменам.

В период подготовки к экзаменам студенты систематизировать уже имеющиеся знания. На консультации перед экзаменом студентов познакомят с основными требованиями, ответят на возникшие у них вопросы. Поэтому посещение консультаций обязательно.

Требования к организации подготовки к экзаменам те же, что и при занятиях в течение семестра, но соблюдаться они должны более строго. Во-первых, очень важно соблюдение режима дня; сон не менее 8 часов в сутки, занятия заканчиваются не позднее, чем за 2-3 часа до сна. Оптимальное время занятий - утренние и дневные часы. В перерывах между занятиями рекомендуются прогулки на свежем воздухе, неутомительные занятия спортом. Во-вторых, наличие хороших собственных конспектов лекций. Даже в том случае, если была пропущена какая-либо лекция, необходимо во время ее восстановить (переписать ее на кафедре), обдумать, снять возникшие вопросы для того, чтобы запоминание материала было осознанным. В-третьих, при подготовке к экзаменам у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра. Здесь можно эффективно использовать листы опорных сигналов.

Вначале следует просмотреть весь материал по сдаваемой дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения, используя при этом листы опорных сигналов.

Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка доклада, оценка презентации, оценка участия в круглом столе, оценка выполнения проекта.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Основная литература:

1. Современные информационные технологии Электронный ресурс : учебное пособие / С.С. Мытько / Д.А. Репечко / И.А. Королькова / А.Р. Ванютин / А.П. Алексеев ; ред. А.П. Алексеев. - Самара : Поволжский государственный университет телекоммуникаций и информатики, 2016. - 101 c. - Книга находится в базовой версии ЭБС IPRbooks., экземпляров неограниченно

2. Адлер, Ю.П. Статистическое управление процессами. «Большие данные» Электронный ресурс : учебное пособие / Е.А. Черных / Ю.П. Адлер. - Статистическое управление процессами. «Большие данные»,2021-09-01. - Москва : Издательский Дом МИСиС, 2016. - 52 c. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-87623-969-3, экземпляров неограниченно

Дополнительная литература:

1. Современные информационные технологии Электронный ресурс : Сборник трудов по материалам 3-й межвузовской научно-технической конференции с международным участием 29 сентября 2017 г. / В. И. Воловач [и др.] ; ред. В. М. Артюшенко. - Королёв : Научный консультант, МГОТУ, 2017. - 191 c. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-9500999-7-7, экземпляров неограниченно

2. Современные мультимедийные информационные технологии Электронный ресурс : учебное пособие / С.С. Мытько / Д.А. Репечко / А.П. Алексеев / А.Р. Ванютин / И.А. Королькова. - Современные мультимедийные информационные технологии,2021-05-

25. - Москва : СОЛОН-ПРЕСС, 2017. - 108 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-91359-219-4, экземпляров неограниченно

Методическая литература:

1. Методические рекомендации для самостоятельной работы студентов по дисциплине «Гуманитарные проблемы обеспечения компьютерной безопасности»
2. Методические указания к практическим работам по дисциплине «Гуманитарные проблемы обеспечения компьютерной безопасности»

Интернет-ресурсы:

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Гуманитарные проблемы обеспечения компьютерной безопасности»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.