Лекция 10. ЗАЩИТА ИНФОРМАЦИИ В ЭКОНОМИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Вопросы:

1. Понятие и правовое обеспечение безопасности ЭИС.

2. Анализ угроз безопасности

3. Методы и средства защиты

4. Проектирование системы защиты информации и ее оценка

Доп. литература: Мельников В.В. Безопасность информации в автоматизированных ИС – М:, Финансы и статистика, 2003.- 368 с.

1. Понятие и правовое обеспечение безопасности ЭИС

Безопасность (security) – состояние защищенности субъекта или объекта от воздействия негативных факторов, которые могут причинить ему вред.

Информационная безопасность (ИБ) - состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.

(Извлечение из документа: Постановление Правления ПФ РФ от 26.01.2001 N 15 "О введении в системе Пенсионного фонда Российской Федерации криптографической защиты информации и электронной цифровой подписи" (вместе с "Регламентом регистрации и подключения юридических и физических лиц к системе электронного документооборота Пенсионного фонда Российской Федерации")

Нормативно-правовые документы по ИБ:

1.Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 06.04.2011) "Об информации, информационных технологиях и о защите информации" (редакция с изменениями не вступившими в силу)

2."Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 03.05.2012) (с изм. и доп., вступающими в силу с 25.05.2012) Статья 13.12. Нарушение правил защиты информации

3."Таможенный кодекс Таможенного союза« (ред. от 16.04.2010) Статья 45. Защита информации и прав субъектов, участвующих в информационных процессах и информатизации

4. Федеральный закон от 03.04.1995 N 40-ФЗ (ред. от 08.12.2011) "О Федеральной службе безопасности" Статья 11.2. Обеспечение информационной безопасности

Нормативно-правовые документы по ИБ:

5. Федеральный закон от 08.12.2003 N 164-ФЗ (ред. от 06.12.2011) "Об основах государственного регулирования внешнеторговой деятельности"
Статья 17. Защита информации

6. Федеральный закон от 07.02.2011 N 7-ФЗ (ред. от 03.12.2011) "О клиринге и клиринговой деятельности" (с изм. и доп., вступающими в силу с 01.01.2012)
Статья 20. Защита информации

7. Федеральный закон от 21.11.2011 N 325-ФЗ "Об организованных торгах"
Статья 23. Защита информации

8. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации». (принят и введен в действие Распоряжением Банка России от 21.06.2010 N Р-705)

Статья 13.12. Нарушение правил защиты информации из Кодекса РФ об административных нарушениях :

1.Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), -влечет наложение административного штрафа на граждан в размере от 300-500 рублей; на должностных лиц - от 500 до 1000 рублей; на юридических лиц - от 5000до 10000 рублей.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации - влечет наложение административного штрафа на граждан в размере от 500 до 1000 рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от 1000 до 2000 рублей; на юридических лиц - от 10000 до 20000 рублей с конфискацией несертифицированных средств защиты информации или без таковой.

Статья 13.12. Нарушение правил защиты информации из Кодекса РФ об административных нарушениях :

3. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), - влечет наложение административного штрафа на граждан в размере от 500 до 1000 рублей с конфискацией средств защиты информации или без таковой; на должностных лиц - от 2000 до 3000 рублей с конфискацией средств защиты информации или без таковой; на юридических лиц - от 10000 до 20000 рублей с конфискацией средств защиты информации или без таковой.

Статья 13.14. Разглашение информации с ограниченным доступом (из Кодекса РФ об административных нарушениях) :

1. Разглашение информации, доступ к которой ограничен ФЗ (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, - влечет наложение административного штрафа на граждан в размере от 500 до 1000 рублей; на должностных лиц - от 4000 до 5000 рублей.

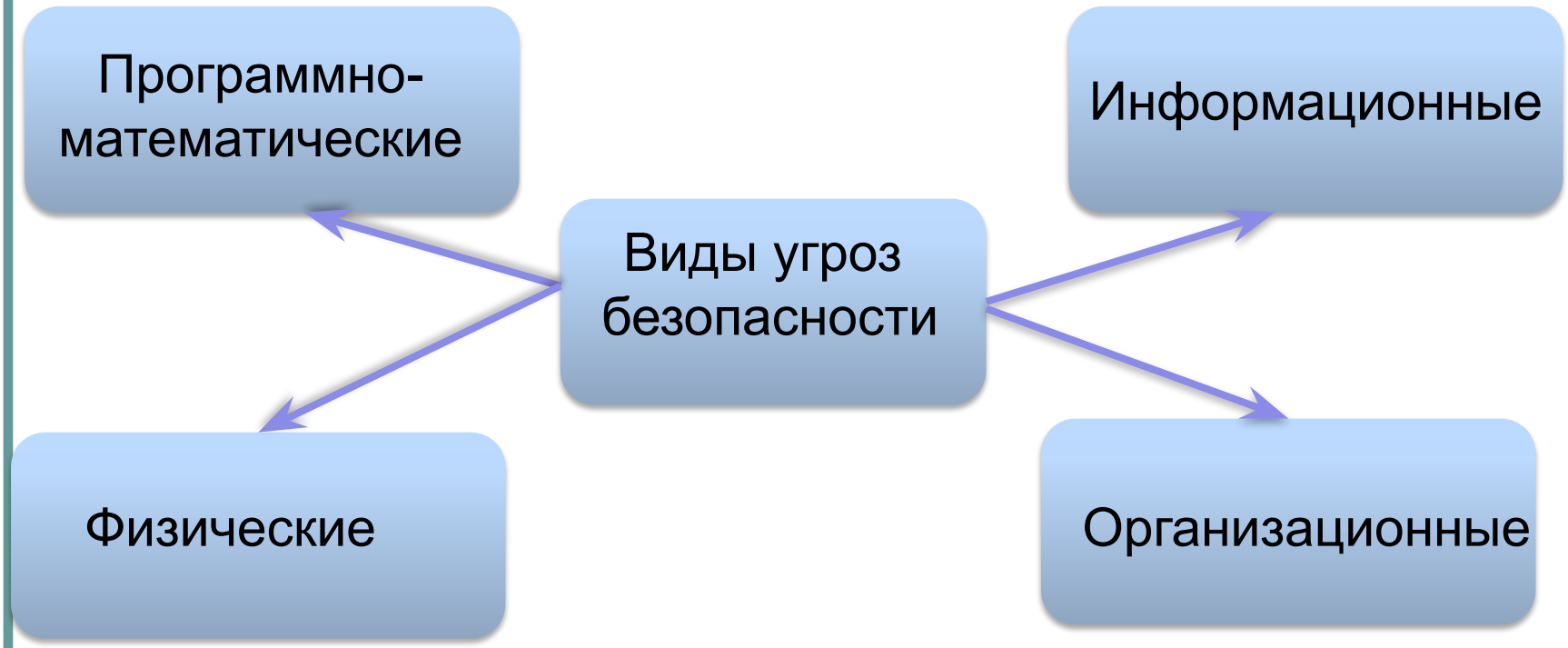
2. Угрозы безопасности

Безопасность ИС- защищенность системы от случайного или преднамеренного вмешательства в процесс ее функционирования, от попыток хищения информации, ее модификации или физического разрушения ее компонентов.

Угроза безопасности ИС- события или действия, которые могут привести к искажению, несанкционированному доступу или разрушению информационных ресурсов, а так же аппаратных и программных средств.

Возможные последствия реализации угроз:

- Разрушение, утрата информации (нарушение доступности и целостности);
- Модификация (подмена содержания информации, нарушение физической и логической целостности);
- Разглашение (утечка) информации, нарушение конфиденциальности;
- Блокирование доступа к информации;
- Нарушение прав собственности (несанкционированное копирование и распространение)


Программно-математические
Информационные
Виды угроз безопасности
Физические
Организационные

Информационные угрозы:

- осуществление НСД к информационным ресурсам и их противоправное использование;
- противозаконный сбор и нарушение адресности информационного обмена;
- хищение информационных ресурсов из банков и баз данных;
- нарушение технологии обработки информации.

Программно-математические угрозы:

- внедрение в аппаратные и программные ресурсы системы компоненты, выполняющие функции, не предусмотренные в документации системы(«логические бомбы»);
- разработка и распространение программ, нарушающих нормальное функционирование ИС и системы защиты информации.

Физические угрозы:

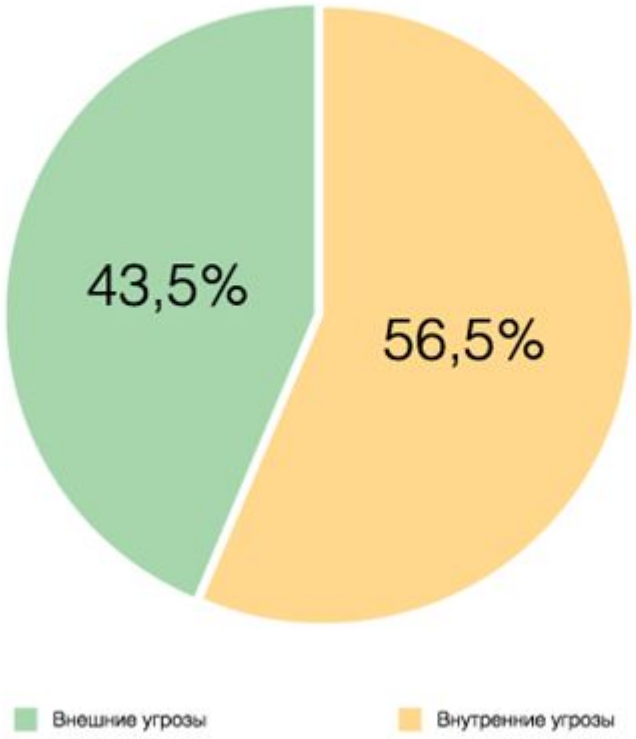
- уничтожение, повреждение, радиоэлектронное подавление или средств и систем обработки информации и телекоммуникаций;
- уничтожение, повреждение, разрушение или хищение машинных и бумажных носителей информации;
- хищение аппаратных и программных ключей и средств криптографической защиты;
- перехват информации в каналах связи и телекоммуникационных системах путем внедрения электронных устройств ;
- Перехват и навязывание ложной информации в сетях и линиях связи.

Организационные угрозы:

- не выполнение требований законодательства в информационной сфере;
- противоправные закупки несовершенных и устаревших ИТ, средств информатизации, телекоммуникаций и связи.

Классификация угроз ИБ

СООТНОШЕНИЕ ОПАСНОСТИ ВНУТРЕННИХ И ВНЕШНИХ УГРОЗ ИБ



Способы реализации преднамеренных угроз

а) применение подслушивающих устройств, дистанционная фото- и видеосъемка, т. п.;

б) хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и персональных ЭВМ);

в) перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

г) незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, имитации интерфейса системы и т. п. с последующей маскировкой под зарегистрированного пользователя («маскарад»);

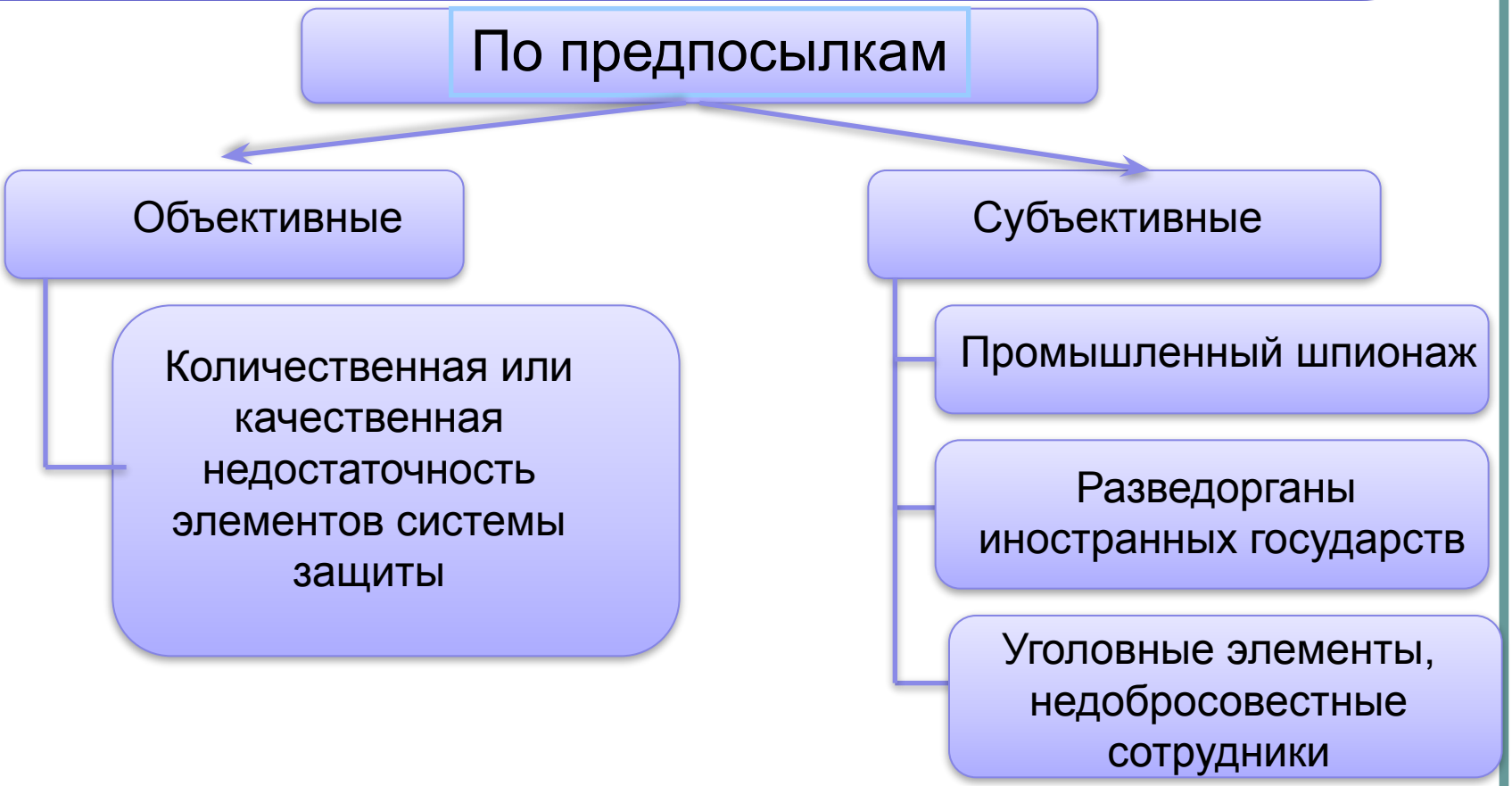
д) чтение остатков информации из оперативной памяти и с внешних запоминающих устройств (буфер памяти принтера);

ж) несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие, как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т. п.;

з)Использование программных ловушек, программных люков (Атака салями);

и) использование вирусов для разрушения системы защиты и самой ИС;

Классификация угроз ИБ



Классификация угроз ИБ

По источникам угроз:

1. Человеческий фактор
2. Технические устройства
3. Модели, алгоритмы программы
4. Технологии обработки информации
5. Внешняя среда

Внутренними нарушителями могут быть лица из следующих категорий персонала:

1. Вспомогательный и обслуживающий персонал (операторы, электрики, техники) системы;
2. Сотрудники отделов разработки и сопровождения программного обеспечения (прикладные и системные программисты);
3. Сотрудники службы безопасности АИТУ;
4. Руководители различного уровня должностной иерархии.
5. По данным исследований , проводимых в БИС более 80% нарушений совершается служащими банка.

Потенциальные угрозы информационной безопасности, вызванные использованием информационных технологий

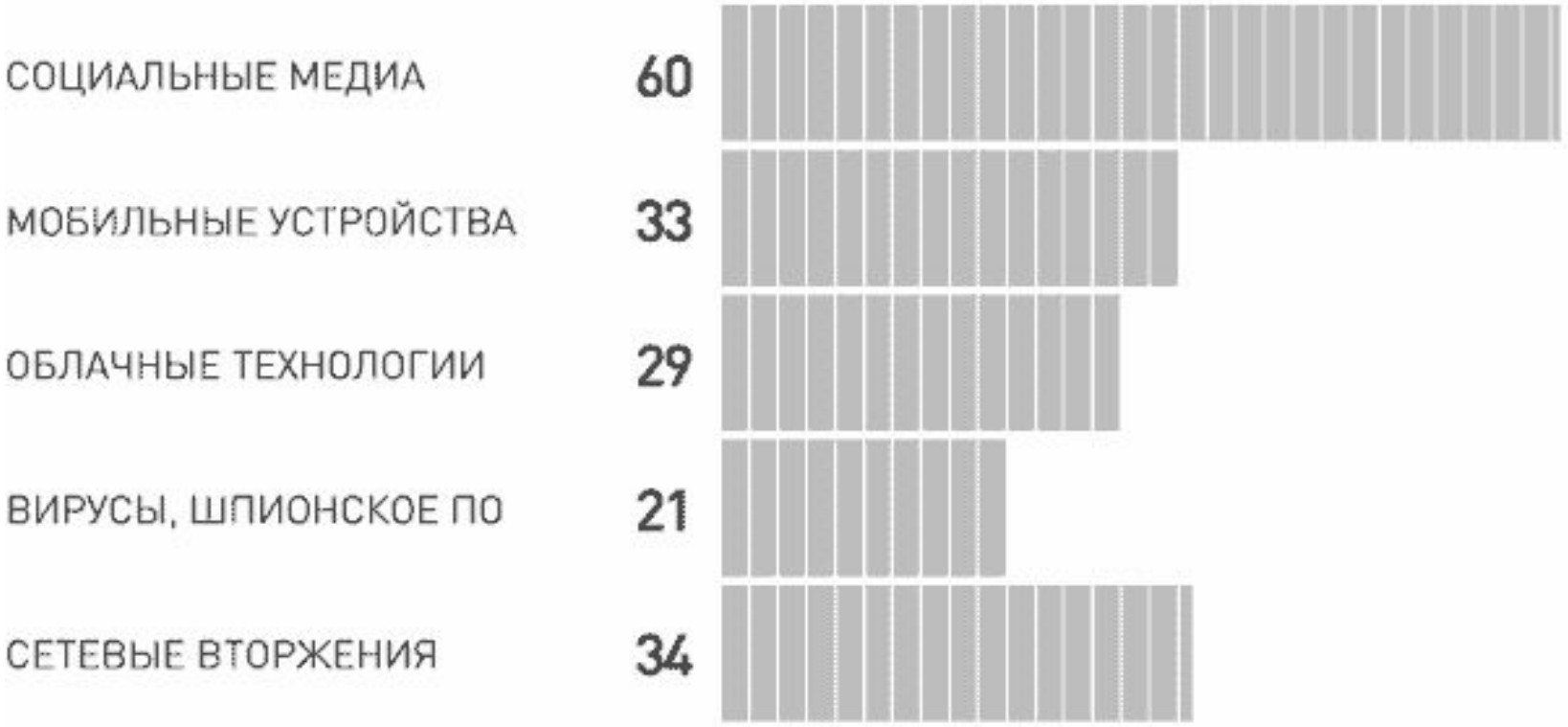
Виды компьютерных манипуляций	Категория персонала	Примеры	Результат
Ввод неправильных данных	Специалисты по ИТ, пользователи. другие сотрудники	Фальсификация исходного документа, изменение данных на носителе информации. введение данных в обход установленного порядка	Дезинформация и возможно дискредитация
Фальсификация программ	Специалисты по ИТ	«Логическая бомба» и др.	Вывод из строя ИС
Изменение первоначально правильных данных	Специалисты по ИТ пользователи	Фальсификация распечаток, замена данных, записываемых на носители, дистанционная передача измененных выходных данных	Дезинформация и возможно дискредитация
Похищение и передача информации заинтересованным лицам	Специалисты по ИТ, пользователи, другие сотрудники, посетители, партнеры	Несанкционированное копирование и вынос информации; атака хакеров	Потеря конкурентных преимуществ от информационной асимметрии
Незаконное использование машинного времени	Специалисты по ИТ пользователи	Использование ИС для дополнительных заработков; использование ресурсов Интернета в личных целях; использование оргтехники и расходных материалов в личных целях	Снижение экономической эффективности использования ИТ
Ошибочные действия персонала	Специалисты по ИТ, пользователи	Потеря распечаток; неправильное уничтожение документов; забывание документов в ксероксе; разглашение информации в личных беседах; отправка деловой корреспонденции по ошибочному электронному адресу	Потеря конкурентных преимуществ от информационной асимметрии, дискредитация

Внешними нарушителями могут быть:

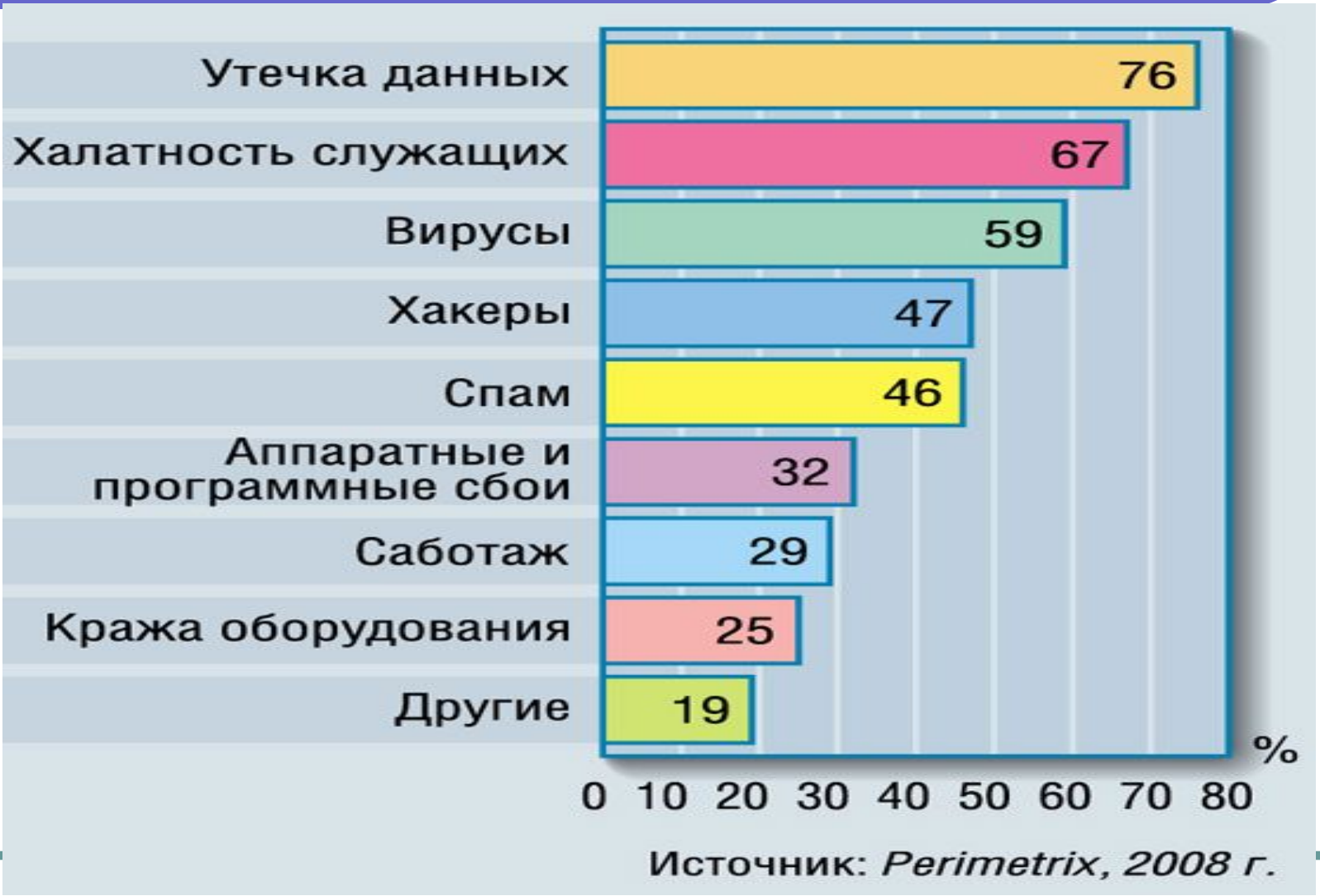
1. Клиенты (представители организаций, граждане);
2. Посетители (приглашенные по какому-либо поводу);
3. Представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжение и т. п.);
4. Представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;

ИСТОЧНИКИ IT-УГРОЗ ДЛЯ БИЗНЕСА В РОССИИ, %

Источник: Лаборатория Касперского



Угрозы и риски в системе ИБ банков и страховых организаций.

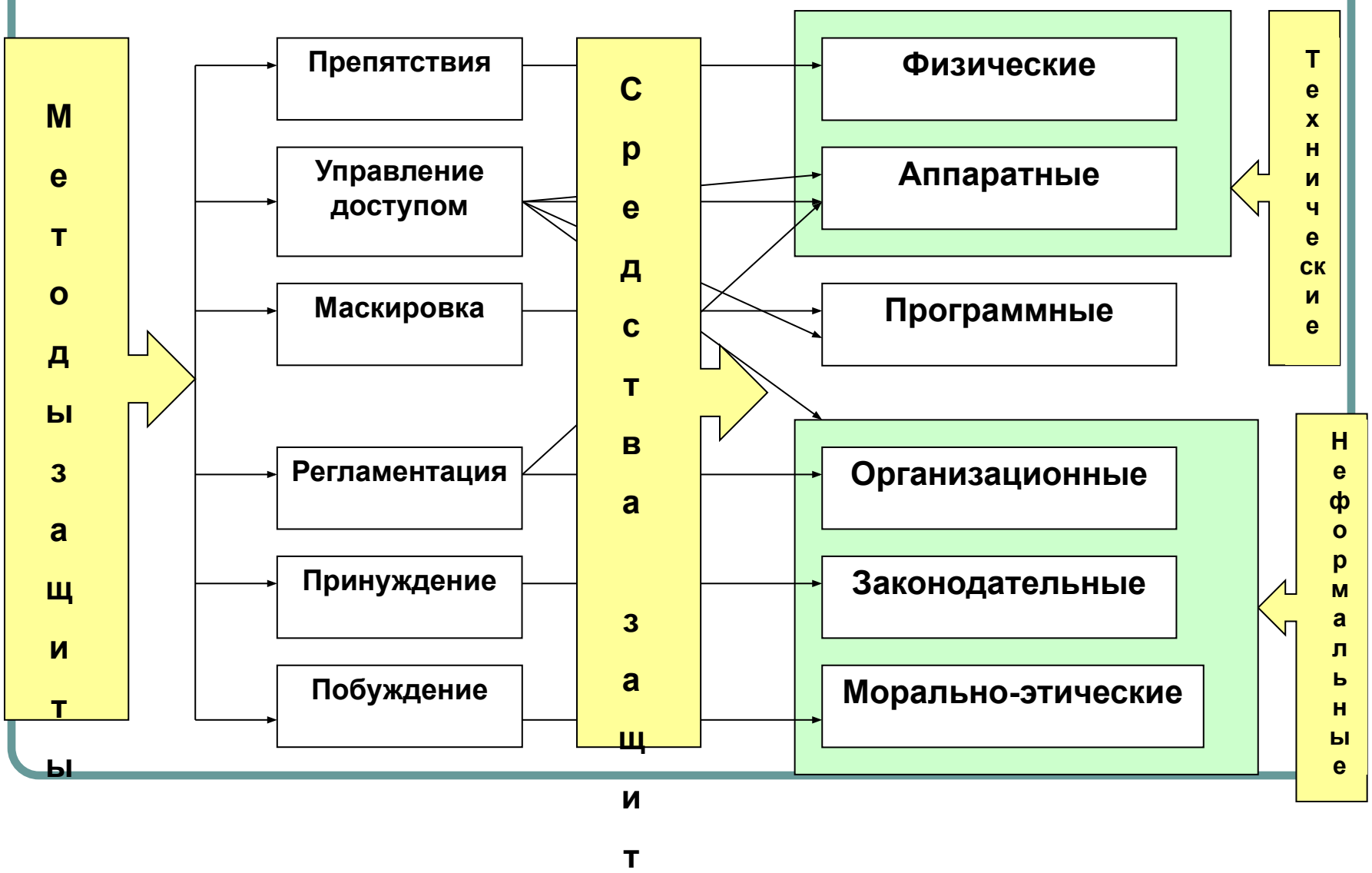


Экономические последствия реализации угроз

- Согласно новейшей статистике российского Министерства внутренних дел, в прошлом году россияне совершили более 17,5 тысяч компьютерных преступлений, что на 25 процентов больше чем в 2008 году.
- Руководство Citigroup признало, что в 2011 г. хакеры похитили 2,7 миллиона долларов со счетов 3 400 держателей кредитных карт банка, сообщает Bloomberg. Пресс-секретарь Citigroup в США Шон Кевелигэн (Sean Kevelighan) пообещал, что банк возместит понесенные клиентами убытки.
- В сентябре 2011 г. 29-летний Виктор Плещук (г. С-Пб)признал себя виновным в участии в международном хакерском преступлении, результатом которого стало незаконное снятие более чем 9 миллионов долларов в банкоматах, которыми управляет RBS WorldPay Inc., американское расчетно-кассовое подразделение британской финансовой группы Royal Bank of Scotland Group Plc.

3. Методы и средства защиты ЭИС

Система защиты ЭИС это совокупность (комплекс) специальных мер правового, административного характера, организационных мероприятий, физических и технических (программно-аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения безопасности информации, информационных технологий и систем.


Методы защиты
Препятствия
Управление доступом
Маскировка
Регламентация
Принуждение
Побуждение
Средства защиты
Физические
Аппаратные
Программные
Организационные
Законодательные
Морально-этические
Технические
Неформальные

Аппаратные средства защиты- устроиства, встраиваемые непосредственно в аппаратуру обработки информации

- Регистры хранения реквизитов защиты (паролей, грифов секретности и т.п.);
- Устройства для измерения индивидуальных характеристик человека (радужная оболочка глаз, формы лица и.т.п.);
- Экранирование ЭВМ;
- Установка генератора помех и др.

Физические средства защиты:

- Механические преграды, турникеты, специальное остекление;
- Сейфы, шкафы;
- Механические, электромеханические замки с дистанционным управлением, кодовые замки;
- Датчики различного типа;
- Теле- и фотосистемы наблюдения и регистрации;
- Устройства маркировки;
- Устройства с идентификационными картами;
- Системы охранного телевидения и охранной сигнализации;
- Системы пожаротушения и оповещения и др.

Программные средства защиты следующих классов:

1.Средства, реализуемые в стандартных операционных системах:

- Разграничение доступа пользователей к ресурсам по паролям;
- Разграничение доступа к информации по ключам защиты и др.

2.Средства защиты в специализированных ИС

- Идентификация пользователей и разрешение работы с информацией на определенном уровне;
- Формирование протоколов обращений к защищаемым данным с идентификацией данных о пользователе и временных характеристик;
- Физическая и программная блокировка работы пользователя при нарушении им определенной последовательности правил или действий;
- Подача сигналов при нарушении правил работы с системой;
- Ведение подробных протоколов работы системы и др.

3. Криптографические программы – основаны на использовании методов шифрования (кодирования)

Криптографические методы наиболее часто подразделяются в зависимости от количества ключей, используемых в соответствующих криптоалгоритмах :

1. Бесключевые, в которых не используются какие-либо ключи.
2. Одноключевые - в них используется некий дополнительный ключевой параметр - обычно это секретный ключ.
3. Двухключевые, использующие в своих вычислениях два ключа: секретный и открытый.


Криптографические методы
Бесключевые
Одноключевые
Двухключевые
Методы криптографического контрольного суммирования
Генерация случайных чисел
Симметричное шифрование
Методы криптографического контрольного суммирования
Генерация псевдослучайных чисел
Аутентификация
Асимметричное шифрование
Электронная подпись
Аутентификация

Механизмы безопасности в ЭИС

- Цифровая электронная подпись;
- Контроль и разграничение доступа;
- Система регистрации и учета информации;
- Обеспечение целостности данных;
- Аутентификация пользователей;
- Управление маршрутизацией;
- Арбитраж и освидетельствование.

4. Проектирование системы защиты информации и ее оценка

Требования к системе защиты информации	
Функциональные	•Обеспечение всех задач по защите ИС •Удовлетворение всем требованиям по
Эргономические	•Минимизация помех пользователям •Удобство для персонала
Экономические	•Минимальные затраты на систему
Технические	•Комплексное использование средств •Оптимизация архитектуры
Организационные	•Структурирование всех элементов •Простота эксплуатации

Этапы проектирования системы защиты информации (СЗИ)

1. Обоснование требований к защите и анализ условий защиты;
2. Определение функций защиты;
3. Определение перечня возможных каналов несанкционированного доступа к информации;
4. Обоснование перечня задач защиты;
5. Выбор средств защиты;
6. Оценка ожидаемой эффективности выбранных механизмов защиты;
7. Обоснование структуры и технологических схем функционирования системы защиты;
8. Технико-экономическая оценка проекта;
9. Разработка организационно-правового обеспечения системы защиты информации.

Рабочие документы службы безопасности информации (более 70 типовых документов):

GTS 1038 Политика и Регламент резервного копирования и восстановления данных
GTS 1040 Комплексный план защиты информационных ресурсов организации от несанкционированного доступа
GTS 1042 Политика обеспечения безопасности при взаимодействии с сетью Интернет
GTS 1043 Антивирусная политика, Инструкция по защите от компьютерных вирусов, Стандарт на антивирусное ПО
GTS 1044 Политика обеспечения безопасности платежных систем организации
GTS 1045 Парольная политика
GTS 1047 Политика, Процедура и План аудита информационной безопасности
GTS 1048 Соглашение о соблюдении режима информационной безопасности, заключаемое со сторонними организациями
GTS 1051 Руководство по защите конфиденциальной информации, Перечень сведений, составляющих конфиденциальную информацию, Соглашение о конфиденциальности
GTS 1053 Регламент использования мобильных устройств
GTS 1055 Политика информационной безопасности
GTS 1064 Положение о службе информационной безопасности

Аудит ИС

Критерии оценки безопасности ИС:

Критерии безопасности компьютерных систем Министерства обороны США (Оранжевая книга) определяют требования к аппаратному, программному и специальному обеспечению и выработки политики безопасности в компьютерных системах военного назначения. В ней приводятся следующие уровни безопасности систем:

- Высший класс- А;
- Промежуточный класс –В;
- Низкий уровень – С;
- Класс систем, не прошедших испытания –Д.

Критерии оценки безопасности ИС:

- Международная рабочая группа ISO/IES JTC разработала стандарт общих критериев оценки безопасности ИТ ИСО. МЭК 15408-99. Представляет универсальную библиотеку требований безопасности ИС.
- В России установлено 7 классов защищенности СВТ от НСД к информации. Самый низкий класс- седьмой, самый высокий- первый.

  При этом защитные мероприятия охватывают подсистемы:

  -Управления доступом;

  -Регистрации и учета;

  -Криптографическая;

  -Обеспечение целостности;

  -Законодательные меры;

  -Физические меры.

Требования к критериям оценки безопасности ИС:

Требование 1. *Политика безопасности.* Система должна поддерживать точно определенную политику безопасности.

Требование 2. *Метки.* С объектами должны ассоциироваться метки безопасности, используемые в качестве атрибутов контроля доступа.

Требование 3. *Идентификация и аутентификация*. Все субъекты должны иметь уникальные идентификаторы.

Требование 4. *Регистрация и учет.* Все события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе.

Требование 5. *Контроль корректности функционирования средств защиты.*

Требование 6. *Непрерывность защиты.*