

**При проведении оценки изделия ИТ  
главными являются следующие  
вопросы:**

**1) отвечают ли функции  
безопасности ОО функциональным  
требованиям?**

**2) корректна ли реализация функций  
безопасности?**

## Французскому натуралисту Арману Давиду подарили шкуру панды



11 марта 1869 года французский натуралист Жан-Пьер Арман Давид, путешествуя по Китаю, получил в дар от охотников шкуру доселе невиданного зверя. Об этом есть запись в его дневнике. Привезённая им в Париж, эта шкура впервые познакомила европейских зоологов с бамбуковым медведем — большой **пандой**. На самом деле большая панда формально не является пандой, а составляет совершенно отдельный вид. Прозвание «бамбуковый медведь» она получила за то, что основу её рациона составляют молодые побеги бамбука. **Панда** пользуется популярностью во всём мире за счет своего внешнего сходства с плюшевой игрушкой, и является неофициальной эмблемой Китая. Также панда относится к вымирающим видам, в свободном состоянии их осталось немногим более полутора тысяч.

# Антивирусы Panda признали себя вирусами

Безопасность

версия для КПК

12.03.15, Чт, 15:30, Мск, Текст: Сергей Попсулин /

**Антивирусные продукты Panda Security из-за сбоя в обновлении приняли за вирус собственные файлы. Некоторые системные администраторы попытались решить проблему с помощью перезагрузки, но это лишь ухудшило ситуацию — на компьютерах пропал доступ в интернет.**



## Читайте также:

- Softline защитила ИТ-инфраструктуру Правительства Камчатского края
- Google выпустил обновленный Android с новыми функциями
- Softline защитила персональные данные департамента финансов администрации Надымского района ЯНАО

Шесть продуктов испанской антивирусной компании Panda Security, включая Panda Antivirus Pro 2015, Panda Internet Security 2015 и Panda Global Protection 2015, после установки бракованного обновления в среду, 11 марта, обнаружили вирус в собственных файлах — psanmodrep.dll и alertsmanager.dll, — сообщает Register. Представитель компании подтвердил изданию эту информацию.

«Вчера мы выпустили обновление с ошибкой. В результате некоторые файлы программного обеспечения были распознаны движком Panda как вредоносные. Мы отозвали это обновление и выпустили вместо него исправное, добавив в него функцию восстановления файлов, помещенных в карантин по ошибке», — рассказал представитель Panda Security изданию Register.

Как пишет издание, на предприятиях, пользующихся продуктами Panda, вследствие выхода бракованного обновления возникли сложности — некоторые из них стали работать со сбоями, на других пропал доступ в интернет.

Один из читателей Register рассказал изданию, что проблемы возникли на каждом пятом компьютере в его компании — на 60 из 300. «Panda Antivirus одновременно на десятках компьютерах в пяти различных офисах сообщил об обнаружении вируса в собственных файлах. И если у вас схожая проблема, и вы перезагрузите компьютер, то у вас пропадет доступ в интернет», — сообщил он.

## Классификация основных стандартов:

1 группа – **оценочные стандарты.**

Они предназначены для **оценки и классификации** ИС и средств защиты информации по требованиям безопасности.

К ним относятся:

1) стандарт «Критерии оценки доверенных компьютерных систем» или «Оранжевая книга»;

2) международный стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» или «Общие критерии».

# Классификация основных стандартов:

2 группа стандартов – это так называемые **спецификации**. Они регламентируют различные вопросы реализации и использования методов и средств защиты информации.

К ним относятся:

1) рекомендации X.800, «Архитектура безопасности для взаимодействия открытых систем» – регламентирует **методы** и **средства** обеспечения ИБ в компьютерных сетях;

2) международный стандарт ISO/IEC 17799 «Практические **правила** управления информационной безопасностью», разработанный на основе одноименного британского стандарта BS 7799;

3) международный стандарт ISO/IEC 27001:2005 «Системы **менеджмента** информационной безопасности. Требования»

<b>Обозначение</b>	<b>Наименование на русском языке</b>
ГОСТ Р 50739-95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования
ГОСТ Р 50922-2006	Защита информации. Основные термины и определения
ГОСТ Р 51188-98	Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство
ГОСТ Р 51583-2014	Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения
ГОСТ Р 53110-2008	Система обеспечения информационной безопасности сети связи общего пользования. Общие положения
ГОСТ Р 53111-2008	Устойчивость функционирования сети связи общего пользования. Требования и методы проверки
ГОСТ Р 53113.1-2008	Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения

ГОСТ Р 53113.2-2009	Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов
ГОСТ Р 54581-2011 / ISO/IEC TR 15443-1:2005	Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы
ГОСТ Р 54582-2011 / ISO/IEC TR 15443-2:2005	Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия
ГОСТ Р 54583-2011 / ISO/IEC TR 15443-3:2007	Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия
ГОСТ Р ИСО 7498-1-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель
ГОСТ Р ИСО 7498-2-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации
ГОСТ Р ИСО/МЭК ТО 13335-5-2006	Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
ГОСТ Р ИСО/МЭК 15408-1-2012	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ГОСТ Р 53113.2-2009 «Информационная технология (ИТ). Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов».

Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.



**Угроза** - это потенциальная возможность определенным образом нарушить информационную безопасность.

- Свойством угрозы является **перечень уязвимостей**, при помощи которых может быть реализована угроза.
- **Уязвимость** – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы.

# Свойствами уязвимости:

- **вероятность (простота) реализации угрозы** через данную уязвимость (Вероятность реализации угрозы через данную уязвимость в течение года – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Указывается в процентах)
- **критичность реализации угрозы** через данную уязвимость (Критичность реализации угрозы – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах. Состоит из критичности реализации угрозы по конфиденциальности, целостности и доступности (ERc, ERi, ERa)).

Попытка реализации угрозы называется **атакой** , а тот, кто предпринимает такую попытку, - злоумышленником . Потенциальные злоумышленники называются источниками угрозы .

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется **окном опасности**, ассоциированным с данным уязвимым местом.

<LI>В состав форм регламентированной отчетности добавлены:

<UL>

<LI>форма статистики № МП(микро) "Сведения об основных показателях деятельности микропредп

<LI>форма статистики № 3-информ "Сведения об использовании информационных и коммуникационн

<LI>Для "алкогольных" деклараций реализована выгрузка в электронном виде в формате версии

<LI>Для форм бухгалтерской отчетности реализована возможность представления в органы стати

<LI>Исправлены выявленные ошибки.</LI></UL>

<H4><FONT color=#823602 face=Verdana>Смотрите также</FONT> </H4>

<OL>

<LI><STRONG>Релиз предназначен для обновления с конфигурациями версий 2.0.52.6 2.0.52.7 2

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда - недель), поскольку за это время должны произойти следующие события:

должно стать известно о средствах использования пробела в защите;

должны быть выпущены соответствующие заплаты;

заплаты должны быть установлены в защищаемой ИС.

# Выводы:

- почти **всегда существуют окна опасности**;
- отслеживание таких окон должно производиться **постоянно**, а выпуск и наложение заплат — как можно **более оперативно**;
- сведения о возможных угрозах, а также об уязвимых местах, через которые эти угрозы могут быть реализованы, необходимы для того, чтобы с одной стороны – выработать требования к создаваемой КСЗИ в ИС, с другой стороны – для того, чтобы выбрать **наиболее экономичные средства** обеспечения безопасности.

# КЛАССИФИКАЦИЯ ВИДОВ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## Внутренний отказ информационной системы

- нарушение от установленных правил эксплуатации
- выход системы из штатного режима эксплуатации
- ошибки при (пере)конфигурировании системы
- вредоносное программное обеспечение
- отказы программного и аппаратного обеспечения
- разрушение данных
- разрушение или повреждение аппаратуры

## Отказ поддерживающей инфраструктуры

- нарушение работы систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования
- разрушение или повреждение помещений
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности

## Статическая

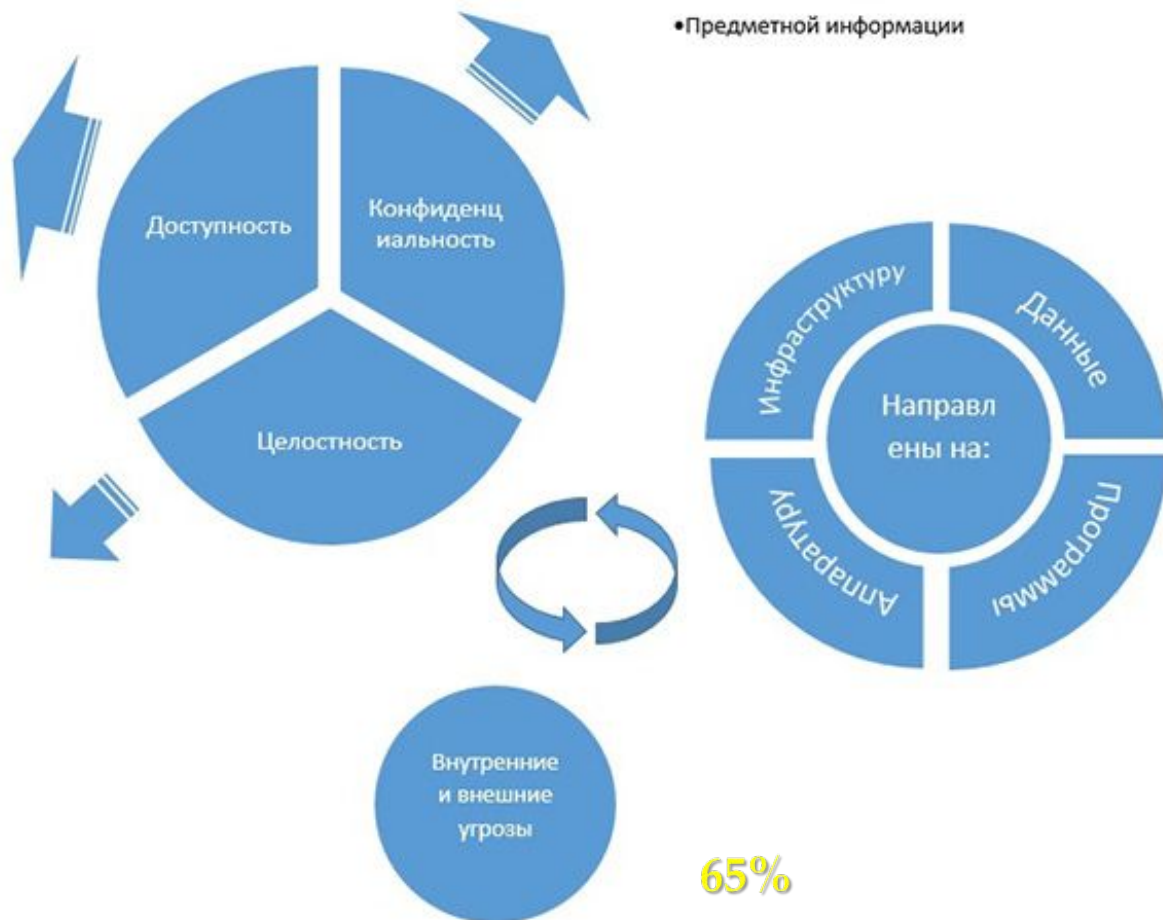
- Добавление неверных данных
- Изменение данных

## Динамическая

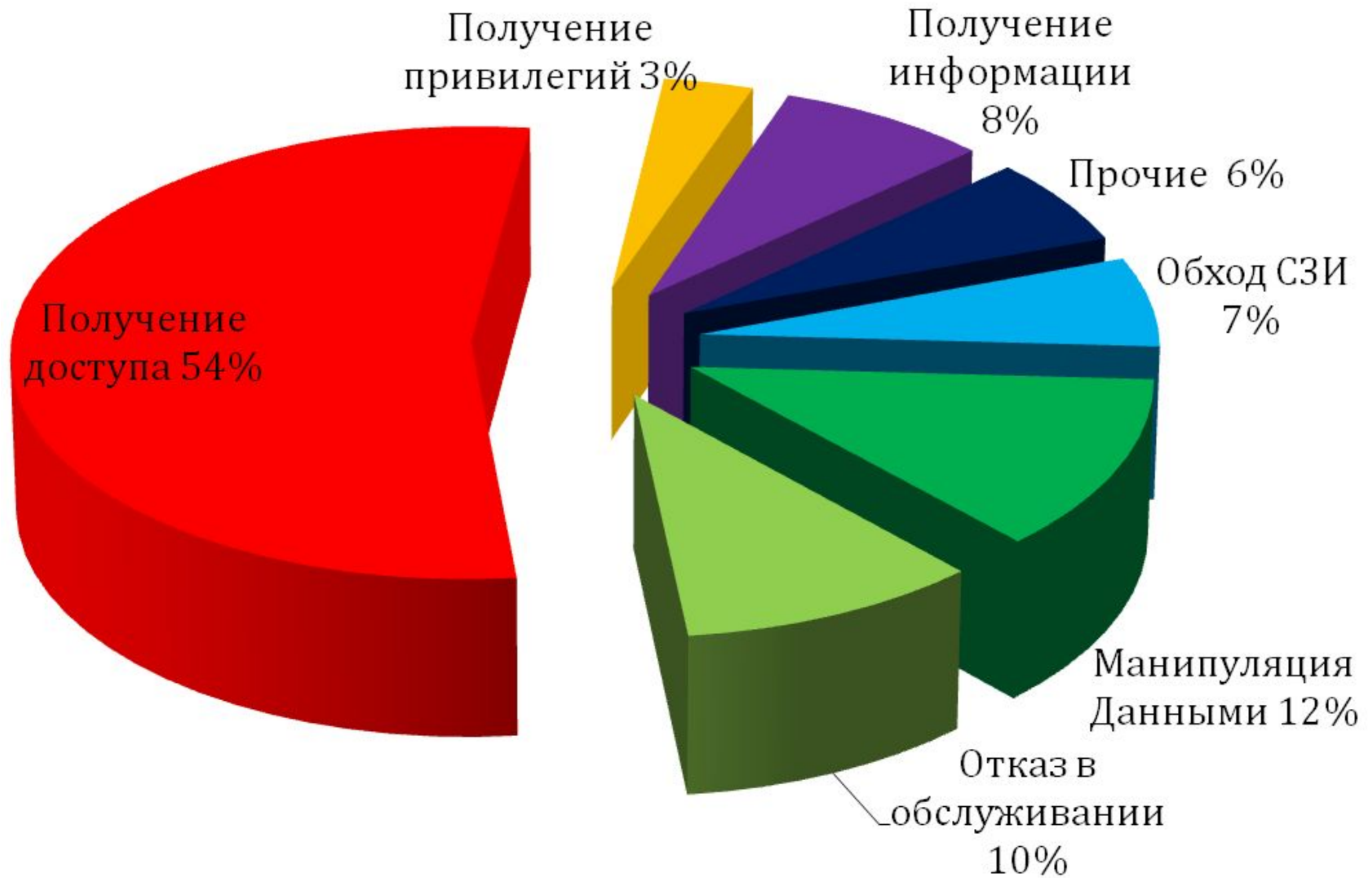
- переупорядочение
- кража
- дублирование
- внесение дополнительных сообщений

## Угрозы

- Служебной информации
- Предметной информации



# Типы уязвимостей



# Классификация угроз (по расположению источника угроз)

- **Внутренние угрозы безопасности объекта защиты:**  
неквалифицированная политика по управлению безопасностью корпорации;  
отсутствие должной квалификации персонала по обеспечению деятельности и  
управлению объектом защиты;





# Классификация угроз

- Главный специалист по ТЗИ – высшее образование по ИБ + стаж – 5 лет и руководящий стаж – 3 года
- Начальник отдела по ТЗИ – высшее образование по ИБ + стаж – 5 лет и руководящий стаж – 2 года
- Специалист по ТЗИ I категории – высшее образование по ИБ + стаж работы по II категории – 3 года
- Специалист по ТЗИ II категории – высшее образование по ИБ + стаж работы по ТЗИ – 3 года
- Специалист по ТЗИ – высшее образование по ИБ
- Администратор по ОБИ - высшее образование по ИБ + стаж работы специалистом – 3 года
- Инженер по ТЗИ – высшее образование по ИБ или среднее образование по ИБ + стаж работы техником по ЗИ I категории 3 года или стаж по другим должностям 5 лет
- Инженер-программист по ТЗИ I категории – высшее образование по ИБ (или техническое) + стаж инженером-программистом II категории 3 года
- Инженер-программист по ТЗИ II категории – высшее образование по ИБ (или техническое) + стаж инженером-программистом 3 года
- Инженер-программист по ТЗИ – высшее образование по ИБ или среднее образование по ИБ + стаж техником по ЗИ I категории 3 года
- Техник по ЗИ I категории – среднее образование по ИБ + стаж работы техником по ЗИ II категории 2 года
- Техник по ЗИ II категории – среднее образование по ИБ + стаж работы техником по ЗИ 2 года
- Техник по ЗИ – среднее образование по ИБ

Приказ Минздравсоцразвития от 22 апреля 2009 г. № 205 "Об утверждении единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел "квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации".

# Классификация угроз

## ДИПЛОМ О ПЕРЕПОДГОТОВКЕ ПО "ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ"

**ДИПЛОМ**  
О ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКЕ

ПП № 0000000

Диплом дает право на ведение нового вида профессиональной деятельности

Настоящий диплом выдан \_\_\_\_\_  
(Фамилия, имя, отчество)

в том, что он(а) с \_\_\_\_\_ г. по \_\_\_\_\_ г.  
прошел(а) профессиональную переподготовку в (на) \_\_\_\_\_  
(наименование образовательного учреждения (организации), осуществляющей дополнительное профессиональное образование)

по \_\_\_\_\_  
(наименование программы дополнительного профессионального образования)

Кемским решением от \_\_\_\_\_ г. удостоверяет право (соответствие квалификации) \_\_\_\_\_  
(Фамилия, имя, отчество)

на ведение профессиональной деятельности в сфере \_\_\_\_\_  
(наименование)

Присваивается квалификация \_\_\_\_\_

и ст. \_\_\_\_\_

Руководитель \_\_\_\_\_

Регистрационный номер \_\_\_\_\_

Город \_\_\_\_\_ год \_\_\_\_\_

# Классификация угроз

- преднамеренные и непреднамеренные действия персонала по нарушению безопасности и т.д.



# Классификация угроз

## Внешние угрозы безопасности объекта защиты:

- - негативные воздействия недобросовестных конкурентов и государственных структур;



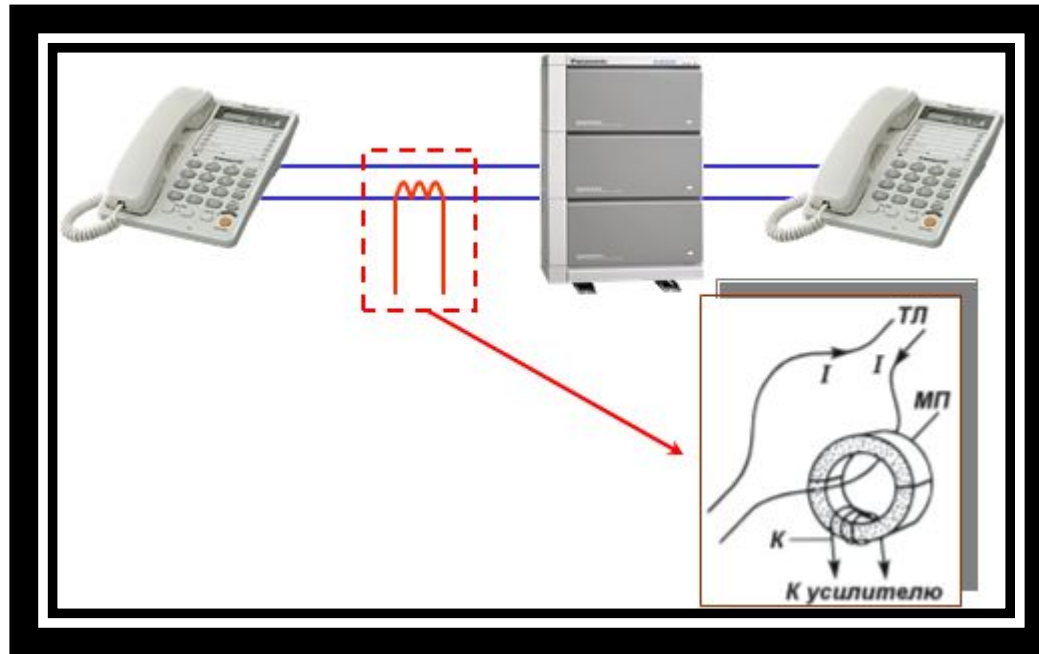
# Классификация угроз

- преднамеренные и непреднамеренные действия заинтересованных структур и физических лиц (сбор информации, шантаж, искажение имиджа, угрозы физического воздействия и др.);



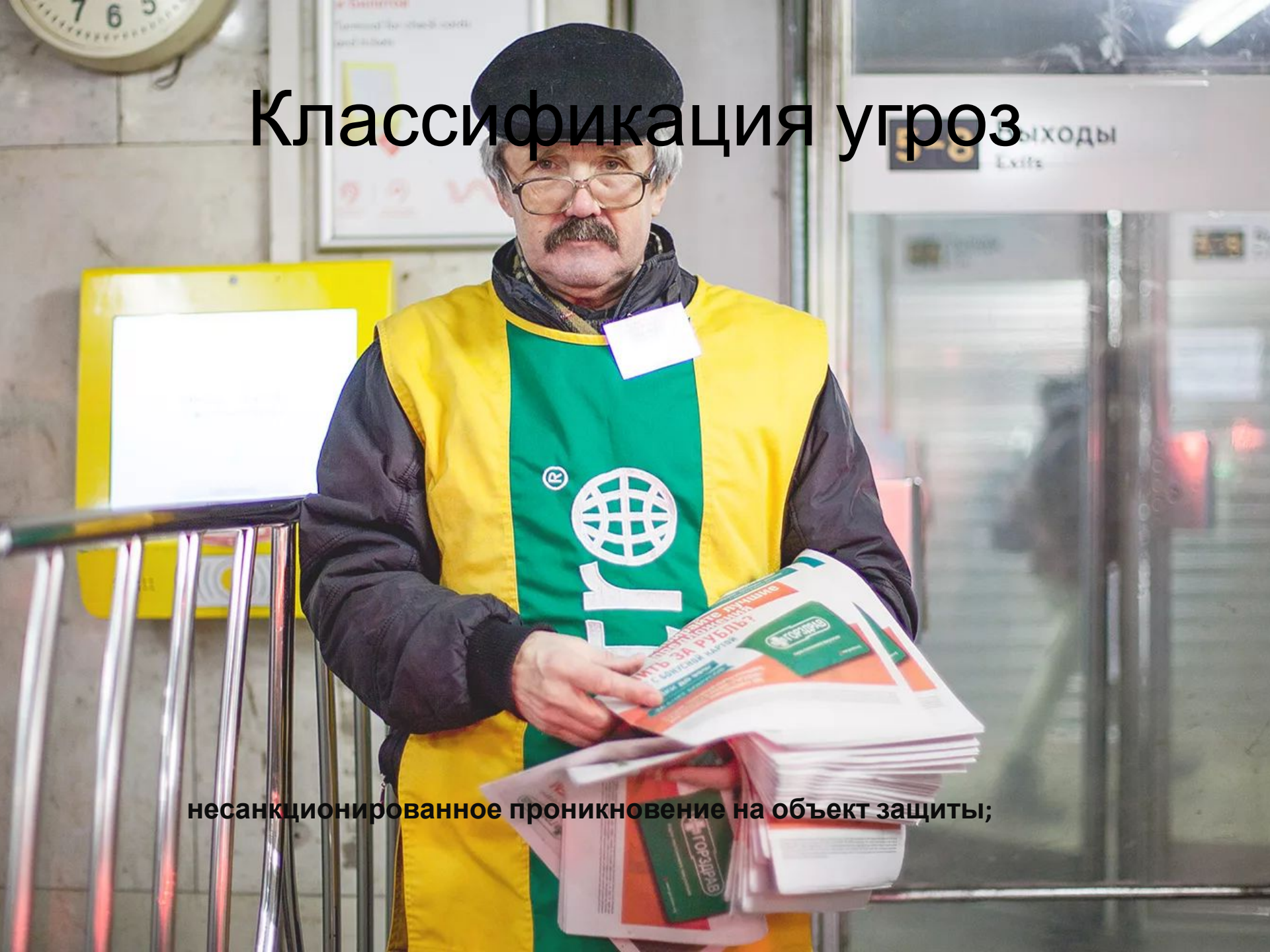
# Классификация угроз

- - утечка конфиденциальной информации из носителей информации и обусловленных каналов связи;



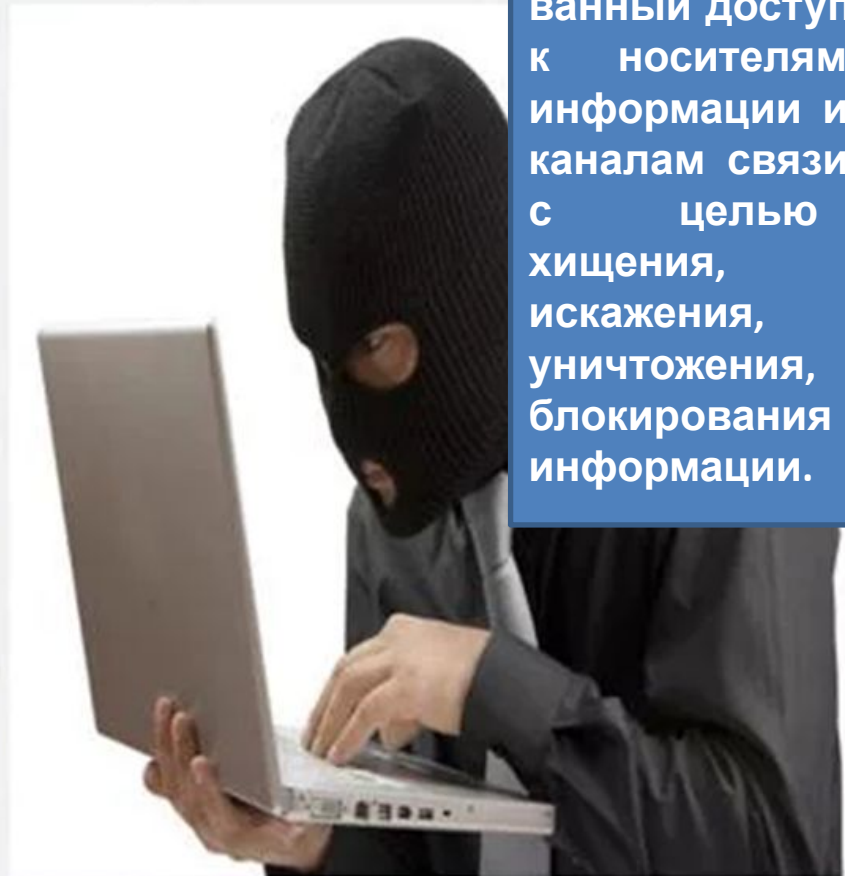
# Классификация угроз

несанкционированное проникновение на объект защиты;



## Причины несанкционированного доступа к информации

- ошибки конфигурации прав доступа
- слабая защищённость средств авторизации
- ошибки в программном обеспечении,
- злоупотребление служебными полномочиями
- прослушивание каналов связи
- использование клавиатурных шпионов, вирусов на компьютерах сотрудников.



несанкционированный доступ к носителям информации и каналам связи с целью хищения, искажения, уничтожения, блокирования информации.



# Основные угрозы конфиденциальности



Конфиденциальность — это защита от **несанкционированного** доступа к информации.

Конфиденциальную информацию можно разделить на **предметную** и **служебную**.

Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

*Невозможно помнить много разных паролей; рекомендации по их регулярной (по возможности — частой) смене только усугубляют положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двум-трем легко запоминаемым (и столь же легко угадываемым) паролям.*

# Основные угрозы конфиденциальности

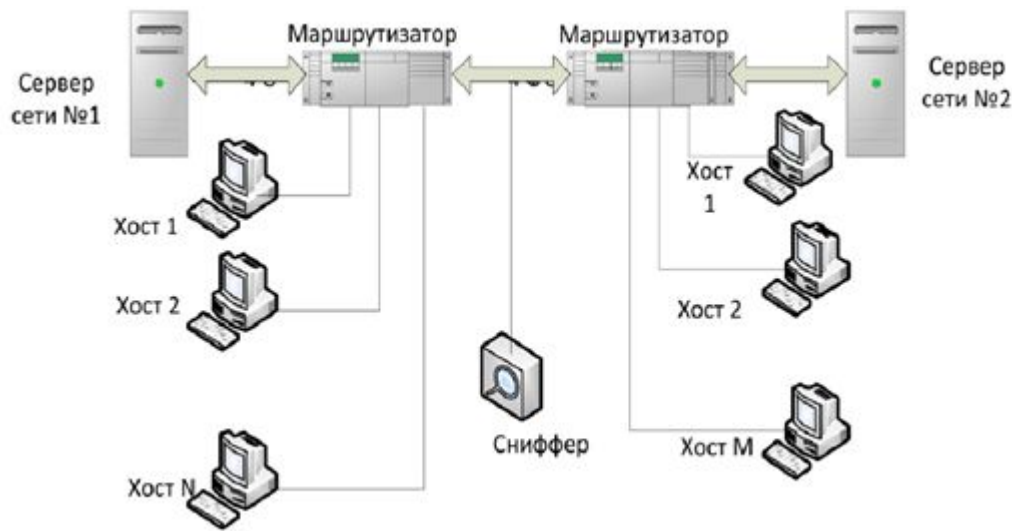
Описанный класс уязвимых мест можно назвать **размещением конфиденциальных** данных в среде, где им не обеспечена (зачастую — и не может быть обеспечена) необходимая защита.

**Выставки**

**хранение данных на резервных носителях**

# Основные угрозы конфиденциальности

**Перехват данных** — очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей.



# Основные угрозы конфиденциальности


**Кражи оборудования** являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных.



# Основные угрозы конфиденциальности

Опасной угрозой конфиденциальности являются методы **морально-психологического воздействия**, такие как маскарад — выполнение действий под видом лица, обладающего полномочиями для доступа к данным.



A close-up photograph of a man in a dark suit and white shirt opening the rear passenger door of a dark blue luxury car. The car's interior features beige leather seats and a matching door panel. A water bottle is visible on the center console. The man is holding a small object, possibly a key fob, in his hand. The background shows a blurred outdoor setting with greenery.

К неприятным угрозам, от которых трудно защищаться, можно отнести **злоупотребление полномочиями**.

# Модель угроз

Модель угроз - это **документ**, определяющий перечень и характеристики основных (актуальных) угроз безопасности и уязвимостей при их обработке в ИС, которые должны учитываться в процессе организации защиты информации, проектирования и разработки систем защиты информации, проведения проверок (контроля) защищенности ИС.

ФЕДЕРАЛЬНАЯ СЛУЖБА  
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

УТВЕРЖДЕНА  
Заместителем директора ФСТЭК России  
15 февраля 2008 г.

БАЗОВАЯ МОДЕЛЬ  
УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ  
ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ  
ПЕРСОНАЛЬНЫХ ДАННЫХ  
(выписка)

# Модель угроз

- Цель разработки модели угроз – определение **актуальных для конкретной ИС** угроз безопасности, источников угроз и уязвимостей. Результаты моделирования должны использоваться в качестве исходных данных для выработки требований ИБ к разрабатываемой системе защиты (СУИБ).



# Персональные данные

Согласно федерального закона от 27.07.2006 № 152-ФЗ (ред. от 29.07.2017) «О персональных данных», статья 4:

**Персональные данные** – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

«1С:Зарплата и управление персоналом 8» – программа массового назначения, позволяющая в комплексе автоматизировать задачи, связанные с расчетом заработной платы персонала и реализацией кадровой политики, с учетом требований законодательства и реальной практики работы предприятий. Она может успешно применяться в службах управления персоналом и бухгалтериях предприятий, а также в других подразделениях, заинтересованных в эффективной организации работы сотрудников, для управления человеческими ресурсами коммерческих предприятий различного масштаба.

➔ Место «1С:Зарплата и управление персоналом 8» в общей системе управления предприятием



«1С:Зарплата и управление персоналом 8» поддерживаются все основные процессы управления персоналом, а также процессы кадрового учета, расчета зарплаты, исчисления налогов, формирования отчетов и справок в государственные органы и социальные фонды, планирования расходов на оплату труда. Учтены требования законодательства, реальная практика работы предприятий и перспективные мировые тенденции развития подходов к управлению персоналом.

«1С:Зарплата и управление персоналом 8» соответствуют требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О защите персональных данных». В программе реализована возможность регистрации событий, связанных с работой с персональными данными (в частности, доступа и отказа в доступе к персональным данным), включая информацию о том пользователе, с которым данное событие было связано.

Добные и гибкие механизмы настройки отчетов позволяют получать полную и достоверную информацию в самых разных аналитических разрезах, для различных категорий пользователей: руководства, службы управления персоналом, кадровой службы и других.

**Оператором персональных данных** является — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

## Регистрация в Роскомнадзоре в качестве оператора персональных данных

Законом предусмотрено, что до начала работы с ПД необходимо обратиться в уполномоченный орган надзора и уведомить о начале работы с личной информацией. Это не значит, что каждая компания должна быть внесена в реестр операторов персональных данных Роскомнадзора. В этот список не включаются:

- работодатели. Они собирают и хранят информацию в соответствии с трудовым законодательством, например, при оформлении трудовых договоров, различных приказов кадрового характера;
- компании сотовой или стационарной телефонной связи, если данные получены исключительно для оказания услуг связи по заключенному договору, не распространяются и не предоставляются третьим лицам без согласия субъекта ПД;
- общественные объединения или религиозные организации, которые получают доступ к данным своих членов (участников) для достижения целей, предусмотренных в учредительных документах;
- организации и частные лица, пользующиеся общедоступными сведениями, которые субъекты ПД сами раскрыли, например, на персональных сайтах;
- любые компании, в которых действует система пропусков. Если паспортные данные гражданина переписываются для оформления однократного пропуска на территорию организации, регистрироваться не придется;

**Обработка персональных данных** — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Права на обработку персональных данных закреплено в положениях о государственных органах, федеральными законами, лицензиями на работу с персональными данными, которые выдает Роскомнадзор или ФСТЭК.

Федеральная служба  
по техническому и  
экспортному контролю  
Правительственный орган



\_\_\_\_\_

(или представителя субъекта персональных данных))

\_\_\_\_\_

(номер основного документа, удостоверяющего личность,

\_\_\_\_\_

и выдавшем его органе),

\_\_\_\_\_

подтверждающего полномочия представителя субъекта

\_\_\_\_\_

Я даю письменное согласие на обработку своих персональных данных свободно,  
своей волей и в своем интересе

\_\_\_\_\_

\_\_\_\_\_

с целью \_\_\_\_\_

\_\_\_\_\_

на обработку персональных данных \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

обработка персональных данных поручается \_\_\_\_\_

\_\_\_\_\_

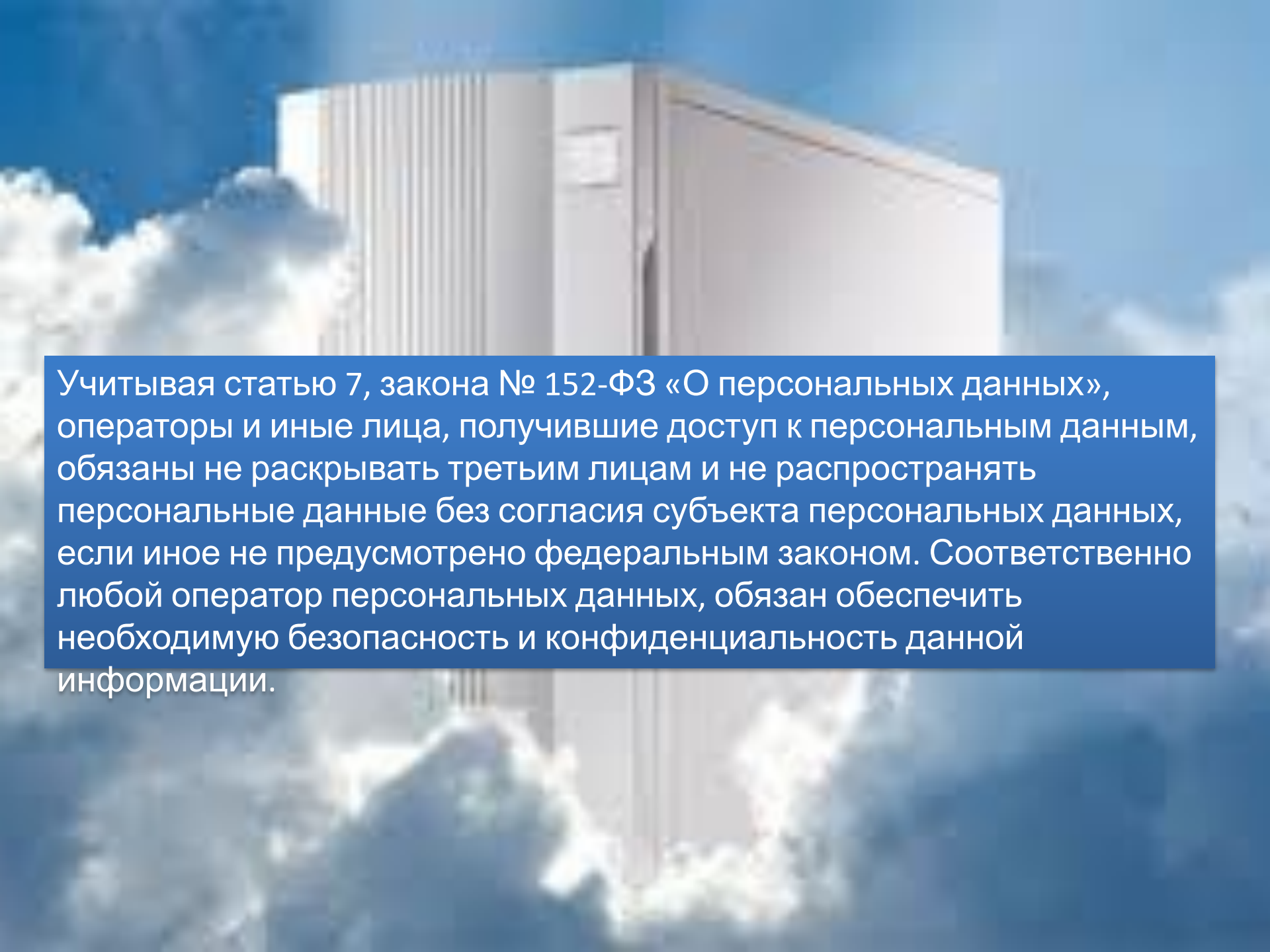
\_\_\_\_\_

\_\_\_\_\_

с персональными данными будут совершаться следующие действия \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_



Учитывая статью 7, закона № 152-ФЗ «О персональных данных», операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Соответственно любой оператор персональных данных, обязан обеспечить необходимую безопасность и конфиденциальность данной информации.

# Действия оператора по выполнению требований Федерального закона

## Начинать надо с определения:

- перечня персональных данных
- категорий обрабатываемых персональных данных
- целей их обработки

## Затем:

- необходимо направить уведомление в Уполномоченный орган

## После этого:

- разработать систему защиты персональных данных
- разработать документы, регламентирующие обработку персональных данных в организации
- реализовать требования по инженерно-технической защите помещений
- провести аттестацию или осуществить декларирование соответствия по требованиям безопасности информации





- Image quality
- NEF (RAW) + JPEG fine (OK)
- NEF (RAW) + JPEG normal
- NEF (RAW) + JPEG basic
- NEF (RAW)
- TIFF (RGB)
- JPEG fine
- JPEG normal
- JPEG basic

Nikon



В том случае, если фотограф или оператор сам осуществляет съемку, закон о ПД на него не распространяется вообще, до тех пор, пока он не **начинает накапливать и систематизировать изображения людей**. В первой статье закона о ПД говорится также, что не применяется он и в случаях обработки данных для личных и семейных нужд.

# Объяснение Роскомнадзора

- Изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта.
- До передачи персональных данных для установления личности снятого человека они не являются биометрическими персональными данными, поскольку не используются оператором (владельцем видеокамеры или лицом, организовавшим ее эксплуатацию) для установления личности.
- Однако материалы, используемые органами, которые осуществляют оперативно-розыскную деятельность, дознание и следствие в рамках проводимых мероприятий, являются биометрическими персональными данными, в случае если целью их обработки является установление личности конкретного физического лица.
- Обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина, за исключением случаев, указанных в законе.



# **Принципы защиты информации**

# Принцип минимальных привилегий



Каждая операция должна выполняться с наименьшим набором привилегий, требуемых для данной операции.

# Принцип прозрачности























СЗИ должна работать в фоновом режиме, быть незаметной и не мешать пользователям в основной работе, выполняя при этом все возложенные на нее функции.

## Performance

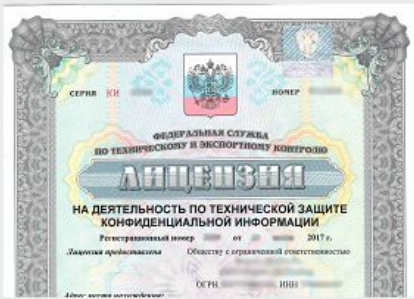
Average influence of the product on computer speed in daily usage

[More information](#)

	Industry average	Standard PC	Industry average	High end PC
<b>Slowing-down when launching popular websites</b> 39 websites visited	 19%	 12%	 17%	 17%
<b>Slower download of frequently-used applications</b> 20 downloaded files	 1%	 3%	 1%	 3%
<b>Slower launch of standard software applications</b> 12 test cases applied	 8%	 10%	 8%	 10%
<b>Slower installation of frequently-used applications</b> 20 installed applications	 25%	 14%	 23%	 14%
<b>Slower copying of files (locally and in a network)</b> 5,914 files copied	 3%	 1%	 4%	 1%
<b>Performance Score</b>	<b>6.0/6.0</b>			

# Принцип превентивности

## Наше предложение



Стоимость услуг: от 80 000 рублей.

Оформление: 45 суток.

Лицензия ФСТЭК по защите информации (СЗКИ) действует бессрочно на всей территории Российской Федерации.

Акция: постпродажное обслуживание.

[УЗНАТЬ ПОДРОБНЕЕ](#)

Если вы срочно хотите участвовать в проекте, рассмотрите вариант покупки готовой компании. Внесение изменений займет ровно 1 день, мы сами подготовим для вас сделку в вашем городе. Получите консультацию эксперта по лицензированию. Телефоны: **+7 (499) 112-44-47** | **+7 (812) 241-17-61**  
Электронная почта: [info@licenziya-fsb.com](mailto:info@licenziya-fsb.com)

## Получение лицензии ФСТЭК по защите конфиденциальной информации

Последствия реализации угроз безопасности информации могут повлечь значительно большие финансовые, временные и материальные затраты по сравнению с затратами на создание комплексной системы защиты.



# Принцип адекватности

Применяемые решения должны быть дифференцированы в зависимости от **вероятности** возникновения угроз безопасности, **прогнозируемого ущерба** от ее реализации, степени **ценности информации** и ее **стоимости**.



# Принцип системного подхода



Заключается во внесении комплексных мер по защите информации на стадии проектирования СЗИ, включая организационные и инженерно-технические мероприятия. Следует помнить оснащение средствами защиты изначально незащищенной АС является более дорогостоящим, чем оснащение средствами

# Принцип непрерывности защиты



Функционирование системы защиты не должно быть периодическим. Защитные мероприятия должны проводиться непрерывно и в объеме предусмотренном политикой безопасности.

# Принцип адаптивности



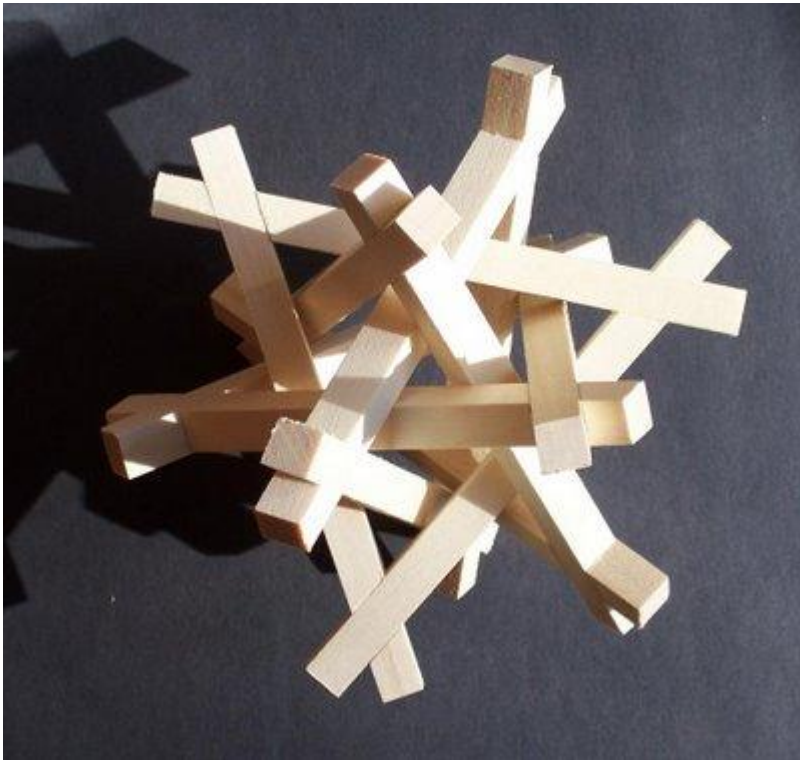
Система защиты должна строиться с учетом возможного изменения конфигурации АС, числа пользователей, степени конфиденциальности и ценности информации. Введение новых элементов АС не должно приводить к снижению достигнутого

# Принцип доказательности



- Результаты работы СЗИ не должны зависеть от субъектов.
- Достигается путём:
  - Использования известных формальных моделей
  - Применения систем аутентификации
  - Использования сертифицированных элементов СЗИ.

# Принцип унификации решений



- Разрабатываемые решения должны быть единообразными в схожих ситуациях.
- Следствием принципа является использование:
  - Типовых проектов
  - Типовой классификации ресурсов
  - Типовых конфигураций.

# Понятие оптимальной защиты



- План защиты – то что было определено специалистами
- Реальная СЗИ – то что было реализовано после стадии управления рисками
- Реальные угрозы – то что интересно нарушителю.

# Уровни зрелости



- 0-й уровень – уровень отсутствия ИБ.
- 1-й уровень – уровень частных решений.
- 2-й уровень – уровень комплексных решений.
- 3-й уровень –



# 0-й уровень



- Информационной безопасностью в компании никто не занимается, руководство компании не осознает важности проблем информационной безопасности.
- Финансирование отсутствует.
- Информационная безопасность реализуется штатными средствами ОС, СУБД и приложений (парольная защита, разграничение доступа к ресурсам и сервисам).

# 1-й уровень



- Информационная безопасность рассматривается руководством как чисто «техническая» проблема, отсутствует единая программа (концепция информационной безопасности, политика) развития СОИБ компании.
- Финансирование ведется в рамках общего ИТ-бюджета.
- Информационная безопасность реализуется средствами нулевого уровня плюс средства резервного копирования, антивирусные средства, межсетевые экраны, средства организации VPN, т.е. традиционные средства защиты.

# 2-й уровень



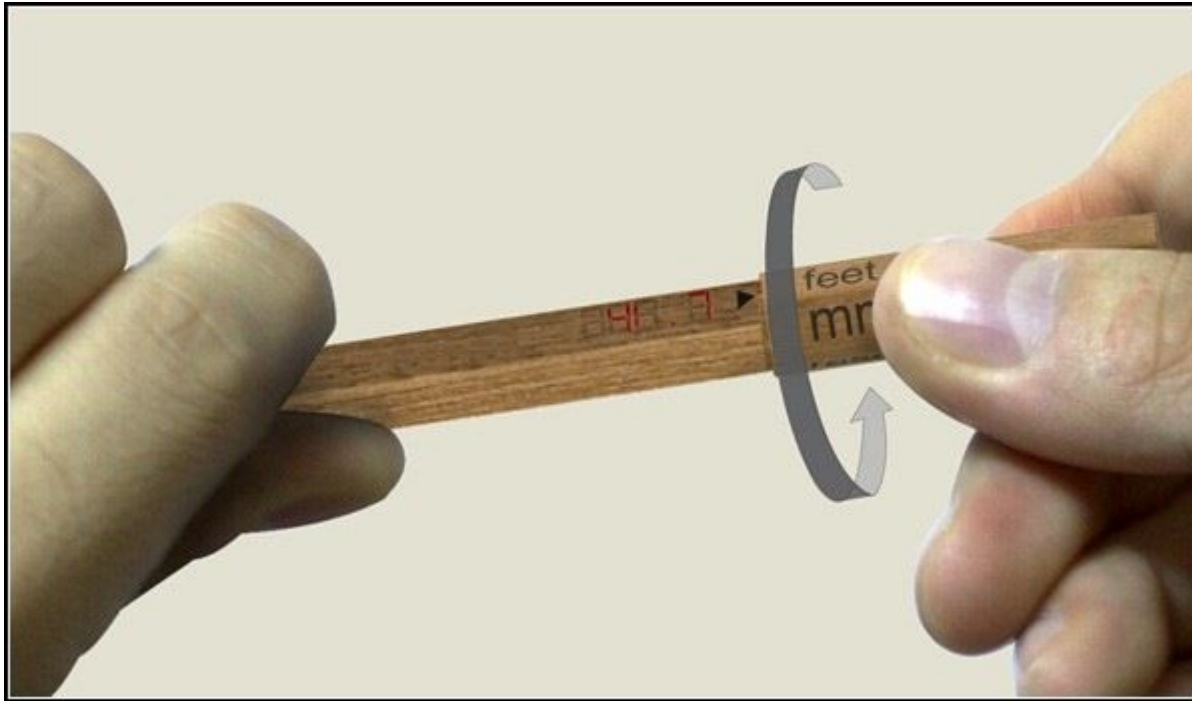
- ИБ рассматривается руководством, как комплекс организационных и технических мероприятий, существует понимание важности ИБ для бизнес-процессов, есть утвержденная руководством программа развития СОИБ.
- Финансирование ведется в рамках отдельного бюджета.
- ИБ реализуется средствами первого уровня плюс средства усиленной аутентификации, средства анализа почтовых сообщений и web-контента, IPS/IDS, средства анализа защищенности, SSO (средства однократной аутентификации), PKI (инфраструктура открытых ключей) и организационные меры (внутренний и внешний аудит, анализ рисков, политика информационной безопасности, положения, процедуры, регламенты и руководства).

# 3-й уровень



- ИБ является частью корпоративной культуры, назначен CISA (старший администратор по вопросам обеспечения ИБ).
- Финансирование ведется в рамках отдельного бюджета.
- ИБ реализуется средствами второго уровня плюс системы управления информационной безопасностью, CSIRT (группа реагирования на инциденты нарушения информационной безопасности), SLA (соглашение об уровне сервиса).

# МЕТРИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



# Зачем измерять ИБ?

- Безопасность с позиции бизнеса – инвестиции в процесс, направленный на достижение бизнес-целей (прибыль, завоёвывание доверия, репутации, расширение рынка).
- Показать вклад ИБ в достижение целей можно только измерив эффективность ИБ.
- Обоснование требований / инвестиций.
- Выполнение требований SLA (Service Level Agreement)

# Метрики безопасности

## Что такое метрика ИБ:

- Метрика ИБ – метод количественного измерения некоторых «безопасных» свойств информационной системы, показывающих её эффективность.

## Зачем метрики ИБ нужны:

- Показ эффективности процессов ИБ в достижении бизнес-целей.
- Показ влияния изменения конкретных «безопасных» свойств ИС на бизнес-

# Метрики безопасности

- Однозначно измеряются, без «экспертного мнения»
- Доступны для расчета и анализа (предпочтительно автоматически)
- Имеют количественное выражение (не "высокий", "средний", "низкий")
- Измеряются в пригодных для анализа величинах, таких как "ошибки", "часы", "стоимость"
- Понятны и указывают на проблемную область и возможные решения (тест «Ну, и?»)



# Примеры метрик

- **Технические средства защиты:**
  - Количество изменений конфигурации МЭ
  - Количество заблокированных соединений / атак
  - %узлов с установленным МЭ
  - %узлов с регулярно обновляемыми антивирусными базами
- **Повышение осведомленности сотрудников:**
  - % обученных, заходы на сайт, % нарушающих парольную политику
- **Соответствие требованиям:**
  - % соответствия стандартам
  - Ап-тайм внешнего сервиса / сайта
  - Среднее время предоставления доступа после запроса
- **Активность:**
  - Среднеквартальное число новых пользователей / клиентов
  - % отказов пользователей (не закончивших регистрацию)
  - Число поступивших жалоб на работу сервиса / сайта /

# Повод для гордости

- Количество «заблокированных вирусов»
- Количество «отраженных сетевых атак»
- Количество отфильтрованного СПАМа

ИЛИ

- Процент узлов с обновляемыми антивирусными базами
- Отношение количества вирусов в исходящей и входящей почте

# Примеры метрик

## Какие метрики вводить не стоит:

- Число случаев несанкционированного использования системы.
- % снижения рисков ИБ.
- % предотвращённых инцидентов.
- Кол-во запущенных проектов.
- Доход от внедрения СЗИ.
- Среднесуточное число сетевых соединений.
- Количество выявленного СПАМа.

# Метрики ИБ



## Принципы:

Цели бизнес-процесса (SLA).

SMART:

- Конкретна
- Измерима
- Применима / достижима
- Значима
- Своевременна

# Параметры метрик

## Параметры метрики:

- Название
- Описание (сущность)
- Единицы измерения
- Цель / диапазон нормальных значений
- Методы измерения
- Периодичность измерения

# Источники метрик

- Антивирусные/антиспам системы
- Системы класса SEIM
- Ручной сбор (системы управления проектами, контроля трудозатрат)
- Результаты аудитов
- Системы управления сетью (инвентаризация)
- Система контроля изменений
- Системы мониторинга и управления уязвимостями
- Системы контроля соответствия стандартам (Compliance management)

- Где брать метрики?
  - NIST Special publication
  - Center of Internet Security
    - <http://www.metricscenter.org/>
    - <http://www.securitymetrics.org>

# Резюме

- Метрики безопасности применимы практически к любому процессу ИБ.
- Метрики позволяют общаться с бизнесом в привычных терминах управления проектами и бизнес-целями.
- Метрики позволяют оценить реальную эффективность процессов ИБ организации в терминах бизнес-целей и помогают в принятии управленческих решений.
- Метрики позволяют оценивать динамику процессов и проводить сравнение с общемировой практикой.
- Большое количество метрик может автоматизировано оцениваться с системами класса SIEM.