ЛЕКЦИЯ
Тема 11 : «Организация охраны объекта»

Вопросы:

1. Категории объектов охраны. Требования к технической укрепленности объектов.
2. Модель нарушителя. Пути и способы его проникновения на охраняемый объект
3. Характеристика основных способов защиты объектов.
4. Система сбора и обработки информации

Вопрос 1. Категории объектов охраны. Требования к технической укрепленности объектов

Безопасность объектов – это комплекс организационных, оперативных, режимных, инженерно-технических, пожарно-профилактических мероприятий и действий физических лиц, направленных на предотвращение ущерба интересам организации и его персоналу в результате хищения материально-технических и финансовых средств, уничтожения имущества и ценностей, разглашения, утраты, утечки и уничтожения информации, нарушения работы технических средств, обеспечивающих деятельность организации.

Главной **целью** любой системы безопасности является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности.

Задачи:

- категорирование объектов организации;
- прогнозирование и своевременное выявление угроз безопасности;
- разработка концепции безопасности организации;
- создание условий, обеспечивающих предупреждение и ликвидацию угроз безопасности объекту;
- создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций;
- создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц.

Система охраны объекта - это сложный, многорубежный комплекс, включающий в себя физическую защиту, инженерные сооружения, технические средства охранной сигнализации, системы телевизионного наблюдения, системы контроля доступа и многое другое.

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.

Выбор уровня оснащения комплекса технических средств охраны 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.

Вопрос 2. **Модель нарушителя. Пути и способы его проникновения на охраняемый объект**

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.

В основе эффективного противодействия угрозе проникновения нарушителя в охраняемые помещения лежит проведение оценок:

- приоритетов в системе защиты;
- путей возможного проникновения нарушителей;
- информации, которой может располагать нарушитель об организации системы защиты организации;
- технических возможностей нарушителя.

Нарушители

По уровню подготовки и 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 технических средств охраны и прошедшие соответствующую подготовку;
- обладающие специальной подготовкой и оснащенные специальными средствами обхода;
- сотрудники учреждения.

Варианты проникновения на объект и его цель

- негласное проникновение одиночного постороннего нарушителя с целью кражи ценностей, для установки специальной аппаратуры или для съема информации;
- негласное проникновение нарушителя-сотрудника организации 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.

Пути физического проникновения «нарушителя»

- 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.

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

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 техническими средствами охранной сигнализации, техническим средствами наблюдения, системами контроля и управления доступом

Факторы, учитываемые при построении модели нарушителя

Исследование возможных угроз:

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.

Исследование типа нарушителя:

- неподготовленный;
- подготовленный;
- квалифицированный;

Изучение способов реализации угроз:

- контактные;
- Бесконтактные.

Изучение способов проникновения на объект.

Контактные и бесконтактные способы реализации угроз

Контактные способы:

1 Контактное проникновение на объект охраны:

- несанкционированное проникновение на территорию объекта охраны;
- проход на основе маскировки;
- установка средств негласного слухового, визуального, электромагнитного и др. наблюдения.

2 Контактное нарушение целостности или характера функционирования объекта:

- нарушение линий жизнеобеспечения объекта охраны;
- физическая ликвидация ресурсов объекта охраны;
- затруднение штатного режима функционирования объекта.

Бесконтактные способы:

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.

Критерии построения модели нарушителя

1 Цели и задачи вероятного нарушителя;

2 Степень принадлежности вероятного нарушителя к объекту;

3 Степень осведомленности вероятного нарушителя об объекте;

4 Степень осведомленности вероятного нарушителя о системе охраны объекта;

5 Степень профессиональной подготовленности вероятного нарушителя;

6 Степень физической подготовленности вероятного нарушителя;

7 Владение вероятным нарушителем способами маскировки;

8 Степень технической оснащенности вероятного нарушителя;

9 Способ проникновения вероятного нарушителя на объект.

Категории нарушителей

- 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 объектов (квалифицированный 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.

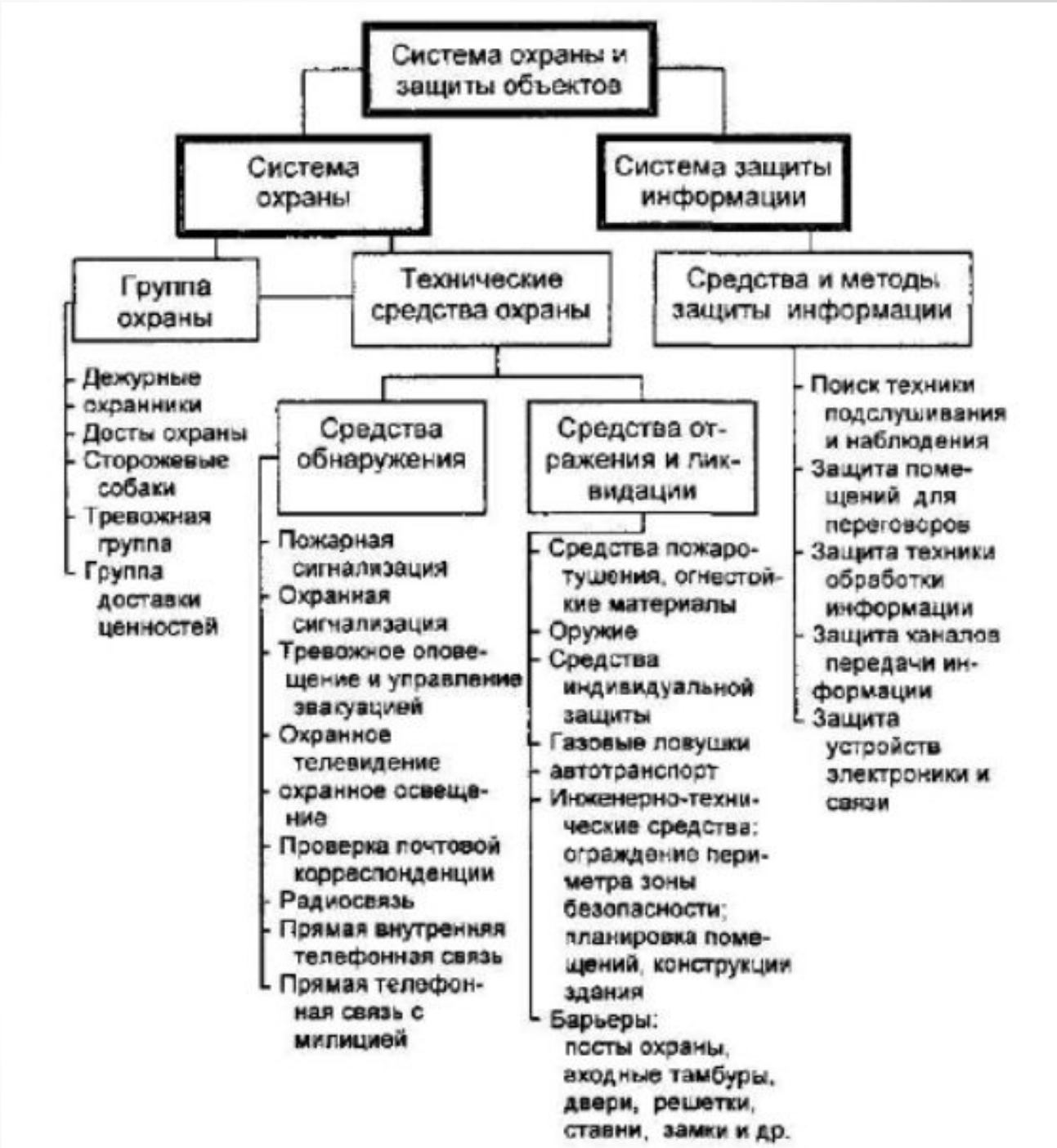
Вопрос 3. Характеристика основных способов защиты информации

Техническое средство охраны - аппаратура (вид техники), используемый в составе комплексов (систем) технических средств, применяемых для охраны объектов (территорий, зданий, помещений) от несанкционированного проникновения

Средство обнаружения - это устройство, предназначенное для автоматического формирования сигнала с заданными параметрами (сигнала тревоги, говорят также - сигнала срабатывания или оповещения) вследствие вторжения или преодоления объектом обнаружения чувствительной зоны (говорят также – зоны обнаружения) данного устройства.

Расположение зон безопасности

Схема системы охраны и защиты объекта



Основные направления деятельности службы охраны по обеспечению комплексной безопасности

- 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 службы охраны;
- 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, несанкционированного копирования, вирусной диверсии и других угроз;
- обеспечение применения специальных технических средств контроля особо важных помещений;
- организация контроля телефонных переговоров с их регистрацией

Типовой порядок создания системы защиты объекта

- 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-техническими и специальными 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.

Функции, обязательные для исполнения в контуре интегрированной системы безопасности

- контроль за большим количеством помещений с созданием нескольких рубежей защиты;
- 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 инструктаж работников охраны о порядке действий в различных штатных и нештатных ситуациях;
- обеспечение полной интеграции систем видеонаблюдения, сигнализации, мониторинга доступа, оповещения, связи между персоналом службы охраны, 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.

Технические средства охраны

- Решение задач обеспечения безопасности объектов все в большей мере опирается на широкое применение технических средств охранной сигнализации.

Технические средства охранной сигнализации по признаку их применения можно разделить на две группы:

- аппаратура, устанавливаемая на объектах народного хозяйства, как правило, охраняемых подразделениями вневедомственной охраны;
- аппаратура, применяемая на объектах, охрана которых, как правило, не находится в ведении вневедомственной охраны

Комплекс технических систем охраны в совокупности с инженерными средствами охраны (инженерно-строительные сооружения, препятствующие проникновению нарушителя), объединенные для решения общей задачи по охране объекта, образуют законченный комплекс инженерно-технических средств охраны.

Под комплексом технических средств охранной сигнализации понимается совокупность функционально связанных средств обнаружения, системы сбора и обработки информации и вспомогательных средств и систем, объединенных задачей по обнаружению нарушителя.

Под системой сбора и обработки информации понимается совокупность аппаратно-программных средств, предназначенных для сбора, обработки, регистрации, передачи и представления оператору информации от средств обнаружения, для управления дистанционно управляемыми устройствами, а также для контроля работоспособности как средств обнаружения, дистанционно управляемых устройств и каналов передачи, так и работоспособности собственных составных элементов.

Аппаратура системы сбора и обработки информации подразделяется на:

- станционную, осуществляющую прием, обработку, отображение и регистрацию информации, поступающей от периферийной аппаратуры системы сбора и обработки информации, а также формирование команд управления и контроля работоспособности;
- периферийную, осуществляющую прием информации от средств обнаружения, ее предварительную обработку и передачу ее по каналу передачи на центральную станционную аппаратуру, а также прием и передачу команд управления и контроля работоспособности.

Способы построения структурных схем технических систем охраны

1 Радиальный (лучевой) бесконцентраторный ;

2 Радиальный (лучевой) с концентраторами ;

3. Шлейфовый (магистральный) без концентраторов;

4. Шлейфовый (магистральный) с концентраторами;

5. Смешанная (радиально-шлейфовая) или древовидная структура

Средства обнаружения

Появление нарушителя в охраняемом помещении в общем случае может быть обнаружено по большому числу физико-химических явлений.

Это обнаружение осуществляется с помощью технических средств, в основу построения которых положены самые различные принципы регистрации изменений состояния среды.

В основу построения соответствующих типов средств обнаружения положены различные типы чувствительных элементов, осуществляющих взаимодействие с внешней средой и нарушителем.

Основные типы средств обнаружения

1 По способу приведения в действие (постановка на охрану, снятие с охраны с центрального пульта) средства обнаружения подразделяют на автоматические и автоматизированные
2 По назначению автоматические средства обнаружения подразделяют:
- для закрытых помещений;
- для открытых площадок и периметров объектов.
3 По виду зоны, контролируемой средства обнаружения, выделяются:
- точечные;
- линейные;
- поверхностные;
- объемные (пространственные).
4.По принципу действия рассматриваются средства обнаружения следующих типов:
- механические (на практике выделяют электроконтактные, магнитоконтактные, ударноконтактные);
- электромагнитные бесконтактные;
- магнитометрические;
- емкостные;
- индуктивные;
- гидроакустические;
- акустические;
- сейсмические;
- оптико-электронные (активные и пассивные);
- радиоволновые;
- радиолучевые (микроволновые);
- ольфактронные (строятся на принципе обнаружения запаха -одорологии);
- комбинированные.

Основные типы средств обнаружения

5.По количеству зон обнаружения, создаваемых средств обнаружения, их подразделяют на однозонные и многозонные.

6.По дальности действия ультразвуковые, оптико-электронные и радиоволновые средства обнаружения для закрытых помещений рассматривают:

- малой дальности действия - до 12 м;
- средней дальности действия - свыше 12 до 30 м;
- большой дальности действия - свыше 30 м (кроме ультразвуковых СО).

7.По дальности действия оптико-электронные и радиоволновые СО для открытых площадок и периметров объектов подразделяют:

- малой дальности действия - до 50 м;
- средней дальности действия - свыше 50 до 200 м;
- большой дальности действия - свыше 200 м.

8.По конструктивному исполнению ультразвуковые, оптико-электронные и радиоволновые средства обнаружения принято подразделять на:

- однопозиционные - один или более передатчиков (излучателей) и приемник(и) совмещены в одном блоке;
- двухпозиционные - передатчик (излучатель) и приемник выполнены в виде отдельных блоков;
- многопозиционные - более двух блоков (один передатчик, два или более приемников; один приемник, два или более передатчиков; два или более приемников).

Средства коммуникации

- Под *системой передачи извещений* понимается совокупность совместно действующих технических средств для передачи извещений о проникновении на охраняемые объекты, служебных и контрольно-диагностических извещений, а также для передачи и приема команд телеуправления.
- Система передачи извещений предусматривает установку оконечных устройств на объектах, ретрансляторов в кроссах автоматических телефонных станций, жилых домах и других промежуточных пунктах и установку пультов централизованного наблюдения в пунктах централизованной охраны.

Вопрос 4. Система сбора и обработки информации

Признаки классификации систем сбора и обработки информации:

- назначение;
- структура построения;
- энергообеспечение;
- степень защиты линии сигнализации от обхода;
- обеспечение контроля работоспособности аппаратуры;
- методы отображения информации;
- обеспечение регистрации информации;
- возможность управления внешними устройствами;
- обеспечение возможности информационного обмена с другими системами с помощью стандартных интерфейсов.

Классификация системы сбора и обработки информации

В зависимости от назначения системы сбора и обработки информации характеризуются следующими признаками:

- Область применения,.
- Камуфлирование.
- Условия окружающей среды.
- Мобильность.

В зависимости от структуры построения системы сбора и обработки информации делятся по следующим признакам:

- структурная схема построения системы сбора и обработки информации
- количество каналов сигнализации;
- способ подключения средств обнаружения к каналу сигнализации;
- тип линии связи;
- наличие периферийных устройств отображения, сигнализации и управления.

Классификация системы сбора и обработки информации

В зависимости от вида электропитания системы сбора и обработки информации делятся на системы с сетевым электропитанием и с автономным электропитанием от аккумуляторов.

В зависимости от способа электропитания средств обнаружения и периферийных устройств системы сбора и обработки информации подразделяют на системы:

- с дистанционным электропитанием средств обнаружения и периферийных устройств;
- без централизованного обеспечения электро-питания средств обнаружения и периферийных устройств;
- с автоматическим переходом на резервный источник электропитания;
- без переключения на резервный источник электропитания.

Классификация системы сбора и обработки информации

В зависимости от степени защиты линии сигнализации от обхода могут быть классифицированы:

- без защиты линий связи от обхода;
- с низкой степенью защиты линий связи от обхода;
- со средней степенью защиты линий связи от обхода;
- с высокой степенью защиты линий связи от обхода.

В зависимости от контроля работоспособности аппаратуры:

- без обеспечения контроля за состоянием аппаратуры;
- с полным контролем;
- с частичным контролем;
- с непрерывным автоматическим контролем;
- с периодическим автоматическим контролем;
- с возможностью диагностики неисправности;
- без возможности диагностики неисправности.

Классификация системы сбора и обработки информации

По методам отображения информации:

- визуальное,
- акустическое,
- текстовое,
- тактильное.

По способам регистрации информации:

- без возможности регистрировать информацию;
- с ОЗУ;
- с возможностью передачи данных на ПЭВМ;
- с возможностью документирования в режиме реального времени;
- с возможностью документирования содержимого ОЗУ;
- с возможностью документирования, посредством распечатки базы данных с ПЭВМ.

Классификация системы сбора и обработки информации

По организации управления внешними устройствами:

- без возможности управления внешними устройствами;
- с возможностью управления внешними устройствами, индивидуальными для каждого канала;
- с возможностью управления общим внешними устройствами;
- с возможностью управления индивидуальными и общим внешними устройствами.