ФИНАНСОВАЯ КОРПОРАЦИЯ
Открытие

# Определение достаточности защиты информации

**М. Левашов**

**28 МАЯ 2009Г.**

ФИНАНСОВАЯ КОРПОРАЦИЯ Открытие

# ISO 15408

**Стандарты о достаточности защиты …..**

- Для принятия решения о достаточности требований безопасности ….. важно, чтобы решаемая задача безопасности ясно понималась всеми участниками оценки.
- В зависимости от сложности и критичности требования к безопасности функционирования системы и доступных ресурсов для ее реализации, стандартом рекомендуется выбирать набор классов и семейств процессов, достаточных для обеспечения необходимого качества комплекса функциональной безопасности проекта (ОУД)….

# Основные принципы:

…достаточность предложенных мер безопасности должна быть продемонстрирована….

Определяются требования, направленные на обеспечение …достаточности…эксплуатационной документации, представленной разработчиком (документация для пользователей и администраторов).

Определяются требования по достаточности тестирования…..

ФИНАНСОВАЯ КОРПОРАЦИЯ Открытие

# ГОСТ Р ИСО/МЭК 18045

Оценщик должен исследовать политики обеспечения конфиденциальности и целостности при их разработке, чтобы сделать заключение о достаточности применявшихся мер безопасности.

Сюда включаются политики управления:

- решением об отнесении информации, относящейся к объекту оценки (ОО) к конфиденциальной с доступом к ней определенного персонала;
- решением о защите информации от несанкционированной модификации с разрешением некоторому персоналу модифицировать ее.

Необходимо сделать заключение о том, описаны ли эти политики в документации по ИБ разработки, совместимы ли применяемые меры ИБ с политиками, являются ли эти меры достаточно полными.

Оценщик делает заключение о достаточности и приемлемости подмножества функции безопасности объекта (ФБО). Покрывается ли этим задание по безопасности (ЗБ).

ФИНАНСОВАЯ КОРПОРАЦИЯ Открытие

# ГОСТ Р ИСО/МЭК 17799-2005г. (27002)

Политику информационной безопасности следует пересматривать с запланированным интервалом или при существенных изменениях для поддержания ее адекватности, достаточности и эффективности…

*

# В. Конявский

**Информация** со временем начинает устаревать, т.е. цена ее уменьшается. За условие **достаточности защиты** принимается превышение …. времени (затрат) на преодоление преграды нарушителем над временем жизни (ценой) **информации**

Требования к достаточности (полноте, применительно к условиям использования) набора механизмов защиты определены документом "Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации"

# А. Щеглов

Например о доступе: должен осуществляться контроль подключения ресурсов, в частности устройств, в соответствии с условиями практического использования защищаемого вычислительного средства, и контроль доступа субъектов к защищаемым ресурсам, в частности к разрешенным для подключения устройствам

Если вопросы достаточности механизмов защиты применительно к набору
защищаемых ресурсов еще как-то поддаются формализации, то
применительно к задачам защиты информации формализовать
подобные требования не представляется возможным.

## В тоже время:

…защиту информации принято считать достаточной, если затраты на ее преодоление превышают ожидаемую ценность самой информации….

# ГОРДЕЙЧИК

Фактически предложил подход, связанный с оценкой рисков невыполнения требований регуляторов….

То есть, если оценить риск как средний ущерб от государства (штрафные санкции, конфискация СЗИ, прекращение бизнеса и т. д.) с учетом вероятности проверки Роскомнадзором выполнения требований федерального законодательства и подзаконных актов, то, в случае принятия этого риска, защита считается достаточной…

Можно таким же образом подойти к оценке достаточности при невыполнении требований международного законодательства (PCI DSS, акт SOX, законы об информировании субъектов конфиденциальной информации об утрате их данных и т.д.….)

ФИНАНСОВАЯ КОРПОРАЦИЯ Открытие

# Достаточность и риск менеджмент

Основа обоснования – качественные и количественные оценки рисков.

Защита информации и ИТ может считаться достаточной, если:

- соблюдается правовая основа, как со стороны национальных и международных регуляторов, так договорная (с клиентами, партнерами и т.д.);
- значения рисков ИБ находятся в допустимых пределах;
- неприемлемые (непринятые) риски непрерывно обрабатываются до того уровня, когда остаточные риски с учетом произведенных на их обработку затрат будут приняты

- результаты внутреннего и внешнего аудитов не содержат серьезных нарушений требований ИБ;
- выявленные недостатки своевременно устраняются;
- процессы обеспечения ИБ имеют высокий (4-5-й) уровень зрелости;

Защиту также можно считать достаточной, если дальнейшее увеличение расходов на нее не уменьшает величину остаточного риска вместе с указанными выше затратами.