«БЕЗОПАСНОСТЬ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ»

Академик Академии проблем безопасности, обороны и правопорядка, кандидат исторических наук, доцент КОЗЛОВ Евгений Станиславович

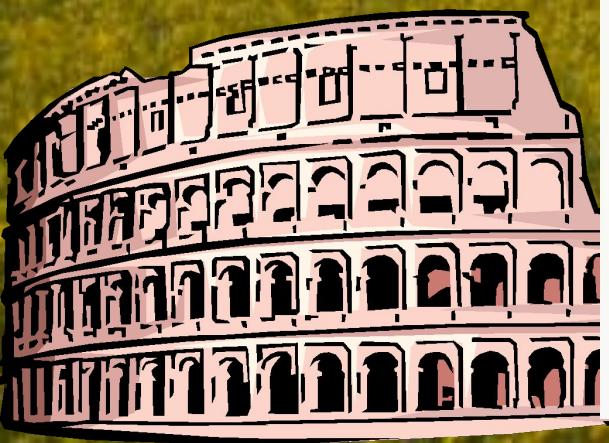
Учебный вопрос

1.Основные положения теории безопасности банковской деятельности

Термин «безопасность» появился в Европе в 1190 г. и означал «спокойное состояние духа человека, считавшего себя защищенным от любой опасности»

Энциклопедический словарь Робера

*В начале **XVII** века с формированием государственных систем данное понятие обрело иную трактовку «создание условий спокойствия в результате отсутствия реальной опасности (как физической, так и моральной) в материальной, политической и экономической сферах»*



Природа безопасности имеет глубокие исторические корни в человеческой цивилизации и наиболее рационально может исследоваться с привлечением различных знаний в области философии, права, теологии, истории, экономики, политологии, социологии, логики, криминалистики, информатики и т.д.

«ОПАСНОСТЬ» можно охарактеризовать как наличие и действие сил (факторов), которые являются деструктивными и дестабилизирующими по отношению к какой-либо конкретной системе (банку)

Деструктивными и дестабилизирующими следует считать те силы (факторы), которые способны нанести ущерб данной системе, временно вывести её из строя или полностью уничтожить

УГРОЗА:

- возможная опасность;
- запугивание, обещание причинить кому – либо неприятность, зло;
- наиболее конкретная и непосредственная форма опасности, создаваемая целенаправленной деятельностью откровенно враждебных сил и т.д.

УРОВЕНЬ УГРОЗЫ – степень потенциальной опасности для объекта

ИСТОЧНИКИ ОПАСНОСТИ – условия и факторы, которые таят в себе и при определенных условиях сами по себе, либо в различной совокупности обнаруживают враждебные намерения, вредоносные свойства, деструктивную природу и по своему генезису имеют естественно-природное, техногенное и социальное происхождение

Предотвращение опасностей в банковской деятельности предполагает своевременное их прогнозирование и принятие необходимых мер, прежде всего:

- постоянное добывание, сбор, анализ информации;

-оценка обстановки;

-выработка и принятие решения;

-осуществление упреждающих действий;

-удержание инициативы в своих руках;

-создание резервов и т.д.

ГЛАВНАЯ ЦЕЛЬ БЕЗОПАСНОСТИ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ -

обеспечение устойчивого функционирования банка и предотвращение внутренних и внешних угроз

Также, защита его законных интересов от противоправных посягательств, безопасность и охрана здоровья персонала, недопущение хищения финансовых и материальных средств, порча и уничтожение имущества, ценностей, разглашение коммерческой тайны, утечки и несанкционированного доступа к служебной информации, нарушения работы технических средств обеспечивающие банковскую деятельность

Учебный вопрос

2.Угрозы безопасности банков

ИСТОЧНИКИ УГРОЗ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ:

-природные (редкое явление);
-технические (связанные с техникой);
-социальные (общество-человек).

Следует обратить внимание, что именно *социальные угрозы* наиболее опасные.

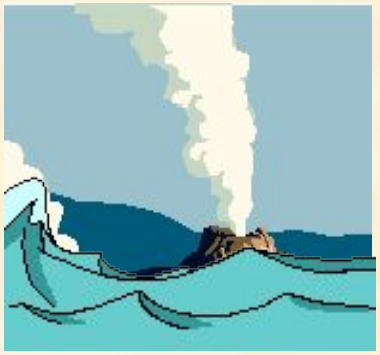
В процессе выявления, анализа и прогнозирования потенциальных угроз интересам банка в рамках безопасности учитываются объективно существующие внешние и внутренние условия, влияющие на банковскую систему в целом

Таковыми являются:

- **нестабильная политическая, социально-экономическая обстановка, обострение криминогенной ситуации, криминальная конкуренция и т.д.;**
- **невыполнение законодательных актов, правовой нигилизм, отсутствие некоторых законов по жизненно важным вопросам;**
- **снижение моральной, психологической, производственной ответственности работников банка и т.д.**

ВИДЫ УГРОЗ БЕЗОПАСНОСТИ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

Внутренние угрозы – это источники, порождаемые внутренними противоречиями или иными факторами, которые могут исходить непосредственно от коллектива, групп людей и отдельных личностей, наделенных определенными полномочиями при выполнении своих обязанностей в данном учреждении.



Внешние угрозы – это источники, которые существуют или могут появляться за рамками организации, в частности банка, и воздействовать на его интересы извне. Основу внешних угроз, как правило, составляет социальные источники опасности (люди), а также и природные.

КЛАССИФИКАЦИЯ ПОТЕНЦИАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ БАНКОВ

Первая группа - физические угрозы.

Вторая группа – технические угрозы.

Третья группа – интеллектуальные угрозы.

Физические угрозы, как воздействие физических лиц, совершающих противоправные действия методом физического насилия, также и природные, техногенные катастрофы.

К физическим угрозам относятся:

- похищения и угрозы похищения сотрудников банка, членов их семей и близких родственников;
- убийства, сопровождаемые насилием, издевательствами и пытками;
- разбойные нападения с целью завладения денежными средствами, ценностями и документами;
- уничтожение собственности банка и собственности банковских работников;
- террористические акции, т.е. совершение преступления в форме взрыва, поджога, применения или угрозы применения взрывных устройств, хим., биологических, токсических, яд. веществ, а также захват заложников, транспортных ср- в и т.д.;
- чрезвычайные обстоятельства – это события вызванные аварией и приведшее на определенной территории к угрозе жизни и здоровью людей, ущербу государственным, коммерческим и иным видам собственности, личного имущества граждан и природной среде

Технические угрозы - это совокупность мероприятий и технических средств, направленных на получение нужной информации, а также на нарушение, нейтрализацию аппаратных средств и программного обеспечения интересующего объекта (банка) , к ним относятся:

- перехват информации;
- радиоразведка связи и управления;
- искажение информации;
- ввод ложной информации;
- информационное нападение;
- уничтожение информации и т.д.

ЦЕЛЬ - перехватить, исказить, уничтожить информацию

Интеллектуальные угрозы, это угрозы направленные на продукт интеллектуального труда, умственные способности индивида.

«Беловоротничковые угрозы (преступления)».

«Белые воротнички» - представители административно-бюрократического аппарата всех сфер управления

«Беловоротничковые угрозы» - это когда предприниматели, гос. служащие, банкиры и другие представители административного аппарата, обладают возможностью по характеру предоставляемых им полномочий совершать такие экономические преступления, как: нарушение антитрестовского законодательства; мошенничества с ценными бумагами, на фондовой бирже, с получением кредитов и ссуд; присвоением банковских средств, уклонение от уплаты налогов, взяточничество и д.р.

"Золотые воротнички" - новая категория персонала, обладающая высокой компьютерной грамотностью: программисты управляемых производственных комплексов, операторы роботизированных систем, специалисты по сверхновым материалам и т.д.

Угрозы психического воздействия можно рассмотреть на двух примерах

ПЕРВЫЙ - психическое нападение - это отрицательные различные психофизиологические состояния, рассматриваемые пострадавшим как "наведение извне", как исходящий от другого человека, с которым "пострадавший" в момент нападения находился в непосредственном контакте.

ВТОРОЙ - психическое насилие - насилие, выражающееся в демонстрации оружия и готовности его применения; на вербальном уровне (словесном) в угрозе нанести побои, связать, лишить свободы передвижения, убить или совершить насилие в отношении близких и родственников жертвы.

Мошенничество – а) хищение чужого имущества или приобретения права на чужое имущество путем обмана или злоупотребления доверием; б) получение кредита путем обмана или злоупотребления доверием и его присвоение.

Мошеннические действия на финансовом рынке РФ совершаются при следующих операциях:

1. Продажа и покупка ценных бумаг.
2. Предоставление и получение кредита.
3. Предоставление вексельного кредита.
4. Инкассирование векселей.
5. Вексельное поручительство банка.
6. Предоставление залога в обеспечение возвратности выданных ссуд.
7. Проведение расчетов по кредитным картам.
8. Страхование кредитов и и сделок.
9. Операции по «уничтожению, обрушению» банка по выдаче невозвратного долга.
10. Получение кредита за взятку, данную сотруднику банка.
11. Получение кредита подставной фирмой.
12. Фальшивое авизо.
13. Умышленные неплатежи и т.д.

Все преступления против чужой собственности подлежат квалификации по ст. 158-168 гл.21 особой части Уголовного кодекса РФ «Преступления против собственности»

Лжепредпринимательство – создание коммерческих организаций без намерения осуществлять предпринимательскую или банковскую деятельность, с целью получения кредитов, освобождения от налогов, извлечение других имущественных выгод или прикрытие запрещенной деятельности.

ЦЕЛЬ - создание банков и других кредитных организаций предназначенных для привлечения и последующего хищения денежных средств других лиц.

Лжепредпринимательство – один из обязательных элементов по отмыванию нелегально полученных доходов через банковскую систему.

Преступления за лжепредпринимательство подлежат квалификации по ст. 173 особой части Уголовного кодекса РФ «Преступления против собственности»

ПРЕСТУПЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ПЛАСТИКОВЫХ ПЛАТЕЖНЫХ СРЕДСТВ

-операции с поддельными картами;
-операции с украденными/поддельными картами;
-многократная оплата услуг и товаров;
-мошенничество с почтовыми/телефонными заказами ;
-многократное снятие со счета;
-мошенничество с использованием подложных слипов;
-использование для выдачи наличных денег через банкомат;
-подключение электронного записывающего устройства к POS – терминалу/банкомату "Skimming" и другие виды мошенничества.

Основные способы подделки пластиковой карты

-изменение информации на магнитном носителе;
-изменение информации эмбоссированная на лицевой стороне;
-их сочетание;
-подделка подписи законного владельца и т.д.

Скимминг – тщательное и полное копирование всего содержимого магнитных треков (дорожек)

Ст. 187 Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов. Уголовного кодекса РФ, раздел VII «Преступления в сфере экономики», гл.22 «Преступления в сфере экономической деятельности» от 2 до 5 лет, группой лиц от 4 до 7 лет

По данным ГУВД г.Москвы за последние три года число мошенничеств по пластиковым картам выросло в 180 раз! В России около 5% кредитных карточек - ФАЛЬШИВЫЕ.

КАРДИНГ – мошенничество с кредитными каточками (кража номеров кредитных карт, продажа поддельных кредитных карт и т.д.)

ФИШИНГ – получение информации от владельцев пластиковых карточек путем рассылки по электронной почте с фальшивыми веб-страницами, имитирующие легитимные сайты, запросов от имени банков и платежных систем

За первые месяцы прошлого года в мире 57 млн. человек подверглись фишинговым атакам. За прошедший год мошенники «заработали» 450 млн. долларов!

Нигерийские письма. Приходят в виде электронного письма или в виде факс-сообщения. Необходим счет в любом зарубежном банке для перечисления «грязных» денег. В качестве вознаграждения за помощь 10-30% от заявленной суммы.

Учебный вопрос:

ЦЕЛИ И ЗАДАЧИ СИСТЕМЫ БЕЗОПАСНОСТИ БАНКА

Система безопасности банковской деятельности – это совокупность специальных органов, служб, средств, методов, взаимосвязанных мероприятий правового характера, осуществляемых в целях защиты банка от внутренних и внешних угроз *(реальных или потенциальных противоправных действий физических или юридических лиц)*

Организация деятельности системы безопасности определяется Положением о системе безопасности банка.

ЦЕЛИ СИСТЕМЫ БЕЗОПАСНОСТИ БАНКА:

- защита прав банка, его структурных подразделений и сотрудников;
- сохранение и эффективное использование финансовых, материальных и информационных ресурсов;
- своевременное выявление и устранение угроз, причин и условий, способствующих нанесению ущерба, нарушению нормального функционирования и развития банка;
- отнесение информации к категории ограниченного доступа к различным уровням уязвимости;
- создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций функционирования;
- эффективное пресечение посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности;
- создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями для ослабления негативных влияний последствий нарушения безопасности на достижение стратегических целей.

ЗАДАЧИ СИСТЕМЫ БЕЗОПАСНОСТИ:

-обеспечение безопасности функционирования банка, его кредитно-финансовой деятельности и защиты конфиденциальной информации;

-организация работы по правовой, организационной и инженерно-технической защите материальных, финансовых и информационных ресурсов;

- организация специального делопроизводства, исключающего несанкционированного получения конфиденциальных сведений;

- выявление и локализация возможных каналов разглашения, утечки и несанкционированного доступа к конфиденциальной информации в процессе повседневной деятельности и в экстремальных ситуациях;

ЗАДАЧИ СИСТЕМЫ БЕЗОПАСНОСТИ:

-обеспечение режима безопасности при проведении всех видов деятельности, включая встречи, переговоры, совещания, связанные с деловым сотрудничеством на национальном и международном уровнях;

-обеспечение охраны зданий, помещений, оборудования и технических средств обеспечения деятельности банка;

- обеспечение безопасности персонала;

- информационно-аналитическая деятельность в интересах оценки ситуации и выявления неправомерных действий злоумышленников и конкурентов.

СИСТЕМА БЕЗОПАСНОСТИ БАНКА

ПРАВОВАЯ

Правовая обеспеченность - состояние при котором все аспекты функционирования системы управления безопасностью регламентированы законодательными актами и соответствующими нормативными документами.

Правовая культура.

Права и обязанности должностных лиц.

Правовое регулирование отношений людей в рабочих коллективах, между различными командными инстанциями, между начальниками и подчиненными и т.д.

Правовой нигилизм - социально-психологическое явление, которое выражается в полном или частичном отрицании полезности и необходимости соблюдения правовых норм отдельными членами общества.

ОРГАНИЗАЦИОННАЯ

Построение и устойчивое функционирование системы управления безопасностью на различных уровнях.

Развитие и создание оптимальной организационно-штатной структуры.

Организационные и другие документы, регламентирующие функционирование системы безопасности банка.

Организация управления безопасностью повседневной деятельности и т.д.

ТЕХНИЧЕСКАЯ

Техническая политика в оснащении банка современными средствами безопасности.

Подбор квалифицированных технических специалистов.

Высокие требования к техническим средствам системы безопасности.

Всестороннее обеспечение системы безопасности техническими средствами.

Диагностика, осмотр, обслуживание технических средств и т.д.

ПСИХОЛОГИЧЕСКАЯ

Психологический анализ управления безопасностью.

Учет психологических факторов в работе банковских служащих в повседневной деятельности и, особенно, в экстремальных ситуациях.

Психологическая подготовка банковских служащих, отвечающая требованиям данного вида деятельности и способствующая эффективному выполнению своих служебных обязанностей и т.д.

Учебный вопрос:

СЛУЖБА БЕЗОПАСНОСТИ БАНКА

Служба безопасности (СБ) банка — подразделение, специально созданное для защиты его законных прав и интересов от криминальной конкуренции со стороны социальных организаций и физических лиц, и функционирующее в соответствии с законом Российской Федерации от 6 июня 2005 г. «О частной детективной и охранной деятельности в Российской Федерации» №52-ФЗ

Затраты зарубежных фирм только на охрану коммерческой тайны достигают 25% всех расходов на производство. В Западной Европе ассигнования на мероприятия, связанные с обеспечением безопасности, составляют от 15 до 20% стоимости охраняемых ценностей. В России эти цифры не превышают 1%. Вместе с тем отказ предприятий от необходимых мер защиты, экономия на защитных мероприятиях, по сути, способствуют развитию преступности

Основные задачи службы безопасности:

-обеспечение безопасности кредитно-финансовой деятельности и защита информации и сведений, составляющих банковскую тайну;

-организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной) защите банковской тайны;

-организация специального делопроизводства, исключающего несанкционированное получение сведений, представляющих банковскую тайну;

-выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной деятельности и в экстремальных ситуациях;

-обеспечение режима безопасности при проведении всех видов деятельности, а т.ж. охрана зданий, помещений и т.п.;

-обеспечение личной безопасности руководства и ведущих сотрудников банка и т.д.

Служба безопасности в своей деятельности руководствуется:

-инструкцией по организации режима и охраны;

-инструкцией по защите банковской тайны;

-перечнем сведений, составляющих банковскую тайну;

-инструкцией по работе с конфиденциальной информацией для руководителей, специалистов и технического персонала;

-инструкцией по организации хранения дел, содержащих конфиденциальную информацию, в архиве;

-инструкцией по инженерно-технической защите информации;

-инструкцией о порядке работы с иностранными представителями и представительствами и т.д.

ПРИМЕРНАЯ СТРУКТУРА СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА
(основные задачи)

Сектор охраны:

-охрана помещений и зданий;
-охрана оборудования и имущества;
-охрана сотрудников и мероприятий;
-охрана перевозок и т.д.

Сектор режима:

-обеспечение секретности документов;
-обеспечение режима допуска;
-контроль посетителей и транспорта;
-расследование случаев нарушения режима и т.д.

ПРИМЕРНАЯ СТРУКТУРА СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА (основные задачи)

Сектор технической защиты:

-выявление технических каналов утечки информации;
-контроль за попытками несанкционированного доступа к информации с помощью техники;
-оборудование банка средствами сигнализации и связи;
-оборудование противопожарными средствами и т.д.

Сектор оперативной работы банка:

-выявление и изучение банков и преступных сообществ, которые являются потенциальными конкурентами или врагами;
-учет и анализ попыток проникновения в секреты банка, осуществления каких-либо враждебных акций;
-выявление возможных «слабых» мест в деятельности банка;
-разработка и осуществление мер противодействия «давлению» из вне и т.д.

ТРЕБОВАНИЯ К РУКОВОДИТЕЛЮ И ВЕДУЩИМ СПЕЦИАЛИСТАМ СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА

Необходимо обладать знаниями в следующих областях:

-информационно-аналитическая работа;

-методы разведки и контрразведки;

-оперативная работа;

-социальная психология и психология личности;

-основы банковского дела и бухгалтерский учет;

-основы менеджмента и маркетинга;

-административное, гражданское и уголовное право.

СПЕЦИАЛИСТ СЛУЖБЫ БЕЗОПАСНОСТИ ОБЯЗАН:

-разработать комплексные меры по обеспечению безопасности банка и личной безопасности его руководства;

-осуществить защиту конфиденциальной информации;

-уметь применять технические средства скрытого наблюдения и прослушивания ;

-противодействовать проведению аналогичных мероприятий конкурентами;

-разбираться в финансовой отчетности;

-заниматься профилактикой правонарушений;

-проводить внутреннее расследование случаев воровства, мошенничества, саботажа и финансовых преступлений;

-организовывать проверки (в т.ч. негласные) благонадежности сотрудников;

-предупреждать (выявлять) случаи сотрудничества персонала банка с конкурентами или криминальными структурами;

-взаимодействовать со следственными органами и милицией при расследовании преступлений или иных происшествий;

-разрешать конфликты между сотрудниками и т.д.

ОСНОВНЫЕ ВИДЫ ПЛАНОВ ПРИ ВОЗНИКНОВЕНИИ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ СО СТОРОНЫ КРИМИНАЛА

План действий при угрозе взрыва.

План действий при захвате заложников или похищении сотрудников.

План действий при нападении на инкассаторов.

План действий при нападении на помещение банка.

План действий при вымогательстве и т.д.

ТИПОВЫЕ ПЛАНЫ – ДОКУМЕНТЫ КОНФИДЕНЦИАЛЬНЫЕ!

Данные документы составляются в 2-3 экз.
Один экз. у руководителя, другой – начальника охраны и третий может быть у лица, заменяющего руководителя банка в его отсутствие.

Учебный вопрос:

ВНУТРЕННЯЯ ЗАЩИТА БАНКА

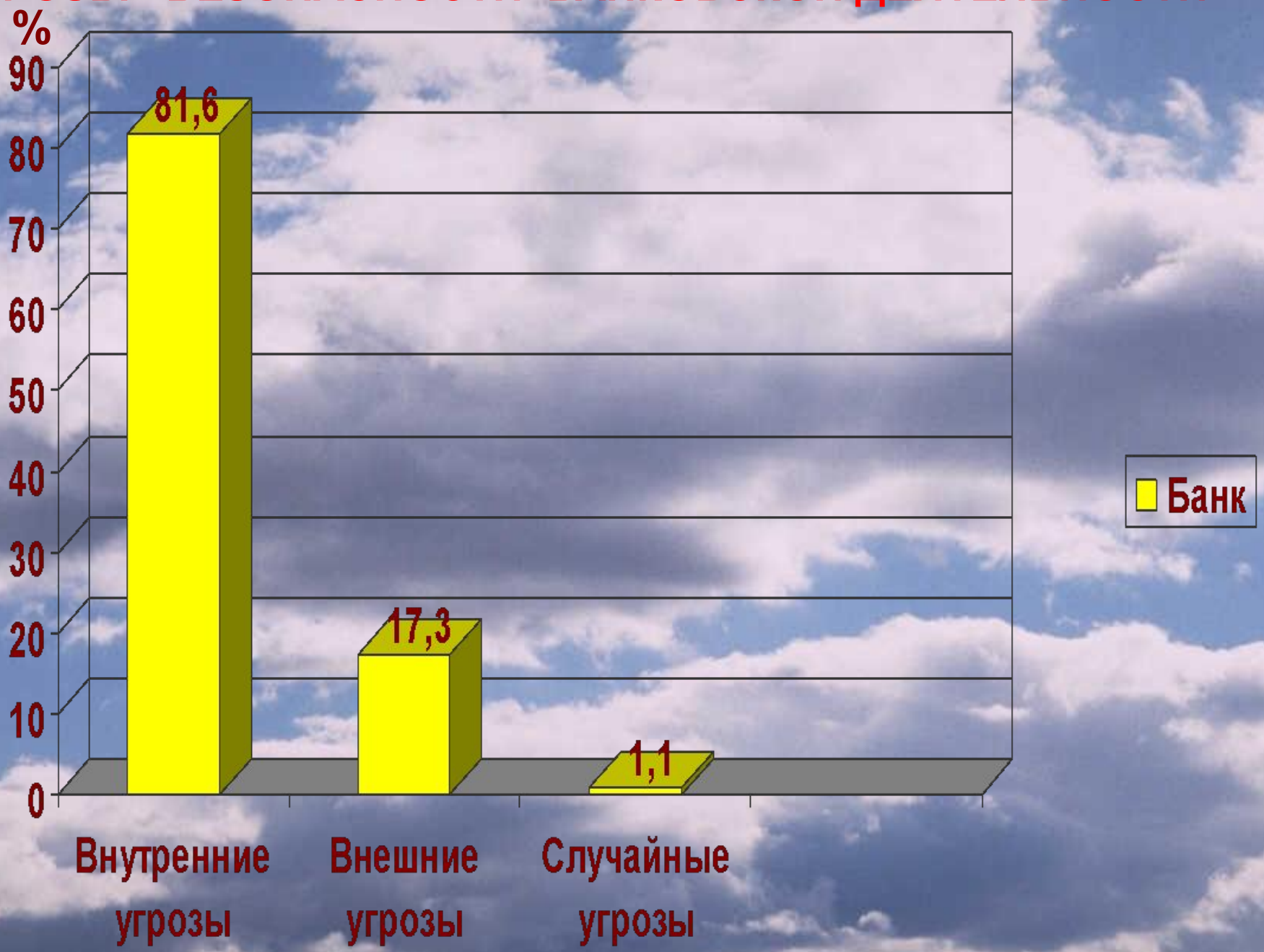
ВНУТРЕННИЕ ИСТОЧНИКИ ОПАСНОСТИ ДЕЯТЕЛЬНОСТИ БАНКА

– это источники, порождаемые внутренними противоречиями и иными факторами, действующими внутри банка, которые делятся на технологические и социальные

К технологическим *источникам опасности относятся отклонения от технологии деятельности организации (банка), которые таят в себе опасность причинения любого ущерба*

К социальным *источникам опасности относятся противоречия между индивидами, различными группами банковских работников, которые могут парализовать всю деятельность банка*

УГРОЗЫ БЕЗОПАСНОСТИ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ



ОСНОВНОЙ ИСТОЧНИК ВНУТРЕННИХ УГРОЗ БАНКА

Внутренний злоумышленник может быть любой сотрудник банка, вступивший в сговор с преступной группой

Внутренний злоумышленник может быть враждебно настроенный служащий, психически неуравновешенные люди или служащие, подвергающиеся шантажу или угрозам со стороны преступников

Внутренний злоумышленник - служащий банка или сотрудник охраны, имеющий доступ на объект, располагающий определенной информацией о режиме работы банка и, может быть, системе охраны

Мотивом преступления является, как правило, личное обогащение. Но, может быть: месть начальству или сотруднику, психическое расстройство и т.д.

ГРУППЫ РИСКА

- секретари
- личные помощники

- водители руководителей

- системные администраторы и технические специалисты

- сотрудники охраны и службы безопасности

-технический персонал (курьеры, уборщики)

Методы активного воздействия – подкуп, шантаж, жесткая угроза, физическое и психологическое воздействие, специфический форсированный допрос, игра на эмоциях, , убеждение, фармакологическое воздействие и т.д.

ВНУТРЕННЯЯ ЗАЩИТА БАНКА – **это комплекс мероприятий, действий, исключающих нанесения внутреннего ущерба банковской деятельности**

ВИДЫ ЗАЩИТЫ

Учебный вопрос:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

ОСНОВНЫЕ КЛАССЫ ИСТОЧНИКОВ ИНФОРМАЦИИ

ЛЮДИ

Сотрудники банка
Обслуживающий персонал
Клиенты
Партнеры и т.д.

ДОКУМЕНТЫ

-организационно-распорядительные;
-плановые;
-статистические;
-бухгалтерские;
-учредительные и др. документы содержащие сведения о составе, состоянии и деятельности банка.

ПУБЛИКАЦИИ

книги;
статьи;
обзоры;
сообщения;
доклады;
тезисы;
рекламные проспекты
и т.д.

ТЕХНИЧЕСКИЕ НОСИТЕЛИ

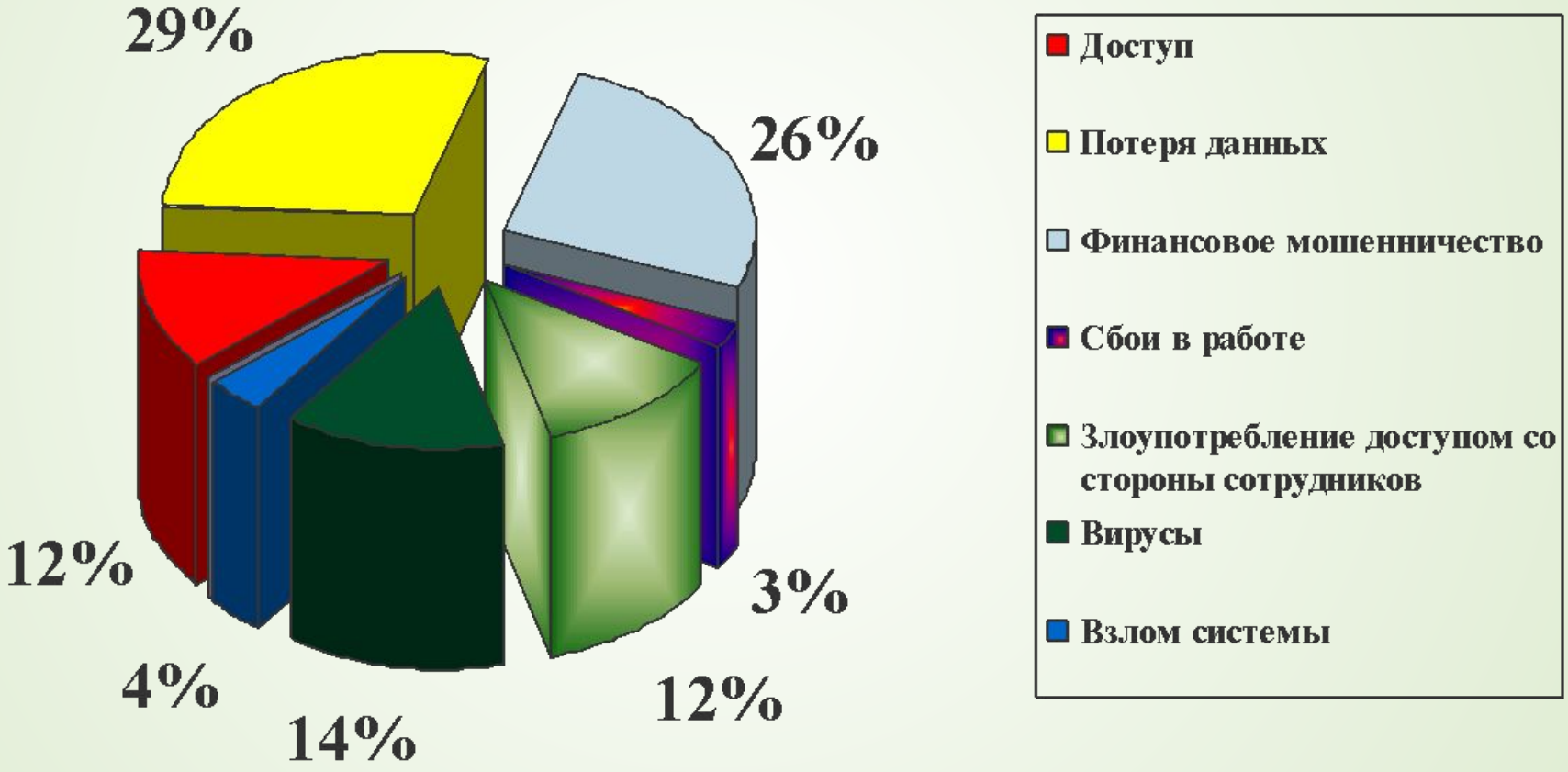
бумажные носители;
кино-, фотоматериалы;
магнитные носители;
видеодиски;
распечатка данных;
информ. на экранах ЭВМ; табло индивид. и коллективного пользования и д.р.

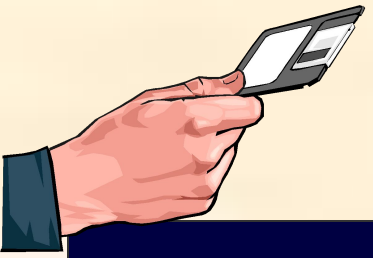
ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ

телефоны, телефонная связь; телевизоры, тв установки; радиоприемники; система ггс; усилительные системы; охранные и пожарные системы и т.д.

МУСОР ОТХОДЫ

УЯЗВИМОСТЬ БАНКОВСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ





«По имеющимся оценкам, из общего числа фактов утечки информации финансово-кредитной сферы подкуп, шантаж, переманивание служащих достигает 43%, копирование программного продукта — 24%, проникновение в компьютер — 18%, кражи документации — 10%, подслушивание телефонных переговоров — 5%»

Экономическая и национальная безопасность: Учебник / Под ред. Е.А. Олейникова. — М.: Издательство «Экзамен», 2005.

ОСНОВНЫЕ СПОСОБЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ИНСАЙДЕР -
лицо, имеющий в силу своего служебного или семейного положения доступ к конфиденциальной информации о делах банка (компании).

ИНИЦИАТИВНОЕ СОТРУДНИЧЕСТВО -
отношение между сотрудничающими сторонами, строящиеся на определенных действиях лиц, чем-то неудовлетворенных или остро нуждающихся в средствах к существованию, или просто алчных и жадных, готовых на любые противоправные действия

Конфиденциальная информация банка

ПОДСЛУШИВАНИЕ
1)перехват или запись данных, передаваемых по тех. средствам связи.
2) несанкционированный перехват данных при их передаче.

СКЛОНЕНИЕ К СОТРУДНИЧЕСТВУ -
как правило, насильственное действие со стороны вербующей стороны, осуществляемое путем подкупа, запугивания, шантажа.

ВЫПЫТЫВАНИЕ
1)стремление под видом невинных вопросов получить определенные сведения.
2) техника получения информации посредством пытки или подготовленного пыточного воздействия.

НАБЛЮДЕНИЕ
КОПИРОВАНИЕ
ХИЩЕНИЕ
ПЕРЕХВАТ
ОЗНАКОМЛЕНИЕ
ПОДКЛЮЧЕНИЕ
ПОДДЕЛКА

ПРЕСТУПНЫЕ ПОКУШЕНИЯ НА КОМПЬЮТЕРНЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ

- совершение преступных действий, направленных на вывод из строя и уничтожение компьютерных и телекоммуникационных систем

Р Е А Л И З У Ю Т С Я

ПО СЕТЯМ ПИТАНИЯ

ПО ПРОВОДНЫМ ЛИНИЯМ

ПО ЭФИРУ

Одной из причин преступных покушений на компьютерные и телекоммуникационные системы является их уязвимость за счет широкого распространения глобальных открытых компьютерных сетей типа Интернет, построенных на основе телекоммуникационных магистралей общего пользования, а также из-за возможности применения средств вычислительной техники с программным обеспечением, позволяющим легко модифицировать, уничтожать или копировать обрабатываемую информацию

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ:

ст. 272, 273,274 УК РФ

-любое деяние, влекущее незаконное вмешательство в имущественные права, возникающие в связи с использованием ЭВМ;

-преступления, прямо или косвенно связанные с ЭВМ, включающих в себя незаконные акты, совершаемые либо с помощью системы электронной обработки данных, либо против неё;

- любое преступление, совершенное с помощью специальных знаний компьютерной технологии.

Преступные посягательства в сфере компьютерной информации банка можно условно объединить в два основных вида

завладение имуществом банка, путем воздействия на информацию

мотивы - корысть

причинение ущерба банку, путем разрушения его инфраструктуры и нарушения порядка управления деятельностью банка

мотивы – корысть, месть, хулиганские мотивы

ВИДЫ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

УНИЧТОЖЕНИЕ (разрушение):
- **технических средств;**
- **носителей информации;**
- **программного обеспечения;**
- **информации (файлов, данных);**
- **паролей и ключевой информации.**

ПОДМЕНА (модификация):
- **операционных систем;**
- **систем управления базами данных;**
- **прикладных программ;**
- **информации (данных), отрицание факта отправки сообщения;**
- **паролей и правил доступа.**

КРАЖА:
- **технических средств;**
- **носителей информации;**
- **информации;**
- **средств доступа.**

НАРУШЕНИЕ НОРМАЛЬНОЙ РАБОТЫ (прерывание):
- **скорости обработки информации;**
- **пропускной способности каналов связи;**
- **объемов свободной оперативной памяти;**
- **объемов свободного дискового пространства;**
- **электропитания технических средств.**

ПЕРЕХВАТ ИНФОРМАЦИИ:
- **за счет побочных электромагнитных излучений от технических средств;**
- **за счет наводок по линиям электропитания;**
- **за счет наводок по посторонним проводникам;**
- **по акустическому каналу при обсуждении вопросов**
- **при подключении к каналам передачи информации**
- **за счет нарушения установленных правил доступа (взлом).**

ПРИЧИНЫ И УСЛОВИЯ СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Отсутствие надлежащего контроля за доступом сотрудников банка, не имеющими соответствующих полномочий.

Халатность сотрудников банка при выполнении требований по использованию средств вычислительной техники.

Низкий уровень прикладного программного обеспечения банковских компьютерных сетей, который не имеет контрольной защиты.

Несовершенство парольной системы от несанкционированного доступа к информационным ресурсам банка.

Отсутствие должностного лица, отвечающего за режим и безопасность банковской информации, в части защиты её от несанкционированного доступа.

Отсутствие четкой системы доступа по категориям персонала к документации строгой финансовой отчетности.

ВИРУС-НЕВИДИМКА – вирус, который скрывает созданные им изменения в файле или загрузочных записях.

ВИРУС-СПУТНИК – программа, которая вместо того, чтобы модифицировать какой-либо существующий файл, создает новую программу (совершенно неожиданно для пользователя).

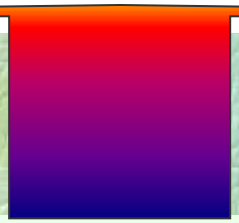
ПОЛИМОРФНЫЙ ВИРУС – программа-вредитель, которая продуцирует непохожие друг на друга копии самой себя, полагая, что программы-сканеры не смогут обнаружить разновидности этого вируса.
«Троян», «Кролик», «Червь» и др.

Логическая бомба - заранее внедряемая в информационно-управляющие центры, компьютерные сети, программно-технические средства, которые самостоятельно (в установленный период – пятница 13) или по специальному сигналу приводятся в действия, уничтожая, модифицируя информацию или дезорганизуя их работу

Временная бомба - разновидность логической бомбы, которая срабатывает при достижении определенного момента в установленное время (12.00 12.12.09)

КРАЙНЕ ОПАСНЫЙ ВИРУС

Червь известный под кодовым названием kido.bw появился после сразу после Нового года в Москве. Вредоносная программа маскируется под приложения системы Windows, а затем запускает себя по расписанию каждый час. Менее чем за сутки такой подпольной работы она способна отключить почтовые сервера, заставить прикладные программы забыть пароли пользователей и отключить обновления системы. Также после активации вируса зараженный компьютер перестает узнавать карты памяти, цифровые фотоаппараты и флешки, которые подсоединяются к компьютеру. Червь пытается обезопасить свою деятельность. Наконец kido.bw начинает посылать запросы на корейские сервера. Таким образом, он либо докладывает об успешном выполнении заражения компьютера, либо «гоняет» Интернет трафик



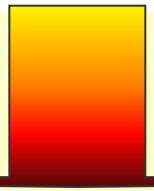
Вирус kido.bw довольно молодой и все его способности еще не изучены. Фирма Microsoft уже выпустила «заплатку» блокирующую вирус. Однако она защищает от будущих угроз, и не исправляет текущей ситуации. Те системы, которые уже заражены, придется сначала вылечить. Но это не тривиальная задача. Даже удаленный специальным софтом червь, возрождается как птица Феникс и начинает работу по расписанию как ни в чем не бывало

Опасности подвергаются только компьютеры с Windows.
На конкурентные операционные системы такие как Linux и Mac OS X червь не действует

ПРОТИВОДЕЙСТВИЕ КОМПЬЮТЕРНЫМ ВИРУСАМ

Наиболее часто для борьбы с компьютерными вирусами применяются *антивирусные программы*, *программы-вакцины* (фильтры), *противоинфекционные* (постоянно контролирующие процессы в системе), реже – аппаратные средства защиты.

Основной способ защиты от вирусов в локальных вычислительных сетях банка является антивирусное программное обеспечение, которое размещается на сетевом сервере. Антивирусный продукт обязан быстро реагировать на новые вирусы, что предполагает регулярное обновление антивирусных баз. В тоже время, хорошему антивирусу необходим набор определенных механизмов.



Эвристический механизм для борьбы с еще не известными программе вирусами. *Принцип действия эвристики (в общем) таков: по характерным для вирусов участкам кода можно с определенной степенью вероятности утверждать о наличии неизвестного программе вируса в объекте. В любом подобном механизме возможны ложные срабатывания; однако процент таких отказов должен быть минимальным, и именно он определяет качество эвристики.*

ПРОТИВОДЕЙСТВИЕ КОМПЬЮТЕРНЫМ ВИРУСАМ

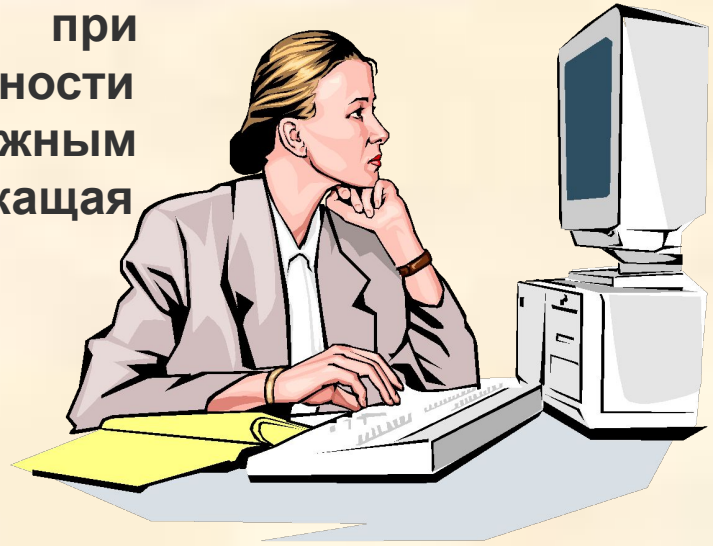
Наиболее часто для борьбы с компьютерными вирусами применяются *антивирусные программы*, *программы-вакцины* (фильтры), *противоинфекционные* (постоянно контролирующие процессы в системе), реже – аппаратные средства защиты.

Основной способ защиты от вирусов в локальных вычислительных сетях банка является антивирусное программное обеспечение, которое размещается на сетевом сервере. Антивирусный продукт обязан быстро реагировать на новые вирусы, что предполагает регулярное обновление антивирусных баз. В тоже время, хорошему антивирусу необходим набор определенных механизмов.

В настоящее время ФСБ России сертифицированы антивирусные средства двух российских компаний - Dr.WEB и Антивирус Касперского, которые обеспечивают надежную защиту информационной системы от вирусного заражения. В ФСБ России создана и функционирует в круглосуточном режиме защищенная криптографическими средствами система доставки обновлений к антивирусным средствам.

Требования к защите информации в информационно - телекоммуникационной системе (ИТКС) банка:

- защита информации при передачи ее по каналам связи, хранении и обработке (конфиденциальность информации);
- обеспечение целостности и подлинности передаваемой, хранимой и обрабатываемой информации;
- аутентификация сторон, устанавливающих связь (подтверждение подлинности отправителя или получателя информации);
- контроль доступа к ресурсам сети, оборудованию и данным абонентов;
- криптоживучесть при компрометации части ключевой системы;
- возможность доказательства неправомочности действий пользователей и обслуживающего персонала в сети;
- обеспечение взаимодействия между различными локальными информационными системами при одновременном исключении возможности «сквозного» проникновения к наиболее важным подсистемам, в которых циркулирует подлежащая защите информация



Стандарт DECT (Digital Enhanced Cordless Telephony - цифровая усовершенствованная система беспроводной телефонии) рассчитан в основном на применение в офисах, учреждениях и производствах, позволяя организовать локальную сотовую сеть и обеспечить пользователей устойчивой цифровой связью.

Система связи на основе стандарта DECT обеспечивает покрытие широкой географической зоны, позволяет осуществлять роуминг и "бесшовную" динамическую передачу вызовов при переходе пользователя из зоны действия одной базовой станции в зону действия другой и представляет пользователю качество связи, не отличающееся от качества связи на фиксированных линиях.

Цифровая передача радиосигналов обеспечивает высокий уровень защиты вызова от прослушивания.

Пионером в разработке DECT по праву считается корпорация Ericsson, оборудование которой лидирует на рынке уже несколько лет.

Первой появилась система DCT-1800 (FreeSet), позволяющая поддерживать до 500-600 абонентов. Далее DECT был интегрирован в УАТС BusinessPhone 250. Сейчас в стандарте DECT работают системы удаленного радиодоступа DRA-1900.

СТАНДАРТ DECT ОТЛИЧАЕТСЯ ОТ ДРУГИХ СИСТЕМ БЕСПРОВОДНОЙ ТЕЛЕФОНИИ РЯДОМ ПРЕИМУЩЕСТВ

Нет привязки к определенной базовой станции, переход от одной соты в другую осуществляется плавно и незаметно. Решение о переходе принимает сама трубка, которая постоянно сканирует свободные каналы и выбирая оптимальный.

Обмен трубки с базовыми станциями ведется в цифровом стандарте пакетами фиксированной длины. Сигнал скремблируется и принудительно шифруется. Применяются устойчивые к взлому криптопротоколы с открытой передачей ключа.

Номинальная мощность излучения передатчиков равна 10 мВт и фиксирована, это абсолютно безопасный уровень для здоровья человека. Увеличение дальности связи достигается укрупнением сети или применением направленных антенн.

Плотность абонентов в сети может быть очень большой и достигать 10 000 абонентов на один квадратный километр.

В настоящее время ни одна система связи, используемая в частных учрежденческих сетях, не обладает подобными параметрами.

Особенности практики защиты информации и информационных систем в банковской сфере

- все сотрудники подписывают обязательство о неразглашении сведений в качестве условия приема на работу

- сотрудникам не разрешается приносить программные средства из дома или других внешних источников, а также выносить магнитные носители

- обучение сотрудников банка мерам безопасности проводится минимум раз в полгода

- все пользователи компьютерных систем имеют пароли, составленные методом случайной генерации

- все случаи нарушения информационной безопасности тщательно расследуются и докладываются руководству банка

- осуществляется постоянный контроль доступа к информации, со стороны сотрудников банка

- ежегодные проверки объектов банковской инфраструктуры по защите информации и информационных систем и т.д.

КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ БАНКА – это создание защищенной среды обработки информации, объединяющей разнородные меры противодействия (правовые, организационные, программно-технические) угрозам и обеспечивающей защиту объекта от нежелательных воздействий.

Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) изложены в документах:

- «ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ»;
- «ПОЛОЖЕНИЕ ПО АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ»;
- «ПОЛОЖЕНИЕМ О ГОСУДАРСТВЕННОМ ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ»;
- «ПОЛОЖЕНИЕМ О СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ»
- «СИСТЕМОЙ СЕРТИФИКАЦИИ ГОСТ-Р» и т.д.

Мобильные телефоны-источники утечки информации

Оказывается, чем «круче» мобильный телефон, тем больше шпионских функций на нем можно задействовать: визуальное фотографирование, акустический контроль, прослушивание всех входящих и исходящих телефонных разговоров, SMS и электронной почты с последующей архивацией, дистанционное задействование GPS-функций, дистанционное прослушивание разговоров через микрофон телефона, даже если основная батарея вынута.

Данные технологии контроля за мобильными телефонами разрабатывались в рамках борьбы с террористами и криминальными элементами и при производстве простых мобильных телефонов указанные функции были реализованы на аппаратном уровне и активизировались только по специальным запросам, которые были известны соответствующим западным спецслужбам. При развитии технологии мобильной связи с появлением смарт-телефонов и коммуникаторов, соединяющих функции телефона и компьютера, реализация «специальных» или, как их называют, «полицейских» функций легла и на операционные системы, которые используются в мобильных технологиях. Перераспределение специальных функций с аппаратной части на программную привела к тому, что опытные программисты стали ее ловко использовать и создали целый ряд так называемых «spy» (шпионских) телефонов на базе серийно выпускаемых мобильных телефонов известнейших в мире производителей, таких как NOKIA, SIEMENS, PANASONIC, MOTOROLA, SAMSUNG, SONY ERICSSON.

ОРТАТИВНЫЙ БЛОКИРАТОР СОТОВЫХ ТЕЛЕФОНОВ "БРИЗ"

омпактный портативный прибор для подавления сотовой связи на ерриториях, где ее использование нежелательно: в конференц-залах, а совещаниях, в учебных аудиториях, в режимных учреждениях, анках. Устройство также эффективно против приборов аудио- и идеонаблюдения, определения местоположения объекта, истанционного управления, работающих на основе сотовых елефонов.

Функциональные особенности: радиус подавления — до 15 м;
блокируемые стандарты — GSM 900, GSM 1800/1900; портативность, небольшие размеры, малый вес; возможность работы от сети 220В и в автономном режиме; индикация разряда аккумулятора; высокая надежность и эффективность. Производство: Россия.

ПОДАВИТЕЛЬ СОТОВЫХ ТЕЛЕФОНОВ "МОЗАИКА ИНТЕРЬЕР"

Устройство для подавления сигналов сотовой связи стилизовано под обычные настольные электронные часы. Оно поможет Вам заблокировать работу аппаратов мобильной связи, приборов незаконной прослушки, видеонаблюдения, исполнительных устройств, которые работают на частотах сотовой связи. Прибор создает узкополосные помехи приемным каналам мобильных телефонов, тем самым блокируя их работу.

Функциональные особенности: стилизован под настольные электронные часы с сохранением всех функций; подавляемые стандарты — GSM, CDMA, DAMPS, AMPS, NMT;
радиус подавления — до 15 метров (зависит от удаленности от базовой станции).

Учебный вопрос:

БЕЗОПАСНОСТЬ БАНКОВСКИХ ЗДАНИЙ, СПЕЦИАЛЬНАЯ ЗАЩИТА БАНКОВСКИХ ОБЪЕКТОВ

Инженерно-техническая защита – совокупность организационных, организационно-технических и технических мероприятий, обеспечивающих защиту персонала банка, материальных и экономических интересов банка и их клиентов от преступных посягательств.

Инженерно-техническая защита применяется для:

-охраны территории и наблюдения за ней;

- охраны зданий, внутренних помещений и наблюдения за ними;

- охраны оборудования, хранилищ и перемещаемых носителей информации;

- контроль доступа в защищаемые зоны, охраняемые помещения и хранилища;

- создание препятствий визуальному наблюдению, подслушиванию и фотографированию;

- исключение возможности перехвата электромагнитных излучений средств связи, информации и ЭВТ и т.д.

Основные средства инженерно-технической защиты банка:

-физические средства защиты;

- аппаратные средства защиты;

- программные средства защиты;

- криптографические (математические) методы защиты.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СТАЦИОНАРНЫХ ОБЪЕКТОВ (БАНКОВ) ПРЕДСТАВЛЯЕТ СОБОЙ МНОГОГРАННЫЙ ПРОЦЕСС РЕАЛИЗАЦИИ ОХРАННЫХ МЕРОПРИЯТИЙ, ПО БОЛЬШЕЙ СТЕПЕНИ ПРЕДУПРЕЖДАЮЩЕГО ХАРАКТЕРА.

В основе разработки системы защиты объекта и организации её функционирования лежит принцип создания последовательных рубежей безопасности, на которых угрозы должны быть своевременно обнаружены. Такие рубежи должны располагаться последовательно, от забора вокруг территории объекта до главного, особо важного помещения, такого, как центральное хранилище.

Инженерно-техническая система охраны банка, ее насыщенность средствами инженерной и технической защиты определяются моделью «нарушителя», категорией и особенностями объекта охраны

МОДЕЛЬ «НАРУШИТЕЛЯ»

!

Модель «нарушителя» допускает разную степень детализации, но в целом она должна определять:

- категории (типы) нарушителей, которые способны воздействовать на объект;
- цели, которые могут преследовать нарушители каждой категории, возможный количественный состав, используемые инструменты, принадлежности, оснащение, оружие и проч.;
- типовые сценарии вероятных действий нарушителей, описывающие последовательность (алгоритм) действий групп и отдельных нарушителей, способы их действий на каждом этапе

КЛАССИФИКАЦИЯ «НАРУШИТЕЛЯ»

!

По уровню подготовки и технической оснащенности "нарушителя" условно можно классифицировать или 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 банка (последние два типа нарушителей можно объединить термином "квалифицированный")

ОБОРУДОВАНИЮ ИНЖЕНЕРНО-ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ОХРАНЫ ПОДЛЕЖАТ:

- охраняемая территория;
- оконные проемы здания;
- двери (основные, запасные);
- двери чердачных, подвальных помещений, люки, вентиляционные шахты и короба;
- помещения кассового узла;
- кассовый зал;
- помещение для хранения оружия;
- кабинет руководителя;
- кабинет главного бухгалтера

Другие помещения банка оборудуются инженерно-техническими средствами охраны по решению руководства учреждения банка, согласованному с вневедомственной охраной

В целях повышения надежности охраны, пропускного режима и технической укрепленности учреждений банка применяются:

- Инженерные средства охраны
- Технические средства охраны
- Телевизионные системы охраны и наблюдения
- Средства контроля доступа

Техническая укрепленность банка – это состояние охраняемой территории, здания, помещений, обеспечивающее необходимое противодействие несанкционированному проникновению в охраняемую зону, взлому и другим преступным посягательствам, которое достигается проведением совокупности инженерных и технических мероприятий.

Техническая укрепленность обеспечивается выполнением требований ведомственных норм проектирования «Здания учреждений Центрального банка Российской Федерации» (ВНП-001-01/Банк России) и руководящих документов МВД России

РД 78.143-92 Системы и комплексы охранной сигнализации. Нормы проектирования. Элементы технической укрепленности объектов

РД 78.145-93 Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ

РД 78.147-93 Единые требования по технической укрепленности и оборудованию сигнализацией охраняемых объектов

В целях повышения надежности охраны, пропускного режима и технической укрепленности учреждений банка применяются:

Инженерные средства охраны

К инженерным средствам охраны относятся:

-ограждения различного типа;

-инженерное оборудование постов охраны и постов караульных собак;

-металлические и бронированные двери, ворота, калитки, решетки;

-защитное остекление;

-металлические шторы, барьеры;

-механические, электромеханические и электронные запоры кладовых ценностей и других помещений;

-охранное освещение;

-средства механизации и автоматизации КПП по пропуску людей и транспорта;

- оборудование постов с пропускными функциями в задании учреждения банка, а т.ж. другие защитные конструкции и т.д.

В целях повышения надежности охраны, пропускного режима и технической укрепленности учреждений банка применяются:

- Инженерные средства охраны
- **Технические средства охраны**

К техническим средствам охраны относятся:

- средства охранной сигнализации;
- пожарной сигнализации;
- охранно-пожарной сигнализации;
- тревожной сигнализации;
- средства электропитания технических средств охраны;
- средства постовой и оперативной связи;
- кабельные сети, шлейфы, коммутационные приборы;
- другие технические и электронные средства.

Аппаратура охранной, охранно-пожарной и тревожной сигнализации, телевизионные системы охраны и наблюдения, системы контроля управления доступом могут быть объединены в единый комплекс технических средств охраны учреждения банка

Вывод информации с составных частей комплекса технических средств охраны осуществляется на центральный пункт управления или отдельные пульты управления систем

Для своевременного обнаружения нарушителя в охраняемом учреждении банка создаются **РУБЕЖИ СИГНАЛИЗАЦИИ**

Под **рубежом сигнализации** понимается совокупность технических средств охраны, позволяющих выдать адресное извещение о проникновении на отдельные номера пультов центрального наблюдения или приемно-контрольных приборов, размещенных в пунктах централизованной охраны, постах охраны банка или в дежурных частях ОВД МВД

Первый рубеж – защита строительных конструкций периметров помещений, оконные и дверные проемы, люки, вентиляционные каналы, тепловые вводы, тонкостенные перегородки и другие элементы помещений, доступные для проникновения с внешней стороны, в т.ч. и тех из них, которые оборудованы стальными решетками

Второй рубеж – с помощью специальных приборов охранной сигнализации защищаются помещения внутри здания

Третий рубеж – перекрывает охраняемые хранилища внутри помещений, средства и материальные ценности.

При наличии в охраняемых помещениях нескольких рубежей сигнализации каждый из них создается **извещателями**, работающими на различных физических принципах

Извещатель – устройство для формирования извещения о тревоге при отклонении контролируемого параметра от допустимой нормы или для инициирования сигнала тревоги потребителем

Извещатели:

– магнитно-контактные;
- пассивные инфракрасные;
- акустические;
- ультразвуковые;
- комбинированные;
- прочие.

Извещатель ультразвуковой – охранное устройство, используемое для создания локальных зон обнаружения или блокирования небольших помещений объемом до 6 кубических метров, принцип действия которого основан на обработке поступающих сигналов от датчика

ОХРАННЫЕ СИСТЕМЫ:

- с микроволновыми датчиками (прерывание излучения);
- с высокочастотными датчиками (изменение электромагнитного поля при перемещении);
- с электрическими переключателями (натяжение проволочных элементов, нагрузка на направляющие);
- с электрическими проволочными петлями (пере- резание или деформация проволочных элементов);
- с микроволновыми датчиками.

Например: интегрированная система охраны «ОРИОН» - это охранная, тревожная, пожарная сигнализация, контроль доступа, видеонаблюдение, управление пожаротушением, инженерными системами зданий.
Кол-во АРМ – до 64; кол-во видеокамер – до 64; кол-во приборов – до 16129

Комплекс банковской безопасности «GOAL-Bank» - установлен в более 55-ти главных управлениях и расчетно-кассовых центрах ЦБ РФ по всей стране. (журнал «Мир и безопасность» № 1, 2006)

В целях повышения надежности охраны, пропускного режима и технической укрепленности учреждений банка применяются:

- Инженерные средства охраны
- Технические средства охраны
- Телевизионные системы охраны и наблюдения

К телевизионным системам охраны и наблюдения относятся:

- видео-, телекамеры;
- мониторы, системные блоки;
- цифровые видеомагнитофоны;
- видеонакопители;
- видеорегистраторы (цифровые видеорегистраторы длительного времени со встроенным мультиплексором);
- видеосерверы;
- кабельные сети, шлейфы, коммутационные приборы;
- компьютерная сеть, источники бесперебойного питания;
- инфракрасные осветители (излучатели) и др. устройства;
- программное обеспечение.

Телевизионная система охраны и наблюдения предназначена для обеспечения круглосуточного наблюдения и постоянной автоматической записи и видеорегистрации событий, происходящих в поле зрения телекамер.

Указанная система обеспечивает автоматическое приоритетное отображение на мониторах зоны, откуда поступают сигналы тревоги или о срабатывании датчика обнаружения (извещателя), а также запись ситуации на видеорегистратор с указанием времени, даты и номера камеры на каждом изображении

Устанавливать телекамеры в местах хранения и операций с ценностями категорически ЗАПРЕЩАЕТСЯ!

В целях повышения надежности охраны, пропускного режима и технической укрепленности учреждений банка применяются:

- Инженерные средства охраны
- Технические средства охраны
- Телевизионные системы охраны и наблюдения
- **Средства контроля доступа**

К средствам контроля доступа относятся:

- программное обеспечение;
- контроллеры (запоминать, обрабатывать и хранить);
- система учета рабочего времени «Таймекс»;
- считыватели карт доступа;
- пропуска-идентификаторы (карты или брелоки)
- шлюзы;
- турникеты, автоматические ворота, шлагбаумы;
- компьютерная сеть, источники бесперебойного питания;
- металлодетекторы, гамма-детекторы, детектор взрывчатых веществ;
- специальные датчики присутствия, инфракрасные барьеры, весовые системы и т.д.

Система контроля доступа должна обеспечивать идентификацию личности по различным признакам (электронной карте-пропуску, личному коду, электронным системам допуска типа «рука-ключ» и т. п.)

Указанная система должна обеспечивать проход через центральный КПП, входы в помещения кассового узла, тамбур-шлюзы, лифт-холлы, а т.ж. через турникеты (кабины) в два этапа: первый – вход в турникет (кабину), второй – выход из турникета (кабины)

Система контроля доступа должна иметь аварийную разблокировку всех турникетов (кабин) с поста охраны или дежурной смены службы безопасности учреждения банка

Пропуск сотрудников учреждения банка через пункты контроля доступа осуществляется:

- в помещение первой зоны доступа – по одному признаку идентификации (например – электронная карта);

- в помещение второй зоны доступа – по двум признакам (электронная карта и код);

- в помещение третьей зоны доступа – не менее чем по двум признакам идентификации

Существует несколько видов охраны, в том числе:

- охрана с помощью технических средств – с подключением на пульте централизованного наблюдения и с установкой автоматической сигнализации;
- охрана путем выставления постов (силами отдела охраны или милиции);
- комбинированная охрана

ЗОНЫ БЕЗОПАСНОСТИ

Зона безопасности объекта – пространство (территория), в пределах которого действуют внутренние положения, установленные режимом работы объекта, и выполняются целевые задачи, поставленные перед системой охраны

ЗОНЫ БЕЗОПАСНОСТИ :

- периметр;
- вход-выход (для персонала и клиентов должны быть раздельные входы плюс отдельно запасный выход для экстренной эвакуации персонала) Также желательно иметь специальный вход (въезд) для инкассаторской машины;
- операционно-кассовый зал (зона клиентов, операционная зона);
- зона руководства (дирекции);
- зона инкассации;
- хранилище ценностей.

Определение зон безопасности требует их категорирования и определение уязвимости по порядковой шкале оценок (высокая, средняя и низкая). Для оценки показателей уязвимости используются методы математического моделирования (специальные модели и методики).

Учебный вопрос:

БЕЗОПАСНОСТЬ ВЕДЕНИЯ ДЕЛОПРОИЗВОДСТВА

Одним из направлений защиты информации является четкая организация системы делопроизводства и документооборота.

Основные составные части делопроизводства:

- документирование информации;
- учет документов;
- организация документооборота;
- обеспечение надежного хранения документов;
- своевременное их уничтожение;
- систематическая проверка их наличия;
- контроль своевременности и правильности их исполнения

Документ – документированная информация, снабженная реквизитами и другими сведениями об её источнике

Документ – это материальный носитель зафиксированной информации (бумага, кино-, фотопленка, магнитная лента, лазерный диск), предназначенной для её передачи во времени и пространстве, при этом, документы могут содержать тексты, изображения, звуки и т.д.

Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается **электронным документом, равнозначных документу, подписанному собственноручной подписью**, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

Документирование - процесс записи (фиксации) и оформления документов, документальному подтверждению (обоснованию) чего-либо, отражению какого-либо факта, события, явления в документах

ДОКУМЕНТИРОВАНИЕ ИНФОРМАЦИИ

(ФЕДЕРАЛЬНОЕ АГЕНСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ)

ГОСТ Р ИСО 15489-1-2007 Система стандартов по информации, библиотечному и издательскому делу

Типовая инструкция по делопроизводству в Федеральных органах исполнительной власти РФ от 08.11. 2005 № 536

ГОСТ Р 6.30-2003 Унифицированные системы документации. Унифицированная система организационно-распорядительной документации

ГОСТ 6.38-90 Система организационно-распорядительной документации. Требования к оформлению документов

ГОСТ 6.10.4-84 Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники

Общероссийский классификатор управленческой документации ОК-2002

ГОСТы предполагают 31 реквизит, который делает информацию документом

Обязательные реквизиты предусмотрены п.2 ст.9 Федерального закона № 129 «О бухгалтерском учете»: наименование документа, код формы, дата составления, содержание хозяйственной операции, измерители (натуральные, денежные), наименование должностей, ответственных за совершение хозяйственной операции и правильность её оформления, их подписи.

Документ поддельный – фальшивый документ, изготовленный с соблюдением установленной формы, либо подлинный документ, но с частично измененными реквизитами (частичная подделка).

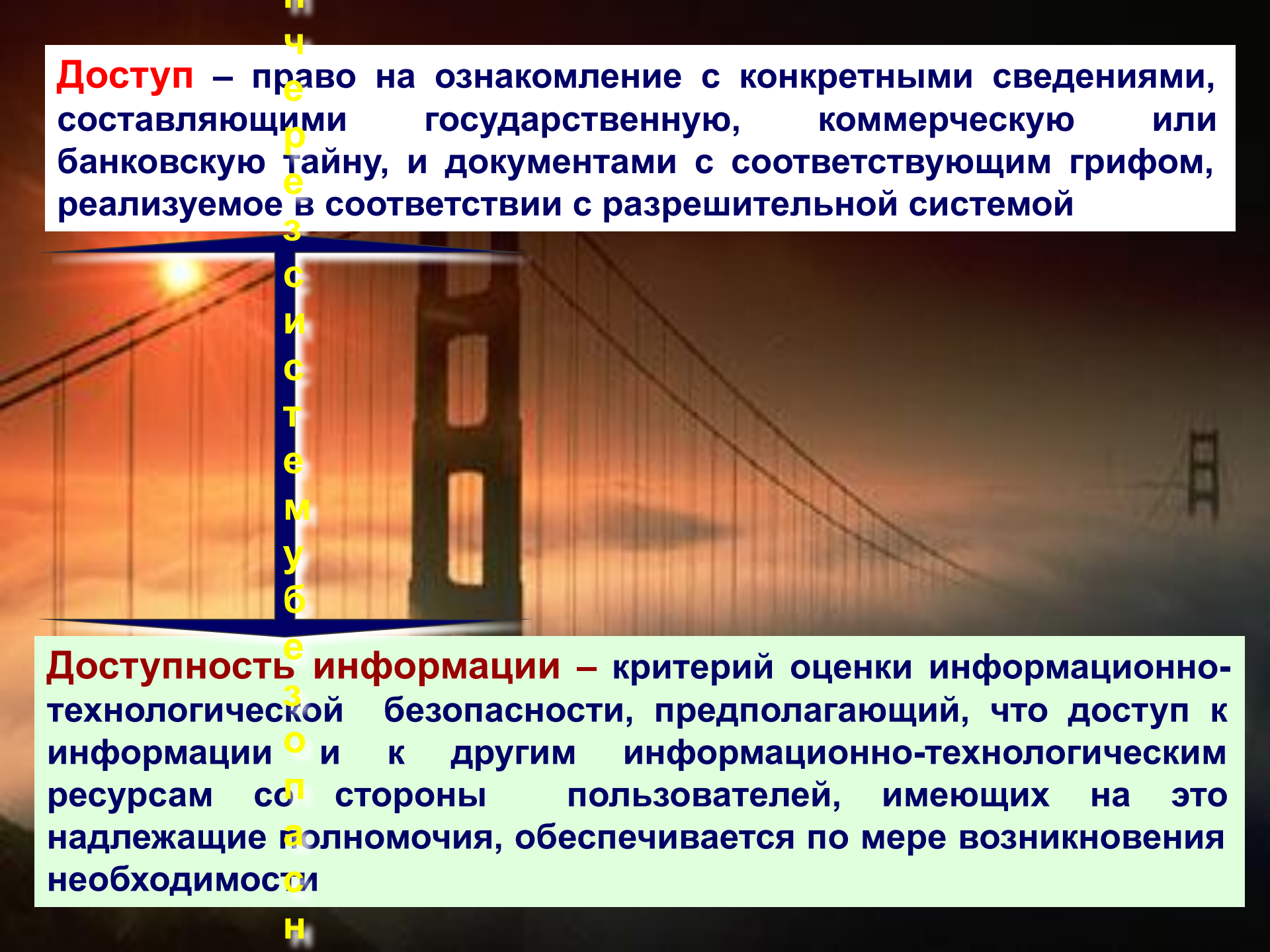
Основные признаки подделки документов

Несоответствие формы, цвета бланка и его реквизитов.
Противоречивость содержания, орфографические ошибки, нестандартный шрифт и т.д.
Следы подчистки – механическое удаление букв, слов, штрихов и т.д.
Травление текста документа – обесцвечивание химическими реактивами.
Следы смывания – удаление штрихов растворителями
Следы дописки или внесения записей на месте удаленного текста.
Изменение композиции – вклейка цифр, переклейка фотографии и т.д.
Подделка методами рисования и черчения.

Рекомендации

1. **Практически любой проверяемый документ может быть поддельным.**
2. **Знать основные способы подделки реквизитов, подписей, печатей и т.д.**
3. **Изучая документ, следует внимательно следить за наличием вышеуказанных признаков.**
4. **В случае обнаружения поддельного документа принять меры для сбора и фиксации доказательств.**
5. **Доклад непосредственному начальнику, в службу безопасности.**

Доступ – право на ознакомление с конкретными сведениями, составляющими государственную, коммерческую или банковскую тайну, и документами с соответствующим грифом, реализуемое в соответствии с разрешительной системой



Доступность информации – критерий оценки информационно-технологической безопасности, предполагающий, что доступ к информации и к другим информационно-технологическим ресурсам со стороны пользователей, имеющих на это надлежащие полномочия, обеспечивается по мере возникновения необходимости

Разглашение конфиденциальной информации через документы возможно:

при сообщении, оглашении (переписка, печать, переговоры и т.д.);
при пересылке документов;
при опубликовании документов, материалов;
при утере, утрате документов;
при бесконтрольном оставлении документов;
при бесконтрольной разработке документов;
при бесконтрольном документообороте;
при бесконтрольном хранении и уничтожении документов;
при бесконтрольном приеме поступающей документации.

Основные принципы управления защитой конфиденциальной информации:

- максимальное ограничение числа лиц допущенных к конфиденциальной информации;
- контроль и персональная ответственность каждого за сохранность информации;
- доведение информации до должностных лиц и исполнителей только в части их касающейся

Допуск сотрудников банка к сведениям, составляющим коммерческую тайну, осуществляется руководителем банка, его заместителями по направлениям работы, руководителями структурных подразделений

К сведениям, составляющих коммерческую тайну, допускаются лица, способные хранить коммерческую тайну, и только после оформления в службе безопасности индивидуального письменного обязательства по сохранению коммерческой тайны

Руководители подразделений и службы безопасности ответственны за подбор лиц, допускаемых к сведениям с грифом «КТ», обязаны обеспечить систематический контроль за тем, чтобы к этим сведениям получали доступ только те лица, которым такие сведения необходимы для выполнения своих функциональных обязанностей

КОММЕРЧЕСКАЯ ТАЙНА

- конфиденциальность информации, позволяющая её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

Режим коммерческой тайны – правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране её конфиденциальности

ПЛАН МЕРОПРИЯТИЙ ПО ЗАЩИТЕ КОММЕРЧЕСКИХ СЕКРЕТОВ

Определение целей плана по защите коммерческой тайны

Анализ сведений, составляющих коммерческую тайну

Обеспечение деятельности по защите коммерческой тайны

- предотвращение краж коммерческих секретов;
-предотвращение разглашения коммерческих секретов;
- предотвращение утечки коммерческих секретов через технические каналы

-определить, какие сведения являются коммерческой тайной;
- установить места их накопления и хранения;
- выявить каналы утечки сведений;
- возможности по перекрытию этих каналов;
- назначить сотрудников по обеспечению безопасности и сохранению коммерческой тайны

-контроль;
-работа с персоналом банка;
-организация работы с конфиденциальными документами;
-организация работы с конфиденциальной информацией;
-защита в организационно-правовых документах (контракты, договора и т.д.)

БАНКОВСКАЯ ТАЙНА

сведения связанные с банковской деятельностью, несанкционированное разглашение которых может нанести банку, предприятию или стране в целом экономический ущерб; обязанность банковских работников в интересах клиентов не разглашать сведений о состоянии их счетов и осуществляемых ими операциях.

Объект	**Банковский счет, вклад** **Операции по счетам** **Сведения о клиенте** **Система банковских связей**
Обладатели	**Только клиенты и их представители**
Условия получения сведений	**Госорганы и их должностные лица, исключительно в порядке, предусмотренном законом: - суды, арбитражные суды, следственные органы – по делам, находящимся в судопроизводстве; - налоговые органы – только по вопросам налогообложения**

В отношении должностных лиц, кредитных организаций может наступить ответственность в случае не предоставления сведений, составляющих банковскую тайну клиента, пользователям из числа государственных органов и их должностным лицам:

- **по запросам суда** - (штраф 50-100 МРОТ (ст.65 ГПК РФ), штраф до 200 МРОТ (ст.54 АПК РФ), административное взыскание (ст.161.1 КоАП РСФСР) или уголовная ответственность (ст.315 УК РФ - максимально - лишение свободы до 2 лет);

- **по запросам Счетной Палаты РФ** - уголовная ответственность (ст.287 УК РФ - максимально - лишение свободы до 8 лет);

- **по запросам налоговых органов** - штраф 5 МРОТ за каждую неделю просрочки (ст.4 Закона РФ “Об основах налоговой системы в РФ”);

- **по запросам федеральных органов налоговой полиции** - штраф до 100 МРОТ (ст.11 Закона РФ “О федеральных органах налоговой полиции”);

- **по запросам таможенных органов** - штраф до 3 МРОТ (ст.437 Таможенного Кодекса РФ);

- **по запросам органов предварительного следствия** - штраф до 50 МРОТ (ст.165.10 КоАП РСФСР).