Вопросы по теме Политики и модели безопасности компьютерных систем:

1)Что такое политка Безопасности?

2)Какие задачи решает систематический подход?

3)В чем цель создания политики безопасности систем?

4)Для чего используется базовые принцыпы защиты системы?

5)Что используют эксперты в качестве анализа адекватности реализации политики безопасности?

Тема 1. Политики и модели безопасности компьютерных систем.

Технология защиты автоматизированных систем начала развиваться относительно недавно, но сегодня уже существует значительное число теоретических моделей, позволяющих описывать различные аспекты безопасности и обеспечивать средства защиты формально подтвержденной алгоритмической базой.

Под политикой безопасности понимается совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое условие безопасности системы. Формальное выражение политики безопасности называют моделью безопасности.

Основная цель создания политики безопасности системы и описания ее в виде формальной модели — это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений.

Кроме того, формальные модели безопасности позволяют решить еще целый ряд задач, возникающих в ходе проектирования, разработки и сертификации защищенных систем, поэтому их используют не только теоретики информационной безопасности, но и другие категории специалистов, участвующих в процессе создания и эксплуатации защищенных информационных систем (производители, потребители, эксперты).

Модели безопасности обеспечивают системотехнический подход, включающий решение следующих важнейших задач :

выбор и обоснование базовых принципов архитектуры защищенных автоматизированных систем, определяющих механизмы реализации средств и методов защиты информации;

подтверждение свойства защищенности разрабатываемых систем путем формального доказательства соблюдения политики безопасности (требований, условий, критериев);

составление формальной спецификации политики безопасности как важнейшей составной части организационного и документационного обеспечения разрабатываемых защищенных компьютерных систем. Производители защищенных информационных систем используют модели безопасности в следующих случаях:

при составлении формальной спецификации политики безопасности разрабатываемой системы;

при выборе и обосновании базовых принципов архитектуры защищенной системы, определяющих механизмы реализации средств защиты;

в процессе анализа безопасности системы, при этом модель используется в качестве эталонной модели;

при подтверждении свойств разрабатываемой системы путем формального доказательства соблюдения политики безопасности.

Потребители путем составления формальных моделей безопасности получают возможность довести до сведения производителей свои требования в четко определенной и непротиворечивой форме, а также оценить соответствие защищенных систем своим потребностям.

Эксперты по квалификации в ходе анализа адекватности реализации политики безопасности в защищенных системах используют модели безопасности в качестве эталонов.

По сути, модели безопасности являются связующим элементом между

производителями, потребителями, экспертами.

Тема 2. Методика и программные продукты для оценки рисков.

методик анализа рисков можно разделить на:

методики, использующие оценку риска на качественномуровн. К таким методикам, в частности, относится FRAP;

количественные методики (риск оценивается через числовое значение). К этому классу относится методика RiskWatch;

методики, использующие смешанные оценки (такой подход используется в CRAMM, методике Microsoft и т.д.).

Методика CRAMM

В основе метода CRAMM лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Метод является универсальным и подходит как для крупных, так и для малых организаций, как правительственного, так и коммерческого сектора. Версии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний (profiles).

Исследование ИБ системы с помощью СRAMM проводится в три стадии.

На первой стадии анализируется все, что касается идентификации и определения ценности ресурсов системы.

На второй стадии рассматривается все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. В конце стадии заказчик получает идентифицированные и оцененные уровни рисков для своей системы.

Третья стадия исследования заключается в поиске адекватных контрмер. По существу, это поиск варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика.

Методика "Facilitated RiskAnalysis Process (FRAP)" В методике, обеспечение ИБ ИС предлагается рассматривать в рамках процесса управления рисками. Управление рисками в сфере ИБ - процесс, позволяющий компаниям найти баланс между затратами средств и сил на средства защиты и получаемым эффектом.

Управление рисками должно начинаться с оценки рисков: должным образом оформленные результаты оценки станут основой для принятия решений в области повышения безопасности системы.

После завершения оценки, проводится анализ соотношения затрат и получаемого эффекта, который позволяет определить те средства защиты, которые нужны, для снижения риска до приемлемого уровня.

Проведение оценки рисков в соответствии с методикой Microsoft

Процесс управления рисками, предлагаемый корпорацией Майкрософт разбивает этап оценки рисков на следующие три шага.

1. Планирование. Разработка основы для успешной оценки рисков.

2. Координированный сбор данных. Операции тематического сбора данных представляют собой основную часть операций взаимодействия и совместной работы различных групп на этапе оценки рисков. Сбор информации о рисках в ходе координированных обсуждений рисков. На этом шаге собираются следующие основные данные.

Активы организации. Вся информация о важных для организации активах.

Описание актива. Краткое описание каждого актива, его ценность и его владелец для облегчения общего понимания актива на этапе оценки рисков.

Угрозы безопасности. Причины и события, которые могут оказывать на актив негативное влияние и приводить к потере конфиденциальности, целостности или доступности актива.

Уязвимости. Слабости или отсутствие элементов контроля, которые могут использоваться для влияния на актив.

Текущая среда контроля. Описание используемых в настоящее время элементов контроля и их эффективности в рамках организации.

Предлагаемые элементы контроля. Предложения по снижения риска.

3. Приоритизация рисков. Ранжирование выявленных рисков на основе непротиворечивого и повторяемого процесса. Процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт, предоставляет рекомендации по выявлению и приоритизации рисков на основе непротиворечивого и повторяемого подхода. Открытый и повторяемый подход помогает группе управления рисками быстро найти удовлетворяющее всех решение, уменьшив потенциальные задержки, вызываемые субъективным характером процесса приоритизации рисков. Задачи и рекомендации, относящиеся к приоритизации рисков, подробно описаны в четвертом разделе данной главы.

Тема 3. Современные стандарты IT в области информационной безопасности

Стандарты информационной безопасности – это обязательные или рекомендуемые к выполнению документы, в которых определены подходы к оценке уровня ИБ и установлены требования к безопасным информационным системам.

Стандарты в области информационной безопасности выполняют следующие важнейшие функции:

- выработка понятийного аппарата и терминологии в области информационной безопасности

- формирование шкалы измерений уровня информационной безопасности

- согласованная оценка продуктов, обеспечивающих информационную безопасность

- повышение технической и информационной совместимости продуктов, обеспечивающих ИБ

- накопление сведений о лучших практиках обеспечения информационной безопасности и их предоставление различным группам заинтересованной аудитории – производителям средств ИБ, экспертам, ИТ-директорам, администраторам и пользователям информационных систем

- функция нормотворчества – придание некоторым стандартам юридической силы и установление требования их обязательного выполнения.

Тема 4.Обзор и сравнительный анализ стандартов информационной безопасности

Опыт эксплуатации существующих компьютерных систем обработки информации показывает, что проблема обеспечения безопасности еще далека от своего решения, а предлагаемые производителями различных систем средства защиты сильно различаются как по решаемым задачам и используемым методам, так и по достигнутым результатам. Это определяет актуальность проблемы построения защищенных систем обработки информации, решение которой следует начать с анализа причин сложившейся ситуации.

Проблема защиты машинной информации на современном уровне развития информатизации общества столь важна и многогранна, что заслуживает более подробного рассмотрения, чем другие аспекты автоматизации профессиональной деятельности. Более подробные сведения можно найти в других источниках (например, [14, 19, 20, 31, 33]).

Для того чтобы объединить усилия всех специалистов в направлении конструктивной работы над созданием защищенных систем, необходимо определить, что является целью исследований, что мы хотим получить в результате и чего в состоянии достичь. Для ответа на эти вопросы и согласования всех точек зрения на проблему создания защищенных систем разработаны и продолжают разрабатываться стандарты информационной безопасности. Это документы, регламентирующие основные понятия и концепции информационной безопасности на государственном или межгосударственном уровне, определяющие понятие «защищенная система» посредством стандартизации требований и критериев безопасности, образующих шкалу оценки степени защищенности вычислительных систем (ВС). В соответствии с этими документами защищенная система обработки информации представляет собой систему, отвечающую тому или иному стандарту информационной безопасности. Этот факт позволяет сопоставлять степени защищенности различных систем относительно установленного стандарта.

Основные понятия и определения.Политика безопасности — совокупность норм и правил, обеспечивающих эффективную защиту системы обработки информации от заданного множества угроз.

Модель безопасности — формальное представление политики безопасности.

Дискреционное, или произвольное, управление доступом — управление доступом, основанное на совокупности правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от грифа секретности информации и уровня допуска пользователя.

Ядро безопасности — совокупность аппаратных, программных и специальных компонентов ВС, реализующих функции защиты и обеспечения безопасности.

Идентификация — процесс распознавания сущностей путем присвоения им уникальных меток (идентификаторов).

Аутентификация — проверка подлинности идентификаторов сущностей с помощью различных (преимущественно криптографических) методов.

Адекватность — показатель реально обеспечиваемого уровня безопасности, отражающий степень эффективности и надежности реализованных средств защиты и их соответствия поставленным задачам (в большинстве случаев это задача реализации политики безопасности).

Квалификационный анализ, квалификация уровня безопасности — анализ ВС с целью определения уровня ее защищенности и соответствия требованиям безопасности на основе критериев стандарта безопасности.

Таксономия — наука о систематизации и классификации сложноорганизованных объектов и явлений, имеющих иерархическое строение. Таксономия основана на декомпозиции явлений и поэтапном уточнении свойств объектов (иерархия строится сверху вниз).

Прямое взаимодействие — принцип организации информационного взаимодействия (как правило, между пользователем и системой), гарантирующий, что передаваемая информация не подвергается перехвату или искажению.

Защищенная система обработки информации для определенных условий эксплуатации обеспечивает безопасность (доступность, конфиденциальность и целостность) обрабатываемой информации и поддерживает свою работоспособность в условиях воздействия на нее заданного множества угроз.

Под защищенной системой обработки информации предлагается понимать систему, которая:

осуществляет автоматизацию некоторого процесса обработки конфиденциальной информации, включая все аспекты этого процесса, связанные с обеспечением безопасности обрабатываемой информации;

успешно противостоит угрозам безопасности, действующим в определенной среде;

соответствует требованиям и критериям стандартов информационной безопасности.

Отсюда вытекают следующие задачи, которые необходимо и достаточно решить, для того чтобы создать защищенную систему обработки информации, а именно:

в ходе автоматизации процесса обработки конфиденциальной информации реализовать все аспекты этого процесса, связанные с обеспечением безопасности обрабатываемой информации;

обеспечить противодействие угрозам безопасности, действующим в среде эксплуатации защищенной системы;

реализовать необходимые требования соответствующих стандартов информационной безопасности.

Угрозы безопасности компьютерных систем.Под угрозой безопасности компьютерных систем понимаются воздействия на систему, которые прямо или косвенно могут нанести ущерб ее безопасности. Приведем наиболее общую классификацию возможных угроз безопасности. Все угрозы можно разделить по их источнику и характеру проявления.

Случайные угрозы возникают независимо от воли и желания людей. Данный тип угроз связан прежде всего с прямым физическим воздействием на элементы компьютерной системы (чаще всего природного характера) и ведет к нарушению работы этой системы и/или физическому уничтожению носителей информации, средств обработки и передачи данных, физических линий связи.

Причиной возникновения технических угроз случайного характера могут быть как сбои вследствие ошибок персонала (порожденные людьми), так и случайные нарушения в работе оборудования системы (например, вследствие поломки какого-либо узла или устройства, сбоя в работе ПО или элементарное короткое замыкание). Последствиями подобных событий могут быть отказы и сбои аппаратуры, искажение или уничтожение информации, нарушение линий связи, ошибки и физический вред персоналу.

Примером реализации случайной угрозы, созданной людьми, может быть физическое нарушение проводных линий связи из-за проведения строительных работ. Другими словами, угрозы данного типа возникают вследствие каких-либо действий людей, целью которых не является нанесение физического вреда и нарушение функционирования работы компьютерной системы и/или отдельных ее сегментов и ресурсов, однако побочный эффект данных действий приводит к нарушениям и сбоям в работе системы.

Преднамеренные угрозы в отличие от случайных могут быть созданы только людьми и направлены именно на дезорганизацию компьютерной системы. Примером реализации такой угрозы может быть как физическое уничтожение аппаратуры и сетевых коммуникаций системы, так и нарушение ее целостности и доступности, а также конфиденциальности обрабатываемой и хранимой ею информации с применением средств и ресурсов самой системы, а также с использованием дополнительного оборудования.

Тема 5 .Критерии оценки безопасности информационных технологий

Общие критерии оценки защищённости информационных технологий, Общие критерии, ОК — принятый в России международный стандарт по компьютерной безопасности. В отличие от стандарта FIPS 140, Common Criteria не приводит списка требований по безопасности или списка особенностей, которые должен содержать продукт.

Критерии оценки безопасности информационных технологий

функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;

требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации

Тема 6 .Структура и содержание нормативно-правовой базы информационной безопасности РК

Концепция информационной безопасности Республики Казахстан (далее - Концепция) разработана в целях обеспечения интересов общества и государства в информационной сфере, а также защиты конституционных прав гражданина.

Концепция отвечает основным положениям Стратегии развития Республики Казахстан до 2030 года "Процветание, безопасность и улучшение благосостояния всех казахстанцев", в которой обеспечение информационной безопасности как составляющей национальной безопасности определено одним из основных долгосрочных приоритетов.

Концепция основана на оценке текущей ситуации и определяет государственную политику, перспективы деятельности государственных органов в области обеспечения информационной безопасности.

Концепция разработана в соответствии с Конституцией Республики Казахстан и законами Республики Казахстан "О национальной безопасности Республики Казахстан", "О государственных секретах", "О противодействии терроризму", "Об электронном документе и электронной цифровой подписи", "Об информатизации", "О техническом регулировании", "О лицензировании", "О средствах массовой информации", "О связи".

При разработке Концепции также учтен имеющийся международный опыт в области обеспечения информационной безопасности, в частности США, Великобритании, Канады, Российской Федерации, Индии, Эстонии. В Концепции выдержан соответствующий международному опыту комплексный подход к реализации вопросов обеспечения информационной безопасности, включающий законодательное, нормативно-методическое, организационное, технологическое и кадровое обеспечение.

Также в положения Концепции включены основные направления Концепции сотрудничества государств-участников Содружества Независимых Государств в сфере обеспечения информационной безопасности, подписанной в г. Бишкеке 10 октября 2008 года, Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, ратифицированного Законом Республики Казахстан от 1 июня 2010 года "О ратификации Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности".

Концепция выражает совокупность официальных взглядов на сущность и содержание деятельности Республики Казахстан по обеспечению информационной безопасности государства и общества, их защите от внутренних и внешних угроз. Концепция определяет задачи, приоритеты, направления и ожидаемые результаты в области обеспечения информационной безопасности личности, общества и государства. Она является основой для конструктивного взаимодействия органов государственной власти, бизнеса и общественных объединений для защиты национальных интересов Республики Казахстан в информационной сфере. Концепция призвана обеспечить единство подходов к формированию и реализации государственной политики обеспечения информационной безопасности, а также методологическую основу для совершенствования нормативных правовых актов, регулирующих данную сферу.

Растущая степень открытости экономик, свободы перемещения товаров, капиталов и трудовых ресурсов, межличностного взаимодействия размывает грань между внутренними и внешними политическими, экономическими и информационными процессами.

Технологическая эволюция становится источником принципиально новых угроз, предоставляя недоступные ранее возможности негативного влияния на личность, общество и государство.

Усиливается роль и влияние средств массовой информации и глобальных коммуникационных механизмов. Информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями.

Настоящая Концепция определяет основные стратегические цели, задачи и направления, стоящие перед страной в целях обеспечения ее информационной безопасности.