Вопрос 5. Средства защиты информации в КИС и сетях.

Рассмотренные методы защиты на практике реализуются применением различных средств защиты. На сегодняшний день существуют две группы средств защиты: формальные и неформальные.20 Первые выполняют функции по защите формально, то есть преимущественно без участия человека (технические). К неформальным относятся средства, основу которых составляет целенаправленная деятельность людей (законодательные, организационные, морально-этические). Названные средства рассматриваются как последовательность барьеров или рубежей защиты информации, последовательно преодолевая которые можно получить доступ к защищаемым объектам системы.

Первый рубеж защиты, встающий на пути злоумышленника, является чисто правовым и связан с необходимостью соблюдения юридических норм при передаче, обработке и хранении информации. К законодательным средствам защиты относятся действующие в стране нормативные правовые акты, регламентирующие вопросы защиты информации. Этим они препятствуют несанкционированному использованию информации и являются сдерживающим фактором для потенциальных нарушителей.

Второй рубеж защиты образуют морально-этические средства. Этический момент при соблюдении требований защиты играет большую роль. Важно, чтобы люди, имеющие доступ к компьютерам, работали в здоровом морально-этическом климате. К морально-этическим средствам относятся нормы поведения, которые традиционно складываются в обществе по мере развития информационных технологий. Они не являются обязательными, но их игнорирование ведет к падению престижа человека, группы лиц или организации.

Третьим рубежом защиты являются организационные средства защиты, регламентирующие процесс функционирования КИС, использования ее ресурсов, деятельность персонала, порядок взаимодействия пользователей с системой с целью затруднения или исключения возможности реализации угроз безопасности. Важно отметить, что пока не будут разработаны и реализованы действенные средства организационной защиты применение другие средств будет неэффективным. Организационные средства защиты представляют мощный барьер на пути незаконного использования ресурсов системы и надежную базу для других уровней защиты.

Четвертый рубеж защиты — технические средства защиты, реализуемы посредством физических, аппаратных, программных, криптографических устройств, выполняющие такие функции защиты, как создание физического препятствия на пути злоумышленника, идентификация и аутентификация субъектов и объектов системы, разграничение доступа к ресурсам, контроль целостности данных, обеспечение конфиденциальности, регистрация и анализ

событий, резервирование ресурсов и компонентов системы электронного документооборота.

Физические средства предназначены для внешней охраны территории объектов, организации пропускного режима, защиты компонентов КИС и реализуются в виде автономных устройств.22 Это различные механические или автоматизированные электронные системы, конструкторскую базу которых составляют различные датчики, электронные ключи, устройства определения биометрических характеристик человека.

Аппаратные средства защиты реализуются в виде электронных, электромеханических устройств, непосредственно встроенных в блоки КИС или используемые в виде самостоятельных устройств, соединенных с блоками системы, применяемые для внутренней защиты элементов системы: терминалов, процессоров, линий связи и т.д. Такие средства позволяют исключить несанкционированный внешний и внутренний доступ к системе. С их помощью осуществляется защита активных и пассивных архивных файлов и баз данных, целостности ПО.

Для выполнения логических и интеллектуальных функций защиты используются **программные средства защиты.**23 Они осуществляют контроль загрузки и входа в систему путем персональной идентификации, разграничение и контроль доступа к ресурсам и компонентам системы, управление потоками конфиденциальной информации с целью предотвращения записи на носитель данных несоответствующего уровня секретности, защиту от вирусов, автоматический контроль за работой пользователей системы.

Еще одной группой средств защиты являются **средства криптографии,** реализуемые в аппаратных, программных комплексах защиты путем шифрования и выработки электронной цифровой подписи.24 В настоящее время применяются два вида алгоритмов шифрования: симметричные алгоритмы (DES, 3-DES, FEAL, IDEA, CAST,) в которых для шифрования и расшифровки используется один и тот же секретный ключ, и асимметричные алгоритмы (RSA, ECC, Эль-Гамаль), в которых для шифрования и расшифровки используется два разных ключа, — один известен всем, а другой держится в тайне.

Надежность и эффективность применения технических средств защиты достигается при неукоснительном выполнении определенных **организационных мероприятий** по защите информации. По данным зарубежных специалистов, несмотря на постоянное совершенствование технических средств, организационные средства защиты составляют значительную часть (50%) системы защиты и применяются тогда, когда компьютерная система не может непосредственно контролировать использование информации.

Под организационным обеспечением защиты информации следует понимать регламентацию производственной деятельности и взаимоотношений

исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка, несанкционированный доступ к информации становятся невозможными или существенно затрудняются за счет проведения организационных мероприятий, совокупности процессов и действий, ведущих к образованию и совершенствованию взаимоотношений между частями целого.

В настоящее время существуют различные подходы в определении и классификации организационных мер защиты информации: по содержанию системы защиты, на основе жизненного цикла КИС и периодичности проведения, на основе нормативно-технической, методической и организационно-распорятительной документации.

Выделяют следующие организационные мероприятия по обеспечению защиты информации КИС:

● формирование и организация деятельности службы защиты КИС (службы безопасности, службы конфиденциального делопроизводства),

● категорирование информационных ресурсов КИС по уровню доступа, составление и регулярное обновление перечня конфиденциальной информации,

● разработка и создание разрешительной системы разграничения доступа сотрудников к КИС и данным,

● организация пропускного режима на территории и в помещениях,

● постоянный контроль над соблюдением сотрудниками правил по защите информации,

● проведение мероприятий по повышению уровня грамотности сотрудников в области защиты информации, организация соответствующих семинаров и тренингов,

● периодическая переподготовка специалистов по защите информации,

● разработка критериев и порядка проведения оценочных мероприятий по установлению степени эффективности системы защиты,

● аттестация помещений и рабочих мест по требованиям безопасности,

● лицензирование используемых средств защиты информации и сертификация КИС по требованиям безопасности.

В силу того, что любая организация является непосредственным субъектом, осуществляющим свою деятельность в рамках государства, то и построение системы защиты КИС самым тесным образом связано не только с решением технических и организационных проблем, но и с вопросами правового регулирования отношений в процессах формирования, обработки и использования информационных ресурсов.

Разработка и применение соответствующих **законодательных средств защиты** решает вопросы правовой защиты информации от искажений, несанкционированного доступа и установления юридической ответственности за обеспечение сохранности информации; разработки мероприятий по приданию юридической силы электронным документам и формирования юридических норм, определяющих лиц, ответственных за доброкачественность

документов; установления единых норм и критериев, в соответствии с которыми должны разрабатываться программные продукты и функционировать созданные КИС; установления правовых норм и юридической ответственности за использование электронно-вычислительных средств в интересах, противоречащих интересам других личностей и общества и могущих нанести вред и т.д.

Законодательную базу области информационной безопасности в Республике Беларусь составляют «Концепция национальной безопасности Республики Беларусь», законы Республики Беларусь «Об информации, информатизации и защите информации», «О государственных секретах», «Об электронном документе», «Об оценке соответствия требованиям технических нормативных актов в области технического нормирования и стандартизации», «О техническом нормировании и стандартизации». Отдельные правовые нормы по вопросам защиты информации содержатся в Гражданском и Уголовном кодексах Республики Беларусь, указах Президента, постановлениях Совета Министров, руководящих документах Национального банка, нормативных правовых актах министерств и иных республиканских органов государственного управления.

Так, например, Закон Республики Беларусь «Об информации, информатизации и защите информации» определяет цели, основные требования и меры защиты (правовые организационные, технические), права и обязанности субъектов информационных отношений по защите информации.

Закон Республики Беларусь «Об электронном документе» определяет правовые основы применения ЭД, основные требования, предъявляемые к ним, а также права, обязанности и ответственность участников

правоотношений в данной сфере.

В Законе содержится определение таких понятий как «электронная цифровая подпись» (далее ЭЦП), «средства ЭЦП», «подлинность», «целостность» ЭД. Однако Закон лишь в общих чертах регулирует вопросы, связанные с выработкой и распространением открытых ключей проверки подписи, не определяя статус, функции, обязательства лица, вырабатывающего и распространяющего открытые ключи. Несовершенство Закона привело к необходимости пересмотра многих его положений. В проект нового Закона «Об электронном документе и электронной цифровой подписи» включено понятие «удостоверяющий центр», а также перечислены задачи и функции Государственной системы управления открытыми ключами. Удостоверяющий центр определяется как юридическое лицо, осуществляющее издание, распространение и хранение сертификатов открытых ключей и списков отозванных сертификатов открытых ключей. Более подробная регламентация применения ЭЦП, функционирования систем управления открытыми ключами должна идти по пути принятия подзаконных актов технического характера.

Особую часть законодательного регулирования информационной безопасности составляют технические нормативные правовые акты — стандарты и предстандарты.

Первая группа стандартов — стандарты серии 34.101 (Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий). Стандарты устанавливают общие подходы к формированию требований и оценке безопасности информационных технологий, определяют виды требований безопасности и содержат их систематизированный каталог, критерии и уровни оценки безопасности информационных технологий, позволяющие оценить правильность реализации средств безопасности, стойкость механизмов защиты.

Вторая группа представлена стандартами по криптографической защите информации — СТБ 1176.1-99 «Информационная технология. Защита информации. Функция хэширования», СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи», применяемыми при разработке средств криптографической защиты и гарантирующими криптостойкость ЭЦП.