Вопрос 6. Система защиты информации.

Система защиты определяется как организованная совокупность всех органов, средств, методов и мероприятий, предусматриваемых в КИС для обеспечения защиты информации от разглашения, утечки и несанкционированно доступа к ней.

В современных условиях процесса информатизации построение системы защиты должно осуществляться на следующих **принципах**: концептуальное единство, соответствие требованиям, адаптируемость, функциональная самостоятельность, удобство эксплуатации, минимизация привилегий, полнота контроля, активность реагирования, невидимость защиты, невозможность перехода в небезопасное состояние, невозможность миновать средства защиты, принцип равнопрочности границ, разделение обязанностей, экономичность.

В соответствии с теорией защиты информации существует два подхода к построению системы защиты: **фрагментарный и системный**

Фрагментарный подход направлен на противодействие четко определенным угрозам. В качестве примеров реализации подхода можно указать отдельные средства управления доступом, автономные средства шифрования, специализированные антивирусные программы и т.д.

Достоинством данного подхода является высокая избирательность к конкретной угрозе. Существенные недостатки отсутствие единой защищенной среды обработки информации, потеря эффективности защиты при видоизменении угрозы безопасности, внешней среды, деятельности организации.

Фрагментарный подход к защите информации применяется только в узких рамках и лишь для обеспечения безопасности относительно простых КИС. В современных же условиях наиболее рациональным и правильным является использование **системного подхода** к защите информации.

Системный подход ориентирован на создание защищенной среды обработки информации, объединяющей в единую систему средства противодействия угрозам. Организация защищенной среды позволяет гарантировать определенный уровень безопасности КИС, что является несомненным достоинством системного подхода. Недостатки подхода — ограничение на свободу действий пользователей системы, большая чувствительность к ошибкам установки и настройки средств защиты, сложности управления. Как правило, системный подход применяют для защиты КИС крупных организаций или небольших систем, выполняющих ответственные задачи или обрабатывающих особо важную информацию.

Процесс разработки системы защиты включает в себя следующие этапы:

— аудит информационной безопасности КИС, для которой строится система защиты;

— выбор методов и средств защиты информации;

— проектирование системы защиты;

— реализация и сопровождение системы защиты.

Аудит информационной безопасности КИС представляет собой процесс сбора и анализа информации, необходимой для оценки существующего уровня защиты, анализа риска и формулирования требований к системе защиты. Как правило, аудит проводится с целью подготовки технического задания на систему защиты либо после внедрения – для оценки ее эффективности. Аудит осуществляется как сторонними компаниями, работающими в данной области, так и силами своих сотрудников.35 На данном этапе работ определяются все информационные ресурсы КИС, подлежащие защите, потенциальные угрозы безопасности, строится неформальная модель нарушителя системы защиты.

Выбор оптимального состава методов и средств защиты является вторым этапом создания системы защиты.

Этап проектирования системы защиты предполагает создание оптимальных механизмов обеспечения защиты информации и механизмов управления ими для заданной КИС.36 Проектирование осуществляется в различных условиях, на которые определяющее влияние оказывают следующие параметры: состояние КИС, для которой разрабатывается система защиты, и уровень затрат на защиту.

Для первого параметра выделяется три состояния системы: система функционирует, имеется готовый проект, система проектируется. Затраты на защиту могут быть ограничены определенным уровнем, либо определяться в процессе проектирования системы защиты и поэтому с точки зрения проектирования будут неограниченными.

Наилучшим вариантом разработки системы защиты является параллельное проектирование системы защиты с проектированием КИС, начиная с момента выработки общего решения построения системы управления и обработки данных. Невыполнение этого принципа, «наложение» системы защиты на готовую КИС может привести к низкой эффективности защиты, снижению производительности и быстродействия средств вычислительной техники, увеличению затрат.

Проектирование системы защиты осуществляется с учетом анализа сведений, полученных в результате исследования угроз безопасности, методов и средств защиты, конфигурации технических средств и технологии обработки информации в КИС.

Результатом проектирования системы защиты является **техническое решение** документ, содержащий требования к системе защиты; цели, задачи, функции защиты; правила обработки информации, обеспечивающие ее защиту от различных угроз; перечень возможных угроз безопасности, перечень защищаемых компонентов КИС.

В общем виде система защиты КИС организации графически представляется в виде соответствующей модели, структурно состоящей из

средств защиты, размещаемых в соответствии с рубежами защиты, и управления, осуществляемым службой защиты информации.

Заключительными этапами построения системы защиты является **реализация и сопровождение.** На этапе реализации производится настройка средств защиты, необходимых для выполнения функций, зафиксированных в техническом решении. На практике применяются два способа реализации механизмов защиты: **добавленная и встроенная.**

В первом случае защита информации при обработке, передаче, хранении обеспечивается дополнительными средствами, не входящими в состав самой КИС. При встроенной защите ее механизмы являются неотъемлемой частью системы, разработанной и реализованной с учетом определенных требований безопасности. При этом средства защиты составляют единый механизм, отвечающий за обеспечение защиты.

Добавленная защита является более гибкой, ее механизмы можно добавлять или удалять по мере необходимости. Встроенная защита обладает жестко фиксированным набором функций, которые трудно расширить или удалить. Как правило, на практике используется комбинация этих вариантов.

Этап сопровождения заключается в контроле использования средств защиты в процессе обработки информации; сборе, обработке и организации баз данных, относящихся к защите; непрерывном распознавании ситуаций относительно защищенности системы; регистрации происходящих событий; принятии решений на оперативное вмешательство в функционирование системы защиты; реализации принятых решений; анализе защищенности системы; разработке предложений по корректировке системы; разработке организационно-распорядительных и методических документов, относящихся к функционированию системы защиты.

Дополнительный материал!!!

Современное развитие человеческой цивилизации, вступившей в XXI в., характеризуется наиболее интенсивным использованием информационных технологий во всех сферах общественной жизни. В настоящее время трудно назвать те области жизнедеятельности, успехи в которых не были бы связаны с применением таких технологий.

Использование же информационных технологий в управлении организацией, позволяют улучшить и эффективно организовать процесс документационного обеспечения управления и информационного обеспечения управления. Тем не менее, повсеместное использование информационных технологий влечет за собой и ряд проблем – появление разнообразных угроз информационной безопасности и, следовательно, необходимость создания комплексной системы защиты информации.

«Сегодня наиболее распространенными и опасными угрозами информационной безопасности являются кража информации, халатность сотрудников организации, вредоносные программы, саботаж, хакерские

атаки, финансовое мошенничество, спам, аппаратно-программные сбои, кража оборудования».

Исходя из перечисленных угроз, целесообразно использовать при создании системы защиты информации именно системный подход, который базируется на комплексном применении организационных, технических, законодательных и морально-этических средств защиты.

Проблема успешной реализации действий, направленных на обеспечение защиты информации возникла очень давно, однако, наиболее интенсивное развитие она получила в период массовой информатизации общества и измеряется в более чем 40 лет. В 70-ые – начало 80-ых гг. выявляются основные направления поиска, разработки и реализации средств защиты информации

Создание системы защиты информации проходит в несколько этапов: 39

1. проведение аудита информационной безопасности системы электронного документооборота (СЭД);
2. выбор методов и средств защиты;
3. проектирование системы защиты, ее реализация и сопровождение системы.

Аудит информационной безопасности является первым этапом конструирования системы защиты информации. Его сущность заключается в поэтапном проведении анализа существующего информационного, программно – аппаратного и кадрового компонента организации, выявлении уязвимостей, оценке рисков и прогнозировании их последствий.

При проведении аудита должны быть учтены и рассмотрены все составляющие – состав информационного массива, способы хранения документированной информации, ее передача, обработка, ценность, степень доступа к ней и др.

В процессе проведения аудита устанавливается степень важности информации для организации и выделяется комплекс документов, при нежелательном воздействии на который организация может понести серьезные убытки. Это может быть производственная, технологическая или финансовая документация.

Параллельно идет обследование программно-технической составляющей системы и персонала. Проводится тестирование конкретных программных продуктов на выявление слабых мест, определяется степень изношенности, соответствие нынешнему развитию программных продуктов на рынке. В кадровом вопросе дело обстоит более тонко. Необходимо назначить функциональные права групп пользователей, распределить доступ к документам. Тонкость состоит в том, что все решения в этой области нужно документировать путем включения принятых положений в локальные нормативные акты организации (должностные инструкции, договоры о неразглашении конфиденциальной информации, положения о структурном

подразделении и т.д.). Это подразумевает под собой существенную переработку организационной документации и возлагает большой объем работы на службу ДОУ.

Следующий этап аудита связан с анализом угроз. Угрозы возникают из-за существования так называемых уязвимостей системы. Уязвимость – это конкретная характеристика, в определенных условиях ведущая к нежелательному изменению элементов системы. Применительно к информационным системам существует следующая классификация уязвимостей40. Уязвимости проектирования связанны с ошибками в проекте или алгоритме. Этот класс наиболее трудоемок в исправлении, так как даже при идеальном воплощении проект будет дефектен, и, следовательно, будет представлять собой уязвимость. Уязвимости реализации возникают в том случае, когда корректный с точки зрения безопасности алгоритм или проект исполняется неправильно. Эти ошибки исправляются легче, потому что объект изначально не несет в себе уязвимости. Уязвимости эксплуатации заключаются в погрешностях при конфигурировании аппаратного и программного обеспечения. Они наиболее распространены и легче всего исправляются.

На заключительном этапе проводится оценка рисков реализации угроз. В настоящий момент основой большинства ошибок при принятии решений по вопросам безопасности как раз таки является неправильная оценка рисков. При проведении оценки рисков определяется41:

- перечень сил и средств защиты, необходимый для гарантии безопасности объекта;
- адекватность задействованных сил и средств защиты, расстановку приоритетов в реализации алгоритмов противодействия;
- реальную оценку возможного экономического ущерба.

Работы по проведению оценки рисков заключаются в следующем:

1. идентификация ключевых ресурсов;
2. определение важности ресурсов;
3. идентификация существующих угроз и уязвимостей;
4. создание неформальной модели нарушителя;
5. вычисление рисков, связанных с осуществлением угроз безопасности.

По результатам аудита формируют запросы и цели дальнейших этапов построения системы защиты информации.

Проведенный аудит позволит обоснованно создать следующие документы:

- Долгосрочный план развития информационной системы.
- Политика безопасности организации.
- Методология работы информационной системы организации.

 План восстановления информационной системы в чрезвычайной ситуации.

Таким образом, можно сказать, что аудит проводят для того, чтобы оперативно получать систематизированную и достоверную информацию для оценки системы, принятия решения, управления ею. Аудит подразумевает под собой соответствие некоему стандарту, и на данный момент таких стандартов существует великое множество. Результаты аудита влияют на принятие решений во многих сферах повседневной деятельности организации, таких как долгосрочные планы развития информационной инфраструктуры, политика в области управления службой безопасности, отдела ДОУ, кадрами в целом. Процесс аудита осуществляется поэтапно, с обязательным документированием всех этапов. Особая нагрузка ложится на службу ДОУ, которая обеспечивает закрепление результатов и решений аудита в организационно-распорядительных документах организации.

Аудит выявляет степень необходимости защиты и в результате составляется экономически обоснованный план, который предопределяет дальнейший ход действий руководства в этой области.

На втором этапе построения системы защиты информации необходимо выбрать состав методов и средств защиты информации.

При создании системы защиты информации целесообразно применять комплексный системный подход, который базируется на совместном применении организационных, технических, законодательных и морально-этических средств защиты.

Все средства защиты информации можно разделить на две группы – формальные и неформальные. К формальным относятся средства, которые выполняют свои функции формально, то есть преимущественно без участия человека. К неформальным относятся средства, основу которых составляет целенаправленная деятельность людей.

Формальные средства защиты представлены техническими средствами, которые в свою очередь состоят из физических, аппаратных, программных и криптографических средств.

Технические средства защиты информации – это средства, в которых основная защитная функция реализуется некоторым техническим устройством44.

Физические средства – механические, электрические, электромеханические, электронные, электронно-механические и тому подобные устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов. Физические средства выполняют следующие функции:

 внешняя защита – защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств объекта;

- внутренняя защита – защита от дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации;
- опознавание – специфическая группа средств, предназначенная для опознавания людей и идентификации технических средств по различным индивидуальным характеристикам.

Физические средства включают организации режима охраны объектов, организацию пропускного режима, противопожарную защиту.

Аппаратные средства – различные электронные, электронно-механические и тому подобные устройства, встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач по защите информации. Аппаратные средства предназначены для нейтрализации технических каналов утечки информации, защиты информации от утечки, поиска закладных устройств съема информации, маскировки сигнала, содержащего конфиденциальную информацию. К аппаратным средствам можно отнести генераторы шума, уничтожители информации на магнитных носителях, электронные замки, блокираторы, устройства сигнализации о попытках несанкционированных действий пользователей.

Программные средства – специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения автоматизированных систем с целью решения задач защиты информации. К основным программным средствам относятся:

- программы идентификации и аутентификации пользователей;
- программы разграничения доступа к ресурсам;
- программы защиты информационных ресурсов от несанкционированного изменения использования и копирования;
- антивирусные программы;
- программы аудита;
- программы имитации работы с нарушителем и т.д.

Криптографические средства защиты информации служат для защиты содержания от раскрытия при помощи различных кодов и шифров.

К несомненным достоинствам технических средств защиты информации относятся широкий круг задач, достаточно высокая надежность, возможность создания развитых комплексных систем защиты, гибкое реагирование на попытки несанкционированных действий, традиционность используемых методов осуществления защитных функций.

Основными недостатками являются высокая стоимость многих средств, необходимость регулярного проведения регламентных работ и контроля, возможность подачи ложных тревог.

Неформальные средства делятся на организационные, законодательные и морально-этические средства.

Организационные средства – специально предусматриваемые в технологии функционирования объекта организационно-методические мероприятия по защите информации, осуществляемые в виде целенаправленной деятельности людей

Насколько важным являются организационные мероприятия в общем арсенале средств защиты, говорит уже хотя бы тот факт, что ни одна система обработки данных не может функционировать без участия обслуживающего персонала. Кроме того, организационные мероприятия охватывают все структурные элементы системы защиты на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверка в эксплуатации аппаратуры, оргтехники, средств обработки и передачи данных.

Одним из основных организационных средств защиты информации является организация защиты персональных электронно-вычислительных машин (далее ПЭВМ), информационных систем и сетей. «Организация защиты ПЭВМ, информационных систем и сетей определяет порядок и схему функционирования основных ее подсистем, использование устройств и ресурсов, взаимоотношения пользователей между собой в соответствии с нормативными требованиями и правилами»

В организациях, использующих в своей деятельности сведения с ограниченным доступом, для проведения мероприятий по защите информации могут создаваться соответствующие службы безопасности (службы защиты информации).

К уровню организационных средств относятся действия общего характера, предпринимаемые руководством организации, относящиеся к правовым мерам. На данном уровне главное – сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел. «Основой программы является политика безопасности, отражающая подход организаций к защите своих информационных активов. Руководство каждой организации должно осознавать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности строится на анализе рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под нее выделяются ресурсы, назначаются ответственные и определяется порядок контроля ее выполнения».

Законодательные средства47 – существующие в стране нормативно-правовые акты, с помощью которых регламентируются права обязанности, связанные с обеспечением защиты информации, всех лиц и подразделений, имеющих отношение к функционированию системы защиты, а также

устанавливается ответственность за нарушение правил обработки информации, следствием чего может быть нарушение защищенности информации.

В нашей стране разработаны следующие нормативно-правовые акты, регламентирующие некоторые вопросы защиты информации: Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», закон Республики Беларусь от 11 августа 1998 г. N 194-З «Об авторском праве и смежных правах» (с последующими изменениями и дополнениями), закон Республики Беларусь «Об электронном документе и ЭЦП», закон Республики Беларусь от 6 октября 1994 г. № 3277-XII «О Национальном архивном фонде и архивах в Республике Беларусь» (в редакции Закона Республики Беларусь от 06.01.1999 N 236-З), Уголовный Кодекс Республики Беларусь, Постановление Совета Министров Республики Беларусь от 10 февраля 2000 г. № 186 «О некоторых мерах по защите информации в Республике Беларусь», СТБ ГОСТ Р 50922-2000 «Защита информации. Основные термины и определения», СТБ 982-94 «Информационные технологии. Термины и определения», СТБ 1176.2-99 «Информационная технология. Защита информации. Процедура выработки и проверки электронной цифровой подписи», СТБ 1176.1-99 «Информационная технология. Защита информации. Функция хэширования».

Законы Республики Беларусь по вопросам защиты информации, в основном, освящают ключевые термины и понятия, относящиеся к данной сфере, цели, объекты, субъекты защиты, их права и обязанности. Так же они регламентируют правонарушения в этой области и меры ответственности за них.

Морально-этические средства48 – сложившиеся в обществе или в данном коллективе моральные нормы и этические правила, соблюдение которых способствует защите информации, а нарушение приравнивается к несоблюдению правил поведения в обществе или коллективе.

Морально-этические средства предполагают, прежде всего, воспитание сотрудника, то есть проведение специальной работы, направленной на формирование у него системы определенных качеств, взглядов и убеждений, и обучение сотрудника правилам и методам защиты информации, привитие ему навыков работы с носителями секретной и конфиденциальной информации.

Абсолютная необходимость создания комплексной системы защиты информации очевидна.

Решение же проблемы создания комплексной системы защиты требует не только научно обоснованных концепций комплексной защиты, но и создания хорошего инструментария в виде разнообразных средств обеспечения защиты информации.

Система защиты информации является по определению «человеко-машинной» системой и работник в ней является не только основным звеном, но и потенциальной угрозой, так как чаще несанкционированный доступ и утечка

информации обусловлены злоумышленными действиями или же небрежностью пользователей и персонала. Эти факторы практически невозможно исключить или локализовать при помощи аппаратных и программных средств, криптографии и физической защиты. Поэтому совокупность организационных средств, применяемых совместно с техническими методами, ставят перед собой цель исключить, уменьшить или полностью устранить потери при действии различных нарушающих факторов.

Третий этап построения системы защиты информации проводится на основе результатов первых двух: при процессе аудита информационной безопасности анализируются риски и формируются требования к системе защиты информации, на основе аудита определяется оптимальный набор методов и средств защиты информации.

Выбранные методы и средства при проектировании трансформируются в систему защиты информации – совокупность механизмов обеспечения информационной безопасности и механизма управления ими. При этом разрабатывается техническое решение и графическое представление в виде соответствующей модели.

Проектирование системы защиты информации лучше всего проводить параллельно с проектирование автоматизированной системы документационного обеспечения управления. В процессе проектирования должны принимать участие не только узкоспециализированные технические работники, но и работники, занимающиеся общими вопросами организации делопроизводства и документооборота (сотрудники службы ДОУ, архивные работники, секретари-референты).

Для повышения эффективности защиты выделяются общеметодологические принципы проектирования системы защиты:

1. концептуальное единство;
2. соответствие выдвинутым требованиям ;
3. невидимость защиты;
4. функциональная самостоятельность;
5. удобство эксплуатации;
6. минимизация привилегий;
7. полнота контроля;
8. невозможность перехода в небезопасное состояние;
9. невозможность миновать средства защиты;
10. экономичность.

При реализации системы защиты информации проводится настройка средств защиты. Реализация осуществляется в соответствии с планом внедрения, который утверждается руководителем организации и содержит сведения о сроках внедрения и ответственных лицах. Планирование связано не только с наилучшим использование всех возможностей, которыми располагает

организации, в том числе выделенных ресурсов, но и с предотвращением ошибочных действий, могущих привести к снижению эффективности системы защиты информации.

Сопровождение системы защиты информации заключается в контроле использования средств защиты, сборе и анализе информации, относящейся к вопросам защиты, мониторинге происходящих событий, анализе защищенности информации, разработке предложений по корректировке системы защиты. Из этого следует, что, когда система построена и реализована, необходимо убедиться, что остаточные риски стали приемлемыми. Проверка системы защиты называется «тестированием на проникновение», ее цель – предоставление гарантий того, что не существует простых путей для неавторизованного пользователя обойти механизмы защиты.

Для организации контроля функционирования системы необходимо разработать план проведения план контрольных мероприятий, содержащий сведения о времени, периодичности, полноте контроля, количестве контролируемых элементов.

При внедрении и функционировании системы защиты информации необходима особо тщательная организация текущей работы с персоналом, включающая периодические мероприятия по повышению уровня грамотности сотрудников в области защиты информации, проведения семинаров и тренингов.

Особое внимание необходимо уделить методическому, нормативному и документационному обеспечению работ по защите информации.

Абсолютная необходимость создания комплексной системы защиты информации очевидна.

Решение же проблемы создания комплексной системы защиты требует не только научно обоснованных концепций комплексной защиты, но и создания хорошего инструментария в виде разнообразных средств обеспечения защиты информации.

Система защиты информации является по определению «человеко-машинной» системой и работник в ней является не только основным звеном, но и потенциальной угрозой, так как чаще несанкционированный доступ и утечка информации обусловлены злоумышленными действиями или же небрежностью пользователей и персонала. Эти факторы практически невозможно исключить или локализовать при помощи аппаратных и программных средств, криптографии и физической защиты. Поэтому совокупность организационных средств, применяемых совместно с техническими методами, ставят перед собой цель исключить, уменьшить или полностью устранить потери при действии различных нарушающих факторов.

Система защиты информации создается непосредственно для организации, исходя из ее специфики и предъявляемых требований по обеспечению информационной безопасности. Следовательно, организация

должна предпринимать в дальнейшем меры по развитию менеджмента информационной безопасности.

Анализ отечественного рынка средств защиты информации (программно-технологическое обеспечение) Белорусский рынок средств защиты в области информационной безопасности можно называть еще только формирующимся. Причем формирование это пока далеко от завершения.

На сегодняшний день на рынке Беларуси распространены программные средства защиты десятка компаний. Но многие из них, несмотря на требование законодательства, являются несертифицированными.

Порядок сертификации средств защиты информации также не совершенен. Можно взять из профиля защиты (стандарт безопасности) произвольно какие-либо функции безопасности и сертифицировать на их наличие. Т.е. можно сертифицировать многофункциональное устройство на какую-либо малозначительную функцию – и все, его можно поставлять, как якобы полноценное средство защиты. Законодательство обуславливает в качестве необходимого условия поставки средств защиты лишь наличие сертификата или положительного экспертного заключения, но вовсе не требует соответствия защитных функций поставляемого средств защиты реальным угрозам безопасности, как должно быть на самом деле.

За основу анализа средств защиты информации возьмем решения компаний, прошедших сертификацию в Оперативно-аналитическом центре при Президенте Республике Беларусь.

BELCrypt — аппаратно-программное средство криптографической защиты информации, решение от **ЗАО «БелХард Групп»** (http://www.belhard.com).

BELCrypt выполнено на основе многофункциональной микропроцессорной карте (ММК) и имеет несколько исполнений:

- в виде смарт-карты с контактным интерфейсом;
- в виде смарт-карты с бесконтактным (радио) интерфейсом;
- в виде USB ключа с SIM модулем.

BHMCrypt32v2 — программное средство криптографической защиты информации. Весьма будет полезна банковским организациям.

BelIPSEC — средство криптографической защиты сетевого протокола IP. Автоматически обеспечивает защиту всех протоколов лежащих на более высоком уровне: TCP, FTP, TFTP, X.400, HTPP, Telnet, SMTP, SNMP, NFS, FTAM, и д.р.

BELCrypt, BHMCrypt32v2, BelIPSEC реализуют функции криптографической защиты информации в соответствии со стандартами Республики Беларусь:

- шифрование данных IP пакетов по алгоритму ГОСТ 28147-89;

 ЭЦП в соответствие с СТБ 1176.2-99;
 функцию хэширования в соответствии с СТБ 1176.1-99;
 процедуру выработки псевдослучайных данных в соответствии с РД РБ 07040.1202-2003 «Банковские технологии. Процедуры выработки псевдослучайных данных с использованием секретного параметра».
 протокол формирования общего ключа шифрования в соответствии с алгоритмом, определенным в проекте руководящего документа Республики Беларусь РД РБ «Банковские технологии. Протоколы формирования общего ключа».

Многофункциональная микропроцессорная карта (ММК) с реализацией средств цифровой подписи и шифрования в соответствии со стандартами Республики Беларусь и международными стандартами.

Система безопасности ММК обеспечивает защиту от несанкционированного доступа, достоверность данных и безопасную передачу сообщений.

Основные функции, выполняемые системой безопасности:

 разграничение прав доступа к данным карты;
 обеспечение конфиденциальности данных;
 обеспечение целостности и достоверности данных;
 подтверждение подлинности данных;
 гибкая система управления ключами.

Программные решения от **ГНПО "Агат"** (http://www.agat.by)

Программа контроля целостности «ПКЦЛ» предназначена для реализации контроля целостности файлов программного обеспечения и данных, хранящихся на ПЭВМ, и доведения до администратора защиты сообщений о результатах работы программы. Контроль осуществляется путем сравнения актуального состояния файлов ПО с контрольными данными (эталонами), которые формируются при установке программы, а также по команде администратора.

Программа «ПКЦЛ» работает совместно с программой расчета значения хэш-функции файла «ХЭШ».

Программа «ХЭШ» предназначена для расчета значения хэш-функции файла. Расчет хэш-функции файлов производится по СТБ 1176.1-99.

Программа «ХЭШ» выполняет следующие функции:

– производит расчет хэш значения файлов;

– выводит результат расчета в командную строку.

Среди разработок компаниии ряд комплексных решений по обеспечению защиты информации. Вызывает интерес **Комплекс программ защиты информации автоматизированного рабочего места администратора защиты** (КП ЗИ АРМ АЗ). Он предназначен для реализации функций

администрирования программных средств защиты на АРМ пользователей и серверах автоматизированной системы, а также настройки, контроля и поддержания в актуальном состоянии программных средств защиты и параметров групповых политик безопасности.

КП ЗИ АРМ АЗ обеспечивает выполнение следующих функций:

- управление контролем целостности программного обеспечения, установленного на ПЭВМ;
- управление опознанием;
- управление доступом;
- управление контролем доступа;
- управление аудитом.

КП ЗИ АРМ АЗ состоит из следующих программ:

- программа "Администратор ЗИ" ЕИРВ.50644-01;
- программа "ПКЦ" ЕИРВ.50607-01;
- программа "ПГН" ЕИРВ.50643-01;
- программа "Сбор НСД".

Кроме самого программного обеспечения, ГНПО "Агат" оказывает услуги в области защиты информации. Предприятие осуществляет следующие виды работ:

- разработка концепций защиты информации корпоративных локальных и распределенных систем обработки информации;
- разработка технических заданий на создание систем защиты информации по СТБ 34.101.9-2004;
- разработка программных средств защиты информации, в т.ч. средств контроля и управления доступом, аудита безопасности, генерации, оценки качества и назначения паролей, проверки целостности данных и ПО;
- разработка протоколов защищенного информационного взаимодействия объектов автоматизированных информационных систем;
- интеграция в информационные системы типовых проектных решений в области защиты информации.

ЗАО «АВЕСТ» завоевала долю рынка с помощью нескольких решений:

1. **Криптопровайдер AVEST CSP** - расширение криптографического ядра системы Microsoft Windows (разработанное в соответствии со спецификацией Microsoft Crypto API), которое позволяет использовать криптографические алгоритмы сертифицированные Государственным Центром Безопасности Информации при Президенте Республики Беларусь (ГЦБИ) всем приложениям Microsoft Windows. В марте 2004 года завершена сертификация криптопровайдера AVEST CSP на соответствие национальному стандарту СТБ, что позволяет использовать его в соответствии с Законом РБ "Об электронном документе" для оформления любых юридических и хозяйственных действий в Республике Беларусь электронным способом. В настоящее время

криптопровайдер AVEST CSP – единственный криптопровайдер в Республике Беларусь.

2. Набор программного обеспечения для организации инфраструктуры открытых ключей **(PKI)** – Центр цифровых сертификатов, Центр регистрации, Персональный менеджер сертификатов.

В настоящее время деятельность предприятия ведется по следующим основным направлениям:

1. Усовершенствование и разработка новых программных решений для организации инфрастуктуры открытых ключей для защиты документооборота в крупных корпорациях, а также по другим направлениям криптографической защиты информации (защита сетевого трафика и др.).

2. Сотрудничество с разработчиками офисного ПО (систем электронного документооборота, электронного архива, систем клиент-банк, и.т.д.) на предмет тестирования работы этих приложений с криптоядром AVEST CSP;

3. Сотрудничество с государственными органами в области разработки нормативно-правовой базы регулирующей защиту информации в электронном документообороте в Республике Беларусь.

Итак, основные разработки ЗАО «АВЕСТ», прошедшие сертификацию:

- программное обеспечение программно-аппаратной платформы республиканского удостоверяющего центра инфраструктуры открытых ключей. Программа автоматической обработки запросов к удостоверяющему центру. AvCAServer.exe;
- программное средство криптографической защиты информации «Криптопровайдер Avest CSP for BelSSF»;
- программный комплекс «Автоматизированное рабочее место плательщика» ;
- программный комплекс «Сервер TLS АВЕСТ»;
- программный комплекс «АВЕСТ TLS tunnel»;
- программный комплекс «Определение статуса цифровых сертификатов Avest Revocation Provider»;
- программное средство электронной цифровой подписи и шифрования «AvCrypt ver.5.0».

Все продукты ЗАО "АВЕСТ" реализуются на основе лицензий, дающих право пользователю на использование данного продукта в рамках условий, определеных в лицензионном договоре.

Для примера приведем цену программного средства "Криптопровайдер Avest CSP" (AvCSP) , включающий сертифицированное программное средство ЭЦП и шифрования "AvCrypt ver.5.0". и программного комплекса "Персональный менеджер сертификатов АВЕСТ" (AvPCM).

Цена колеблется в зависимости от количества приобретаемого продукта и срока действия лицензии. Так стоимость 1-10 продуктов сроком лицензии на 1

год составит всего 17 у.е. Приобретая более 500 лицензий на 10 лет достаточно потратить 26 у.е. Совсем недорого для большой организации.

А вот программное обеспечение для организации инфраструктуры открытых ключей обойдется в сотни раз дороже (цены в USD).

Программный комплекс "Центр цифровых сертификатов АВЕСТ" - лицензия на организацию корневого и одного подчиненного Удостоверяющего центра составляет 9300.

Программный комплекс "Центр цифровых сертификатов АВЕСТ" - лицензия на организацию одного дополнительного подчиненного Удостоверяющего центра составляет 2500.

Программный комплекс "Центр регистрации АВЕСТ" (AvRA) - первая лицензия составит 1500.

ЗАО "НПП БЕЛСОФТ" (www.belsoft.by) предлагает услуги по оценке защищенности ИТ-инфраструктуры, обеспечению безопасности корпоративных сетей и непрерывности бизнеса, а также проведению аудита информационной безопасности.

Среди последних программных продуктов компании – **решение IP-guard**. IP-guard позволяет управлять внутренними и внешними угрозами, минимизируя риски утечки информации и блокируя внешние атаки.

IP-guard управляет инсайдерскими угрозами

Программа позволяет анализировать, контролировать и управлять доступом сотрудников и партнеров к информационным активам компании и интеллектуальной собственности. С помощью IP-guard осуществляется контроль над тем, какие данные доступны для работы, какие данные запрашиваются и когда. Также с помощью данного продукта можно быстро и легко внедрить принципы "разделения обязанностей" и "наименьшего уровня привилегий", предусматривающие доступ сотрудников только к необходимым ресурсам для выполнения их работы.

IP-guard как способ управления внешними угрозами

В IP-guard есть возможность обнаружения вторжений и расширенного контроля сети для минимизации внешних угроз. При помощи различных модулей, администратор видит любое неадекватное поведение в сети, которое может означать угрозу. Также встроенные модули программы позволяют блокировать незаконный доступ неавторизованных компьютеров и портов.

Еще один участник рынка средств защиты – **ООО «Солидекс»** (http://www.solidex.by). Это консалтинговая компания, которая фокусируется на трех направлениях:

- создание и развитие сетей передачи данных и центров обработки данных как для предприятий, так и для операторов связи;
- защита информационных ресурсов;

 создание и развитие коммуникационных систем — телефонных систем, базирующихся на принципах пакетной коммутации; систем видеоконференцсвязи; центров обработки вызовов.

Среди сертифицированных средств защиты информации наиболее успешными являются:

 Многофункциональное устройство защиты информации «FortiMail - 100» с программным обеспечением версии 3.0;

 Многофункциональное устройство защиты информации «FortiMail - 400» с программным обеспечением версии 3.0.

Компания **«С-Терра Бел»** (http://www.s-terra.by) специализируется на разработке продукции в сфере сетевой информационной безопасности, содержащей встроенные средства криптографической защиты информации, сертифицированные в Республике Беларусь.

Продукция **Bel VPN** предназначена для защиты межсетевого взаимодействия и удаленного доступа в ведомственных (корпоративных) географически распределенных IP-сетях, банковских платежных системах, IP-телефонии, видеоконференциях. Продукты Bel VPN содержат встроенные средства криптографической защиты информации, сертифицированные в Республике Беларусь и работают как под управлением Unix-систем (Solaris, Linux), так и под управлением ОС семейства Windows (Windows XP, Windows Vista).

Основной продукт компании – **«Шлюз безопасности Bel VPN Gate»** полностью встроен в систему централизованного управления Cisco Security Manager 3.2 (CSM).

Преимущества:

1. Технологичность и универсальность.
2. Достигается многообразием используемых сетевых решений Cisco Systems и глубокой интеграцией с ними продуктов Bel VPN.
3. Сертифицированная криптография.
4. Трафик защищен белорусскими криптоалгоритмами, в основе которых лежат следующие стандарты: СТБ 1176.1-99, СТБ 1176.2-99, СТБ П 34.101.31-2007, РД РБ 07040.1202-2003.
5. Уникальность.

Программный комплекс «Шлюз безопасности Bel VPN Gate 3.0» с лицензией на неограниченное количество туннелей шифрования (Bel VPN Gate 7000) стоит примерно 15 млн. бел. руб, плюс еще услуги по установке экземпляра ПО обойдутся в 370 тыс. бел. руб, годовая подписка на сервис составляет около 1,6 млн. бел. руб.

ООО «Хедтекнолоджи Бел» (www.headtechnology.by) успешно закрепилась на рынке как эксклюзивный поставщик продуктов по информационной безопасности от ведущих мировых разработчиков: Lumension, F5, Astaro, Aventail, Clavister, IronPort, Insightix и других.

Акцент компании сделан на защите информации в сети Интернет.

Компания предлагает:

• фильтрацию электронной почты, анти-СПАМ

• фильтрацию WEB-трафика

• защиту WEB-приложений.

Наиболее популярное решение компании – программа «Blue Coat».

Продукт обеспечиваеи наивысшей степени безопасность при защите пользователей Web и Web-ориентированных приложений (фильтр нежелательного Web-контента, сканирование и блокировку шпионского ПО и вирусов, а также распознавание вредоносного контента внутри зашифрованных SSL-туннелей). Более того, Blue Coat поддерживает все известные системы аутентификации, что помогает предотвратить какие-либо попытки неавторизованного доступа к важной корпоративной информации с использованием Web. Как результат – все внутренние и внешние угрозы, имеющее отношение к Web – минимизированы.

Несмотря на все достоинства представляется, что программа еще не одаптирована под белорусские реалии. Так устройства Blue Coat работают под управлением операционной системы SGOS – облегч нной специализированно операционной системы. Хотя данное средство сертифицировано в Беларуси.

Широкий спектр аппаратных решений предлагает **ОАО «ЭНИГМА»**(www.enigma.by). Наиболее популярный среди них – аппаратный продукт CryptoKey 2001. Его назначение: генерация и хранение ключей криптозащиты, выполнение криптографических функций - ЭЦП, хеширование, шифрование, протоколы формирования общего ключа, защита от несанкционированного доступа к персональному компьютеру.

Сфера применения: системы электронного документооборота, включая "Банк-Клиент".

Перечень криптофункций, выполняемых на процессоре устройства.

- хеширование по СТБ1176.1-99;
- выработка подписи по СТБ 1176.2-99;
- проверка подписи по СТБ1176.2-99;
- выработка общего ключа для зашифрования (односторонний протокол схемы ОРК);
- выработка общего ключа для расшифрования (односторонний протокол схемы ОРК).

Аналогичное аппаратное обеспечение предлагает компания **«БелТим»,** определяющая основынм направлением деятельности создание комплексных

систем безопасности и защиты информации. Так компания предлагает **Электронный ключ Guardant Sign,** скоростной USB-ключ с асимметричной криптографией, аппаратной реализацией AES и возможностью работы без драйверов.

Выбор модели ключа будет зависеть от лицензионной политики разработчика и особенностей защищаемого программного продукта:

Для защиты тиражного программного обеспечения, лицензируемого по классическим схемам, рекомендуется использовать локальный ключ Guardant Sign, либо его сетевой аналог — Guardant Sign Net.

Для защиты программного обеспечения, лицензируемого по времени использования, применяется Guardant Time. Для сетевого программного обеспечения следует использовать Guardant Time Net.

Для защиты особенно ценного программного обеспечения, распространяемого единичными копиями, эффективнее использовать технологию Загружаемый код, реализованную в электронном ключе Guardant Code и его модификации с часами реального времени — Guardant Code Time.

Рынок средств защиты в области информационной безопасности в Беларуси можно называть еще только формирующимся. Функционируют десятки организаций, в основном начинающих, еще не укрепившихся на рынке средств защиты. Еще только идет борьба за клиентов в сфере предоставления услуг по защите информации. Тем не менее, программно-аппаратные решения во многом носят идентичный характер, а в условиях жесткой конкуренции рационально было бы предлагать альтернативу.

Среди компаний, которые были исследованы, вызывают интерес такие организации как **ООО «Хедтекнолоджи Бел», ЗАО «Авест» и их решения:**

Криптопровайдер AVEST CSP – аппаратно-программное средство выработки и проверки ЭЦП, а также криптографической защиты информации;

Программа **«Blue Coat»,** которая обеспечивает фильтрацию электронной почты, анти-СПАМ; фильтрацию WEB-трафика; защиту WEB-приложений.

Выбор данных средств защиты основан на следующих критериях и требованиях, которые можно предъявить к современной системе защиты:

1. Прочность. Абсолютно надежной защиты не бывает, но выбранная система должна обеспечить выигрыш во времени, пока потенциальные нарушители не научатся вскрывать данный продукт.

2. Обоснованность. Во-первых, для недорогой программы нельзя использовать дорогую защиту. Во-вторых, при расчете стоимости защиты учитываем стоимость защищаемого программного продукта.

3. Гибкость. Защита может быть эффективной, если она находится в состоянии постоянного развития. Если разработчики защиты отслеживают хакерские форумы и делают выводы о недостатках собственных систем.

4. Не препятствует свободному копированию защищенных данных (должна запрещать только несанкционированный запуск);

5. Защита должна быть подобрана с учетом традиций данного сегмента рынка ПО. Т.е. средства должны быть обязательно сертифицированы.

6. По возможности не использовать для защиты дорогие дополнительные аппаратные приспособления, которые только повышают стоимость защиты, а значит, и конечного продукта

7. По возможности не привязываться к аппаратной конфигурации компьютера, поскольку отдельные компоненты персонального компьютера могут и должны быть заменяемыми по мере старения.