Информационная безопасность

Лекция 11 Системы управления базами данных

В. М. Куприянов, Национальный центр ИНИС МАГАТЭ, НИЯУ МИФИ

НЦ ИНИС МИФИ

Литература

Основная литература для изучения дисциплины:

- Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности.- М.: Горячая линия – Телеком, 2006.
- Петраков А.В. Основы практической защиты информации.- М.: Радио и связь, 2001.
- Шумский А.А., Шелупанов А.А. Системный анализ в защите информации.- М.: Гелиос АРВ, 2005.
- Герасименко В.А., Малюк А.А. Основы защиты информации.- М.: Инкомбук, 1997.
- Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.- М.: Энергоатомиздат, 1994.
- Семкин С.Н., Семкин А.Н. Основы информационной безопасности объектов обработки информации.- Орел: ОВИПС, 2000.

Безопасность СУБД

Обеспечение безопасности корпоративных баз данных - сегодня одна из самых актуальных тем. И это понятно. Однако парадокс заключается в том, что уделяя огромное внимание защите баз данных снаружи, многие забывают защищать их изнутри.

Существует три большие группы пользователей СУБД, которых условно можно назвать операторами; аналитиками; администраторами.

Под операторами в предложенной классификации понимаются в основном те, кто либо заполняет базу данных (вводят туда вручную информацию о клиентах, товарах и т. п.), либо выполняют задачи, связанные с обработкой информации: кладовщики, отмечающие перемещение товара, продавцы, выписывающие счета и т. п.

Под аналитиками понимаются те, ради кого, собственно, создается эта база данных: логистики, маркетологи, финансовые аналитики и прочие. Эти люди по роду своей работы получают обширнейшие отчеты по собранной информации.

Термин "администратор" говорит сам за себя. Эта категория людей может только в общих чертах представлять, что хранится и обрабатывается в хранилище данных. Но они решают ряд важнейших задач, связанных с жизнеобеспечением системы, ее отказо- и катастрофоустойчивости.

Указанные группы различаются еще и по способу взаимодействия с СУБД.

Операторы чаще всего работают с информацией через различные приложения. Безопасность и разграничение доступа к информации тут реализованы очень хорошо, проработаны и реализованы методы защиты. Производители СУБД, говоря о возможностях своих систем, акцентируют внимание именно на такие способы защиты. Доступ к терминалам/компьютерам, с которых ведется работа, разграничение полномочий внутри приложения, разграничение полномочий в самой СУБД - все это выполнено на высоком техническом уровне. Честно внедрив все эти механизмы защиты, специалисты по безопасности чувствуют успокоение и удовлетворение.

Проблема с аналитиками заключается в том, что они работают с СУБД на уровне ядра. Они должны иметь возможность задавать и получать всевозможные выборки информации из всех хранящихся там таблиц. Включая и запросы общего типа "select * *".

С администраторами дело обстоит ненамного лучше. Начиная с того, что в крупных информационных системах их число сопоставимо с числом аналитиков. И хотя абсолютно полными правами на СУБД наделены лишь два-три человека, администраторы, решающие узкие проблемы (например резервное копирование данных), все равно имеют доступ ко всей информации, хранящейся в СУБД.

- Между аналитиками и администраторами на первый взгляд нет никакой разницы: и те и другие имеют доступ ко всей обрабатываемой информации. Но все же отличие между этими группами есть, и состоит оно в том, что аналитики работают с данными, используя некие стандартные механизмы и интерфейсы СУБД, а администраторы могут получить непосредственный доступ к информации, например на физическом уровне, выполнив лишний раз ту же операцию по резервному копированию данных.
- В любой СУБД есть встроенные возможности по разграничению и ограничению доступа на уровне привилегий пользователей. Но возможность эта существует только чисто теоретически. Кто хоть раз имел дело с администрированием большой СУБД в большой организации, хорошо знает, что на уровне групп пользователей что-либо разграничить слишком сложно, ибо даже, помимо многообразия организационных ролей и профилей доступа, в дело вмешиваются проблемы обеспечения индивидуального доступа, который вписать в рамки ролей практически невозможно.

Очень часто обработка данных ведется не самим пользователем, а созданным и запущенным в СУБД скриптом. Так, например, поступают для формирования типовых или периодических отчетов. В этом случае скрипт запускается не от имени пользователя, а от имени системной учетной записи, что серьезно затрудняет понимание того, что же на самом деле происходит в базе данных. Притом сам скрипт может содержать практически любые команды, включая пресловутое "select * *". В ходе работы скрипт может сформировать новый массив данных, в том числе и дублирующий все основные таблицы. В итоге пользователь получит возможность работать с этим набором данных и таким образом обходить установленные нами средства аудита.

Попытка использовать для разграничения доступа криптографию также обречена на провал: это долго, ресурсоемко и опасно с точки зрения повреждения данных и их последующего восстановления. К тому же возникают проблемы с обработкой информации, ибо индексироваться по зашифрованным полям бесполезно. А самое главное, что некоторым администраторам все равно придется дать "ключи от всех замков".

В результате, если перед компанией стоит задача по сохранению своих корпоративных СУБД, то ее нельзя разрешить простым ограничением и разграничением доступа к информации. Как мы разобрались, где это хоть как-то возможно, это уже сделано. Во всех остальных случаях можно лишь по факту понимать, что происходило с данными.

- Защититься от физического доступа к базам данных также возможно только путем введения жестких регламентов съема и хранения информации и слежения за отступлениями от этих регламентов. К примеру, изготовление лишней резервной копии. Если процессы происходят по сети, с несанкционированными всплесками сетевого трафика по силам справиться средствам обнаружения и предотвращения атак. Стоит ли говорить, что отдельно надо побеспокоиться о безопасном хранении самих резервных копий. В идеале физический доступ к ним должен быть строго ограничен, а администратор, отвечающий за процесс, должен либо настроить расписание, либо иметь возможность только запустить этот процесс и контролировать его прохождение без доступа к резервным носителям информации.
- Подводя итог, скажем: безопасность - процесс комплексный. И еще раз хочется предостеречь пользователей от стереотипа, что опасность корпоративным ресурсам, в том числе и базам данных, угрожает только из внешнего окружения компании или организации.

- ISO 27000 - Международные стандарты управления информационной безопасностью
- **Операции с документом**
- Семейство Международных Стандартов на Системы Управления Информационной Безопасностью 27000 разрабатывается ISO/IEC JTC 1/SC 27. Это семейство включает в себя Международные стандарты, определяющие требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению.

ISO27000

ISO/IEC 27000:2009 Information technology. Security techniques. Information security management systems. Overview and vocabulary - Определения и основные принципы. Выпущен в июле 2009 г.

ISO27001

ISO/IEC 27001:2005/BS 7799-2:2005 Information technology. Security techniques. Information security management systems. Requirements - Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования. Выпущен в октябре 2005 г.

ISO27002 ISO/IEC 27002:2005, BS 7799-1:2005,BS ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management - Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью. Выпущен в июне 2005 г.

ISO27003 ISO/IEC 27003:2010 Information Technology. Security Techniques. Information Security Management Systems Implementation Guidance - Руководство по внедрению системы управления информационной безопасностью. Выпущен в январе 2010 г.

ISO27004 ISO/IEC 27004:2009 Information technology. Security techniques. Information security management. Measurement - Измерение эффективности системы управления информационной безопасностью. Выпущен в январе 2010 г.

ISO27005

ISO/IEC 27005:2008 Information technology. Security techniques. Information security risk management - Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности. Выпущен в июне 2008 г.

ISO27006

ISO/IEC 27006:2007 Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems - Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью. Выпущен в марте 2007 г.**ISO27007**ISO/IEC 27007 Information technology. Security techniques. Guidelines for Information Security Management Systems auditing (FCD) - Руководство для аудитора СУИБ. Проект находится в финальной стадии. Выпуск запланирован на 2011 год.

ISO27008

ISO/IEC 27008 Information technology. Security techniques. Guidance for auditors on ISMS controls (DRAFT) - Руководство по аудиту механизмов контроля СУИБ. Будет служить дополнением к стандарту ISO 27007. Выпуск запланирован в конце 2011 года.

ISO27010

ISO/IEC 27010 Information technology. Security techniques. Information security management for inter-sector communications (DRAFT) - Управление информационной безопасностью при коммуникациях между секторами. Стандарт будет состоять из нескольких частей, предоставляющих руководство по совместному использованию информации о рисках информационной безопасности, механизмах контроля, проблемах и/или инцидентах, выходящей за границы отдельных секторов экономики и государств, особенно в части, касающейся "критичных инфраструктур".

ISO27011

ISO/IEC 27011:2008 Information technology. Security techniques. Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 - Руководство по управлению информационной безопасностью для телекоммуникаций. Выпущен в мае 2009 г.

ISO27013

ISO/IEC 27013 IT Security. Security techniques. Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001 (DRAFT) - Руководство по интегрированному внедрению ISO 20000 и ISO 27001. Выпуск запланирован в 2011 году.

ISO27014

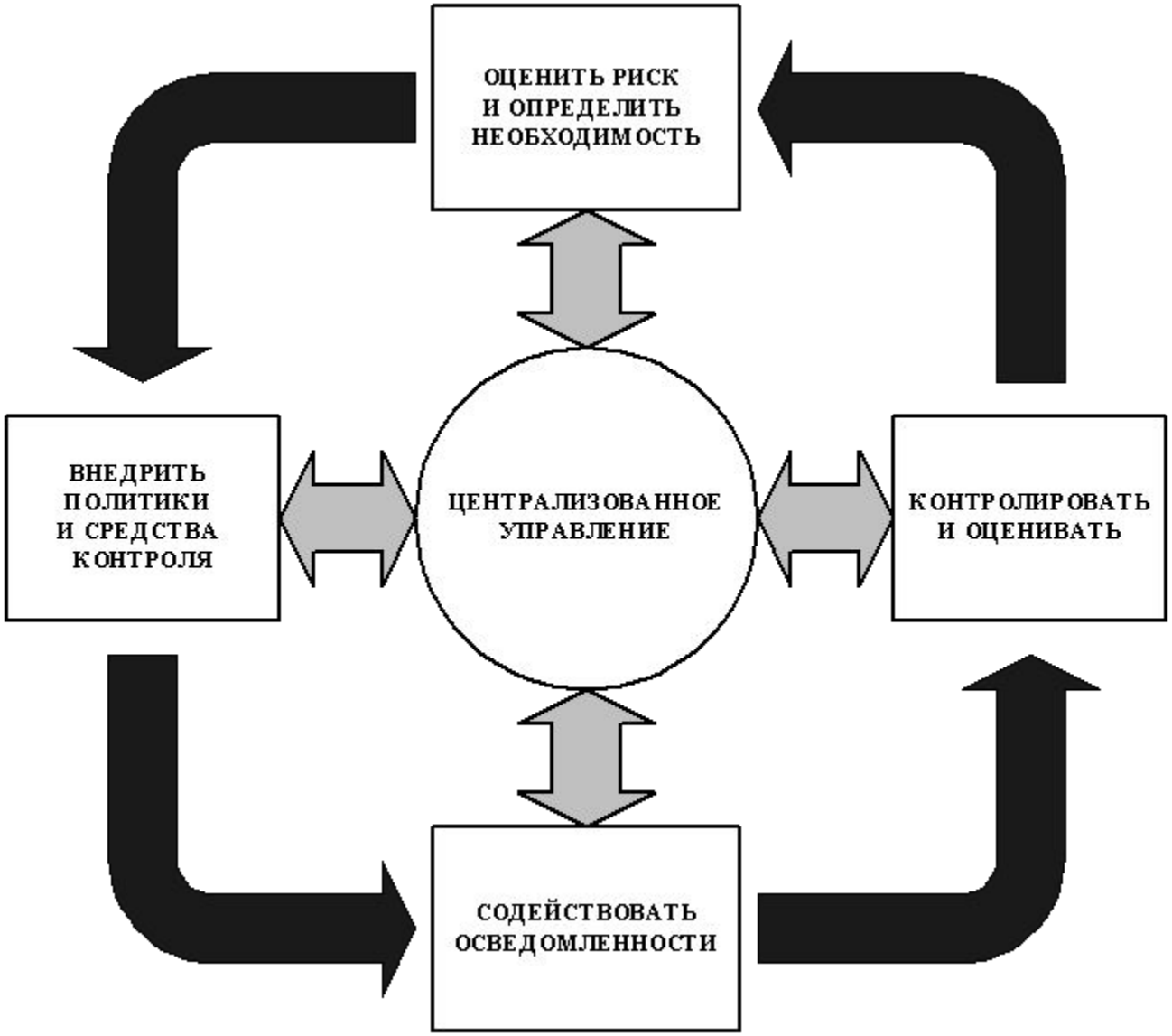
ISO/IEC 27014 Information technology. Security techniques. Information security governance framework (DRAFT) - Базовая структура управления информационной безопасностью. Проект находится в разработке.

- **ISO27015**
- ISO/IEC 27015 Information technology. Security techniques. Information security management systems guidelines for financial and insurance sectors (DRAFT) - Руководство по внедрению систем управления информационной безопасностью в финансовом и страховом секторе. Проект проходит начальную стадию обсуждения.
- **ISO27031**
- ISO/IEC 27031 Information technology. Security techniques. Guidelines for information and communications technology readiness for business continuity (FDIS) - Руководство по обеспечению готовности информационных и коммуникационных технологий к их использованию для управления непрерывностью бизнеса. Проект находится в финальной стадии. Выпуск запланирован в начале 2011 года.
- **ISO27032**
- ISO/IEC 27032 Information technology. Security techniques. Guidelines for cybersecurity (2nd CD) - Руководство по обеспечению кибербезопасности. Проект находится в начальной стадии разработки.

Основные принципы управления рисками информационной безопасности

Несмотря на разные операции, продукты и услуги, организации использовали пять принципов управления рисками информационной безопасности.

- Оценить риск и определить потребности
- Установить централизованное управление
- Внедрить необходимые политики и соответствующие средства контроля
- Содействовать осведомленности сотрудников
- Контролировать и оценивать эффективность политик и механизмов контроля


ОЦЕНИТЬ РИСК
И ОПРЕДЕЛИТЬ
НЕОБХОДИМОСТЬ
ВНЕДРИТЬ
ПОЛИТИКИ
И СРЕДСТВА
КОНТРОЛЯ
ЦЕНТРАЛИЗОВАННОЕ
УПРАВЛЕНИЕ
КОНТРОЛИРОВАТЬ
И ОЦЕНИВАТЬ
СОДЕЙСТВОВАТЬ
ОСВЕДОМЛЕННОСТИ


ПРИНЦИПЫ
МЕТОДЫ (ПРАКТИКИ)
ОЦЕНИТЬ РИСК И ОПРЕДЕЛИТЬ НЕОБХОДИМОСТЬ
1. Признать информационные ресурсы в качестве существенных активов организации
2. Разработать практические процедуры оценки рисков, связующих безопасность и требования бизнеса
3. Установить ответственность менеджеров бизнес-подразделений и менеджеров программы
4. Непрерывно управлять рисками
УСТАНОВИТЬ ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ
5. Определить руководящую группу для выполнения ключевых действий
6. Предоставить руководящей группе простой и независимый доступ к менеджменту организации
7. Определить и выделить бюджет и персонал
8. Повышать профессионализм и технические знания персонала


ВНЕДРИТЬ ПОЛИТИКИ И СРЕДСТВА КОНТРОЛЯ
9. Установить взаимосвязь политик и бизнес-рисков
10. Установить различие между политиками и руководящими принципами
11. Обеспечить сопровождение политик руководящей группой
СОДЕЙСТВОВАТЬ ОСВЕДОМЛЕННОСТИ
12. Непрерывное обучение пользователей (сотрудников) на примере рисков и соответствующих политик
13. Использовать дружественный подход
КОНТРОЛИРОВАТЬ И ОЦЕНИВАТЬ ПОЛИТИКИ И ЭФФЕКТИВНОСТЬ СРЕДСТВ КОНТРОЛЯ
14. Контролировать факторы, влияющие на риски и указывающие на эффективность информационной безопасности
15. Использовать полученные результаты для координации будущих усилий и ответственности менеджмента
16. Отслеживать новые методы, инструменты и средства контроля

- **Установить централизованное управление**
- Руководящая группа выступает, прежде всего, в роли советника или консультанта бизнес-подразделений, и не может навязывать методы (средства) информационной безопасности.
- **Определить руководящую группу для выполнения ключевых действий**
- В целом, руководящая группа должна являться (1) катализатором (ускорителем) процесса, гарантирующим, что риски информационной безопасности рассматриваются непрерывно; (2) центральным консультационным ресурсом для подразделений организаций; (3) средством доведения до руководства организации информации о состоянии информационной безопасности и принимаемых мерах. Кроме того, руководящая группа позволяет централизовано управлять поставленными задачами, в противном случае эти задачи могут дублироваться различными подразделениями организации.

- **Предоставить руководящей группе простой и независимый доступ к высшему менеджменту организации**
- Отметим необходимость обсуждения проблем информационной безопасности менеджерами руководящей группы с высшим менеджментом организации. Такой диалог позволит действовать эффективно и избежать разногласий. В противном случае возможны конфликтные ситуации с менеджерами бизнес-подразделений и разработчиками систем, желающими скорейшего внедрения новых программных продуктов, и, потому, оспаривающими применение средств контроля, которые могут препятствовать эффективности и "комфортности" работы с программным обеспечением. Таким образом, возможность обсуждения проблем информационной безопасности на высшем уровне сможет гарантировать полное понимание рисков и их допустимость до принятия окончательных решений.
- **Определить и выделить бюджет и персонал**
- Бюджет позволит планировать и устанавливать цели программы информационной безопасности. Как минимум, бюджет включает заработную плату сотрудников и затраты на обучение. Штатная численность руководящей группы (подразделения безопасности) может варьироваться и зависить как от поставленных целей, так и от проектов, находящихся на рассмотрении. Как было отмечено ранее, к работе в группе могут привлекаться как технические специалисты, так и сотрудники бизнес-подразделений.

- **Повышать профессионализм и технические знания сотрудников**
- Сотрудники организации должны участвовать в различных аспектах программы информационной безопасности и обладать соответствующими навыками и знаниями. Необходимый уровень профессионализма сотрудников может быть достигнут с помощью тренингов, проводить которые могут как специалисты организации, так и внешние консультанты.
- **Внедрить необходимые политики и соответствующие средства контроля**
- Политики в области информационной безопасности являются основанием принятия определенных процедур и выбора средств (механизмов) контроля (управления). Политика – первичный механизм, с помощью которого менеджмент доводит свое мнение и требования сотрудникам, клиентам и деловым партнерам. Для информационной безопасности, как и для других областей внутреннего контроля, требования политик напрямую зависят от результатов оценки уровня риска.
- **Установить взаимосвязь политик и бизнес-рисков**
- Всесторонний набор адекватных политик, доступных и понятных пользователям, является одним из первых шагов в установлении программы обеспечения информационной безопасности. Стоит подчеркнуть важность непрерывного сопровождения (корректировки) политик для своевременного реагирования на выявляемые риски и возможные разногласия.

Установить отличия между политиками и руководящими принципами

Общий подход к созданию политик информационной безопасности должен предусматривать

(1) краткие (лаконичные) политики высокого уровня и

более детальную информацию, представленную в практических руководствах и стандартах.

Политики предусматривают основные и обязательные требования, принятые высшим менеджментом. В то время как практические руководства не являются обязательными для всех бизнес-подразделений. Такой подход позволяет высшему менеджменту акцентировать внимание на наиболее важных элементах информационной безопасности, а также предоставить возможность маневрирования менеджерам бизнес-подразделений, сделать политики легкими для понимания сотрудников.

Обеспечить сопровождение политик руководящей группой

- Руководящая группа должна быть ответственна за разработку политик информационной безопасности организации во взаимодействии с менеджерами бизнес-подразделений, внутренними аудиторами и юристами. Кроме того, руководящая группа должна обеспечить необходимые разъяснения и предоставить ответы на вопросы пользователей. Это поможет уладить и предотвратить недоразумения, а также принять необходимые меры, не предусмотренные политиками (руководящими принципами).
- Политики стоит сделать доступными, так чтобы пользователи, при необходимости, могли получить доступ к их актуальным версиям. Пользователи должны расписываться в том, что они ознакомлены с политиками до предоставления им доступа к информационным ресурсам организации. Если пользователь будет вовлечен в инцидент безопасности, это соглашение послужит свидетельством того, что он или она были проинформированы о политике организации, как и о возможных санкциях, в случае ее нарушения.

- **Содействовать осведомленности**
- Компетентность пользователей является обязательным условием для успешного обеспечения информационной безопасности, а также позволяет гарантировать, что средства контроля работают должным образом. Пользователи не могут следовать политике, которую они не знают или не понимают. Не зная о рисках, связанных с информационными ресурсами организации, они не могут видеть необходимости исполнения политики, разработанной с целью уменьшения рисков.
- **Непрерывное обучение пользователей и других сотрудников на примере рисков и соответствующих политик**
- Руководящая группа должна обеспечить стратегию постоянного обучения сотрудников, так или иначе влияющих на информационную безопасность организации. Группа должна сосредоточить усилия на всеобщем понимании рисков, связанных с информацией, обрабатываемой в организации, а также политиках и методах (средствах) контроля, направленных на уменьшение этих рисков.
- **Использовать дружественный подход**
- Руководящая группа должна использовать разнообразные методы обучения и поощрения (стимулирования) чтобы сделать политику организации доступной и обучить пользователей. Стоит избегать встреч, проводимых раз в год со всеми сотрудниками организации, напротив обучение лучше проводить в небольших группах сотрудников.

Контролировать и оценивать эффективность политик и механизмов контроля

Как и любой вид деятельности, информационная безопасность подлежит контролю и периодической переоценке, чтобы гарантировать адекватность (соответствие) политик и средств (методов) контроля поставленным целям.

Контролировать факторы, влияющие на риски и указывающие на эффективность информационной безопасности

Контроль должен быть сосредоточен, прежде всего, на (1) наличии средств и методов контроля и их использования, направленного на уменьшение рисков и (2) оценке эффективности программы и политик информационной безопасности, улучшающих понимание пользователей и сокращающих количество инцидентов. Такие проверки предусматривают тестирование средств (методов) контроля, оценку их соответствия политикам организации, анализ инцидентов безопасности, а также другие индикаторы эффективности программы информационной безопасности.

Эффективность работы руководящей группы может быть оценена, основываясь, например, на следующих показателях (но, не ограничиваясь ими):

- число проведенных тренингов и встреч;
- число выполненных оценок риска (рисков);
- число сертифицированных специалистов;
- отсутствие инцидентов, затрудняющих работу сотрудников организации;
- снижение числа новых проектов, внедренных с задержкой из-за проблем информационной безопасности;
- полное соответствие или согласованные и зарегистрированные отклонения от минимальных требований информационной безопасности;
- снижение числа инцидентов, влекущих за собой несанкционированный доступ, потерю или искажение информации.

Использовать полученные результаты для координации будущих усилий и повышения ответственности менеджмента

Контроль, безусловно, позволяет привести организацию в соответствие с принятыми политикам информационной безопасности, однако полные выгоды от контроля не будут достигнуты, если полученные результаты не используются для улучшения программы обеспечения информационной безопасности. Анализ результатов контроля предоставляет специалистам в области информационной безопасности и менеджерам бизнес-подразделений средства (1) переоценки ранее идентифицированных рисков, (2) определения новых проблемных участков, (3) переоценки достаточности и уместности существующих средств и методов контроля (управления) и действий по обеспечению информационной безопасности, (4) определения потребностей в новых средствах и механизмах контроля, (5) переадресации контрольных усилий (контролирующих действий). Кроме того, результаты могут использоваться для оценки деятельности бизнес-менеджеров, ответственных за понимание и уменьшение рисков в бизнес-подразделениях.

Отслеживать новые методы и средства контроля

Важно гарантировать, что (1) специалисты в области информационной безопасности не "отстают" от разрабатываемых методов и инструментов (приложений) и располагают самой последней информацией об уязвимости информационных систем и приложений, (2) высший менеджмент гарантирует, что располагает для этого необходимыми ресурсами.

- Развитие программы информационной безопасности, соответствующей основным принципам, описанным в этом документе – первый и основной шаг организации на пути построения эффективной системы информационной безопасности. Таким образом, организация должна непрерывно
  - **(1) исследовать и оценивать риски информационной безопасности, влияющие на бизнес-процессы,**
  - **(2) установить централизованное управление информационной безопасностью,**
  - **(3) установить политики, стандарты, и средства (механизмы) контроля (управления), направленные на уменьшение этих рисков,**
  - **(4) содействовать осведомленности и пониманию, описанной проблемы среди сотрудников,**
  - **(5) оценивать соответствие и повышать эффективность.**

Гармонизированные национальные стандарты, разработанные и утвержденные в 2007- 2008 г.г.

ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации»

ГОСТ Р ИСО ТО 13569 «Финансовые услуги. Рекомендации по информационной безопасности»

ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» Части 1, 2, 3

ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»

ГОСТ Р ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем»

ГОСТ Р ИСО/МЭК ТО 15446 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности»

ГОСТ Р ИСО/МЭК 27006 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности»

ГОСТ Р ИСО/МЭК 18028-1 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Часть 1. Менеджмент сетевой безопасности»

ГОСТ Р ИСО/МЭК ТО 24762 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения»

ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации»

- ГОСТ Р ИСО/МЭК 27000 «Информационная технология. Методы и средства безопасности. Системы менеджмента информационной безопасности. Обзор и словарь»
- ГОСТ Р ИСО/МЭК 27002 «Информационная технология. Методы и средства безопасности. Практические правила менеджмента информационной безопасности»
- ГОСТ Р ИСО/МЭК 27005 «Информационная технология. Измерения менеджмента информационной безопасности»
- ГОСТ Р ИСО/МЭК 21827 «Информационная технология. Проектирование систем безопасности. Модель зрелости»
- ГОСТ Р «Защита информации. Автоматизированные системы и базы данных. Требования по обеспечению безопасности информации»
- ГОСТ Р «Защита информации. Оценка безопасности информации, циркулирующей в автоматизированных системах. Общие положения»
- ГОСТ Р «Защита информации. Техника защиты информации. Требования к формированию баз синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»
- ГОСТ Р «Система обеспечения информационной безопасности сети связи общего пользования. Методика оценки риска причинения ущерба сетям и системам связи»
- Источник: ГНИИИ ПТЗИ ФСТЭК России

2. Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации

Структура функциональных требований по защите от НСД к СВТ