

Технические средства и комплексное обеспечение безопасности

ГБПОУ БПЭК

ИБ

Темы докладов

- ◆ Системы оповещения
- ◆ Системы опознавания
- ◆ Оборонительные системы
- ◆ Охранное освещение
- ◆ Автоматизированные системы контроля доступа
- ◆ Биометрические системы идентификации (отпечаток пальца, геометрия руки, геометрия лица)
- ◆ Биометрические системы идентификации (радужная оболочка глаза, сетчатка глаза, голосовая идентификация)
- ◆ Биометрические системы идентификации (клавиатурный почерк, подпись)
- ◆ Технические средства обеспечения безопасности подвижных объектов
- ◆ Технические средства охранной сигнализации физических лиц
- ◆ Физическая защита ПК и носителей информации

Комплексная безопасность

- ◆ Предполагает обязательную непрерывность процесса обеспечения безопасности как во времени, так и в пространстве (по всему технологическому циклу деятельности) с обязательным учетом всех возможных видов угроз (несанкционированный доступ, съем информации, терроризм, пожар, стихийные действия и т.п.)

Комплексная безопасность

- ◆ Ограничение доступа к информации
- ◆ Техническое и криптографическое закрытие информации
- ◆ Ограничения уровней паразитных излучений технических средств
- ◆ Техническая укрепленность объектов
- ◆ Охрана
- ◆ Тревожная сигнализация

Подсистемы физической безопасности

- ◆ Управление доступом (с функцией досмотра)
- ◆ Обнаружение проникновения, аварийная и пожарная сигнализации
- ◆ Инженерно-техническая защита (пассивная защита)
- ◆ Отображение и оценка обстановки

Подсистемы физической безопасности

- ◆ Управление в аварийных и тревожных ситуациях
- ◆ Оповещение и связь в экстремальных ситуациях
- ◆ Личная безопасность персонала

Средства противодействия

- ◆ Здания и строительные препятствия, мешающие действиям злоумышленника и задерживающие его
- ◆ Аппаратура тревожной сигнализации
- ◆ Системы связи, обеспечивающие сбор, объединение и передачу тревожной информации и других данных

Средства противодействия

- ◆ Системы управления, необходимые для отображения и анализа тревожной информации
- ◆ Персонал охраны
- ◆ Процедуры обеспечения безопасности

Объединенная система обеспечения безопасности

Препятствующая и задерживающая подсистема

Ограждения, стены, ворота, заборы, тамбуры, свободные зоны, запретные зоны, автоматические устройства сигнализации

Подсистема обнаружения

Датчики, источники электропитания, электронные средства поиска

Подсистема оценки

Дозорные вышки, система телевидения, посты, патрули, звукоусилители, освещение

Подсистема управления и отображения

Тревожные сообщения, управления данными, дисплеи

Подсистема связи

Радиосвязь, линии передачи данных, телефон

Подсистема персонала и оборудования

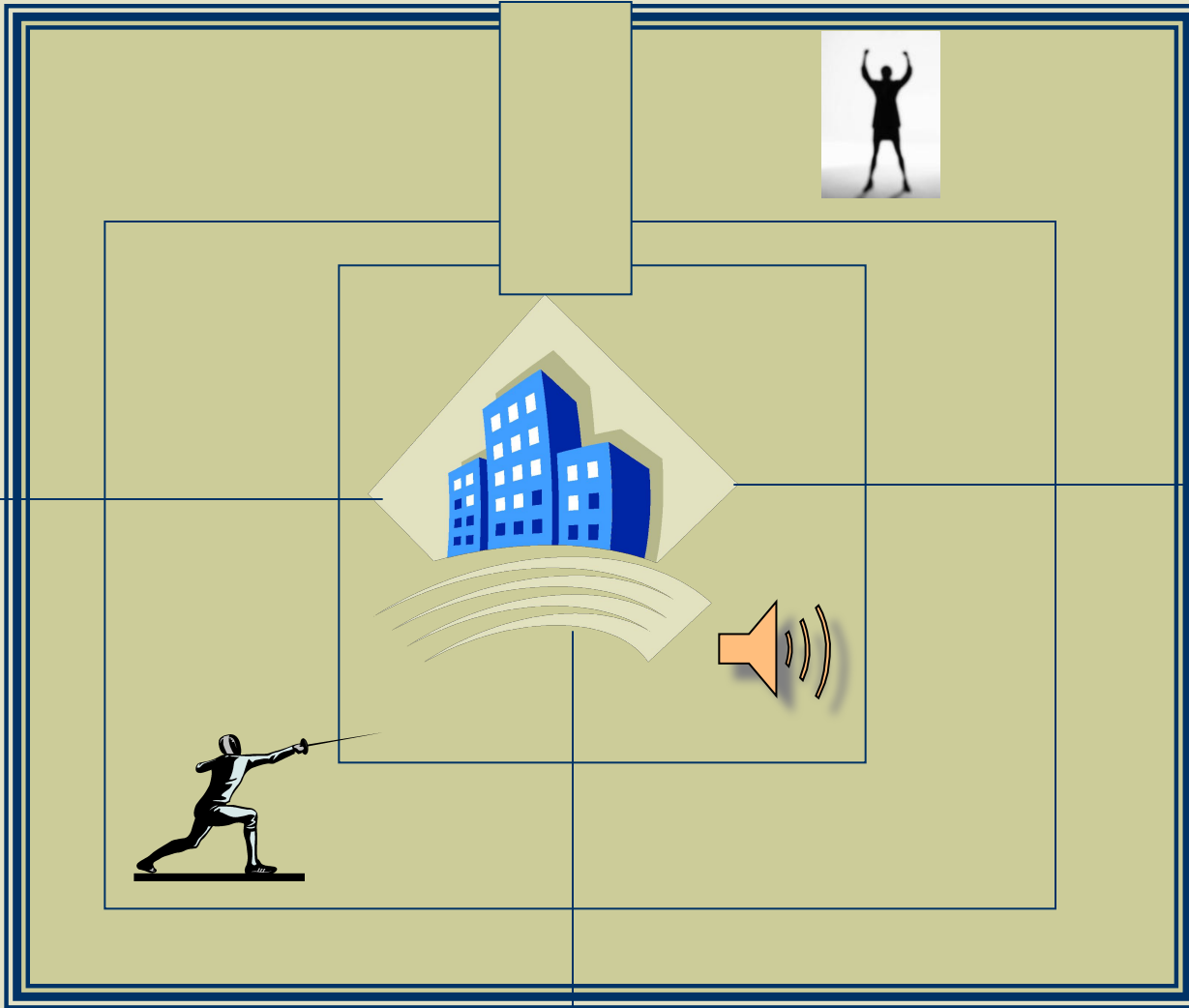
Вспомогательные службы, оружие, транспорт, защитные средства

Подсистема доступа

Спецвходы, автоматические системы доступа, системы и средства идентификации и проверки персонала


Процедурная подсистема

Тренировка, тактические планы, оперативные процедуры, обследование, контроль доступа



Концепция комплексной защиты информации должна удовлетворять следующей совокупности требований:


- ◆ Должны быть разработаны и доведены до уровня регулярного использования все необходимые механизмы гарантированного обеспечения требуемого уровня защищенности информации;
- ◆ Должны существовать механизмы практической реализации требуемого уровня информации;
- ◆ Необходимо располагать средствами рациональной реализации всех необходимых мероприятий по защите информации на базе достигнутого уровня развития науки и техники.
- ◆ Должны быть разработаны способы оптимальной организации и обеспечения проведения всех мероприятий по защите в процессе обработки информации



Технические и механические средства защиты



◆ Средства защиты информации —

- 
- ◆ это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Средства обеспечения защиты информации

- ◆ *Технические*
- ◆ *Программные*
- ◆ *Смешанные*
- ◆ *Организационные*

Основная задача технических мероприятий – обеспечение физической и информационной безопасности.

- ◆ выбор инженерно-технических средств, исключающих несанкционированный доступ к объектам и техническим средствам;
- ◆ блокирование каналов утечки информации, включая использование процедур контролируемой ликвидации данных;
- ◆ блокирование несанкционированного физического доступа к активным компонентам АС (информации или ресурсам ИС), находящимся в контролируемой зоне;
- ◆ выявление электронных устройств перехвата информации;
- ◆ выбор и проверка исправности и работоспособности технических средств обеспечения информационной деятельности.

Главная задача технических средств защиты информации

- ◆ Предотвращение умышленного или случайного несанкционированного доступа к информации и ресурсам АС (с целью ознакомления, использования, модификации или уничтожения информации) со стороны авторизованных пользователей или посторонних лиц, которые находятся в пределах зон безопасности информации АС, независимо от способа доступа к ЭТИМ зонам.

Технические мероприятия

- ◆ построение модели защищенной системы;
- ◆ управление доступом к ресурсам АС;
- ◆ обеспечение целостности и конфиденциальности;
- ◆ обеспечение наблюдаемости;
- ◆ защита от воздействий вирусов и иных воздействий, вызывающих любую несанкционированную модификацию информации;
- ◆ защита информации при передаче информации

Средства ТЗИ

Средства Под системы защиты информации

Обеспечения конфиденциальности:
1. Доверительной
2. Административной
3. Анализа скрытых каналов

Обеспечения целостности:
1. Доверительной
2. Административной

Обеспечения наблюдаемости

Средства прикладного и базового программного обеспечения

Обеспечения конфиденциальности в части повторного использования объектов

Обеспечения целостности в части отката

Обеспечения доступности:
1. Использования ресурсов
2. Стойкости к отказам
3. Горячей замены
4. Восстановления после сбоев

Неавтоматизируемые первичные средства ТЗИ

Средства ТЗИ телекоммуникаций

Обеспечения конфиденциальности и целостности в части обмена

Обеспечения наблюдаемости в части обеспечения достоверного канала, идентификации и аутентификации при обмене.

Распределение обязанностей:
1. Выделение администратора;
2. Распределение обязанностей администраторов;
3. Распределение обязанностей на основе привилегий.

Регистрация:
1. Внешний анализ
2. Защищенный журнал
3. Сигнализация об опасности
4. Детальная регистрация
5. Анализ в реальном времени

Целостность КСЗ:
1. КСЗ с контролем целостности
2. КСЗ с гарантией целостности
3. КСЗ с функциями диспетчера доступа

Идентификация и аутентификация:
1. Внешние идентификация и аутентификация;
2. Одноразовая идентификация и аутентификация;
3. Множественная идентификация и аутентификация.

Самотестирование:
1. По запросу
2. При старте
3. В реальном времени

Аутентификация отправителя и получателя:
1. Базовая
2. С подтверждением

Принципы организации ТЗИ

- ◆ **Принцип системности** предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности.
- ◆ **Принцип комплексности** предполагает согласованное применение разнородных средств при построении целостной системы защиты.
- ◆ **Принцип непрерывности** предполагает, что защита информации - это непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер в ходе всего рассматриваемого периода защиты информации.

Принципы организации ТЗИ

- ◆ **Разумная достаточность** предполагает то, что важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.
- ◆ **Принцип гибкости** системы защиты направлен на обеспечение возможности варьирования уровнем защищенности.
- ◆ **Принцип открытости алгоритмов и механизмов защиты** предполагает, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. При этом знание алгоритмов работы системы защиты не должно давать возможности ее преодоления.

Общий алгоритм организации ТЗИ на объекте информатизации

- ◆ Оценка обстановки
- ◆ Обоснование требований по защите информации
- ◆ Формулирование задач ТЗИ
- ◆ Разработка замысла или концепции ТЗИ
- ◆ Выбор способов (мер и средств) ТЗИ
- ◆ Решение вопросов управления и обеспечения ТЗИ
- ◆ Планирование ТЗИ
- ◆ Привлечение подразделений организации, специализированных сторонних организаций к разработке и развертыванию системы ТЗИ
- ◆ Разработка документации по вопросам организации ТЗИ
- ◆ Развертывание и ввод в опытную эксплуатацию системы ТЗИ

Техника защиты информации

- ◆ Устройства защиты от утечки акустической информации
- ◆ Устройства защиты телефонных переговоров от прослушивания
- ◆ Комплексы защиты информации компьютеров и компьютерных сетей от несанкционированного доступа
- ◆ Технические системы контроля эффективности защиты информации
- ◆ Подавители диктофонов
- ◆ Устройства защиты от утечки информации по электросети



Устройства защиты от утечки акустической информации

- ◆ **Шторм.** Устройство противодействия радиоэлектронным средствам промышленного шпионажа. Зона подавления – пространственный сектор с углом 60 град. и радиусом до 6 м. Обеспечивает нейтрализацию подслушивающих устройств, скрытых видеокамер, диктофонов.

Устройства защиты от утечки акустической информации

- ◆ **ANG-2200.** Генератор шума для акустического зашумления помещения и его защиты от утечки информации по виброканалам (250...5000 Гц).

Устройства защиты от утечки акустической информации

- ◆ **Барон.** Комплекс виброакустической защиты объектов информатизации. Обеспечивает максимально возможное противодействие техническим средствам перехвата речевой информации (стетоскопы, направленные и лазерные микрофоны, выносные микрофоны) по виброакустическим каналам.

Устройства защиты от утечки акустической информации

- ◆ **Вето.** Устройство активной защиты информации. Формирует широкополосное шумоподобное радиоизлучение с целью создания помеховой обстановки, затрудняющей работу различных систем контроля, в составе которых используется радиопередающая и радиоприемная аппаратура.

Устройства защиты телефонных переговоров от прослушивания

- ◆ **Прокруст-2000.** Устройство защиты телефонных переговоров от прослушивания и записи. Организуется участок дополнительной защищенности для гарантированного предотвращения снятия и передачи информации по телефонной линии при положенной трубке.

Устройства защиты телефонных переговоров от прослушивания

- ◆ **Прокруст-2000.** Устройство защиты телефонных переговоров от прослушивания и записи. Организуется участок дополнительной защищенности для гарантированного предотвращения снятия и передачи информации по телефонной линии при положенной трубке. Возможность дистанционного управления, включение одной кнопкой, световая индикация пиратского использования линии в промежутках между переговорами, возможность подключения звукозаписывающих устройств для документирования переговоров.

Устройства защиты телефонных переговоров от прослушивания

- ◆ **ГИ-1500.** Выжигатель устройств съема информации в проводных линиях связи и в обесточенной электросети для защиты от несанкционированного прослушивания переговоров как по телефону, так и в помещении с помощью устройств, работающих в проводных линиях, либо в электросети.

Комплексы защиты информации компьютеров и компьютерных сетей от несанкционированного доступа

- ◆ **X-Files.** Программа для контроля за выполнением персоналом правил безопасности при работе с компьютером, а также выявления и пресечения попыток несанкционированного доступа к конфиденциальным данным, хранящимся на ПК или в корпоративной локальной вычислительной сети.

Комплексы защиты информации компьютеров и компьютерных сетей от несанкционированного доступа

- ◆ **X-Files.** Программа для контроля за выполнением персоналом правил безопасности при работе с компьютером, а также выявления и пресечения попыток несанкционированного доступа к конфиденциальным данным, хранящимся на ПК или в корпоративной локальной вычислительной сети. Принцип работы программы основан на незаметном «фотографировании» изображения с экрана компьютера через определенные промежутки времени с регистрацией даты и времени снимка.

Технические системы контроля эффективности защиты информации

- ◆ **Навигатор (мобильный E4402B).** Переносной комплекс для проведения инженерных исследований и исследований на сверхнормативные побочные электромагнитные излучения.
- ◆ **Спрут-6.** Комплекс для проведения акустических и виброакустических измерений.

Подавители диктофонов



- ◆ **Мангуст.** Предназначен для защиты от несанкционированного получения информации при помощи цифровых и кинематических диктофонов. Возможно применение прибора для предотвращения утечки информации при помощи проводных микрофонов, а так же малогабаритных передатчиков. Зона подавления представляет собой шаровой сектор с радиусом до 4 м.

Подавители диктофонов

- ◆ **Шторм.** Предназначен для защиты от несанкционированного получения информации при помощи цифровых и кинематических диктофонов.

Подавители диктофонов



- ◆ **Барсетка.** Предназначен для защиты от несанкционированного получения информации при помощи цифровых и кинематических диктофонов. Речеподобная помеха. Возможно применение подавителя диктофонов для предотвращения утечки информации при помощи проводных микрофонов, а так же малогабаритных передатчиков. Зона подавления представляет собой шаровой сектор с радиусом до 2 м.

Устройства защиты от утечки информации по электросети

- ◆ **ГРОМ-ЗИ-4.** Многофункциональный генератор шума.
- ◆ **ЛФС-40-1Ф.** Однофазный сетевой помехоподавляющий фильтр для максимального рабочего тока 40 А.
- ◆ **Соната-РС1.** Генератор шума по сети электропитания.

Алмаз



- ◆ Для обнаружения и локализации минивидеокамер по оптическому признаку. Позволяет находить как работающие, так и не работающие на момент обнаружения видеокамеры, в т.ч. скрытые внутри упаковки, в стенах и потолках, внутри электромагнитного экрана и т. д.

Омега.



- ◆ Компьютерный комплекс представляет собой мощную расширяемую аппаратную платформу, предназначенную для решения различных задач радиоконтроля и анализа электромагнитной обстановки, в том числе для автоматического обнаружения, идентификации, локализации и нейтрализации подслушивающих устройств, передающих данные по радиоканалу и проводным линиям. Может использоваться для организации как стационарных, так и мобильных постов радиоконтроля.



Арфа

- ◆ Для проверки радиоэлектронной аппаратуры, подключаемой к проводным силовым и коммуникационным линиям на наличие возможных каналов утечки информации под воздействием сигнала высокочастотного навязывания.

Системы контроля доступа



Биометрические средства защиты

