ПРИОРИТЕТНЫЙ НАЦИОНАЛЬНЫЙ ПРОЕКТ «ОБРАЗОВАНИЕ»
РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

А.В. ОВЧИННИКОВ, В.Г. СЕМИН

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ТРАНСНАЦИОНАЛЬНЫХ КОРПОРАЦИЙ (АСТК)

Учебное пособие

Москва
2008

Инновационная образовательная программа
Российского университета дружбы народов

«Создание комплекса инновационных образовательных программ и формирование инновационной образовательной среды, позволяющих эффективно реализовывать государственные интересы РФ через систему экспорта образовательных услуг»

Экспертное заключение –

доктор технических наук, профессор кафедры автоматизации и информатизации систем управления Московского государственного индустриального университета

В.Н. Дианов

Овчинников А.В., Семин В.Г.

Обеспечение информационной безопасности автоматизированных систем транснациональных корпораций (АСТК): Учеб. пособие. – М.: РУДН, 2008. – 290 с.: ил.

В пособии изложены основные теоретические и практические результаты в области информационной безопасности. Приведены базовые понятия информационной безопасности, которые положены в основу методологии построения системы видов обеспечений информационной безопасности АСТНК. Значительное внимание уделено методам моделирования и построения средств обеспечения информационной безопасности на основе принципа гарантированного результата. Рассмотрены задачи управления рисками информационной безопасности и организации аудита информационной безопасности АСТНК.

Для студентов-магистров, обучающихся по специальности «Автоматизированные системы управления.

Учебное пособие выполнено в рамках инновационной образовательной программы Российского университета дружбы народов, направление «Комплекс экспортоориентированных инновационных образовательных программ по приоритетным направлениям науки и технологий», и входит в состав учебно-методического комплекса, включающего описание курса, программу и электронный учебник.

СОДЕРЖАНИЕ

Р а з д е л 1. Сущность, задачи и организационно–правовые основы проблемы информационной безопасности АСТНК

Лекция 1. Место и роль информационной безопасности в общей совокупности проблем современного этапа развития глобальной и национальной экономических систем

Актуальность проблемы

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, являющейся важным фактором общественной жизни, во многом определяющим перспективы успешного осуществления социально–политических экономических преобразований. При этом с одной стороны продолжается процесс научно–технической революции в области средств вычислительной техники и средств телекоммуникаций и интеллектуализации основных факторов производства, а с другой – существенно расширяются потребности социально активной части общества в расширении и формировании процессов информационного взаимодействия как внутри страны, так и с внешним миром.

Глобальное экономическое развитие сегодня определяется сочетанием двух основных тенденций: возрастающим влиянием международного транснационального капитала и конкуренцией национальных экономических систем.

Известно, что транснациональные корпорации (ТНК) соединили мировую торговлю с международным производством. Они действуют через свои дочерние предприятия и филиалы в десятках стран мира по единой научно–производственной и финансовой стратегии управления, формируемой в их «мозговых трестах», обладают громадным научно–

производственным и рыночным потенциалом, обеспечивающим высокий динамизм развития.

На рис. 1 можно увидеть динамику уровня траснационализации компаний.

Рис.1. Динамика количества ТНК и их зарубежных филиалов.

По состоянию на начало 2008г. в мире действовало более 64 тыс. ТНК, контролирующих более 830 тыс. иностранных филиалов.

Транснациональная компания (корпорация) — компания (корпорация), владеющая производственными подразделениями в нескольких странах. По другим источникам определение транснациональной компании звучит так: компания, международный бизнес которой является существенным.

Страна базирования — страна, в которой находится штаб–квартира ТНК. Принимающие страны — страны, в которых размещена собственность ТНК. ТНК часто делятся на три больших группы:

- Горизонтально интегрированные ТНК—управляют подразделениями, расположенными в различных странах, производящих одинаковые или подобные товары.
- Вертикально интегрированные ТНК—управляют подразделениями в определенной стране, которые производят товары поставляемые в их подразделения в других странах.
- Раздельные ТНК — управляют подразделениями, расположенными в различных странах, которые вертикально или горизонтально не объединены.

В целом ТНК обеспечивают около 50% мирового промышленного производства. На ТНК приходится более 70% мировой торговли, причем 40% этой торговли происходит внутри ТНК, то есть они происходят не по рыночным ценам, а по так называемым трансфертным ценам, которые формируются не под давлением рынка, а под долгосрочной политикой материнской корпорации.

ТНК играют весомую роль в мировых научно–исследовательских и опытно–конструкторских разработках (НИОКР). На долю ТНК приходится более 80% зарегистрированных патентов, при этом на долю ТНК приходится и около 80% финансирования НИОКР.

ТНК это не только производственные компании, такие, как, например,Simens,но и транснациональные банки, телекоммуникационные, страховые, аудиторские компании, инвестиционные и пенсионные фонды.

Развитие российских международных компаний и финансово–промышленных групп

Уже в советские времена существовали отечественные международные фирмы. Примером российской ТНК с «советским прошлым» может служить «Ингосстрах» со своими дочерними и ассоциированными фирмами и отделениями в США, Нидерландах,

Великобритании, Франции, Германии, Австрии, а также ряде стран СНГ. Большинство российских международных корпораций сформировались после распада СССР. Приватизация в России сопровождалась возникновением достаточно мощных организационно–хозяйственных структур нового типа (государственных, смешанных и частных корпораций, концернов, финансово–промышленных групп), способных успешно действовать на внутреннем и внешнем рынках, – например, таких как «Газпром». «Газпром» контролирует 34% мировых разведанных запасов природного газа, обеспечивает почти пятую часть всех западноевропейских потребностей в этом сырье. Ему полностью принадлежат примерно 60 дочерних фирм, он участвует в уставном капитале еще почти 100 российских и зарубежных компаний. Подавляющее большинство отечественных ТНК относятся к сырьевым отраслям, особенно к нефтяной и нефтегазовой. Есть и международные российские корпорации, не связанные с экспортом сырья, – «АвтоВАЗ», «Микрохирургия глаза» и др. Хотя российский бизнес очень молод, многие отечественные фирмы уже вошли в списки ведущих ТНК планеты. Так, в составленный газетой «Файнэншл Таймс» рейтинг 500 крупнейших компаний мира 2003 г. вошли такие российские компании, как РАО «Газпром», «ЛУКойл» и РАО «ЕЭС России». В списке 100 крупнейших военно–промышленных корпораций мира, составленного в 2003 г. американским еженедельником «Дефэнс ньюс», присутствуют два российских объединения – ВПК «МАЛО» (32–е место) и АО «ОКБ Сухого» (64–е место). Необходимо отметить, что роль ТНК в современном мировом хозяйстве оценивают при помощи следующих показателей:

– ТНК контролируют примерно 2/3 мировой торговли;

– на них приходится около 1/2 мирового промышленного производства;

– на предприятиях ТНК работают примерно 10% всех занятых в несельскохозяйственном производстве (из них почти 60% работают в материнских компаний, 40% – в дочерних подразделениях);

– ТНК контролируют примерно 4/5 всех существующих в мире патентов, лицензий и ноу–хау.

Подобно тому, как ТНК являются элитой бизнеса, среди ТНК есть своя элита – суперкрупные фирмы, соперничающие со многими государствами и по производству, и по бюджету, и по числу «подданных». Крупнейшие 100 ТНК контролируют 12% от совокупного размера зарубежных активов и 16% от совокупного объема зарубежных продаж.

Причины возникновения ТНК

Причины возникновения транснациональных корпораций весьма разнообразны, но все они в той или иной степени связаны с преимуществами использования элементов планирования в сравнении с «чистым» рынком. Поскольку «большой бизнес» заменяет стихийное саморазвитие внутрифирменным планированием, ТНК оказываются своеобразными «плановыми экономиками», сознательно использующими преимущества международного разделения труда. Транснациональные корпорации имеют ряд неоспоримых преимуществ перед обычными фирмами:

– возможности повышения эффективности и усиления конкурентоспособности, которые являются общими для всех крупных промышленных фирм, интегрирующих в свою структуру снабженческие, производственные, научно–исследовательские, распределительные и сбытовые предприятия;

– мобилизация связанных с экономической культурой «неосязаемых активов» (производственного опыта, навыков управления), которые становится возможным использовать не только там, где они складываются,

но и переносить в другие страны (путем, например, внедрения американских принципов личной ответственности в филиалах действующих по всей планете фирм США);

– дополнительные возможности повышения эффективности и усиления конкурентоспособности путем доступа к ресурсам иностранных государств (использование более дешевой или более квалифицированной рабочей силы, сырьевых ресурсов, научно–исследовательского потенциала, производственных возможностей и финансовых ресурсов принимающей страны);

– близость к потребителям продукции иностранного филиала фирмы и возможность получения информации о перспективах рынков и конкурентном потенциале фирм принимающей страны. Филиалы транснациональных корпораций получают важные преимущества перед фирмами принимающей страны в результате использования научно–технического и управленческого потенциалов материнской фирмы и ее филиалов;

– возможность использовать в своих интересах особенности государственной, в частности, налоговой политики в различных странах, разницу в курсах валют и т.д.;

– способность продлевать жизненный цикл своих технологий и продукции, перенося их по мере устаревания в зарубежные филиалы и сосредотачивая усилия и ресурсы подразделений в материнской стране на разработке новых технологий и изделий;

– возможность преодолевать разного рода протекционистские барьеры на пути проникновения на рынок той или иной страны путем замены экспорта товаров экспортом капиталов (т.е. создавая зарубежные филиалы);

– способность крупной фирмы уменьшать риски производственной деятельности, рассредотачивая свое производство между разными странами мира.

Важную роль в стимулировании развития ТНК играет государство, независимо от того, желает ли оно помочь «своим» предпринимателям или помешать «чужим». Во–первых, правительства поощряют деятельность «своих» ТНК на мировой арене, обеспечивают им рынки сбыта и возможности для иностранных инвестиций путем заключения различных политических, экономических и торговых союзов и международных договоров. Во–вторых, стимул для прямых зарубежных инвестиций создают национальные тарифные барьеры, создаваемые для защиты «своего» бизнеса от зарубежных конкурентов. Объективные требования экономической глобализации ведут к тому, что практически любая по–настоящему крупная национальная фирма вынуждена включаться в мировое хозяйство, превращаясь тем самым в транснациональную. Поэтому списки крупнейших компаний можно рассматривать и как списки ведущих ТНК.

Роль информационной безопасности в развитии ТНК

В настоящее время распределенные сетевые технологии преобразования информации стали основным вычислительным инструментом автоматизированных систем управления большими социально–экономическими системами и АСТНК, в частности, резко возросла зависимость общества от условий устойчивого функционирования информационной инфраструктуры.

При этом информационная сфера сравнительно недавно стала выделяться в качестве самостоятельной сферы общественной жизни. Она образуется совокупностью информации и информационной инфраструктуры общества, общественных отношений по поводу информации и информационной инфраструктуры как объектов интересов индивида,

общества и государства, а также субъектов этих отношений. Интенсивное развитие информационной инфраструктуры – масштабное внедрение средств информатизации, телекоммуникации и связи в общественную жизнь и связанная с ним глобализация процессов общественного развития увеличили зависимость общества, различных сфер его жизнедеятельности от процессов производства, распространения и использования информации. Так, в сфере материального производства бурно развивается сектор, связанный с созданием и внедрением современных информационных технологий, средств информатизации. телекоммуникации и связи, продуктов информационных технологий, баз данных и знаний. В сфере духовной жизни эти технологии существенно изменили содержание интеллектуального труда, повысили его эффективность, обеспечили возможность быстрого доступа к его результатам. В сфере НИОКР активно развиваются эффективные автоматизированные технологии непрерывной информационной поддержки жизненного цикла продукции с целью обеспечения её конкурентоспособности. В социальной сфере современные информационные технологии усилили зависимость благосостояния и безопасности человека от правильности информации, накапливаемой и хранящейся в общественных, государственных информационных системах, от способности этих учреждений обеспечить соблюдение необходимого режима использования информации. Таким образом, выделение общественных отношений, связанных с производством, хранением, распространением и использованием информации, обусловило формирование информационной сферы в качестве самостоятельной сферы общественной жизни, что привело к формированию понятия «информационное общество». В связи с этим резко возросла актуальность проблем, связанных с обеспечением безопасности личности, общества и государства при использовании современных информационных и

телекоммуникационных технологий, а также с созданием позитивных условий для гармонизации интересов различных государств в информационной сфере. Понятие «информационная безопасность» стало широко употребляться не только специалистами в области информационных технологий, но и представителями крупного бизнеса, экономистами и финансистами. При этом информация как объект безопасности выступает в двух формах: сведения и сообщения. Сведения характеризуют содержательную сторону информации, которая раскрывается получающим ее субъектом. Она становится объектом национальных интересов в информационной сфере в случае, если относится к ценностям, отражающим национальную идентичность, а также к знаниям в области создания, развития и использования современных информационных технологий, информационной инфраструктуры общества. Сообщения, как основная форма существования информации, в виде отторгнутом от индивида, становится объектом национальных интересов в связи с необходимостью реализации интересов посылающих и получающих их субъектов, индивидов, общественных и государственных организаций, т.е. как объект общественных отношений сложившихся в информационной сфере. Безопасность информации заключается в защищенности от угроз ее свойства удовлетворять потребности субъектов национальных интересов. При этом информационная инфраструктура становится объектом национальных интересов в связи с ее использованием для реализации важных функций общества и, прежде всего, передачи циркулирующей в обществе информации, управления социально–экономическими системами и технологическими процессами критически важных производств (энергоснабжение, транспорт и т.д.). Все эти обстоятельства определяют актуальность проблемы обеспечения информационной безопасноси АСТНК.

Лекция 2. Структура категории «обеспечение информационной безопасности». Введение в основы информационной безопасности АСТНК

Понятие «обеспечение»

Это понятие раскрывается двояко: как один из видов деятельности и как средство деятельности. Как вид деятельности оно означает совокупность действий, предпринимаемых для того, чтобы сделать нечто «вполне возможным, действительным, реально выполнимым», а как средство деятельности — «то, чем обеспечивают кого–нибудь или что–нибудь». Обеспечение как средство деятельности, т.е. «то, чем обеспечивают кого–нибудь или что–нибудь», представляет собой совокупность материальных объектов, финансовых, правовых и организационных средств, которые повышают эффективность деятельности по достижению целей. Его конкретное содержание определяется предметной сферой обеспечения как вида деятельности.

Таким образом, обеспечение представляет собой совокупность деятельности по обеспечению, средств обеспечения и субъектов обеспечения. Деятельность по обеспечению заключается в оказании помощи субъектам в достижении поставленных ими целей.

Средства обеспечения образуются совокупностью материальных, финансовых, правовых, организационных и технических средств, необходимых для осуществления деятельности по обеспечению.

Субъектами обеспечения являются индивиды, организации и органы государства, осуществляющие деятельность по обеспечению.

Общая структура понятия «обеспечение» представлена на рис. 2.

К числу важных принципов «обеспечения» относятся комплексность и системность. *Комплексность* проявляется как свойство «обеспечения» учитывать все условия и факторы, оказывающие существенное влияние на

процесс достижения цели: объективные и субъективные, правовые и организационные.

Системность проявляется как свойство согласованного использования для достижения цели имеющихся сил и средств.

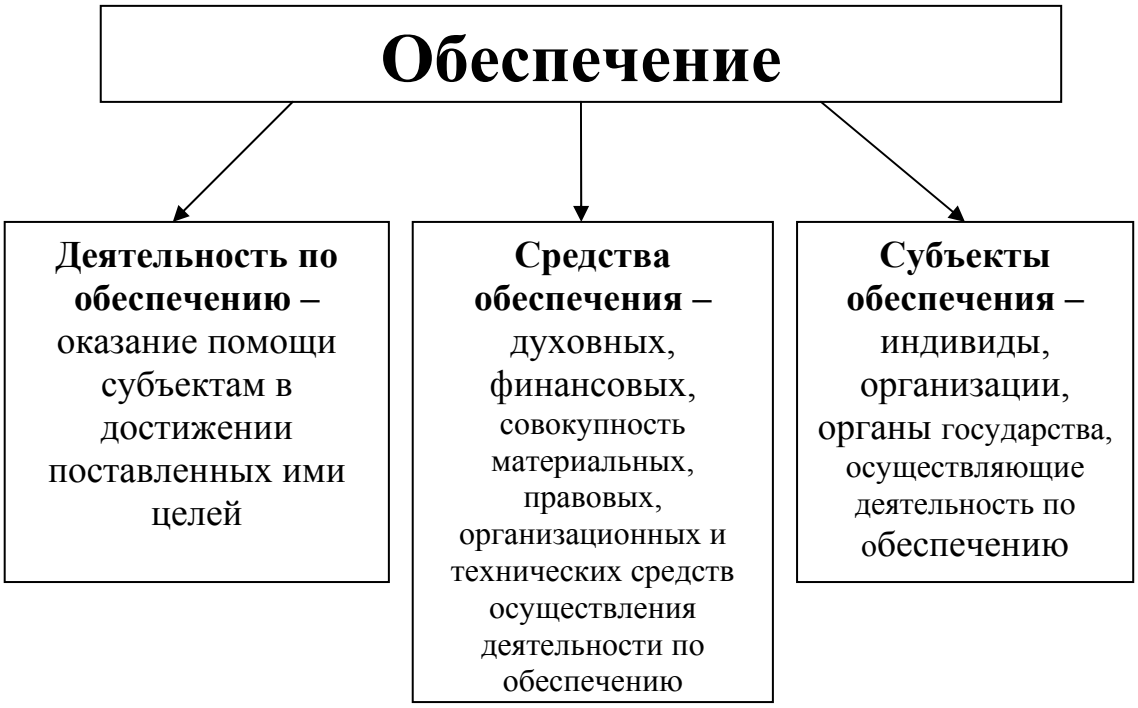

Рис 2. Общая структура понятия «обеспечение»

Цель может заключаться в автоматизации решения некоторой задачи управления бизнес – процессом. Тогда ее обеспечение будет включать создание необходимой технической основы (техническое обеспечение), программ (программное обеспечение), систематизированных наборов данных (информационное обеспечение), языковых средств взаимодействия пользователя с техническими и программными средствами (лингвистическое обеспечение), набора нормативных документов, определяющих порядок взаимодействия с системой и поддержания ее работоспособности (нормативное обеспечение).

Если в качестве предмета обеспечения выступает выполнение некоторым должностным лицом (в том числе государственным) возложенных на него обязанностей, то обеспечение будет заключаться в определении структуры необходимого аппарата, его кадровом наполнении, осуществлении определенной организационной, хозяйственной, информационно–аналитической и другой необходимой деятельности.

Понятие «безопасность»

С рассматриваемой точки зрения безопасность является одним из возможных предметов обеспечения. Безопасность представляет собой сложное социально–политическое явление, и его изучением занимаются специалисты, работающие в различных отраслях знаний.

Это отражается и в предлагаемых этими специалистами определениях понятия «безопасность». На уровне обыденного сознания понятие «безопасность» определяется как «отсутствие опасности», «состояние, при котором не угрожает опасность, есть защита от опасности». В свою очередь понятие «опасность» означает «возможность, угрозу чего–нибудь опасного, т.е. способного причинить какой–нибудь вред», а понятие «угроза» – «возможную опасность, запугивание, обещание причинить кому–нибудь неприятность, зло».

Таким образом, понятие «безопасность» трактуется как отсутствие угрозы кому–нибудь, чему–нибудь. Аналогичным образом данное понятие раскрывается в справочной литературе — «ситуация, при которой кому– или чему–нибудь не существует угрозы со стороны кого– или чего–либо, при этом не исключается наличие одновременно нескольких источников опасности. Исходя из этого, будем полагать, что безопасность есть невозможность нанесения вреда кому–нибудь или чему–нибудь вследствие проявления угроз, т.е. их защищенность от угроз.

В структуре понятия «безопасность», представленной на рис.3, выделяются объект безопасности, угрозы этому объекту и обеспечение его

безопасности от проявления угроз. С рассматриваемой точки зрения безопасность является одним из возможных предметов обеспечения.

Объект безопасности — это то, что защищается от угроз. Этот объект во многом определяет содержание явления «безопасность», обусловливая возможные угрозы и, соответственно, характеристики состояния защищенности от угроз. Безопасность объекта проявляется через безопасность его наиболее важных свойств или свойств, структурных составляющих. В наиболее общем случае содержание его «безопасности» будет заключаться в защищенности от угроз.

Рис. 3. Структура понятия «безопасность»

Угрозы объекту безопасности

Необходимо отметить, что угроза безопасности не является чем–то, существующим самостоятельно. Она может быть либо проявлением взаимодействия объекта безопасности с другими объектами, способным нанести вред его функционированию и свойствам, либо подобным проявлением взаимодействия подсистем и элементов самого объекта безопасности.

Обеспечение безопасности объекта

Обеспечение безопасности объекта образуется совокупностью деятельности, средств и субъектов обеспечения безопасности.

Важно подчеркнуть, что обеспечение безопасности всегда носит вспомогательный характер, создавая условия для достижения основных целей существования объекта безопасности.

Обеспечение безопасности объекта основывается на использовании субъектами обеспечения материальных, финансовых, правовых и организационных средств. Эти средства должны соответствовать опасности угроз и быть достаточны для надежной защиты объекта.

Понятие «информационная безопасность»

Как было отмечено выше, безопасность проявляется в отсутствии возможности нанесения вреда функционированию и свойствам объекта либо его структурных составляющих. Это положение служит методологическим основанием для выделения видов безопасности. Одной из важных структурных составляющих многих объектов безопасности является информация или деятельность, предметом которой является информация. Наличие угроз этим объектам позволяет говорить об их информационной безопасности — безопасности их «информационного измерения». Распространение информации в современном обществе осуществляется с помощью информационной

инфраструктуры. Нанесение вреда этой инфраструктуре, передаваемым сообщениям и содержащимся в них сведениям может привести к нарушению информационной коммуникации и, как следствие, — к нарушению целостности общества, нарушению деятельности его институтов, разрушению основ его существования. Исходя из этого, информационная безопасность общества заключается в невозможности нанесения вреда его духовной сфере, культурным ценностям, социальным регуляторам поведения людей, информационной инфраструктуре и передаваемым с ее по мощью сообщениям.

Информационная безопасность государства заключается в невозможности нанесения вреда деятельности государства по выполнению функций управления делами общества, предметом которой выступает информация и информационная инфраструктура общества.

Человек, общество и государство не являются единственно возможными объектами безопасности. Таким объектом может быть сама информация. В этом случае содержание «информационной безопасности» будет заключаться в защищенности информации от угроз.

Так, в жизни человека возникает немало ситуаций, распространение информации о которых может негативным образом сказаться на его социальном статусе, других условиях его жизни. Подобная информация закрывается, и устанавливаемый режим использования такой информации призван предупредить возможность несанкционированного ознакомления с ней лиц, не имеющих соответствующих полномочий. В этом случае объектом безопасности выступает режим доступа к информации, а информационная безопасность заключается в невозможности нарушения этого режима. Примером могут служить информационно–телекоммуникационные системы и средства связи, предназначенные для обработки и передачи сведений, составляющих государственную тайну. Основным объектом безопасности в них является режим доступа к секретной информации.

Информационная безопасность таких систем заключается в защищенности этой информации от несанкционированного доступа, уничтожения, изменения и других опасных действий.

Объектом информационной безопасности может быть коммерческая организация. Тогда содержание «информационной безопасности» будет заключаться в защищенности интересов собственника данного предприятия, удовлетворяемых с помощью информации, либо связанных с защитой от несанкционированного доступа тех сведений, которые представляются собственнику достаточно важными. Интересы проявляются через объекты, способные служить для их удовлетворения, и через действия, предпринимаемые для обладания этими объектами. Соответственно, и интересы как объект безопасности могут быть представлены в качестве совокупности информации, способной удовлетворять интерес собственника, и его действий, направленных на овладение или сокрытие информации. Эти составляющие объекта информационной безопасности защищаются от внешних и внутренних угроз.

В случае, когда собственник предприятия не видит необходимости в защите своих действий (например, в связи с тем, что это не окупается), содержание информационной безопасности предприятия может быть сведено к защищенности конкретной информации, раскрытие которой может принести заметный ущерб коммерческой деятельности. Подобную информацию обычно относят к коммерческой тайне.

Исходя из изложенного, в наиболее общем виде информационная безопасность может быть определена, как невозможность нанесения вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой. Структура данного понятия приведена на рис.4.

Рис. 4. Структура понятия «информационная безопасность»

Обеспечение информационной безопасности

На основании анализа рассмотренных понятий можно сформулировать следующее определение: обеспечение информационной безопасности есть совокупность деятельности по недопущению вреда

свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой, а также средств и субъектов этой деятельности.

Понятие «обеспечение информационной безопасности» круг явлений жизни и деятельности человека, материальной, политической, экономической, духовной и социальной сфер жизнедеятельности общества и функционирования государства. Являясь видом обеспечении безопасности, обеспечение информационной безопасности обладает сложной структурой, включающей объект безопасности, угрозы объекту безопасности, деятельность по защите объекта безопасности от угроз, средства и субъекты этой деятельности.

Определение информационной безопасности АСТНК

В словаре терминов и определений по вопросам безопасности «информация» определяется как «сведения о лицах, предметах, событиях, явлениях, процессах и объектах (независимо от формы их представления), используемые в целях получения знаний, оптимизации принимаемых решений управления объектами. Под системой понимается организованная совокупность элементов живой и неживой природы, находящаяся в связях и отношениях и объединенных информационным процессом для достижения целей, для множества внешних и внутренних воздействий в соответствии с некоторым критерием эффективности. Под структурой определяется множество отношений и связей (информационных, энергетических, экономических, организационных, электрических и т.д.), заданных на множестве элементов системы. Таким образом, система – структура, для достижения целей в условиях множества входных воздействий. Качество процесса достижения цели характеризуется критерием оптимальности.

Под автоматизированной системой транснациональной корпорации понимается организационно–техническая система, образованная множеством следующих компонентов: технических средств и средств вычислительной техники, телекоммуникации и связи; алгоритмов и методов обработки информации для сбора, обработки, хранения, преобразования и выдачи в виде, пригодном для поддержки и принятия решений по задачам управления; системного и прикладного программного обеспечения, продуктов информационных технологий; информации на различных носителях (базы данных, массивы и наборы данных); пользователей и персонала, находящихся в различных организационно–структурных отношениях с целью реализации автоматизированной технологии обработки информации для реализации программ и целей ТНК. Под информационной безопасностью АСТНК понимается организация множества ее организационно–структурных и структурно–функциональных компонентов с целью невозможности нанесения различного рода ущерба свойствам АС, обусловливаемым информацией и информационной инфраструктурой, а также способность к противодействию внешним и внутренним информационным угрозам и функционированию в режиме целевого назначения без создания информационных угроз для компонентов АС и внешней среды. Под обеспечением информационной безопасности АСТНК понимается организация совокупности различных видов деятельности по недопущению нанесения вреда свойствам АСТНК, обуславливаемым информацией и информационной инфраструктурой, а также средств и субъектов этой деятельности.

Лекция 3. Организационно–правовые основы информационной безопасности АСТНК. Защита коммерческой тайны

Основные законодательные положения

Организационно–правовые основы информационной безопасности АС ТНК базируются на основных положениях законов Российской Федерации «О безопасности», «О государственной тайне», «О связи», «Об участии в международном информационном обмене», «Об информации , информатизации и защите информации» , «О концепции национальной безопасности Российской Федерации», «Об основах государственной политики в сфере информатизации», «Об утверждении перечня сведений конфиденциального характера», «О доктрине информационной безопасности Российской Федерации».

Современное понимание проблемы безопасности в Российской Федерации отражено в официальных документах, основными из которых являются: Закон Российской Федерации № 2446–1 от 5 марта 1992 г. «О безопасности»;

«Концепция национальной безопасности Российской Федерации», утвержденная Указом Президента Российской Федерации от 17 декабря 1997 г. N 1300 в редакции Указа Президента Российской Федерации от 10 января 2000 г. № 24. В доктрине информационной безопасности Российской Федерации термин «информационная безопасность» используется в широком смысле и определяется как состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства. Необходимо отметить, что в законе «Об участии в международном информационном обмене», этот термин определяется аналогично как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в

интересах граждан, организаций, государства. Доктрина информационной безопасности Российской Федерации представляет собой официально принятую систему взглядов на проблему обеспечения информационной безопасности, методы и средства защиты жизненно важных интересов личности, общества и государства в информационной сфере.

Доктрина развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере и служит основой для формирования государственной политики в области обеспечения информационной безопасности Российской Федерации.

В доктрине определены четыре основные составляющие национальных интересов Российской Федерации в информационной сфере:

- соблюдение конституционных прав и свобод человека и гражданина в области получения и использования информации;
- информационное обеспечение государственной политики Российской Федерации;
- развитие современных информационных технологий, отечественной индустрии информации; в том числе индустрии средств информатизации, телекоммуникации и связи,
- защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем как уже развернутых, так и создаваемых на территории России.

Методы обеспечения информационной безопасности Российской Федерации

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно–технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации.

Организационно–техническими методами обеспечения информационной безопасности Российской Федерации являются:

- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;
- разработка, использование и совершенствование средств защиты, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно–телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;
- формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:

- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно–технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Правовой статус информации

Организации защиты информации препятствует одно обстоятельство, связанное с природой информации, а именно – с ее нематериальным характером.

Рассмотрим в качестве примера случай утечки информации и сравним его с кражей. В случае кражи какого–либо материального объекта этот объект до кражи был у хозяина. После кражи украденный предмет отсутствует у хозяина и находится в другом месте. В случае, когда злоумышленник в результате несанкционированного доступа скопировал файл с жесткого диска, его владелец продолжает владеть записанной в файле информацией и использовать ее. Более того, носитель остался таким же целым, каким был до «кражи». В описанных условиях привлечь злоумышленника к ответственности за утечку информации в соответствии с традиционным законодательством практически невозможно.

Юридические меры защиты информации являются той основой, без которой невозможно законное использование других мер защиты информации.

При этом законодательство об информации и защите информации должно в первую очередь помочь :

- определить правовой статус информации. Этот статус должен обеспечить возможность защиты любой полезной информации от уничтожения или искажения.
- из общего объема информации, которой владеет человечество, необходимо выделить некую ее часть , которая не должна быть общедоступной. На доступ к ней и ее использование должны накладываться ограничения. Собственно, это обстоятельство отражено и в "Декларации прав и свобод человека и гражданина". Там указаны ограничения на характер информации, на доступ к которой и использование могут накладываться ограничения: ...Ограничения этого права (права искать, получать и распространять информацию) могут устанавливаться законом только в целях охраны личной, семейной, профессиональной, коммерческой и государственной тайны, а также нравственности... .

Основу законодательства Российской Федерации по защите информации в настоящее время составляют следующие законы:

- Федеральный закон «Об информации, информатизации и защите информации"», принятый Государственной думой 25 января 1995 г.;
- Закон Российской Федерации «О государственной тайне», принятый Верховным Советом Российской Федерации в 1993 г. и вступивший в полную силу с 1 января 1995 г.;
- Закон Российской Федерации «О правовой охране программ для ЭВМ и баз данных», принятый Верховным Советом Российской Федерации 23 сентября 1992 г;

- Федеральный закон «Об электронной цифровой подписи». Принят Государственной думой и утвержден Президентом Российской Федерации в 2002 году.

В принятом в 1996 г. и введенном в действие с 1 января 1997 г. новом Уголовном кодексе Российской Федерации впервые предусмотрена уголовная ответственность за ряд компьютерных преступлений.

В дополнение к законодательному обеспечению проблем защиты информации изданы и разрабатываются ряд нормативных документов исполнительных органов государственной власти, на которые законом возложены обязанности по защите информации. Эти нормативные документы детализируют законодательные положения по защите информации и определяют конкретные пути их реализации.

Сфера действия Федерального закона «Об информации, информатизации и защите информации»

Этот закон регулирует отношения, возникающие при:

- формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;
- создании и использовании информационных технологий и средств их обеспечения;
- защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

Закон опирается на следующие определения основных понятий, связанных с информацией:

- информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления;

- документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
- информационная система – организационно–упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующая информационные процессы;
- средства обеспечения автоматизированных информационных систем и их технологий – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании систем и обеспечивающие их эксплуатацию;
- информация о гражданах (персональные данные) – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Статья 4 Закона определяет основы правового режима информационных ресурсов.

Информационные ресурсы являются объектами отношений физических, юридических лиц, государства, составляют информационные ресурсы России и защищаются законодательством наряду с другими ресурсами.

Правовой режим информационных ресурсов определяется нормами, устанавливающими:

- порядок документирования информации;
- права собственности на документы и массивы документов в информационных системах;
- категории информации по уровню доступа к ней;
- порядок правовой защиты информации.

Государственная тайна определяется в Законе как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно–розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Отметим обязательность всех трех компонент, характеризующих понятие «государственная тайна»:

- защищенность информации;
- ее принадлежность только к перечисленным областям деятельности государства;
- наличие ущерба безопасности государству при распространении этой информации.

Перечень сведений, составляющих государственную тайну – это– совокупность категорий сведений, в соответствии с которыми, сведения относятся к государственной тайне и засекречиваются на основании и в порядке, установленном федеральным законодательством.

Перечень сведений, составляющих государственную тайну, является содержанием Статьи 5 Закона. В соответствии с этой Статьей Государственную тайну составляют:

сведения в военной области; сведения в области экономики, науки и техники; сведения в области внешней политики и экономики; о

внешнеполитической, внешнеэкономической деятельности Российской Федерации; финансовой политике в отношении иностранных государств, а такж**е** о финансовой или денежно–кредитной деятельности, преждевременное раскрытие которых может нанести ущерб безопасности государства.

Носители сведений, составляющих государственную тайну – это материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде , образов, сигналов, технических решений и процессов.

Степени секретности сведений и грифы секретности носителей этих сведений

При разработке принципов защиты государственной тайны предусмотрен дифференцированный подход к выработке мер защиты в зависимости от важности защищаемой информации. В соответствии с этим Закон (Статья 8) устанавливает три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням гри фы секретности для носителей указанных сведений:

- «особой важности»;
- «совершенно секретно»;
- «секретно».

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

Цели защиты информации и прав субъектов

Целями защиты информации и прав субъектов в области информатизационных процессов и информатизации являются:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз информационной безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, секретности, конфиденциальности документированной информации в соответствии с действующими законодательными актами;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, информационных технологий и средств их обеспечения.

Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю.

Законодательство Российской Федерации по защите сведений, составляющих коммерческую тайну**,** не носит характера завершенности. Однако отдельные положения по рассматриваемой проблеме нашли отражение в других законах. Кроме того, положения закона «О

государственной тайне» дают возможность рассматривать вопросы защиты коммерческой тайны как с позиции общности ряда решаемых проблем, так и с учетом различий в способах их решения.

В соответствии с Гражданским кодексом Российской Федерации, информация составляет служебную или коммерческую тайну в случае, когда она имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности.

В формулировке приведенной статьи видны аналогии с тремя составляющими сведений, составляющих государственную тайну.

В Законе Российской Федерации «О конкуренции и ограничении монополистической деятельности на товарных рынках» в разделе, посвященном недобросовестной конкуренции говорится, что не допускается недобросовестная конкуренция, в том числе получение использование, разглашение научно–технической, производственной или торговой информации, в том числе коммерческой тайны, без согласия ее владельца».

Какие сведения подлежат защите на каждом предприятии принимает решение его руководитель. Поэтому перечни сведений, составляющих коммерческую тайну, носят локальный характер. Но перечень сведений, которые не могут считаться коммерческой тайной ни при каких обстоятельствах, определен законодательно. К нему в первую очередь относятся сведения, которые запрещено относить к категории ограниченного доступа в соответствии с Федеральным законом «Об информации, информатизации и защите информации». Кроме того, к коммерческой тайне не могут относиться сведения, содержащиеся в уставных документах и документах, представляемых в качестве отчетных в финансовые, налоговые и другие органы.

Для сохранности сведений, составляющих коммерческую тайну, и их носителей целесообразно ведение делопроизводства с нанесением на документы реквизитов, характеризующих конфиденциальность информации по аналогии с тем, как это делается при работе со сведениями, составляющими государственную тайну. Напомним только, что грифы секретности должны отличаться от грифов, используемых в соответствии с «Законом о государственной тайне». Можно использовать, например, грифы «Конфиденциально» или «Коммерческая тайна». При взаимодействии различных организаций, например, при выполнении научно–исследовательских, опытно–конструкторских и технологических работ, объем сведений, признаваемых конфиденциальными, и порядок их защиты, как правило, оговариваются в договоре. Но в любом случае стороны обязаны обеспечить конфиденциальность сведений, а публикация сведений, признанных конфиденциальными, может осуществляться только с согласия другой стороны (Статья 771 Гражданского кодекса Российской Федерации).

Отметим одну важную особенность коммерческой тайны. Если сведения, составляющие коммерческую тайну для некоторого предприятия, получены посторонним лицом или организацией не путем незаконного завладения, а в результате самостоятельных научных, теоретических или экспериментальных исследований, то новый владелец этой информации обладает всеми правами использования этой информации.

Лекция 4. Классификация угроз и методов обеспечения информационной безопасности

Основные определения и классификация источников угроз

Под угрозой понимается совокупность факторов и условий, возникающих в процессе взаимодействия, объектов и способных оказывать негативное воздействие на объект безопасности. При этом общая структура угрозы представляет собой совокупность объекта угрозы, источника угрозы и проявления угрозы. Под угрозой информационной безопасности понимается потенциально возможное событие, явление или действие, которое может привести к нанесению различного рода ущерба интересам и целям объекта безопасности в информационной сфере.

К источникам внешних угроз Российской Федерации относятся:

- деятельность иностранных политических, экономических, военных и разведывательных структур, направленная против интересов Российской Федерации в информационной сфере;
- проводимая рядом стран политика доминирования в мировой информационной сфере, направленная на противодействие доступу Российской Федерации к новейшим информационным технологиям;
- деятельность международных террористических и преступных сообществ, организаций и групп;
- разработка рядом государств концепций «информационных войн», предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушения нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов или получения несанкционированного доступа к ним.

К источникам внутренних угроз относятся:

- отсутствие исторического, политического и социального опыта жизни в гражданском обществе и правовом государстве, что существенно затрудняет реализацию конституционных прав и свобод граждан, в том числе в информационной сфере;
- неспособность отечественных отраслей электронной промышленности производить наукоемкую продукцию, что приводит к вынужденному широкому использованию импортных программно–аппаратных средств при создании и развитии отечественной информационной инфраструктуры;
- усиление организованной преступности и увеличение числа компьютерных преступлений;
- снижение уровня образованности граждан, что осложняет проблему подготовки квалифицированных кадров, в том числе в информационной сфере;
- недостаточная координация деятельности федеральных органов исполнительной власти по формированию и реализации единой государственной политики обеспечения информационной безопасности России;
- отставание России по уровню информатизации органов государственной власти.

Угрозы информационной безопасности Российской Федерации

Угрозы ИБ подразделяются на следующие виды:

- угрозы конституционным правам и свободам человека и гражданина в области информационной деятельности;
- угрозы информационному обеспечению государственной политики Российской Федерации;

- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи ;
- угрозы безопасности информационных и телекоммуникационных средств и систем, в том числе:
- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно–телекоммуникационных ситстем;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно–ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

Моделирование угроз ИБ АСТНК по классам источников

Широкое внедрение информационных технологий в государственных и коммерческих организациях привело к созданию корпоративных информационных систем различных классов и назначения и автоматизированных систем ТНК, в частности. Увеличение роли информационных технологий в поддержке процессов принятия решений и возрастающая сложность самих информационных процессов обострили проблемы безопасного использования этих систем. Это, с одной стороны, связано с усложнением и расширением состава функций и элементов таких корпоративных систем, а с другой стороны, интеграцией этих систем в единое информационное пространство путем использования ими сервисов, предоставляемых системами общего пользования (СОП), включая Интернет. Такая интеграция предполагает, прежде всего, использование коммуникационных ресурсов СОП для поддержки взаимодействия территориально–распределенных элементов корпоративной системы друг с другом. Кроме того, СОП позволяют организовать как информационный обмен между различными корпоративными информационными системами,

так и доступ собственных пользователей СОП к общедоступным информационно–вычислительным ресурсам АСТНК. Расширение сферы информационных отношений, разработка и внедрение новых информационных систем с одновременным накоплением больших объемов распределенной информации приводит к увеличению угроз нарушения конфиденциальности, целостности и доступности информации в процессе реализации функций управления АСТНК. Процесс совместного функционирования корпоративных информационных систем и СОП подвержен в своей основе внешним и внутренним угрозам нарушения его характеристик по конфиденциальности, целостности и доступности.

Внешние угрозы обусловлены возможностью:

- несанкционированных действий со стороны пользователя СОП или некоторой корпоративной информационной системы на отдельные фрагменты (сетевое оборудование, серверы, рабочие станции, информационный фонд и т.д.) АСТНК;
- несанкционированных действий со стороны пользователя СОП или некоторой корпоративной информационной системы на процесс взаимодействия различных фрагментов другой корпоративной системы друг с другом;
- несанкционированных действий со стороны пользователя СОП или некоторой корпоративной информационной системы на процесс взаимодействия двух корпоративных систем друг с другом.

Внутренние угрозы обусловлены возможностью:

- несанкционированных действий со стороны легитимного пользователя корпоративной информационной системы АСТНК на отдельные элементы этой системы;

- несанкционированных действий со стороны нелегитимного пользователя корпоративной информационной системы АСТНК на отдельные элементы этой системы;
- несанкционированного распространения информации со стороны пользователя корпоративной информационной системы за пределы этой системы с помощью сервисов СОП.

В качестве источников угроз рассматриваются следующие классы субъектов, которые могут в той или иной мере осуществлять воздействие на информационные процессы в АСТНК:

- пользователи СОП или других корпоративных систем;
- сотрудники организации, не являющиеся легитимными пользователями АСТНК;
- легитимные локальные пользователи–аналитики АСТНК ;
- легитимные удаленные пользователи–аналитики АСТНК;
- пользователи из группы администратора АСТНК;
- пользователи из группы администратора безопасности.

Некоторые модели возможных источников угроз информационной безопасности АСТНК по обобщенным сценариям информационного воздействия внешних и внутренних нарушителей приведены в табл. 1.

Таблица 1. Модели возможных источников угроз по сценариям информационного воздействия.

Класс источника	Цель воздействия	Характерные сценарии воздействия
Пользователь СОП или другой корпоративной системы	Анализ АСТНК с целью выявления уязвимостей изучения возможностей для проведения дальнейших воздействий	• сканирование портов; • анализ трафика сети; • сбор информации о АСТНК с помощью общедоступных данных и приложений; • перехват имен и паролей; • подбор паролей
	Нарушение целостности и/илидоступности программно–технических средств и технологических процессов АСТНК	• внедрение вредоносного программного обеспечения; • несанкционированное включение и передача пакетов; • искажение пакетов данных; • вставка ложной информации или вредоносных команд в обычный поток данных; • воздействия с целью превышения допустимой нагрузки функционирования сети, операционной системы или приложения АСТНК; • запись и повторная передача санкционированных пакетов; • информационное воздействие с использованием прикладных программ • перехват и нарушение адресации пакетов; • прямой доступ, модификация, порча, удаление данных
	Непреднамеренные действия	• распространение вредоносного программного обеспечения; • превышения допустимой нагрузки функционирования сети, операционной системы или приложения из–за ошибочных действий

Продолжение табл. 1

Класс источника	Цель воздействия	Характерные сценарии воздействия
Сотрудник организации, не являющийся легитимным пользователем АСТНК, но имеющий доступ на территории объекта информатизации	Анализ возможности доступа к АРМ,серверам, устройствам ввода/вывода, хранилищам носителей информации с целью изучения возможностей воздействия	• выявление помещений, где располагаются АРМы, серверы, устройства ввода/вывода и хранилища носителей информации; • выявление информационных систем и СУБД где хранится служебная информация; • изучение установленного режима допуска в помещения, к информационным и вычислительным ресурсам АСТНК; • выявление (хищение) идентификаторов и паролей легитимных пользователей; • хищение криптографических ключей легитимных пользователей
	Нарушение целостности и/или доступности программно–технических средств и технологических процессов АСТНК	• физическое нарушение целостности и/или доступности программно–технических средств АСТНК • внедрение вредоносного программного обеспечения разрушающего действия.
	Ознакомление со служебной информацией	• установка электронных средств съема информации; • внедрение вредоносного программного обеспечения типа “троянский конь”; • хищение бумажных и магнитных носителей информации; • копирование информации из прикладных систем под видом легитимного пользователя АСТНК

Окончание табл. 1

Класс источника	Цель воздействия	Характерные сценарии воздействия
	Непреднамеренные действия	• физическое нарушение целостности и/или доступности программно–технических средств АСТНК; • непреднамеренное получение информации об установленных запретатах
Легитимный локальный пользователь АСТНК	Анализ возможности доступа к прикладным системам и хранилищам служебной информации, к которым он не имеет доступа	• подслушивание разговоров и наблюдение за сотрудниками, которые имеют доступ к служебной информации; • изучение эксплуатационной, технологической и другой документации, из которой можно получить эти сведения; • несанкционированная установка и запуск системных утилит и программ, позволяющих собрать информацию о типах программного и информационного обеспечения; • выявление технологий доступа к прикладным системам, обрабатывающим служебную информацию. • вскрытие или хищение идентификаторов, паролей, ключей.

Классификация методов обеспечения информационной безопасности АСТНК

Независимо от конкретных видов угроз АСТНК должна обеспечивать эффективный режим целевого назначения в условиях информационных атак. При этом должны гарантироваться следующие свойства информации.

Конфиденциальность информации – субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью АСТНК сохранять эту информацию в тайне от субъектов, не имеющих полномочий доступа к ней. Целостность информации – существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному её состоянию). Доступность информации – свойства АСТНК, в которой циркулирует информация, характеризующаяся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей информации готовность автоматизированных средств к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость. Поэтому для автоматизированных систем рассматривают три вида угроз. Угроза нарушения конфиденциальности, т.е. информация стала доступна субъектам, не имеющим полномочий доступа к ней. Угроза нарушения целостности включает в себя любое умышленное изменение информации, хранящейся в АС, или передаваемой из одной системы в другую. Угроза отказа автоматизированных служб возникает, когда в результате преднамеренных действий, предпринимаемых субъектами, блокируется доступ к некоторому ресурс средств вычислительной техники. Рассмотренные виды угроз являются первичными. К опосредованным угрозам относятся угрозы раскрытия параметров АС, которая имеет в

своем составе систему защиты информации. Классификация методов обеспечения ИБ строится путем отображения множества основных угроз нарушения в множество методов обеспечения конфиденциальности, целостности и доступности информации.

Лекция 5. Информационные воздействия и несанкционированный доступ. Каналы несанкционированного доступа

Анализ причин нарушений информационной безопасности в АСТНК

Нарушение безопасности информации в АСТНК возможно как вследствие различных возмущающих воздействий, в результате которых происходит уничтожение (модификация) данных или нарушение работоспособности системы, так и вследствие несанкционированного доступа к ней со стороны злоумышленника (нарушителя). Воздействия, в результате которых может быть нарушена безопасность информации, включают в себя:

- воздействия внешней среды (случайные воздействия природной среды, отказы технических средств, не входящих в состав ВС, но влияющих на ее работоспособность, например, системы электроснабжения или каналов связи, и т.д.);
- внутренние возмущающие факторы (отказы технических средств ВС, ошибки в математическом и программном обеспечении, недостаточная квалификация и непреднамеренные ошибки в действиях персонала, приводящая к сбоям и т.п.);
- целенаправленные воздействия нарушителя (использование каналов несанкционированного доступа и/или средств информационного воздействия).

Системный подход к проблеме обеспечения безопасности информации требует комплексного применения общих и специальных (зависящих от особенностей защищаемой системы) технических, программных и организационных средств защиты. Однако в аспектах, касающихся воздействия внешней среды и внутренних возмущающих факторов, автоматизированная информационная система ТНК в целом схожа с другими сложными техническими системами и испытывает по сути риски, имеющие одинаковую основу (внешняя и внутренняя среда, надежность технических средств, человеческий фактор). Отличительным же и наиболее характерным типом воздействий на автоматизированную информационную систему являются целенаправленные воздействия нарушителя. Угрозы нарушения конфиденциальности и целостности данных и работоспособности ВС в целом со стороны нарушителя осуществляются посредством несанкционированного доступа к информации.

Каналы несанкционированного доступа

Под несанкционированным доступом (НСД) понимаются злоумышленные или случайные действия, выполненные с нарушением технологической схемы применения ВС и приведшие к нарушению безопасности системы.

Под каналом НСД будем понимать особенность автоматизированной информационной системы, создающую потенциальную возможность осуществления НСД. Все каналы НСД можно разделить на косвенные и прямые. Косвенными называются такие каналы НСД, использование которых для НСД не требует непосредственного доступа к системе.

Косвенные каналы НСД возникают, например, вследствие недостаточной изоляции помещений, просчетов в организации работы

автоматизированной информационной системы и предоставляют нарушителю возможность применения средств дистанционного фотографирования, перехвата электромагнитных излучений (ЭМИ), хищения носителей данных и производственных отходов (распечаток, документации и т.п.). Косвенные каналы НСД позволяют нарушителю осуществлять только пассивный сбор сведений о системе, которые, однако, могут быть использованы для подготовки прямых каналов НСД.

Прямые каналы НСД требуют непосредственного доступа к техническим средствам вычислительной системы. Необходимо отметить, что в данном случае «непосредственный доступ» означает не физический, а информационный доступ, то есть он может быть как локальным, так и удаленным. Наличие прямых каналов НСД обусловлено недостатками технических и программных средств защиты ВС, недостатками операционных систем (ОС), математического и программного обеспечения, а также просчетами в организации технологического процесса работы ВС.

Прямые каналы НСД, позволяют нарушителю получить доступ к информации, обрабатываемой в вычислительной системе, выполнить действия по ее модификации и уничтожению, равно как и действия по исследованию и изменению программного обеспечения ВС (в том числе – внедрению программных закладок, модификации операционной системы и системы обеспечения безопасности, и т.д.) и нарушению работоспособности системы в целом, то есть осуществить любую угрозу безопасности. Схематически взаимосвязь информационных воздействий, каналов несанкционированного доступа и угроз безопасности информации показана на рис. 5.

Рис. 5. Карта информационных воздействий и угроз безопасности информации

Таксономия изъянов систем защиты информации

Разработка таксономии причин нарушения информационной безопасности АСТНК, вместе с перечнем функциональных требований, предъявляемых к системе обеспечения безопасности информации, является первым необходимым этапом решения задачи обеспечения информационной безопасности АСТНК.

Разработка такой таксономии сводится к исследованию изъянов систем зашиты информации (ИСЗ).

При этом под изъяном понимается свойство систем защиты, способствующее успешной реализации угрозы информационной безопасности.

Наиболее серьезные усилия по анализу причин нарушений ИСЗ в системах защиты с помощью экспериментов по их преодолению нашли свое отражение в методологии гипотетического выявления ИСЗ (Flaw Hypothesis Methodology).

Данная методология предусматривает проведение исследований в три этапа.

Первый этап состоит в общем комплексном изучении системы, причем особое внимание уделяется принципам функционирования механизмов защиты.

На втором этапе происходит выдвижение предположений (гипотез) о потенциально уязвимых узлах, которые затем тщательно проверяются на основании анализа документации по системе, реальных особенностей и деталей ее функционирования, и с помощью проведения специальных тестов, призванных подтвердить или опровергнуть присутствие предполагаемой бреши в системе защиты.

На третьем, заключительном этапе, полученные результаты обобщаются и формируются списки (перечни) выявленных ИСЗ и успешных атак.

Подобные исследования проводились так же по проектам RISOS (Research in Secured Operating System) и PA (Protection Analysis). В обоих проектах были предприняты попытки формального описания и систематизации информации об ИСЗ.

Суммируя результаты данных исследований, можно выявить следующие классы ИСЗ:

1. Недостаточно надежная идентификация, аутентификация и авторизация субъектов и объектов, приводящая к возможности использования нескольких имен для обозначения одной и той же сущности (субъекта или объекта) и неявному нарушению политики безопасности.

2. Ошибки контроля значений критичных параметров и границ объектов.

3. Асинхронный контроль и отложенное использование параметров и другие ошибки в последовательности действий, влекущие за собой прерывание атомарных операций.

4. Ошибки управления защитой памяти, хранение данных в незащищенных областях и неполное уничтожение объектов или их окружения после использования.

5. Ошибки в логике функционирования механизмов защиты и неадекватная реакция на нарушения безопасности.

С точки зрения технологии создания защищенных систем наибольшее значение имеют следующие вопросы, на которые должна дать ответ таксономия ИСЗ:

1. Каким образом ошибки, приводящие к появлению ИСЗ, вносятся в систему защиты? (классификация ИСЗ по способу внесения и источнику появления).

2. Когда, на каком этапе они вносятся? (классификация ИСЗ по этапу возникновения).

3. Где, в каких узлах системы защиты (или АСТНК в целом) они возникают и проявляются? (классификация ИСЗ по размещению в системе).

Наконец, для решения практических задач наибольший интерес представляет таксономия ИСЗ по причинам их возникновения.

Классификация ИСЗ по источнику появления

Как следует из определения ИСЗ, источником ее появления является ошибка или недоработка в системе безопасности.

Под источником появления понимается основа существования ИСЗ, т.е. либо характеристики ВС, которые обусловливают ее существование, либо принцип функционирования средств, использующих ИСЗ для осуществления атаки.

Исследованию ошибок, тем или иным образом связанных с безопасностью, всегда уделялось много внимания.

Результаты исследований свидетельствуют о том, что подобные ошибки носят неслучайный характер.

Классификация ИСЗ по источнику появления, приведена в таблице 2. Аббревиатура РПС означает «разрушающие программные средства».

Таблица 2. Таксономия ИСЗ по источнику появления

Ошибки в системах защиты, служащие источником появления ИСЗ		**Тип ошибки**	**Кол-во примеров**
Преднамеренно внесенные	С наличием деструктивных функций (Активные РПС)	Несамовоспроизводящиеся РПС ("троянские кони")	3
		Самовоспроизводящиеся РПС (вирусы)	7
	Без деструктивных функций (средства слежения и скрытого сбора информации)	Черные ходы, скрытые возможности проникновения в систему	2
		Скрытые каналы утечки информации	8
Случайные (непреднамеренные)	Ошибки контроля допустимых значений параметров		10
	Ошибки определения областей (доменов)		7
	Ошибки последовательности действий и использования нескольких имен для одного объекта		2
	Ошибки идентификации/аутентификации		5
	Ошибки проверки границ объектов.		4
	Другие ошибки в логике функционирования		4

Классификация ИСЗ по этапам внедрения

Проблему выявления этапа внедрения ошибок целесообразно рассматривать с учетом жизненного цикла программного обеспечения. На самом верхнем уровне представления жизненного цикла систем можно выделить три этапа:

- этап разработки, который охватывает весь период создания исходной рабочей версии системы;
- этап сопровождения, в ходе которого происходит модификация, совершенствование, развитие системы и появление ее очередных версий;
- этап эксплуатации, т.е. непосредственного применения конкретной версии системы.

Хотя на практике все эти этапы перекрываются во времени, им присущи различные особенности, которые позволяют четко выделить соответствующие категории ИСЗ. Таксономия ИСЗ по этапу внедрения, основанная на этих положениях, приведена в таблице 3.

Таблица 3. Таксономия ИСЗ по этапу возникновения

Этап внедрения ошибки и возникновения ИСЗ	**Тип ошибки**	**Количество примеров**
На стадии разработки	Ошибки в требованиях и спецификациях	22
	Ошибки в исходных текстах программ	15
	Ошибки в исполняемом коде	1
В ходе сопровождения		3
В ходе эксплуатации		9

Классификация ИСЗ по размещению в системе

ИСЗ можно также классифицировать по их размещению в АС, в зависимости от того, в каких компонентах системы они находятся (табл.4). Большинство ошибок, приводящих к возникновению ИСЗ и нарушению требований защиты, присутствует в программном обеспечении; в то же время они встречаются и в аппаратных средствах. Значительное внимание уделено исследованию таксономии ИСЗ в программном обеспечении вообще и в операционных системах в частности.

Однако АСТНК в своем функционировании всецело зависит от программно – аппаратной платформы. Этот факт, а также то, что ИСЗ может использовать ошибки аппаратных средств, определяет необходимость внесения в разрабатываемую классификацию соответственно категорий «ошибки в программном обеспечении» и «ошибки аппаратных платформ».

Таблица 4. Таксономия ИСЗ по размещению в системе

Местоположение уязвимых мест			**Кол-во примеров**
Программное обеспечение	Операционные системы	Инициализация ОС (загрузка)	8
		Управление выделением памяти	2
		Управление процессами	10
		Управление устройствами	3
		Управление файловой системой	6
		Средства идентификации и аутентификации	5
	Сервисные программы и утилиты	Привилегированные утилиты	10
		Непривилегированные утилиты	1
	Прикладные программы		1
Аппаратное обеспечение			3

Таксономия причин возникновения ИСЗ

Рассмотренная таксономия ИСЗ дает достаточно полное представление о классификации ИСЗ с точки зрения источника их появления, этапа возникновения и размещения в АСТНК. Поэтому представляется целесообразным провести анализ случаев нарушения безопасности с точки зрения таксономии причин появления ИСЗ, чтобы получить представление о первоисточниках данного явления. С точки зрения теории обеспечения безопасности информации, система защиты должна обеспечивать эффективное противодействие всем видам угроз без исключения, вне зависимости от их источников и характера. Залог успешных преднамеренных действий злоумышленника, как и предпосылки случайных нарушений, предопределены свойствами самой АСТНК – ее архитектурой, реализацией и администрированием. Иными словами, безопасность – свойство вычислительной системы в целом.

С позиций прагматического подхода к разработке и созданию защищенных систем, анализ безопасности должен основываться на выявлении их свойств, создающих предпосылки нарушения безопасности. В этом аспекте особенно важны таксономия причин нарушений безопасности ВС, или причин возникновения ИСЗ, связывающих случаи нарушения безопасности с принципами организации защиты ВС, обусловившими их существование. Таксономия причин возникновения ИСЗ должна дать ответ на имеющий ключевое значение с практической точки зрения вопрос: что явилось причиной успешного осуществления нарушения безопасности в том или ином случае? Знание природы этих причин позволит оценить способность системы противостоять преднамеренным атакам на систему, исключить возможности случайного нарушения безопасности, а также выявить недостатки в существующих средствах защиты, которые привели к соответствующим нарушениям, и построить защищенную систему, лишенную этих недостатков.

Р а з д е л 2. Основные результаты в области теории информационной безопасности

Лекция 6. Политика безопасности и основные типы политик безопасности

Понятие «политика безопасности»

Одними из важнейших понятий в теории обеспечения информационной безопасности информации являются политика безопасности и модель безопасности. Политика безопасности определяет множество требований по обеспечению безопасности информации, которые должны быть выполнены в АСТНК посредством системы обеспечения безопасности информации (СОБИ). В свою очередь, любая реализация системы обеспечения безопасности информации основывается на определенной модели безопасности. Под моделью безопасности понимается формальное математическое описание механизмов защиты информации в терминах «сущность», «субъект», «объект», «ресурс», «операция», «доступ», «уровень безопасности», «степень доверия», не привязанное, однако, к конкретной реализации СОБИ. В то время, как политика безопасности определяет множество требований для конкретной системы, модель безопасности есть абстрактное описание целого класса систем на формальном математическом языке, без рассмотрения конкретных деталей их реализации. В результате, модели безопасности являются полезным инструментарием при разработке политик безопасности для конкретных систем. Структура СОБИ, состав, входящих в нее средств защиты и принципы их применения полностью определяются совокупностью

принятой для данной АСТНК политики безопасности и лежащей в ее основе модели безопасности.

Политика безопасности компьютерной системы может быть выражена формальным и неформальным образом. Преимуществом неформального способа представления политики безопасности является то, что она гораздо легче для понимания разработчиков и пользователей, чем формальное описание, т.к. для ее понимания не требуется специальных математических знаний. Это снижает уровень риска непреднамеренных ошибок, совершаемых персоналом при эксплуатации такой системы. Основным недостатком, однако, является то, что при такой форме представления гораздо легче допустить ошибки принципиального характера. Особенно это справедливо для политик безопасности нетривиальных систем, отличающихся большой сложностью, подобно многопользовательским операционным системам. По этой причине для разработки систем обеспечения безопасности информации используются формальные средства описания политик безопасности.

В основе формальных политик безопасности лежат модели безопасности, заданные на формальном математическом языке. Преимуществом формального описания является возможность теоретического доказательства безопасности системы при соблюдении всех условий политики безопасности. Для формального описания моделей безопасности используются понятия субъекта, объекта и доступа.

Субъекты, объекты и доступ

Под сущностью будем понимать любую именованную составляющую компьютерной системы. *Субъект* определятся как активная сущность, которая может инициировать запросы на доступ к

объектам и использовать их для выполнения каких–либо операций. Субъектами являются пользователи и процессы. *Объект* определятся как пассивная сущность, используемая для хранения или получения информации. Примерами объектов являются рабочие станции, файлы, директории, и т.д.

Хотя основная концепция разделения сущностей на субъекты и объекты ясна, необходимо отметить, что одна и та же сущность может выступать как в качестве субъекта, так и в качестве объекта. Например, с точки зрения ОС, запускаемые ею процессы являются и объектами, и субъектами, в то время как директории и хранящиеся в них файлы – только объектами.

В процессе исполнения субъекты выполняют *операции*. При исполнении субъектами операций происходит взаимодействие субъектов и объектов, называемое доступом. *Доступ* – взаимодействие между субъектом и объектом, в результате которого происходит перенос информации между ними. Существуют две основные операции, переносящие информацию между субъектами и объектами. Под операцией чтения понимается операция, результатом которой является перенос информации от объекта к субъекту. Под операцией записи понимается операция, результатом которой является перенос информации от объекта к субъекту. Данные операции являются минимально необходимым базисом для описания широкого круга абстрактных формальных моделей, описывающих защищенные системы. Для практического применения таких абстрактных моделей данный базис должен быть расширен в соответствии с парадигмой обработки информации, характерной для конкретной вычислительной системы.

Уровни безопасности, доверие и секретность

Каждой сущности автоматизированной информационной системы присущ определенный набор характеристик. С точки зрения системы обеспечения безопасности информации, основными характеристиками сущностей являются степень секретности и степень доверия. Уровень безопасности (иногда данная характеристика называется степенью секретности или классом защиты) определяется как иерархический атрибут, который может быть ассоциирован с сущностью автоматизированной системы для обозначения степени ее критичности в смысле безопасности. Данная степень критичности может помечать, например, степень ущерба от нарушения безопасности данной сущности в автоматизированной системе. Классический набор уровней безопасности информации включает в себя уровни «для свободного доступа», «для служебного пользования», «секретно», «совершенно секретно» и «особой важности».

Степень доверия (класс допуска) некоторой сущности задает, максимальный уровень безопасности информации, к которой возможен доступ данной сущности, например сущность со степенью доверия «секретно» может осуществить доступ к объектам, имеющим степень секретности (уровень безопасности) не выше «секретно». Таким образом, степень секретности есть атрибут объекта, а класс допуска субъекта.

Классификация моделей обеспечения безопасности информации

Системы защиты информации в идеальном случае должны обеспечивать противодействие всем видам угроз безопасности. А поскольку системы защиты базируются на формальных моделях обеспечения безопасности, то одним из принципов, положенных в основу классификации последних, является их целевое предназначение.

В соответствии с целевым предназначением, заключающемся в защите от определенного типа угроз, существует три класса моделей, на основании которых разрабатываются конкретные системы обеспечения безопасности:

- модели обеспечения конфиденциальности информации (также называемые моделями управления доступом или моделями разграничения доступа);
- модели обеспечения целостности информации;
- модели защиты от отказов в обслуживании.

Модели управления доступом в настоящее время являются наиболее проработанными и совершенными, поскольку в силу исторических причин и практической необходимости (защита государственных и военных секретов) им уделялось основное внимание. Модели управления доступом служат для синтеза политик безопасности, направленных на предотвращение угрозы нарушения конфиденциальности информации (т.е. раскрытия ее содержания).

Данный класс включает в себя модели управления доступом, построенные по принципу разграничения доступа и предоставления прав, семантические модели, информационные модели и вероятностные модели.

Основными типами моделей предоставления прав являются модели дискретного и мандатного доступов. Модели данного типа используются в большинстве реальных систем, используемых в настоящее время. Модели дискретного управления доступом (DAC, Discretionary Access Control), например, присутствуют во многих операционных системах, где они реализованы в виде списков контроля доступа (ACLs, Access Control Lists). Классическим примером мандатной модели доступа (MAC, Mandatory Access Control) является модель Белла–Лападулы. Требования,

на которых основаны данные модели, лежат в основе всех современных стандартов безопасности.

Информационные (потоковые) модели определяют ограничения на отношение ввода/вывода системы, которые достаточны для реализации системы. Данные модели являются результатом применения теории информации К. Шеннона к проблеме безопасности систем. К данным моделям относятся модели невмешательства и невыводимости. Теория информационных моделей разграничения доступа в настоящее время развивается.

Вероятностные модели исследуют вероятность преодоления системы защиты за определенное время. Достоинствам моделей данного типа можно отнести числовую оценку стойкости системы защиты. К недостаткам – изначальное допущение того, что система защиты может быть вскрыта. Задача модели – минимизация вероятности преодоления системы защиты. Примерами вероятностных моделей являются игровая модель и модель системы защиты с полным перекрытием.

Семантические модели являются относительно новым и наиболее перспективным классом моделей управления доступом. В отличие от классических DAC– и MAC–моделей, использующих консервативную терминологию субъектов, объектов, уровней безопасности и (лишенных семантики) операций доступа, семантические модели являются первыми шагами на пути создания «осмысленных» систем обеспечения безопасности. Представителями данного класса являются модели управления доступом, базирующиеся на ролях (RBAC, Role–Based Access Control) и целевых задачах (TBAC, Task–Based Access Control). В RBAC–модели каждый субъект отождествляется с ролью, выполняемой им в системе, и правила управления доступом требуют контроля семантики выполняемых им операций и их соответствия роли субъекта. В центре TBAC–модели находится концепция целевой задачи того или иного

уровня общности, решаемой системой, и правила управления доступом заключаются в контроле соответствия семантики и последовательности выполняемых операций целевой задаче.

Модели обеспечения целостности используются для синтеза механизмов контроля целостности информации в системе.

Примерами моделей целостности являются модель Биба (зеркальное отображение модели Белла–Лападулы), и модель Кларка–Вилсона.

Последняя модель является примером неформального представления требований безопасности, выраженных в терминах набора правил функционирования компьютерной системы для обеспечения уровня защиты целостности некоторого заданного подмножества данных.

Модели защиты от угрозы отказа в обслуживании на сегодняшний день являются наименее развитым классом моделей обеспечения безопасности, поскольку до настоящего времени большинство исследований компьютерной безопасности было связано с угрозами раскрытия и целостности.

В качестве возможной замены моделей защиты от отказа в обслуживании целесообразно рассматривать модели распределения ресурсов (например, модель Миллена), которую можно использовать для описания стратегий защиты от отказа в обслуживании.

Другими признаками классификации моделей обеспечения безопасности данных является принцип описания процессов защиты данных и используемый для этого математический аппарат. Существующие технологии формального описания процессов обеспечения безопасности информации основываются на понятиях разных разделов математики – теории конечных автоматов, теории множеств, теории графов, временной и математической логики и теории предикатов.

При этом применяемый для описания модели математический аппарат вносит некоторые ограничения на степень детализации процессов защиты, что обусловлено различием физической сущности описываемых с помощью используемых понятий процессов. Например, модели, основанные на теории множеств, с большей детальностью описывают процессы контроля доступа к ресурсам системы, так как имеют развитый аппарат определения взаимоотношений между множествами субъектов и объектов.

В то же время модели, основанные на теории графов, позволяют описать информационные потоки и глубоко детализировать процессы доступа и передачи данных в системе.

Лекция 7. Основные определения и базовые принципы построения формальных моделей политик безопасности

Определения и основные положения формальных моделей политик безопасности

Рассмотрим основные положения наиболее распространенных политик и моделей безопасности, основанных на контроле доступа субъектов к объектам в пространстве состояний, одни из которых являются безопасными, а другие – небезопасными. Все рассматриваемые модели безопасности основаны на следующих базовых представлениях:

1. Система является совокупностью взаимодействующих сущностей – субъектов и объектов. Объекты можно интуитивно представлять в виде контейнеров, содержащих информацию, а субъекты можно считать выполняющимися программами, которые воздействуют на объекты различными способами. При таком представлении системы безопасность обработки информации обеспечивается путем решения задачи управления доступом субъектов к объектам в соответствии с заданным набором

правил и ограничений, которые образуют политику безопасности. Считается, что система безопасна, если субъекты не имеют возможности нарушить правила политики безопасности. Необходимо отметить, что общим подходом для всех моделей является именно разделение множества сущностей, составляющих систему, на множества субъектов и объектов, хотя сами определения понятий « объект» и «субъект» в разных моделях могут существенно различаться.

2. Все взаимодействия в системе моделируются установлением отношений определенного типа между субъектами и объектами. Множество типов отношений определяется в виде набора операций, которые субъекты могут производить над объектами.

3. Все операции контролируются монитором взаимодействий и либо запрещаются, либо разрешаются в соответствии с правилами политики безопасности.

4. Политика безопасности задается в виде правил, в соответствии с которыми должны осуществляться все взаимодействия между субъектами и объектами. Взаимодействия, приводящие к нарушению этих правил, пресекаются средствами контроля доступа и не могут быть осуществлены.

5. Совокупность множеств субъектов, объектов и отношений между ними (установившихся взаимодействий) определяет состояние системы. Каждое состояние системы является либо безопасным, либо небезопасным в соответствии с предложенным в модели критерием безопасности.

6. Основной постулат модели безопасности – имеющая формальное доказательство теорема о том, что система, находящаяся в безопасном состоянии, не может перейти в небезопасное состояние при соблюдении всех установленных правил и ограничений.

Алгоритмизация понятия «политика безопасности»

Политика безопасности включает:

- множество возможных операций над объектами;
- множество разрешенных операций, являющееся подмножеством возможных операций для каждой пары «субъект,объект».

Например, операции «создание объекта», «удаление объекта», «перенос информации от произвольного объекта к предопределенному объекту» (операция «чтения») и т. д.

Рассмотрим базовые аксиомы построения формальных политик безопасности.

Аксиома 1. В защищенной АС всегда присутствует активный компонент (субъект), выполняющий контроль операций субъектов над объектами. Этот компонент фактически отвечает за реализацию некоторой политики безопасности.

Аксиома 2. Для выполнения в защищенной АС операций над объектами необходима дополнительная информация (и наличие содержащего ее объекта) о разрешенных и запрещенных операциях субъектов с объектами.

Аксиома 3. Все вопросы безопасности информации в АС описываются доступами субъектов к объектам.Политика безопасности должна быть поддержана во времени, следовательно, в процесс изучения свойства защищаемой системы должны быть определены процедуры управления безопасностью.

При рассмотрении вопроса гарантирования политики безопасности выделяют четыре класса взаимосвязанных задач:

- формулирование и изучение политик безопасности;
- реализация политик безопасности;
- гарантирование заданной политики безопасности;
- управление безопасностью.

В теории информационной безопасности практически всегда рассматривается модель произвольной АС в виде конечного множества элементов. Указанное множество можно разделить на два подмножества: множество объектов и множество субъектов. Данное разделение основано на свойстве элемента «быть активным» или «получать управление» (применяется также термин «использовать ресурсы» или «пользоваться вычислительной мощностью»).

Полагаем разделение АС на субъекты и объекты априорным. Будем считать также, что существует априорный безошибочный критерий различения субъектов и объектов в АС (по свойству активности). Кроме того, предполагаем, что декомпозиция АС на субъекты и объекты фиксирована.

Аксиома 4. Субъекты в АС могут быть порождены из объектов только активным компонентом (субъектами).

Специфицируем механизм порождения новых субъектов следующим определением.

Определение 1. Объект Oj называется источником для субъекта S_m, если существует субъект Sj, в результате воздействия которого на объект Oi в АС возникает субъект S_m .

Субъект Sj , порождающий новый субъект из объекта Oi , называется активизирующим субъектом для субъекта S_m , S_m назовем порожденным объектом.

Свойство субъекта «быть активным» реализуется и в возможности выполнения действия над объектами. Необходимо отметить, что пассивный статус объекта требует существования потока информации от объекта к объекту (в противном случае невозможно говорить об изменении объектов), причем данный поток инициируется субъектом $S_т$.

Определение 2. Объект Oi в момент времени t ассоциирован с субъектом $S_т$,если состояние объекта Oi повлияло на состояние субъекта в следующий момент времени.

***Определение* 3.** Потоком информации между объектом O_m. и объектом Oj называется произвольная операция над объектом Oj, реализуемая в субъекте Si и зависящая от O_m.

В определении подчеркнуто, что поток информации рассматривается не между субъектом и объектом, а между объектами, например, объектом и ассоциированными объектами субъекта (либо между двумя объектами). Активная роль субъекта выражается в реализации данного потока (это означает, что операция порождения потока локализована в субъекте и отображается состоянием функционально ассоциированных объектов.

Из определения 3 следует также, что поток всегда инициируется (порождается) субъектом.

Определение 4. Доступом субъекта Si к объекту Oj, будем называть порождение потока информации между некоторым объектом (например, ассоциированным с субъектом объектами Si($\{O_m\}$)) и объектом Oj.

Выделим все множество потоков P для фиксированной декомпозиции АС на субъекты и объекты во все моменты времени (все множество потоков является объединением потоков по всем моментам дискретного времени) и произвольным образом разобьем его на два непересекающихся подмножества: N и L.

Обозначим: N – подмножество потоков, характеризующее несанкционированный доступ; L – подмножество потоков, характеризующих легальный доступ. Дадим некоторые пояснения к разделению на множества L и N. Понятие "безопасности" подразумевает наличие и некоторого состояния опасности – нежелательных состояний какой–либо системы (в данном случае АС). Будем считать парные категории типа «опасный–безопасный»

априорно заданным для АС и описываемыми политикой безопасности, а результатом применения политики безопасности к АС – разделение всего множества потоков на множества «опасных» потоков N и множество «безопасных» L. Деление на L и N может описывать как свойство целостности (потоки из N нарушают целостность АС) или свойство конфиденциальности (потоки из N нарушают конфиденциальность АС), так и любое другое произвольное свойство.

Определение 5. Правила разграничения доступа субъектов к объектам есть формально описанные потоки, принадлежащие подмножеству L .

В предлагаемой субъектно–ориентированной модели не уточняются известные модели политик безопасности (политика безопасности описывает только критерии разбиения на множества L и N), но формулируются условия корректного существования элементов АС , обеспечивающих реализацию той или иной политики безопасности. Поскольку критерий разбиения на множества L и N не связан со следующими далее утверждениями (постулируется лишь наличие субъекта, реализующего фильтрацию потоков), то можно говорить об инвариантности субъектно–ориентированной модели относительно любой , принятой в АС политики безопасности (не противоречащей условиям утверждений).

Для разделения всего множества потоков в АС на подмножества L и N необходимо существование активного компонента (субъекта), который:

- активизировался бы при возникновении любого потока;
- производил бы фильтрацию потоков в соответствии с принадлежностью множествам L или N.

Определение 6. Монитор обращений (МО) – субъект, активизирующийся при возникновении потока от любого субъекта к любому объекту.

Можно выделить два вида МО: индикаторный МО – устанавливающий только факт обращения субъекта к объекту; содержательный МО –

субъект, функционирующий таким образом, что при возникновении потока от ассоциированного объекта O_m любого субъекта Si к объекту Oj и обратно существует ассоциированный с МО объект O_{mo} (в данном случае речь идет об ассоциированных объектах–данных), тождественный объекту $O_т$ или одному из Si($\{O_m\}$) . Содержательный МО полностью участвует в потоке от субъекта к объекту (в том смысле, что информация проходит через его ассоциированные объекты–данные и существует тождественное отображение объекта на какой–либо ассоциированный объект МО).

Теперь сформулируем понятие монитора безопасности (в литературе также применяется понятие монитора ссылок). Это понятие связано с упоминаемой выше задачей фильтрации потоков. Поскольку целью является обеспечение безопасности АС, то и целевая функция монитора –фильтрация для обеспечения безопасности (отметим еще раз, что разделение на N и L. задано априорно).

Определение 7. Монитор безопасности объектов (МБО) – монитор обращений, который разрешает поток, принадлежащий только множеству легального доступа L. Разрешение потока в данном случае понимается как выполнение операции над объектом–получателем потока, а запрещение–как невыполнение (т.е. неизменность объекта–получателя потока). Монитор безопасности объектов фактически является механизмом реализации политики безопасности в АС.

Понятие «доверенная вычислительная среда» (Trusted Computing Base – TCB)

Смысл характеристики «доверенная» поясняется следующим образом. Содержание характеристики «безопасный» (в том смысле, что либо нечто является безопасным, полностью удовлетворяя ряду предъявляемых требований, либо не является, если одно или несколько требований не

выполнены) в сочетании с утверждением «ничто не бывает безопасным на сто процентов» приводит к необходимости ввести более гибкий термин, позволяющий оценивать то, в какой степени разработанная защищенная АС соответствует ожиданиям заказчиков. В этом отношении характеристика «доверенный» более адекватно отражает ситуацию, где оценка, выраженная этой характеристикой (безопасный или доверенный), основана не на мнении разработчиков, а на совокупности факторов, включая мнение независимой экспертизы, опыт предыдущего сотрудничества с разработчиками, и в конечном итоге, является прерогативой заказчика, а не разработчика.

Доверенная вычислительная среда (ТСВ) включает все компоненты и механизмы защищенной автоматизированной системы, удовлетворяющие приведенным ранее аксиомам и определениям и отвечающие за реализацию политики безопасности. Все остальные части АС , а также ее заказчик полагаются на то, что ТСВ корректно реализует заданную политику безопасности даже в том случае, если отдельные модули или подсистемы АС разработаны высококвалифицированными злоумышленниками с тем, чтобы вмешаться в функционирование ТСВ и нарушить поддерживаемую ее политику безопасности.

Лекция 8. Дискреционная модель Харрисона–Рузо–Ульмана разграничения, управления и контроля за распространением прав доступа. Критерий безопасности

Дискреционная модель Харрисона–Руззо–Ульмана

Модель безопасности Харрисона–Руззо–Ульмана, являющаяся классической дискреционной моделью, реализует произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа.

В рамках этой модели система обработки информации представляется в виде совокупности активных сущностей – субъектов (множество S), которые осуществляют доступ к информации, пассивных сущностей – объектов (множество O), содержащих защищаемую информацию, и конечного множества прав доступа R = {r1, ..., rN}, означающих полномочия на выполнение соответствующих действий (например, чтение, запись, выполнение).

Причем для того, чтобы включить в область действия модели и отношения между субъектами, принято считать, что все субъекты одновременно являются и объектами – $S \subset O$. Поведение системы моделируется с помощью понятия состояния. Пространство состояний системы образуется декартовым произведением множеств составляющих ее объектов, субъектов и прав – OxSxR. Текущее состояние системы Q в этом пространстве определяется тройкой, состоящей из множества субъектов, множества объектов и матрицы прав доступа M, описывающей текущие права доступа субъектов к объектам, Q=(S,O,M). Строки матрицы соответствуют субъектам, а столбцы – объектам, поскольку множество объектов включает в себя множество субъектов, матрица имеет вид прямоугольника. Любая ячейка матрицы M[s,o] содержит набор прав субъекта s к объекту o, принадлежащих множеству прав доступа R. Поведение системы во времени моделируется переходами между различными состояниями. Переход осуществляется путем внесения изменений в матрицу M с помощью команд следующего вида:

command $\alpha(x_1, \ldots, x_k)$

if r_1 in $M[x_{s1}, x_{o1}]$ and; (условия выполнения команды)

r_2 in $M[x_{s2}, x_{o2}]$ and;

….

r_m in M[x_{sm} , x_{om}] and;

then

op_1 , op_2 , ..., op_n . (операции, составляющие команду)

Здесь α – имя команды; x_i – параметры команды, являющиеся идентификаторами субъектов и объектов, s_i и o_i – индексы субъектов и объектов в диапазоне от 1 до k; op_i – элементарные операции. Элементарные операции, составляющие команду, выполняются только в том случае, если все условия, означающие присутствие указанных прав доступа в ячейках матрицы M, являются истинными. В классической модели допустимы только следующие элементарные операции:

enter r into M[s,o] (добавление субъекту s права r для объекта o);
delete r from M[s,o] (удаление у субъекта s права r для объекта o);
create subject s (создание нового субъекта s);
create object o (создание нового объекта o);
destroy subject s (удаление существующего субъекта s);
destroy object o (удаление существующего объекта o).

Операция enter вводит право r в существующую ячейку матрицы доступа. Содержимое каждой ячейки рассматривается как множество, т.е. если это право уже имеется, то ячейка не изменяется. Операция называется enter монотонной, поскольку она только добавляет права в матрицу доступа и ничего не удаляет. Действие операции delete противоположно действию операции enter. Она удаляет право из ячейки матрицы доступа, если оно там присутствует. Поскольку содержимое каждой ячейки рассматривается как множество, delete не делает ничего, если удаляемое право отсутствует в указанной ячейке. Поскольку delete удаляет информацию из матрицы доступа, она называется немонотонной

операцией. Операции create subject и destroy subject представляют собой аналогичную пару монотонной и немонотонной операций.

Применение любой элементарной операции op в системе, находящейся в состоянии Q=(S,O,M) влечет за собой переход в другое состояние Q'=(S',0',M'), которое отличается от предыдущего состояния Q по крайней мере одним компонентом.

Формальное описание некой конкретной системы ∑(Q,R,C) будет состоять из следующих элементов:

1. Конечный набор прав доступа $R = \{r_1, \dots, r_n\}$;

2. Конечные наборы исходных субъектов $S_0 = \{s_1, ..., s_l\}$ и объектов $O_0 = \{o_1, ..., o_m\}$, где $S_0 \subseteq O_0$;

3. Исходная матрица доступа, содержащая права доступа субъектов к объектам – M_0;

4. Конечный набор команд $C = \{\alpha_i(x_i,... x_k,)\}$, –каждая из которых состоит из условий выполнения и интерпретации в терминах перечисленных элементарных операций.

Поведение системы во времени моделируется с помощью последовательности состояний $\{Q_i\}$, в которой каждое последующее состояние является результатом применения некоторой команды из множества C к предыдущему $Q_{n+1} = C_n(Q_n)$. Таким образом для заданного начального состояния только от условий команд из C и составляющих их операций зависит, сможет ли система попасть в то или иное состояние, или нет. Каждое состояние определяет отношения доступа, которые существуют между сущностями системы в виде множества субъектов, объектов и матрицы прав. Поскольку для обеспечения безопасности необходимо наложить запрет на некоторые отношения доступа, для заданного начального состояния системы должна существовать возможность определить множество состояний, в которые она сможет из него попасть. Это позволит задавать такие начальные условия

(интерпретацию команд C, множества объектов O_0, субъектов S_0 и матрицу доступа M_0), при которых система никогда не сможет попасть в состояния, нежелательные с точки зрения безопасности. Следовательно, для построения системы с предсказуемым поведением необходимо для заданных начальных условий получить ответ на вопрос: сможет ли некоторый субъект s когда–либо приобрести право доступа r для некоторого объекта o.

Поэтому критерий безопасности модели Харрисона–Руззо–Ульмана формулируется следующим образом:.

Для заданной системы начальное состояние $Q_0=(S_0,O_0,M_0)$ является безопасным относительно права r, если не существует применимой к Q_0 последовательности команд, в результате которой право r будет занесено в ячейку матрицы M, в которой оно отсутствовало в состоянии Q_0.

Смысл данного критерия состоит в том, что для безопасной системы субъект никогда не получит право r доступа к объекту, если он не имел его изначально.

Из критерия безопасности следует, что для данной модели ключевую роль играет выбор значений прав доступа и их использование в условиях команд. Хотя модель не налагает никаких ограничений на смысл прав и считает их равнозначными, те из них, которые участвуют в условиях выполнения команд, фактически представляют собой не права доступа к объектам (как, например, чтение и запись), а права управления доступом, или права на осуществление модификации ячеек матрицы доступа. Таким образом, по сути дела данная модель описывает не только доступ субъектов к объектам, но и распространение прав доступа от субъекта к субъекту, поскольку именно изменение содержания ячеек матрицы доступа определяет возможность выполнения команд, в том числе команд, модифицирующих саму матрицу доступа, которые потенциально могут привести к нарушению критерия безопасности.

С точки зрения практики построения защищенных систем модель Харрисона–Руззо–Ульмана является наиболее простой в реализации и эффективной в управлении, поскольку не требует никаких сложных алгоритмов, и позволяет управлять полномочиями пользователей с точностью до операции над объектом, чем и объясняется ее распространенность среди современных систем. Предложенный в данной модели критерий безопасности является весьма сильным в практическом плане, поскольку позволяет гарантировать недоступность определенной информации для пользователей, которым изначально не выданы соответствующие полномочия.

Однако, Харрисон, Руззо и Ульман доказали, что в общем случае не существует алгоритма, который может для произвольной системы, ее начального состояния $Q_0=(S_0,O_0,M_0)$ и общего права r решить, является ли данная конфигурация безопасной. Доказательство опирается на свойства машины Тьюринга, с помощью которой моделируется последовательность переходов системы из состояния в состояние. Для того, чтобы можно было доказать указанный критерий, модель должна быть дополнена рядом ограничений. Указанная задача является разрешимой в любом из следующих случаев:

- команды $\alpha_i(x_1, \ldots, x_k)$ являются монооперационными, т. е. состоят не более чем из одной элементарной операции;
- команды $\alpha_i(x_1, \ldots, x_k)$ являются одноусловными и монотонными. Содержат не более одного условия и не содержат операций destroy и delete;
- команды $\alpha_i(x_1, \ldots, x_k)$ не содержат операций create.

Эти условия существенно ограничивает сферу применения модели, поскольку трудно представить себе реальную систему, в которой не будет происходить создание или удаление сущностей.

Таким образом, дискреционная модель Харрисона–Руззо–Ульмана в своей общей постановке не дает гарантий безопасности системы, однако, именно она послужила основой для целого класса моделей политик безопасности, которые используются для управления доступом и контроля за распространением прав во всех современных системах.

Типизованная матрица доступа

Другая дискреционная модель, получившая название "Типизованная матрица доступа" (Type Access Matrix – далее TAM) , представляет собой развитие модели Харрисона–Руззо–Ульмана, дополненной концепцией типов, что позволяет несколько смягчить те условия, для которых возможно доказательство безопасности системы.

Формальное описание модели TAM включает следующие элементы:

1. Конечный набор прав доступа $R = \{r_1, \ldots, r_n\}$.

2. Конечный набор типов $T = \{t_1, ..., t_g\}$.

3. Конечные наборы исходных субъектов $S_0 = \{s_1, ..., s_n\}$ и объектов $O_0 = \{o_1, ..., o_n\}$, где $S_0 \subseteq O_0$.

4. Матрица M, содержащая права доступа субъектов к объектам, и ее начальное состояние M_0.

5. Конечный набор команд $C = \{\alpha_i(x_1, \ldots, x_k)\}$, включающий условия выполнения команд и их интерпретацию в терминах элементарных операций.

Тогда состояние системы описывается четверкой Q=(S,O,t,M), где S, O, и M обозначают соответственно множество субъектов, объектов и матрицу доступа, а $t: O \rightarrow T$ – функция, ставящая в соответствие каждому объекту некоторый тип:

Состояние системы изменяется с помощью команд из множества C. Команды ТАМ имеют тот же формат, что и в модели Харрисона–Руззо–Удьмана, но всем параметрам приписывается определенный тип:

command $\alpha(x_1:t_1, \ldots, x_k:t_k)$
if r_1 in $M[x_{s1}, x_{o1}]$ and ;(условия выполнения команды)
  r_2 in $M[x_{s2}, x_{o2}]$ and;
  ….
  r_m in $M[x_{sm}, x_{om}]$ and;
then
  op_1 , op_2 ... op_n .(операции, составляющие команду)

Перед выполнением команды происходит проверка типов фактических параметров, и, если они не совпадают с указанными в определении, команда не выполняется. Фактически, введение контроля типов для параметров команд приводит к неявному введению дополнительных условий, т. к. команды могут быть выполнены только при совпадении типов параметров. В модели используются те же шесть элементарных операций, что и в модели Харрисона–Руззо–Ульмана. Отличие состоит только в использовании типизованных параметров в операциях создания субъектов и объектов:

enter r into M[s,o];
delete r from M[s,o];
create subject s of type t;
create object o of type t;
destroy subject s;
destroy object o.

Таким образом, ТАМ является обобщением модели Харрисона–Руззо–Ульмала, которую можно рассматривать как частный случай ТАМ с одним единственным типом, к которому относятся все объекты и субъекты. Появление в каждой команде дополнительных неявных условий, ограничивающих область применения команды только сущностями соответствующих типов, позволяет несколько смягчить жесткие условия классической модели, при которых критерий безопасности является разрешимым.

Авторы модели показали, что критерий безопасности дискреционной модели может быть доказан для систем, в которых все команды $\alpha_i(x_i, \ldots x_k)$ являются одноусловными и монотонными. Строгий контроль соответствия типов позволяет смягчить требование одноусловности, заменив его ограничением на типы параметров команд, при выполнении которых происходит создание ловых сущностей и доказать критерий безопасности систем для более приемлемых ограничений, что существенно расширило область ее применения.

Лекция 9. Классическая мандатная модель политики безопасности Белла–Лападулы, особенности и области применения. Критерий безопасности

Мандатная модель Белла–Лападулы

Мандатная модель управления доступом основана на правилах секретного документооборота, принятых в государственных и правительственных учреждениях многих стран. Основным положением политики Белла–Лападулы, взятым ими из реальной жизни, является назначение всем участникам процесса обработки защищаемой информации, и документам, в которых она содержится, специальной

метки, например, «секретно», «сов. секретно» и т.д., получившей название уровня безопасности. Все уровни безопасности упорядочиваются с помощью установленного отношения доминирования, например, уровень «сов секретно» считается более высоким чем уровень «секретно», или доминирует над ним. Контроль доступа осуществляется в зависимости от уровней безопасности взаимодействующих сторон на основании двух простых правил:

1. Уполномоченное лицо (субъект) имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности.

2. Уполномоченное лицо (субъект) имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного уровня безопасности.

Первое правило обеспечивает защиту информации, обрабатываемой более доверенными (высокоуровневыми) лицами, от доступа со стороны менее доверенных (низкоуровневых). Второе правило предотвращает утечку информации (сознательную или несознательную) со стороны высокоуровневых участников процесса обработки информации к низкоуровневым.

Таким образом, если в дискреционных моделях управление доступом происходит путем наделения пользователей полномочиями осуществлять определенные операции над определенными объектами, то мандатные модели управляют доступом неявным образом — с помощью назначения всем сущностям системы уровней безопасности, которые определяют все допустимые взаимодействия между ними. Следовательно, мандатное управление доступом не различает сущностей, которым присвоен одинаковый уровень безопасности, и на их взаимодействия ограничения отсутствуют. Поэтому, в тех ситуациях, когда управление доступом требует более гибкого подхода, мандатная

модель применяется совместно с какой–либо дискреционной, которая используется для контроля за взаимодействиями между сущностями одного уровня и для установки дополнительных ограничений, усиливающих мандатную модель.

Система в модели безопасности Белла–Лападулы, как и в модели Харрисона–Руззо–Ульмана, представляется в виде множеств субъектов S, объектов O (множество объектов включает множество субъектов, $S \subset O$), и прав доступа read (чтение) и write (запись). В мандатной модели рассматриваются только эти два вида доступа, и, хотя она может быть расширена введением дополнительных прав (например, правом на добавление информации, выполнение программ и т.д.), все они будут отображаться в базовые (чтение и запись). Использование столь жесткого подхода, не позволяющего осуществлять гибкое управление доступом, объясняется тем, что в мандатной модели контролируются не операции, осуществляемые субъектом над объектом, а потоки информации, которые могут быть только двух видов: либо от субъекта к объекту (запись), либо от объекта к субъекту (чтение).

Уровни безопасности субъектов и объектов задаются с помощью функции уровня безопасности $F: S \cup O \rightarrow L$, которая ставит в соответствие каждому объекту и субъекту уровень безопасности, принадлежащий множеству уровней безопасности L.

Классическая мандатная модель Белла–Лападулы

В мандатных моделях функция уровня безопасности F вместе с решеткой уровней определяют все допустимые отношения доступа между сущностями системы, поэтому множество состояний системы V представляется в виде набора упорядоченных пар (F, M), где M – это матрица доступа, отражающая текущую ситуацию с правами доступа субъектов к объектам, содержание которой аналогично матрице прав

доступа в модели Харрисона–Руззо–Ульмана, но набор прав ограничен правами read и write. Модель системы $\sum(v_0,R,T)$ состоит из начального состояния V_0, множества запросов R и функции перехода $T:(VxR)\rightarrow V$, которая в ходе выполнения запроса переводит систему из одного состояния в другое. Система, находящаяся в состоянии $v\in V$, при получении запроса $r\in R$, переходит в следующее состояние $v^* = T(v,r)$. Состояние v достижимо в системе $\sum(v_0,R,T)$ тогда и только тогда, когда существует последовательность $<(r_0,v_0),...,(r_{n-1},v_{n-1}),(r_n,v)>$ такая, что $T(r_i, v_i) = v_{i+1}$ для $0<=i<n$. Заметим, что для любой системы v_0 тривиально достижимо.

Как и для дискреционной модели состояния системы делятся на безопасные, в которых отношения доступа не противоречат установленным в модели правилам, и небезопасные, в которых эти правила нарушаются, и происходит утечка информации.

Белл и Лападула предложили следующее определение безопасного состояния:

1. Состояние (F,M) называется безопасным по чтению (или просто безопасным) тогда и только, когда для каждого субъекта, осуществляющего в этом состоянии доступ чтения к объекту, уровень безопасности этого субъекта доминирует над уровнем безопасности этого объекта: $\forall s \in S, \forall o \in O, read \in M[s,o] \rightarrow F(s) \geq F(o)$.

2. Состояние (F,M) называется безопасным по записи (или *–безопасным), тогда и только, когда для каждого субъекта, осуществляющего в этом состоянии доступ записи к объекту, уровень безопасности этого объекта доминирует над уровнем безопасности этого субъекта: $\forall s \in S, \forall o \in O, write \in M[s,o] \rightarrow F(o) \geq F(s)$.

3. Состояние безопасно тогда и только тогда, когда оно безопасно и по чтению, и по записи.

В соответствии с предложенным определением безопасного состояния критерий безопасности системы выглядит следующим образом:

Система $\sum(v_0,R,T)$ безопасна тогда и только тогда, когда ее начальное состояние v_0 безопасно и все состояния, достижимые из v_0 путем применения конечной последовательности запросов из R безопасны.

Авторы модели доказали теорему, формально доказывающую безопасность системы при соблюдении определенных условий, получившую название основной теоремы безопасности. Система $\sum(v_0,R,T)$ безопасна тогда и только тогда, когда:

- начальное состояние v_0 безопасно и для любого состояния v , достижимого из v_0 путем применения конечной последовательности запросов из R, таких, что T(v,r)= v* , v= (F,M) и v*=(F*,M*) для каждого $s \in S$, и $o \in O$ выполняются следующие условия:

1) если $read \in M^*[s,o]$ и $read \notin M[s,o]$, то $F^*(s) \geq F^*(o)$;

2) если $read \in M[s,o]$ и $F^*(s) < F^*(o)$, то $read \notin M^*[s,o]$;

3) если $write \in M^*[s,o]$ и $write \notin M[s,o]$, то $F^*(o) \geq F^*(s)$;

4) если $write \in M[s,o]$ и $F^*(o) < F^*(s)$, то $write \notin M^*[s,o]$.

Доказательство:

1. Необходимость. Если система безопасна, то состояние v_0 безопасно по определению. Допустим, существует некоторое состояние v*, достижимое из v_0 путем применения конечного числа запросов из R и полученное путем перехода из безопасного состояния v: T(v,r)= v*. Тогда, если при этом переходе нарушено хотя бы одно из первых двух ограничений, накладываемых теоремой на функцию T, то состояние v* не будет безопасным по чтению, а если функция T нарушает хотя бы одно

из последних двух условий теоремы, то состояние v* не будет безопасным по записи. В любом случае при нарушении условий теоремы система небезопасна.

2. Достаточность. Проведем доказательство от противного. Предположим, что система небезопасна. В этом случае, либо v_0 небезопасно, что явно противоречит условиям теоремы, либо должно существовать небезопасное состояние v*, достижимое из безопасного v_0 путем применения конечного числа запросов из R. В этом случае обязательно будет иметь место переход T(v,r)= v*, при котором состояние v безопасно, а состояние v* нет, однако , четыре условия теоремы делают такой переход невозможным.

Таким образом, теорема утверждает, что система с безопасным начальным состоянием является безопасной тогда и только тогда, когда при любом переходе системы из одного состояния в другое не возникает никаких новых и не сохраняется никаких старых отношений доступа, которые будут небезопасны по отношению к функции уровня безопасности нового состояния. Формально эта теорема определяет все необходимые и достаточные условия, которые должны быть выполнены для того, чтобы система, начав свою работу в безопасном состоянии, никогда не достигла небезопасного состояния.

Применение мандатных моделей

В завершении темы мандатных моделей необходимо отметить трудности, которые связаны с их применением на практике. Все мандатные модели, как и модель Белла–Лападулы, используют только два права доступа – чтение и запись. На практике информационные системы поддерживают значительно более широкий спектр операций над информацией, например, создание, удаление, передача и т.д. Следовательно, для того чтобы применить мандатную модель к реальной

системе, необходимо установить подходящее соответствие между чтением и записью и операциями, реализованными в конкретной системе. Идеальным соответствием считается такое, при котором объект не может воздействовать на поведение субъекта до тех пор, пока субъект не осуществит к нему доступ чтения, и когда субъект не может воздействовать на объект, пока не осуществит к нему доступ *записи.* Определение такого соответствия представляет собой нетривиальную задачу, поскольку в реальной жизни невозможно ограничиться однонаправленными потоками информации, идущими строго от субъекта к объекту, или наоборот. Ведь для того, чтобы, например, осуществить операцию чтения *с*убъект должен сначала послать запрос службе, реализующей доступ к интересующему его объекту, т.е. осуществить передачу информации, или операцию записи. Если рассматривать функционирование системы с такой точки зрения, то применение мандатной политики становится невозможным, потому что попытки распространить мандатную модель на низкоуровневые механизмы, реализующие контролируемые взаимодействия, автоматически приводят к нарушению этой политики. Самым простым примером непрактичности мандатной модели является невозможность ее применения для сетевых взаимодействий – нельзя построить распределенную систему, в которой информация передавалась бы только в одном направлении, потому что всегда будет существовать обратный поток информации, содержащий ответы на запросы, подтверждения получения и т.д.

Таким образом, хотя мандатная модель управления доступом является базовой моделью безопасности, ее применение на практике связано с серьезными трудностями. Она используется только в системах, обрабатывающих классифицированную информацию, и применяется только в отношении ограниченного подмножества субъектов и объектов.

Лекция 10. Ролевая модель управления доступом. Формальные модели ролевой политики безопасности. Критерий безопасности

Ролевая политика безопасности

Ролевая политика безопасности представляет собой существенно усовершенствованную модель Харрисона–Руззо–Ульмана, однако ее нельзя отнести ни к дискреционным, ни к мандатным, потому что управление доступом в ней осуществляется как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям и их активацию во время сеансов. Поэтому ролевая модель представляет собой совершенно особый тип политики, основанной на компромиссе между гибкостью управления доступом, характерной для дискреционных моделей, и жесткостью правил контроля доступа, присущей мандатным моделям.

В ролевой модели классическое понятие субъект замещается понятиями пользователь и роль.

Пользователь – это человек, работающий с системой и выполняющий определенные служебные обязанности.

Роль – это активно действующая в системе абстрактная сущность, с которой связан ограниченный, логически связанный набор полномочий, необходимых для осуществления определенной деятельности. Самым распространенным примером роли является присутствующий почти в каждой системе административный бюджет (например, root для UNIX и Administrator для Windows NT), который обладает специальными полномочиями и может использоваться несколькими пользователями.

При использовании ролевой политики управление доступом осуществляется в две стадии: во–первых, для каждой роли указывается набор полномочий, представляющий набор прав доступа к объектам, и,

во–вторых, каждому пользователю назначается список доступных ему ролей. Полномочия назначаются ролям в соответствии с принципом наименьших привилегий, из которого следует, что каждый пользователь должен обладать только минимально необходимым для выполнения своей работы набором полномочий.

Ролевая модель описывает систему в виде следующих множеств:

U – множество пользователей;

R – множество ролей;

P – множество полномочий на доступ к объектам, представленное, например, в виде матрицы прав доступа;

S – множество сеансов работы пользователей с системой.

Для перечисленных множеств определяются следующие отношения (рис. 6):

PA $\subseteq$ PxR – отображает множество полномочий на множество ролей, устанавливая для каждой роли набор присвоенных ей полномочий;
UA $\subseteq$ UxR – отображает множество пользователей множество ролей, определяя для каждого пользователя набор доступных ему ролей.

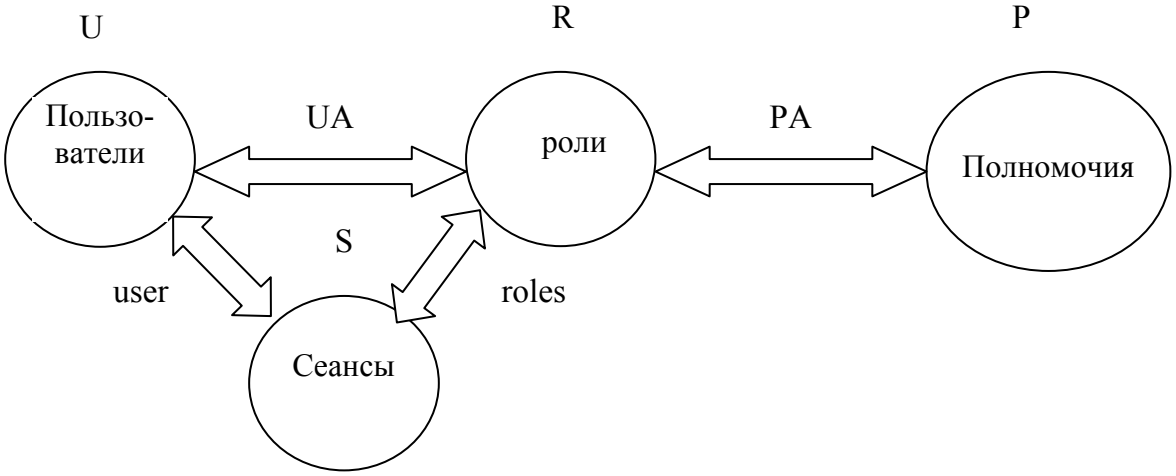

Рис. 6. Ролевая модель управления доступом.

Правила управления доступом ролевой политики безопасности определяются следующими функциями:

user: $S \rightarrow U$ – для каждого сеанса s эта функция определяет пользователя, который осуществляет этот сеанс работы с системой: user(s) = u;

roles: $S \rightarrow P(R)$ – для каждого сеанса s эта функция определяет набор ролей из множества R, которые могут быть одновременно доступны пользователю в этом сеансе: $roles(s) = \{ r_i | (user(s), r_i) \in UA\}$;

permissions: $S \rightarrow P$ – для каждого сеанса s эта функция задает набор доступных в нем полномочий, который определяется как совокупность полномочий всех ролей, задействованных в этом сеансе: $permissions(S) = U_{r \in roles}\{p_i \mid (p_i,r) \in PA\}$.

В качестве критерия безопасности ролевой модели используется следующее правило: система считается безопасной, если любой пользователь системы, работающий в сеансе s, может осуществлять действия, требующие полномочия p только в том случае, если $p \in$ permissions(s).

Из формулировки критерия безопасности ролевой модели следует, что управление доступом осуществляется главным образом не с помощью назначения полномочий ролям, а путем задания отношения UA, назначающего роли пользователям, и функции roles, определяющей доступный в сеансе набор ролей. Поэтому многочисленные интерпретации ролевой модели различаются видом функций user, roles и permission, а также ограничениями, накладываемыми на отношения PA и UA. В качестве примеров рассмотрим ролевую политику управления доступом с иерархической организацией ролей, а также несколько наиболее часто встречающихся типовых ограничений на отношения PA и UA и функции user и roles.

Иерархическая ролевая модель

Иерархическая организация ролей представляет собой наиболее распространенный тип ролевой модели, поскольку она очень точно отражает установившееся в реальном мире отношение подчиненности между участниками процессов обработки информации и разделение между ними сфер ответственности. Роли в иерархии упорядочиваются по уровню предоставляемых полномочий. Чем выше роль находится в иерархии, тем больше с ней связано полномочий, поскольку считается, что если пользователю присвоена некоторая роль, то ему автоматически назначаются и все подчиненные ей по иерархии роли. Иерархия ролей допускает множественное наследование. Иерархическая ролевая модель отличается от классической следующими отношениями:

$RH \subseteq RxR$ – частичное отношение порядка на множестве R, которое определяет иерархию ролей и задает на множестве ролей оператор доминирования >=, такой что, если $r_1 >= r_2$, то r_1 находится в иерархии выше чем r_2;

$UA^h \subseteq UxR$ – назначает каждому пользователю набор ролей, причем вместе с каждой ролью в него включаются и все роли, подчиненные ей по иерархии, т. е. для $\forall r, r' \in R, u \in U: r \geq r' \wedge (u, r) \in UA^h \Rightarrow (u,r') \in UA^h$.

$Roles^h : S \rightarrow P(R)$ – назначает каждому сеансу s набор ролей из иерархии ролей пользователя, работающего в этом сеансе: $roles^h(s) \in \{r_i \mid (\exists r' \geq r_i (user(s),r') \in UA^h)\}$;

$permissions^h: S \rightarrow P$ – определяет полномочия сеанса как совокупность полномочий всех задействованных в нем ролей и полномочий всех ролей, подчиненных им: $permissions^h(S)=U_{r \in roles^{h(s)}} \{p_i \mid (\exists r'' < r (p_i,r'') \in PA)\}$.

Таким образом, каждому пользователю назначается некоторое подмножество иерархии ролей, а в каждом сеансе доступна совокупность полномочий ролей, составляющих фрагмент этой иерархии.

Такой подход позволяет существенно упростить управление доступом за счет неявного назначения полномочий, поскольку пользователи, как правило, жестко упорядочены по степени ответственности, соответствующей уровню полномочий, которыми они обладают.

Завершая анализ свойств ролевой политики управления доступом следует констатировать, что в отличие от других политик она практически не гарантирует безопасность с помощью формального доказательства, а только определяет характер ограничений, соблюдение которых и служит критерием безопасности системы.

Такой подход позволяет получать простые и понятные правила контроля доступа, которые легко могут быть применены на практике, но лишает систему теоретической доказательной базы.

Архитектура криптоадаптера

В некоторых ситуациях это обстоятельство затрудняет использование ролевой политики, однако, в любом случае, оперировать ролями гораздо удобнее, чем субъектами, поскольку это более соответствует распространенным технологиям обработки информации, предусматривающим разделение обязанностей и сфер ответственности между пользователями.

Кроме того, ролевая политика может использоваться одновременно с другими политиками безопасности, когда полномочия ролей, назначаемых пользователям, контролируются дискреционной или мандатной политикой, что позволяет строить многоуровневые схемы контроля доступа.

Р а з д е л 3. Критерии и спецификации безопасности автоматизированных систем и информационных технологий

Лекция 11. Стандарты и спецификации информационной безопасности автоматизированных систем

Роль стандартов информационной безопасности

Главная задача стандартов информационной безопасности — создать основу для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий. Каждая из этих групп имеет свои интересы и свои взгляды на проблему информационной безопасности.

Потребители, во–первых, заинтересованы в методике, позволяющей обоснованно выбрать продукт, отвечающий их нуждам и решающий их проблемы (для чего им необходима шкала оценки безопасности), и, во–вторых, нуждаются в инструменте, с помощью которого они могли бы формулировать свои требования производителям. При этом потребителей (что вполне естественно) интересуют исключительно характеристики и свойства конечного продукта, а не методы и средства их достижения.

Многие потребители не понимают, что требования безопасности обязательно противоречат функциональным требованиям (удобству работы, быстродействию и т.п.), накладывают ограничения на совместимость и, как правило, вынуждают отказаться от очень широко распространенных незащищенных прикладных программных средств.

Производители, в свою очередь, нуждаются в стандартах для сравнения возможностей своих продуктов и в применении процедуры сертификации для объективной оценки их свойств, а также в

стандартизации определенного набора требований безопасности, который мог бы ограничить фантазию заказчика конкретного продукта и заставить его выбирать требования из этого набора. С точки зрения производителя, требования должны быть максимально конкретными и регламентировать необходимость применения тех или иных средств, механизмов, алгоритмов и т.д. Кроме того, требования не должны вступать в конфликт с существующими парадигмами обработки информации, архитектурой вычислительных систем и технологиями создания информационных продуктов. Этот подход также не может быть признан в качестве доминирующего, так как он не учитывает нужд пользователей (удовлетворение которых — главная задача разработчика) и пытается подогнать требования защиты под существующие системы и технологии, а это далеко не всегда возможно осуществить без ущерба для безопасности.

Таким образом, перед стандартами информационной безопасности стоит непростая задача — примирить три точки зрения (экспертов, потребителей и производителей) и создать эффективный механизм взаимодействия всех сторон.

Наиболее значимыми стандартами информационной безопасности являются (в хронологическом порядке): «Критерии безопасности компьютерных систем министерства обороны США», Руководящие документы Гостехкомиссии России (только для нашей страны), «Европейские критерии безопасности информационных технологий», «Федеральные критерии безопасности информационных технологий США», «Канадские критерии безопасности компьютерных систем» и «Единые критерии безопасности информационных технологий».

Руководящие документы Гостехкомиссии России

В 1992 г. Гостехкомиссия (ГТК) при Президенте Российской Федерации опубликовала серию Руководящих документов, посвященных вопросам защиты от несанкционированного доступа к информации. Рассмотрим важнейшие их них:

- «Концепция защиты средств вычислительной техники от несанкционированного доступа к информации»;
- «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;
- «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Идейной основой этих документов является «Концепция защиты средств вычислительной техники от несанкционированного доступа к информации (НСД)», содержащая систему взглядов ГТК на проблему информационной безопасности и основные принципы защиты компьютерных систем.

С точки зрения разработчиков данных документов основная и едва ли не единственная задача средств безопасности – это обеспечение защиты от несанкционированного доступа (НСД) к информации.

Если средствам контроля и обеспечения целостности уделяется некоторое внимание, то поддержка работоспособности систем обработки информации (как мера защиты от угроз работоспособности) вообще не упоминается.

Определенный уклон в сторону поддержания секретности объясняется тем, что эти документы были разработаны в расчете на применение в информационных системах министерства обороны и

спецслужб РФ, а также недостаточно высоким уровнем информационных технологий этих систем по сравнению с современным.

Таксономия критериев и требований безопасности

Руководящие документы ГТК предлагают две группы критериев безопасности: показатели защищенности средств вычислительной техники (СВТ) от НСД и критерии защищенности автоматизированных систем (АС) обработки данных. Первая группа позволяет оценить степень защищенности (правда только относительно угроз одного типа — НСД) отдельно поставляемых потребителю компонентов ВС, а вторая - рассчитана на полнофункциональные системы обработки данных.

Показатели защищенности СВТ от НСД

Данный руководящий документ устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Под СВТ понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Данные показатели содержат требования защищенности СВТ от НСД к информации и применяются к общесистемным программным средствам и операционным системам (с учетом архитектуры ЭВМ). Конкретные перечни показателей определяют классы защищенности СВТ и описываются совокупностью требований. Совокупность всех средств защиты составляет комплекс средств защиты (КСЗ).

Установлено семь классов защищенности СВТ от НСД к информации. Самые низкие требования предъявляются к системам, соответствующим седьмому классу самые высокие — к первому. Показатели защищенности и установленные требования к классам приведены в таблице 5.

Таблица 5. Распределение показателей защищенности по классам СВТ.

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	–	–	+	=	=	=
Очистка памяти	–	+	+	+	=	=
Изоляция модулей	–	–	+	=	+	=
Маркировка документов	–	–	+	=	=	=
Защита ввода и вывода на отчужденный физический носитель информации	–	–	+	=	=	=
Сопоставление пользователя с устройством	–	–	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	–	+	+	+	+	+
Регистрация	–	+	+	+	=	=
Взаимодействие пользователя с КСЗ	–	–	–	+	=	=
Надежное восстановление	–	–	–	+	=	=
Целостность КСЗ	–	+	+	+	=	
Контроль модификации	–	–	. –	–	+	=
Контроль дистрибуции	–	–	–	–	+	=
Гарантии архитектуры	–	–	–	–	–	+
Тестирование	+	+	+	+	+	=
Руководство пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Текстовая документация	+	+	+	+	+	=
Конструкторская(проектная)документация	+	+	+	+	+	+

Обозначения:

«–» – нет требований к данному классу;

«+» – новые или дополнительные требования;

«=» – требовании совпадают с требованиями предыдущего класса;

«КСЗ» – комплекс средств защиты.

Требования к защищенности автоматизированных систем

Данные требования являются составной частью критериев защищенности автоматизированных систем обработки информации от НСД. Требования сгруппированы вокруг реализующих их подсистем защиты.

В отличие от остальных стандартов, отсутствует раздел, содержащий требования по обеспечению работоспособности системы, зато присутствует раздел, посвященный криптографическим средствам (другие стандарты не содержат упоминания о криптографии, так как рассматривают ее исключительно в качестве механизма, реализующего остальные требования, такие, как аутентификацию, контроль целостности и т.д.).

Таксономия требований к средствам защиты АС от НСД приведена на рис 7

Рис. 7. Таксономия требований к средствам защиты АС от НСД

Классы защищенности автоматизированных систем

Документы ГТК устанавливают девять классов защищенности АС от НСД, каждый из которых характеризуется определенной совокупностью требований к средствам защиты. Классы подразделяются на три группы, отличающиеся спецификой обработки информации в АС. Группа АС определяется на основании следующих признаков:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий пользователей АС на доступ к конфиденциальной информации;
- режим обработки данных в АС (коллективный или индивидуальный).

В пределах каждой группы соблюдается иерархия классов защищенности АС. Класс, соответствующий высшей степени защищенности для данной группы, обозначается индексом NA, где N – номер группы (от 1 до 3). Следующий класс обозначается NБ и т.д.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса: 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые полномочия доступа ко всей информации, обрабатываемой и/или хранимой в АС на носителях различного уровня конфиденциальности. Группа содержит два класса : 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности. Не все пользователи имеют равные права доступа. Группа содержит пять классов : 1Д, 1Г, 1В, 1Б и 1А.

В таблице 6 приведены требования к подсистемам защиты для каждого класса.

Таблица 6. Требования к классам защищенности АС

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1.Подсистема управления доступом 1.1.Идентификация.Проверка подлинности и контроль доступа субъектов: в систему;	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;				+		+	+	+	+
к программам;				+		+	+	+	+
к томам, каталогам, файлам, записям, полям записей				+		+	+	+	+
1.2. Управление потоками информации				+			+	+	+
2. Подсистема регистрации и учета				+	+	+	+	+	+
2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети);	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов;		+		+		+	+	+	+
запуска/завершения программ и процессов (заданий, задач);				+		+	+	+	+
доступа программ субъектов, доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, каталогам, файлам, записям, полям записей;				+		+	+	+	+
изменения полномочий субъектов доступа;							+	+	+
создаваемых защищаемых объектов доступа.				+			+	+	+
2.2 .Учет носителей информации.	+	+	+	+	+	+	+	+	+

Продолжение табл. 6

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти и внешних накопителей.		+		+		+	+	+	+
2.4.Сигнализация попыток нарушения защиты.							+	+	+
3. Криптографическая подсистема 3.1.Шифрование конфиденциальной информации.				+				+	+
3.2 Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах.									+
3.3. Использование аттестованных (сертифицированных) криптографических средств.				+				+	+
4. Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации.	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации.	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС.							+	+	+
4.4. Периодическое тестирование СЗИ НСД.	+	+	+	+	+	+	+	+	+

Окончание табл. 6

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
4.5.Наличие средств восстановления СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.6.Использование сертифицированных средств защиты		+		+			+	+	+

Обозначения: «+» – требование к данному классу присутствует.

Разработка руководящих документов ГТК явилась следствием бурно развивающегося в России процесса внедрения информационных технологий. До начала 90–х годов необходимости в подобных документах не было, так как в большинстве случаев обработка и хранение конфиденциальной информации осуществлялись без применения вычислительной техники. Поэтому разработка стандартов подобного рода представляет собой относительно новую область деятельности для соответствующих институтов и учреждений, что позволяет трактовать данные документы как первую стадию формирования отечественных стандартов в области информационной безопасности.

Лекция 12. Федеральные критерии безопасности информационных технологий. Понятия продукта информационных технологий, профиля защиты, проекта защиты

Цель разработки критериев

Создание «Федеральных критериев безопасности информационных технологий» преследовало следующие цели:

1. Определение универсального и открытого для дальнейшего развития набора основных требований безопасности, предъявляемых к современным информационным технологиям.
2. Совершенствование существующих требований и критериев безопасности, как в государственном, так и в частном секторе.
3. Приведение в соответствие между собой принятых в разных странах требований и критериев безопасности информационных технологий.

Основными объектами применения требований безопасности «Федеральных критериев» являются продукты информационных технологий (Information Technology Products) и системы обработки информации (Information Technology Systems).

Под продуктом информационных технологий (далее просто «ИТ–продукт») понимается совокупность аппаратных и/или программных средств, которая представляет собой поставляемое конечному потребителю готовое к использованию средство обработки информации. Как правило, ИТ–продукт эксплуатируется не автономно, а интегрируется в систему обработки информации, представляющую собой совокупность ИТ–продуктов, объединенных в функционально полный комплекс. С точки зрения безопасности принципиальное различие между ИТ–продуктом и системой обработки информации определяется средой их эксплуатации. Продукт информационных технологий обычно разрабатывается в расчете на то, что он будет использован во многих

системах обработки информации, и, следовательно, разработчик должен ориентироваться только на самые общие предположения о среде эксплуатации своего продукта, включающие условия применения и общие угрозы. Напротив, система обработки информации разрабатывается для решения прикладных задач в расчете на заданные требования конечных потребителей. Положения «Федеральных критериев» касаются только собственных средств обеспечения безопасности ИТ–продуктов, т.е. механизмов защиты, встроенных непосредственно в эти продукты в виде соответствующих программных и аппаратных средств.

Ключевым понятием концепции информационной безопасности «Федеральных критериев» является понятие «профиль защиты» (Protection Profile). Профиль защиты — это нормативный документ, который регламентирует все аспекты безопасности ИТ–продукта в виде требований к его проектированию, технологии разработки и квалификационному анализу. Основное внимание в профиле защиты уделяется требованиям к составу средств защиты и качеству их реализации, а также их адекватности предполагаемым угрозам безопасности. «Федеральные критерии» представляют процесс разработки систем обработки информации, начинающийся с формулирования требований потребителями и заканчивающийся введением в эксплуатацию в виде последовательности следующих основных этапов:

1. Разработка и анализ профиля защиты. Требования, изложенные в профиле защиты, определяют функциональные возможности ИТ–продуктов по обеспечению безопасности и условия эксплуатации, при соблюдении которых гарантируется соответствие предъявляемым требованиям. Кроме требований безопасности профиль содержит требования по соблюдению технологической дисциплины в процессе

разработки, тестирования и квалификационного анализа ИТ–продукта. Профиль безопасности анализируется на полноту, непротиворечивость и техническую корректность.

2. Разработка и квалификационный анализ ИТ–продуктов. Разработанные ИТ–продукты подвергаются независимому анализу, целью которого является определение степени соответствия характеристик продукта сформулированным в профиле защиты требованиям и спецификациям.
3. Компоновка и сертификация системы обработки информации в целом. Успешно прошедшие квалификацию уровня безопасности ИТ–продукты интегрируются в систему обработки информации. Полученная в результате система должна удовлетворять заявленным в профиле защиты требованиям при соблюдении указанных в нем условий эксплуатации.

«Федеральные критерии» регламентируют только первый этап этой схемы — разработку и анализ профиля защиты. Процесс создания ИТ–продуктов и компоновка систем обработки информации остаются вне рамок этого стандарта.

Профиль защиты

Профиль защиты предназначен для определения и обоснования состава и содержания средств защиты, спецификации технологии разработки и регламентации процесса квалификационного анализа ИТ–продукта. Профиль защиты состоит из следующих пяти разделов: описание, обоснование, функциональные требования к ИТ–продукту, требования к технологии разработки ИТ–продукта, требования к процессу квалификационного анализа ИТ–продукта.

Описание профиля содержит классификационную информацию, необходимую для его идентификации в специальной картотеке. «Федеральные критерии» предлагают поддерживать такую картотеку на

общегосударственном уровне. Это позволит любой организации воспользоваться созданными ранее профилями защиты непосредственно или использовать их в качестве прототипов для разработки новых.

В описании профиля защиты должна быть охарактеризована основная проблема или группа проблем обеспечения безопасности, решаемых с помощью применения данного профиля.

Обоснование содержит описание среды эксплуатации, предполагаемых угроз безопасности и методов использования ИТ–продукта. Кроме того, этот раздел содержит подробный перечень задач по обеспечению безопасности, решаемых с помощью данного профиля. Эта информация дает возможность определить, в какой мере данный профиль защиты пригоден для применения в той или иной ситуации.

Раздел «Функциональные требования к ИТ–продукту» содержит описание функциональных возможностей средств защиты ИТ–продукта и определяет условия, в которых обеспечивается безопасность в виде перечня угроз, которым успешно противостоят предложенные средства защиты.

Раздел «Требования к технологии разработки ИТ–продукта» охватывает все этапы его создания, начиная от разработки проекта и заканчивая вводом готовой системы в эксплуатацию.

Раздел содержит требования как к самому процессу разработки, так и к условиям, в которых она проводится, к используемым технологическим средствам, а также к документированию этого процесса.

Раздел «Требования к процессу квалификационного анализа ИТ–продукта» регламентирует порядок проведения квалификационного анализа в виде методики исследований и тестирования ИТ–продукта. Объем и глубина требуемых исследований зависят от наиболее вероятных типов угроз, среды применения и планируемой технологии эксплуатации.

Единые критерии безопасности информационных технологий

«Единые критерии» рассматривают безопасность как совокупность конфиденциальности, целостности и доступности ресурсов ВС и ставят перед средствами защиты задачи противодействия соответствующим типам угроз и реализации политики безопасности, а также позволяют учитывать угрозы, которые не могут быть отнесены ни к одному из перечисленных выше типов.

Задачи защиты — базовое понятие «Единых критериев», выражающее потребность носителей ИТ–продукта в противостоянии заданному множеству угроз безопасности или в необходимости реализации политики безопасности.

Профиль защиты — специальный нормативный документ, представляющий собой совокупность задач защиты, функциональных требований, требований адекватности и их обоснования. Служит руководством для разработчика ИТ–продукта при создании проекта защиты.

Проект защиты — специальный нормативный документ, представляющий собой совокупность задач защиты, функциональных требований, требований адекватности, общих спецификаций средств защиты и их обоснования. В ходе квалификационного анализа служит в качестве описания ИТ–продукта.

Согласно «Единым критериям» безопасность информационных технологий может быть достигнута посредством применения предложенной в них технологии разработки, сертификации и эксплуатации ИТ–продуктов.

Профиль защиты в единых критериях безопасности информационных технологий.

Рассмотрим назначение и содержание разделов профиля защиты.

Введение содержит всю информацию, необходимую для поиска профиля защиты в библиотеке профилей. Идентификатор профиля защиты представляет собой уникальное имя, пригодное для его поиска среди подобных ему профилей и обозначения ссылок на него.

Обзор содержания содержит краткую аннотацию профиля защиты, на основании которой потребитель может сделать вывод о пригодности данного профиля для его нужд.

Описание ИТ–продукта должно содержать его краткую характеристику, функциональное назначение, принципы работы, методы использования и т. д. Эта информация не подлежит анализу и сертификации, но предоставляется производителям и экспертам по квалификации для пояснения требований безопасности и определения их соответствия задачам, решаемым с помощью ИТ–продукта, а также для общего понимания его структуры и принципов работы.

Среда эксплуатации. Этот раздел содержит описание всех аспектов функционирования ИТ–продукта, связанных с безопасностью. Угрозы безопасности. Описание угроз безопасности, присущих среде эксплуатации ИТ–продукта, которым должна противостоять защита. Для каждой угрозы должен быть указан ее источник, а также метод воздействия и его объект.

Политика безопасности. Описание политики безопасности должно определять и, при необходимости, объяснять правила политики безопасности, которая должна быть реализована в ИТ–продукте.

Условия эксплуатации. Описание условий эксплуатации ИТ–продукта должно содержать исчерпывающую характеристику среды его эксплуатации с точки зрения безопасности.

Задачи защиты отражают потребности пользователей в противодействии указанным угрозам безопасности и/или в реализации политики безопасности.

Требования безопасности. В этом разделе профиля защиты содержатся требования безопасности, которым должен удовлетворять ИТ–продукт для решения задач защиты.

Раздел функциональных требований должен содержать только типовые требования, предусмотренные соответствующими разделами «Единых критериев».

Раздел требований адекватности также состоит из типовых требований соответствующих разделов «Единых критериев».

Раздел требований к среде к эксплуатации является необязательным .

Дополнительные сведения – раздел, содержащий любую дополнительную информацию, которая может быть полезна для проектирования, разработки, квалификационного анализа и сертификации.

Обоснование должно демонстрировать, что профиль защиты содержит полное и связное множество требований и что удовлетворяющий им ИТ–продукт будет эффективно противостоять угрозам безопасности среды эксплуатации.

Обоснование задач защиты должно демонстрировать, что задачи защиты, предложенные в профиле, соответствуют свойствам среды эксплуатации безопасности.

Обоснование требований безопасности показывает, что требования безопасности позволяют решить задачи защиты, так как совокупность целей, преследуемых отдельными функциональными требованиями, соответствует установленным задачам защиты. Профиль защиты служит отправной точкой для производителя ИТ–продукта, который должен на основании этого материала и предложенных им технических решений

разработать проект защиты. Структура профиля защиты представлена на рис.8.

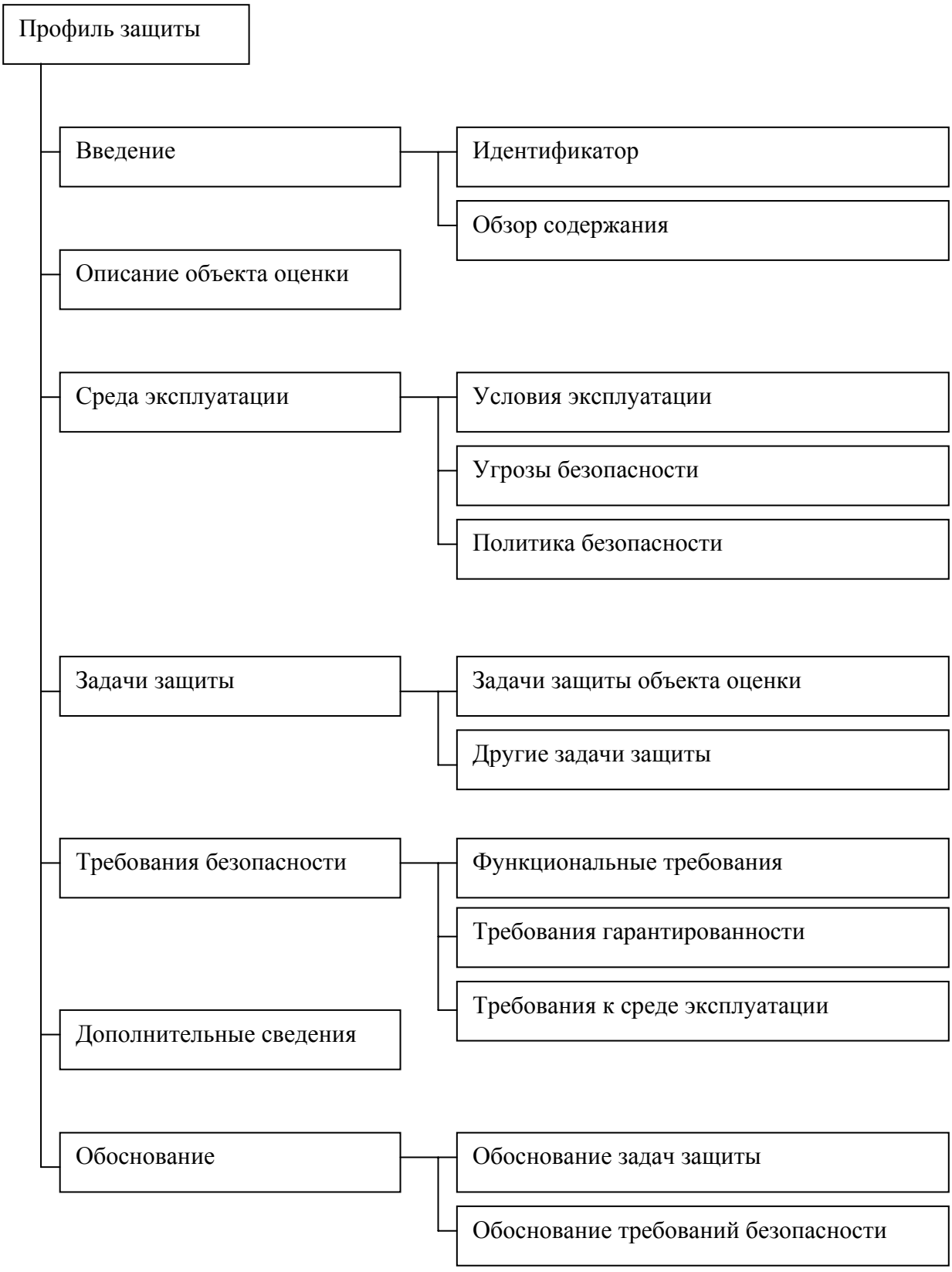

Рис. 8. Структура профиля защиты «Единых критериев»

Проект защиты

Проект защиты содержит требования и задачи защиты ИТ–продукта, а также описывает уровень функциональных возможностей реализованных в нем средств защиты, их обоснование и подтверждение степени их адекватности. Многие разделы проекта защиты совпадают с одноименными разделами профиля защиты, поэтому рассмотрим только те разделы, которые специфичны для проекта защиты, а также те, которые претерпели изменения.

. Введение содержит информацию, необходимую для идентификации проекта защиты, определения назначения, а также обзор его содержания.

Идентификатор представляет собой уникальное имя проекта защиты, необходимое для поиска и идентификации проекта защиты и соответствующею ему ИТ–продукта.

Обзор содержания представляет собой достаточно подробную аннотацию проекта защиты, позволяющую потенциальным потребителям определить пригодность ИТ–продукта для решения их задач.

Заявка на соответствие «Единым критериям» содержит описание всех свойств ИТ–продукта, подлежащих квалификационному анализу на основе «Единых критериев».

Раздел требований безопасности проекта защиты содержит требования безопасности к ИТ–продукту, которыми руководствовался производитель в ходе его разработки, что позволяет ему заявлять об успешном решении поставленных задач защиты. Этот раздел несколько отличается от аналогичного раздела профиля защиты.

Раздел функциональных требований к ИТ–продукту в отличие от соответствующего раздела профиля защиты допускает использование кроме типовых требований «Единых критериев» других, специфичных для данного продукта и среды его эксплуатации. Структура проекта защиты представлена на рис.9.

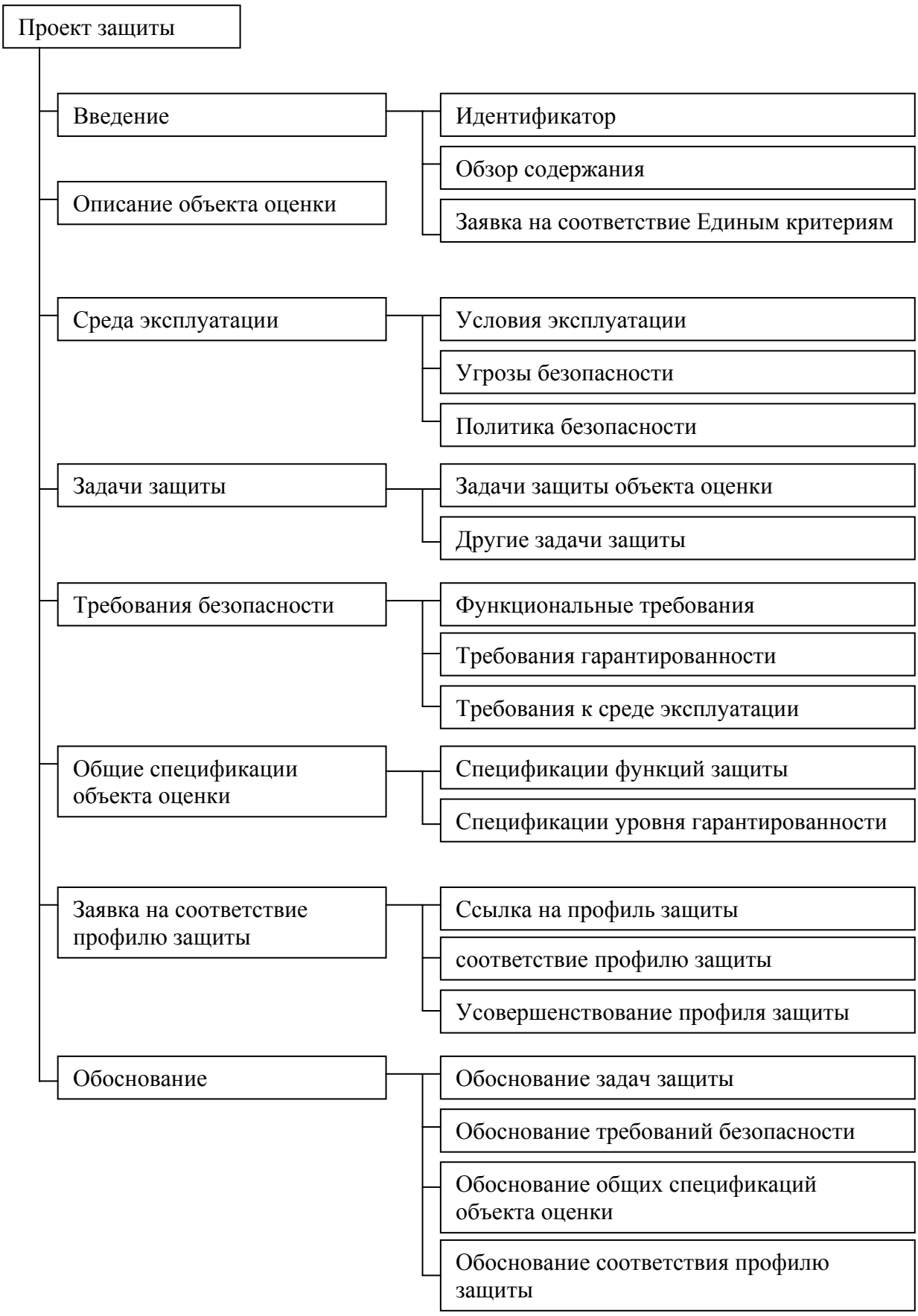

Рис. 9. Структура проекта защиты

Раздел требований адекватности по сравнению с соответствующим разделом профиля защиты может включать уровни адекватности, не предусмотренные в «Единых критериях». В этом случае описание уровня адекватности должно быть четким, непротиворечивым и обладать степенью подробности, допускающей его использование в ходе квалификационного анализа. При этом желательно использовать стиль и подробность описания уровней адекватности, принятые в «Единых критериях».

Общие спецификации ИТ–продукта отражают реализацию ИТ–продуктом требований безопасности с помощью определения высокоуровневых спецификаций функций защиты, реализующих функциональные требования и требования адекватности.

Спецификации функций защиты описывают функциональные возможности средств защиты ИТ–продукта, заявленные его производителем как реализующие требования безопасности. Форма представления спецификаций должна позволять определять соответствия между функциями защиты и требованиями безопасности.

Спецификации уровня адекватности определяют заявленный уровень адекватности защиты ИТ–продукта и его соответствие требованиям адекватности в виде представления параметров технологии проектирования и создания ИТ–продукта. Эти параметры должны быть представлены в форме, позволяющей определить их соответствие требованиям адекватности.

Заявка на соответствие профилю защиты. Проект защиты претендует на удовлетворение требований одного или нескольких профилей защиты. Этот необязательный раздел содержит материалы, необходимые для подтверждения заявки. Для каждого профиля защиты, на реализацию которого претендует проект защиты, этот раздел должен содержать следующую информацию.

Ссылка на профиль защиты однозначно идентифицирует профиль защиты, на реализацию которого претендует проект безопасности, с

указанием случаев, в которых обеспечиваемый уровень защиты превосходит требования профиля.

Соответствие профилю защиты определяет возможности ИТ–продукта, которые реализуют задачи защиты и требования, содержащиеся в профиле защиты.

Усовершенствование профиля защиты отражает возможности ИТ–продукта, которые выходят за рамки задач защиты и требований, установленных в профиле защиты.

Обоснование должно демонстрировать, что проект защиты содержит полное и связное множество требований, что реализующий его ИТ–продукт будет эффективно противостоять угрозам безопасности среды эксплуатации и что общие спецификации функций защиты соответствуют требованиям безопасности. Обоснование проекта защиты включает следующие разделы:

– обоснование задач защиты;

– обоснование требований безопасности;

– обоснование функций защиты;

– обоснование уровня адекватности.

Обоснование соответствия профилю защиты показывает, что требования проекта защиты поддерживают все требования профиля защиты. Как видно из приведенных структуры и обзора содержания профиля защиты и проекта защиты, эти документы наиболее полно регламентируют взаимодействие потребителей, производителей и экспертов по квалификации в процессе создания ИТ–продукта.

Фактически положения этих документов определяют технологию разработки защищенных систем. Они определяют перспективу создания единого информационного пространства, в котором сертификация безопасности систем обработки информации будет осуществляться на глобальном уровне, что предоставит возможности для интеграции национальных информационных систем, что в свою очередь откроет совершенно новые сферы применения информационных технологий.

Раздел 4. Организационно-режимные меры и программно-аппаратные средства обеспечения конфиденциальности, целостности и доступа к информации

Лекция 13. Методы и средства обеспечения информационной безопасности от угрозы нарушения конфиденциальности информации

Задачи обеспечения информационной безопасности

Основными задачами обеспечения информационной безопасности АС от угрозы раскрытия конфиденциальности на уровне машинных носителей информации (МНИ) являются:

- исключение прохождения носителей по технологическим участкам, не обусловленным производственной необходимостью;
- предупреждение непосредственного доступа к носителям персонала, не отвечающего за операции с носителям (минимизация доступа), предупреждение утраты или хищения носителей информации.

Первая задача решается за счет рациональной организации производственного процесса движения носителей информации, обеспечивающего целенаправленное распределение носителей по технологическим участкам, вторая – за счет четкой и обоснованной регламентации порядка обращения с носителями.

Регламентация порядка обращения с носителями предусматривает выполнение комплекса мер:

- запись информации (создание носителей с информацией) на рабочих местах, обеспечивающих условия для предотвращения утечки по техническим каналам и физической сохранности носителей;

- постановку на учет МНИ с простановкой соответствующей маркировки на зарегистрированном носителе. Одним из элементов маркировки должен быть гриф секретности информации, хранящейся на данном носителе;
- передачу МНИ между подразделениями организации, эксплуатирующей АС, под расписку;
- вынос МНИ за пределы организации только с разрешения уполномоченных лиц;
- хранение МНИ в условиях, исключающих несанкционированный доступ посторонних. Для хранения рекомендуется использовать надежно запираемые и опечатываемые шкафы. Надлежащие условия хранения должны быть обеспечены для всех учтенных носителей, независимо от того, находятся ли они в эксплуатации или нет;
- уничтожение МНИ, которые утратили свои эксплуатационные характеристики или не используются из–за перехода на новый тип носителя, специально организованными комиссиями согласно актам, утверждаемым уполномоченными лицами;
- периодический контроль контролирующими подразделениями соблюдения установленных правил обращения с носителями и их физической сохранности.

В соответствии с данными условиями можно установить требования, выдвигаемые к обслуживающему персоналу АС. Лицам, эксплуатирующим и обслуживающим АС, запрещается:

- использовать для работы с конфиденциальной информацией незарегистрированные МНИ;
- хранить на МНИ информацию с более высокой степенью секретности, чем определено для него в момент регистрации;

- работать с неучтенными экземплярами конфиденциальных документов, полученных в ходе обращений в АС, и передавать их другим сотрудникам;
- выносить из помещений, где установлены средства вычислительной техники (СВТ) АС, без разрешения ответственных за режим в этих помещениях: МНИ, содержащие конфиденциальные данные, подготовленные в АС документы, а также другую документацию, отдельные блоки, аппаратуру и иное оборудование;
- вносить в помещения, где расположены СВТ АС, постороннее имущество и материалы, в том числе кинофотоаппаратуру и радиоаппаратуру;
- делать на этикетках МНИ или на их упаковках пометки и надписи, раскрывающие содержание этих носителей;
- уничтожать МНИ и документы без санкции соответствующего должностного лица и оформления в установленном порядке.

Парольные системы для защиты от несанкционированного доступа к информации.

Под несанкционированным доступом к информации (НСД), согласно руководящим документам Гостехкомиссии, будем понимать доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств, предоставляемых СВТ или АС. НСД может носить случайный или преднамеренный характер.

Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:

- организационные;
- технологические;
- правовые.

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты – присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников. Вторую категорию составляют механизмы защиты, реализуемые на базе программно–аппаратных средств, например систем идентификации и аутентификации или охранной сигнализации. Последняя категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации. Реализуемые на практике методы, как правило, сочетают в себе элементы нескольких из перечисленных категорий. Так, управление доступом в помещения может представлять собой взаимосвязь организационных (выдача допусков и ключей) и технологических (установку замков и систем сигнализации) способов защиты.

Рассмотрим подробнее такие взаимосвязанные методы защиты от НСД, как идентификация, аутентификация и используемое при их реализации криптографическое преобразование информации.

Идентификация – это присвоение пользователям идентификаторов (понятие идентификатора будет определено ниже) и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация –это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Под безопасностью (стойкостью) системы идентификаций и аутентификации будем понимать степень обеспечиваемых ею гарантии того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя. В этом смысле, чем выше стойкость системы

аутентификации, тем сложнее злоумышленнику решить указанную задачу. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

- индивидуального объекта заданного типа;
- знаний некоторой известной только ему и проверяющей стороне информации;
- индивидуальных биометрических характеристик.

К первой группе относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно–аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, использующие пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно–аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза и др. Такие средства позволяют с высокой точностью аутентифицировать обладателя конкретного биометрического признака, причем «подделать» биометрические параметры практически невозможно. Однако широкое распространение подобных технологий сдерживается высокой стоимостью необходимого оборудования.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией (direct password authentication). Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны (trusted third party authentication). При этом третью сторону называют сервером аутентификации (authentication server) или арбитром (arbitrator).

Общие подходы к построению парольных систем

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Из–за своего широкого распространения и простоты реализации парольные схемы часто в первую очередь становятся мишенью атак злоумышленников. Эти методы включают следующие разновидности способов аутентификации:

- по хранимой копии пароля или его свёртке (plaintext–equivalent);
- по некоторому проверочному значению (verifier–based);
- без непосредственной передачи информации о пароле проверяющей стороне (zero–knowledge);
- с использованием пароля для получения криптографического ключа (cryptographic).

В первую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен «троянский конь»). Пример системы парольной защиты («доказательство с нулевым разглашением»), построенной по данному принципу, будет рассмотрен ниже.

Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств, задействованных в них математических и криптографических преобразований, и может быть строго доказана. Обычные парольные системы проще и дешевле для реализации, но менее безопасны, чем системы с криптографическими протоколами. Последние обеспечивают более надежную защиту и дополнительно решают задачу распределения ключей. Однако используемые в них технологии могут быть объектом законодательных ограничений.

Передача пароля по сети

В большинстве случаев аутентификация происходит в распределённых системах и связана с передачей по сети информации о параметрах учетных записей пользователей. Если передаваемая по сети в процессе аутентификации информация не защищена надлежащим образом, возникает угроза ее перехвата злоумышленником и использования для нарушения защиты парольной системы. Известно, что многие компьютерные системы позволяют переключать сетевой адаптер в режим прослушивания адресованного другим получателям сетевого трафика в сети, основанной на широковещательной передаче пакетов данных.

Напомним основные виды защиты сетевого трафика:

- физическая защита сети;
- оконечное шифрование;
- шифрование пакетов.

Распространены следующие способы передачи по сети паролей:

- в открытом виде;
- зашифрованными;
- в виде свёрток;
- без непосредственной передачи информации о пароле («доказательство с нулевым разглашением»).

Первый способ применяется и сегодня во многих популярных приложениях (например, TELNET, FTP и других). В защищенной системе его можно применять только в сочетании со средствами защиты сетевого трафика.

При передаче паролей в зашифрованном виде или в виде сверток по сети с открытым физическим доступом возможна реализация следующих угроз безопасности парольной системы:

- перехват и повторное использование информации;
- перехват и восстановление паролей;

- модификация передаваемой информации с целью введения в заблуждение проверяющей стороны;
- имитация злоумышленником действий проверяющей стороны для введения в заблуждение пользователя.

Схемы аутентификации «с нулевым знанием» или «с нулевым разглашением», впервые появились в начале 90–х г.. Их основная идея заключается в том, чтобы обеспечить возможность одному из пары субъектов доказать истинность некоторого утверждения второму, при этом не сообщая ему никакой информации о содержании самого утверждения. Например, первый субъект («доказывающий») может убедить второго («проверяющего»), что знает определенный пароль, в действительности не передавая тому никакой информации о самом пароле. Эта идея и отражена в термине «доказательство с нулевым разглашением». Применительно к парольной защите это означает, что если на месте проверяющего субъекта оказывается злоумышленник, он не получает никакой информации о доказываемом утверждении и, в частности, о пароле.

Общая схема процедуры аутентификации с нулевым разглашением состоит из последовательности информационных обменов (итераций) между двумя участниками процедуры, по завершению которой проверяющий с заданной вероятностью делает правильный вывод об истинности проверяемого утверждения. С увеличением числа итераций возрастает вероятность правильного распознавания истинности (или ложности) утверждения.

Классическим примером неформального описания системы аутентификации с нулевым разглашением служит так называемая пещера Али–Бабы. Пещера имеет один вход , путь от которого разветвляется в глубине пещеры на два коридора, сходящихся затем в одной точке, где установлена дверь с замком. Каждый, кто имеет ключ от замка, может

переходить из одного коридора в другой в любом направлении. Одна итерация алгоритма состоит из последовательности шагов:

1. Проверяющий становится в точку A.

2. Доказывающий проходит в пещеру и добирается до двери (оказывается в точке C или O). Проверяющий не видит, в какой из двух коридоров тот свернул.

3. Проверяющий приходит в точку B и, в соответствии со своим выбором, просит доказывающего выйти из определенного коридора.

4. Доказывающий, если нужно, открывает дверь ключом и выходит из названного проверяющим коридора.

Итерация повторяется столько раз, сколько требуется для распознавания истинности утверждения «доказывающий владеет ключом от двери» с заданной вероятностью. После i–и итерации вероятность того, что проверяющий попросит доказывающего выйти из того же коридора, в который вошел доказывающий, равна (1/2).

Еще одним способом повышения стойкости парольных систем, связанной с передачей паролей по сети, является применение *одноразовых* (one–time) паролей. Общий подход к применению одноразовых паролей основан на последовательном использовании хеш–функции для вычисления очередного одноразового пароля на основе предыдущего. В начале пользователь получает упорядоченный список одноразовых паролей, последний из которых также сохраняется в системе аутентификации. При каждой регистрации пользователь вводит очередной пароль, а система вычисляет его свёртку и сравнивает с хранимым у себя эталоном. В случае совпадения пользователь успешно проходит аутентификацию, а введенный им пароль сохраняется для использования в качестве эталона при следующей регистрации. Защита от сетевого перехвата в такой схеме основана на свойстве необратимости хеш–функции. Наиболее известные

практические реализации схем с одноразовыми паролями – это программный пакет S/KEY и разработанная на его основе система OPIE.

Криптографические методы защиты

При построении защищенных АС роль криптографических методов для решения различных задач информационной безопасности трудно переоценить. Криптографические методы в настоящее время являются базовыми для обеспечения надежной аутентификации сторон информационного обмена, защиты информации в транспортной подсистеме АС, подтверждения целостности объектов АС и т.д.

К средствам криптографической защиты информации (СКЗИ) относятся аппаратные, программно–аппаратные и программные средства, реализующие криптографические алгоритмы преобразования информации с целью:

- защиты информации при ее обработке, хранении и передаче по транспортной среде АС;
- обеспечения достоверности и целостности информации (в том числе с использованием алгоритмов цифровой подписи) при ее обработке, хранении и передаче по транспортной среде АС;
- выработки информации, используемой для идентификации и аутентификации субъектов, пользователей и устройств;
- выработки информации, используемой для защиты аутентифицирующих элементов защищенной АС при их выработке, хранении, обработке и передаче.

Предполагается, что СКЗИ используются в некоторой АС (в ряде источников – информационно–телекоммуникационной системе или сети связи), совместно с механизмами реализации и гарантирования политики безопасности.

Не останавливаясь детально на определении криптографического преобразования, отметим его несколько существенных особенностей:

- в СКЗИ реализован некоторый алгоритм преобразования информации (шифрование, электронная цифровая подпись, контроль целостности и др.);
- входные и выходные аргументы криптографического преобразования присутствуют в АС в некоторой материальной форме (объекты АС);
- СКЗИ для работы использует некоторую конфиденциальную информацию (ключи);
- алгоритм криптографического преобразования реализован в виде некоторого материального объекта, взаимодействующего с окружающей средой (в том числе с субъектами и объектами защищенной АС).

Таким образом, роль СКЗИ в защищенной АС – преобразование объектов. В каждом конкретном случае указанное преобразование имеет особенности. Так, процедура зашифрования использует как входные параметры объект–открытый текст и объект–ключ, результатом преобразования является объект–шифрованный текст. Процедура расшифрования использует как входные параметры шифрованный текст и ключ. Процедура простановки цифровой подписи использует как входные параметры объект–сообщение и объект – секретный ключ подписи, результатом работы цифровой подписи является объект–подпись, как правило, интегрированный в объект–сообщение.

Можно говорить о том, что СКЗИ производит защиту объектов на семантическом уровне. В то же время объекты–параметры криптографического преобразования являются полноценными объектами АС и могут быть объектами некоторой политики безопасности

(например, ключи шифрования могут и должны быть защищены от НСД, открытые ключи для проверки цифровой подписи – от изменений и т.д.).

Лекция 14. Методы и средства обеспечения информационной безопасности от угрозы нарушения целостности информации

Организационно–технологические меры защиты целостности информации на машинных носителях

Организационно–технологические меры защиты целостности информации на машинных носителях можно разделить на две основные группы:

- организационные меры по поддержке целостности информации, хранящейся на МНИ;
- технологические меры контроля целостности битовых последовательностей, хранящихся на МНИ.

В свою очередь, организационные меры разделяются на две группы:

- создание резервных копий информации, хранимой на МНИ;
- обеспечение правильных условий хранения и эксплуатации МНИ.

Для создания резервных копий могут использоваться специализированные системы резервного копирования, адаптированные к конкретной АС.

Целостность данных в АС

Под целостностью данных понимается отсутствие ненадлежащих изменений. Смысл понятия «ненадлежащее изменение» раскрывается

Д. Кларком и Д. Вилсоном: ни одному пользователю АС, в том числе и авторизованному, не должны быть разрешены такие изменения данных, которые повлекут за собой их разрушение или потерю.

При рассмотрении вопроса целостности используется интегрированный подход , основанный на ряде работ Кларка и Вилсона, и включающий в себя девять абстрактных теоретических принципов, каждый из которых раскрывается ниже:

- корректность транзакций;
- аутентификация пользователей;
- минимизация привилегий;
- разграничение функциональных обязанностей;
- аудит произошедших событий;
- объективный контроль;
- управление передачей привилегий;
- обеспечение непрерывной работоспособности;
- простота использования защитных механизмов.

Модель контроля целостности Кларка–Вилсона

Модель Кларка–Вилсона появилась в результате проведенного авторами анализа реально применяемых методов обеспечения целостности документооборота в коммерческих компаниях. Все содержащиеся в системе данные подразделяются на контролируемые и неконтролируемые элементы данных (constrained data items – CDI и unconstrained data items – UDI соответственно). Целостность первых обеспечивается моделью Кларка–Вилсона. Последние содержат информацию, целостность которой в рамках данной модели не контролируется (этим и объясняется выбор терминологии).

Далее, модель вводит два класса операций над элементами данных: процедуры контроля целостности (integrity verification procedures – IVP) и

процедуры преобразования (transformation procedures – TP). Первые из них обеспечивают проверку целостности контролируемых элементов данных (CDI), вторые изменяют состав множества всех CDI (например, преобразуя элементы UDI в CDI). Наконец, модель содержит девять правил, определяющих взаимоотношения элементов данных и процедур в процессе функционирования системы.

Правило C1. Множество всех процедур контроля целостности (IVP) должно содержать процедуры контроля целостности любого элемента данных из множества всех CDI.

Правило C2. Все процедуры преобразования (TP) должны быть реализованы корректно в том смысле, что не должны нарушать целостность обрабатываемых ими CDI. Кроме того, с каждой процедурой преобразования должен быть связан список элементов CDI, которые допустимо обрабатывать данной процедурой. Такая связь устанавливается администратором безопасности.

Правило E1. Система должна контролировать допустимость применения TP к элементам CDI в соответствии со списками, указанными в правиле C2.

Правило E2. Система должна поддерживать список разрешенных конкретным пользователям процедур преобразования с указанием допустимого для каждой TP и данного пользователя набора обрабатываемых элементов CDI.

Правило C3. Список, определенный правилом C2, должен отвечать требованию разграничения функциональных обязанностей.

Правило E3. Система должна аутентифицировать всех пользователей, пытающихся выполнить какую–либо процедуру преобразования.

Правило C4. Каждая TP должна записывать в журнал регистрации информацию, достаточную для восстановления полной картины каждого

применения этой ТР. Журнал регистрации – это специальный элемент CDI, предназначенный только для добавления в него информации.

Правило С5. Любая ТР, которая обрабатывает элемент UDI, должна выполнять только корректные преобразования этого элемента, в результате которых UDI превращается в CDI.

Правило Е4. Только специально уполномоченное лицо может изменять списки, определенные в правилах С2 и Е2. Это лицо не имеет права выполнять какие–либо действия, если оно уполномочено изменять регламентирующие эти действия списки.

Роль каждого из девяти правил модели Кларка–Вилсона в обеспечении целостности информации можно пояснить, показав, каким из теоретических принципов политики контроля целостности отвечает данное правило. Напомним, что первые шесть из сформулированных выше принципов это:

1) корректность транзакций;

2) аутентификация пользователей;

3) минимизация привилегий;

4) разграничение функциональных обязанностей;

5) аудит произошедших событий;

6) объективный контроль.

Соответствие правил модели Кларка–Вилсона перечисленным принципам показано в табл. 7. Как видно из табл. 7, принципы 1 (корректность транзакций) и 4 (разграничение функциональных обязанностей) реализуются большинством правил, что соответствует основной идее модели.

Таблица 7.

Правило модели Кларка–Вилсона	Принципы политики контроля целостности, реализуемые правилом
C1	1,6
C2	1
E1	3,4
E2	1,2,3,4
C3	4
E3	2
C4	5
C5	1
E5	4

Защита памяти

В АС, в частности в любой ОС, память разделена (по меньшей мере логически) на области, которые используют ее компоненты, а также программы пользователей. При этом необходимо обеспечить защиту областей памяти от вмешательства в них посторонних компонентов, т.е. разграничить доступ приложений к областям памяти, а в многозадачной среде – и к областям памяти друг друга. Кроме того, необходимо решить проблему организации совместного доступа различных приложений к некоторым областям памяти.

Цифровая подпись

Средства контроля целостности программ и файлов данных должны обеспечивать защиту от несанкционированного изменения этой информации нарушителем, особенно при ее передаче по каналам связи. Цифровая (электронная) подпись является одним из часто используемых для решения данной задачи механизмов.

Кроме того, информация в вычислительных сетях нередко нуждается в аутентификации, т.е. в обеспечении заданной степени уверенности получателя или арбитра в том, что она была передана отправителем и при этом не была заменена или искажена. Если целью шифрования является защита от угрозы нарушения конфиденциальности, то целью аутентификации является защита участников информационного обмена не только от действий посторонних лиц, но и от взаимного обмана.

В чем состоит проблема аутентификации данных или цифровой подписи? В конце обычного письма или документа исполнитель или ответственное лицо обычно ставит свою подпись. Подобное действие преследует две цели. Во–первых, получатель имеет возможность убедиться в истинности письма, сличив подпись с имеющимся у него образцом. Во–вторых, личная подпись является юридическим гарантом авторства документа. Последний аспект особенно важен при заключении разного рода торговых сделок, составлении доверенностей, обязательств и т.д.

Если подделать подпись человека на бумаге весьма непросто, а установить авторство подписи современными криминалистическими методами – техническая деталь, то с цифровой подписью дело обстоит иначе. Подделать цепочку битов, просто ее скопировав, или незаметно внести нелегальные исправления в документ сможет любой пользователь.

В самой общей модели аутентификации сообщений представлено пять участников. Это отправитель А, получатель В, злоумышленник С, доверенная сторона Д и независимый арбитр Е. Задача отправителя А заключается в формировании и отправке сообщения Т получателю В. Задача получателя В заключается в получении сообщения Т и в установлении его подлинности. Задача доверенной стороны Д является документированная рассылка необходимой служебной информации

абонентам вычислительной сети, чтобы в случае возникновения спора между A и B относительно подлинности сообщения представить необходимые документы в арбитраж. Задача независимого арбитра E заключается в разрешении спора между абонентами A и B относительно подлинности сообщения T.

Перечислим возможные способы обмана (нарушения подлинности сообщения) при условии, что между участниками модели A, B, C отсутствует кооперация.

Способ A: отправитель A заявляет, что он не посылал сообщение T получателю B, хотя в действительности его посылал (подмена отправленного сообщения или отказ от авторства).

Способ B1: получатель B изменяет полученное от отправителя A сообщение T и заявляет, что данное измененное сообщение он получил от отправителя A (подмена принятого сообщения).

Способ B2: получатель B сам формирует сообщение и заявляет, что получил его от отправителя A (имитация принятого сообщения).

Способ C1: злоумышленник C искажает сообщение, которое отправитель A передает получателю B (подмена передаваемого сообщения).

Способ C2: злоумышленник C формирует и посылает получателю B сообщение T от имени отправителя A (имитация передаваемого сообщения).

Способ C3: злоумышленник C повторяет ранее переданное сообщение, которое отправитель A посылал получателю B (повтор ранее переданного сообщения).

Аутентификация (цифровая подпись) при условии взаимного доверия между участниками информационного обмена обеспечивается имитозащитой информации с помощью криптостойких преобразований.

Приведем сравнительный анализ обычной и цифровой подписи.

При обычной подписи:

- каждая личность использует индивидуальные, только ей присущие характеристики – почерк, давление на ручку и т.д.;
- попытка подделки подписи обнаруживается с помощью графологического анализа;
- подпись и подписываемый документ передаются только вместе на одном листе бумаги; передавать подпись отдельно от документа нельзя; подпись не зависит от содержания документа, на котором она поставлена;
- копии подписанных документов недействительны, если каждая из этих копий не имеет своей настоящей (а не скопированной) подписи.

При цифровой подписи:

- каждая личность использует для подписи документов свой уникальный секретный ключ;
- попытка подписать документ без знания соответствующего секретного ключа практически не имеет успеха;

цифровая подпись документа есть функция от содержания этого документа и секретного ключа; цифровая подпись может передаваться отдельно от документа;

- копия документа с цифровой подписью не отличается от его оригинала (нет проблем каждой копии).

Для аутентификации информации Диффи и Хеллман в 1976 г. предложили концепцию «цифровой подписи». Она заключается в том, что каждый абонент сети имеет личный секретный ключ, на котором он формирует подпись и известную всем другим абонентам сети проверочную комбинацию, необходимую для проверки подписи (эту проверочную комбинацию иногда называют открытым ключом). Цифровая подпись вычисляется на основе сообщения и секретного ключа

отправителя. Любой получатель, имеющий соответствующую проверочную комбинацию, может аутентифицировать сообщение по подписи. При этом знание лишь проверочной комбинации не позволяет подделать подпись. Такие схемы называются асимметричными схемами аутентификации.

Термин «цифровая подпись» используется для методов, позволяющих устанавливать подлинность автора сообщения при возникновении спора относительно авторства этого сообщения. Цифровая подпись применяется в информационных системах, в которых отсутствует взаимное доверие сторон (финансовые системы, системы контроля за соблюдением международных договоров и др.).

Известны два класса формирования цифровой подписи.

Первый класс способов использует труднообратимые функции типа возведения в степень в конечных полях большой размерности (сотни и даже тысячи битов). К этому классу относится Российский ГОСТ на цифровую подпись (ГОСТ Р 34.10–94 и ГОСТ Р 34.11–94). Он является усложнением алгоритмов цифровой подписи RSA и Эль–Гамаля.

Второй класс способов использует криптостойкие преобразования, зависящие от секретного ключа.

В обоих случаях требуется предварительная заготовка и рассылка возможным получателям информации контрольных комбинаций. Общедоступные контрольные комбинации должны быть нотариально заверены, чтобы ни отправитель, ни получатель не смогли впоследствии от них отказаться. Оба класса способов не нуждаются в закрытых каналах. Контрольные комбинации и подписи пересылаются открыто. Единственным секретным элементом во всех способах является личный секретный ключ отправителя.

Алгоритмы контроля целостности данных

В руководящих документах Гостехкомиссии РФ целостность информации определяется следующим образом:

Целостность информации – это способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

Под угрозой нарушения целостности понимается любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения.

Наиболее простым и одним из самых первых методов обеспечения целостности данных является метод контрольных сумм. Под контрольной суммой понимается некоторое значение, полученное путем сложения всех чисел входных данных в конечном множестве.

Пусть:

α – массив данных, элементами которого являются числовые значения.

Length(α) – количество элементов массива α.

Sum – результат суммирования всех элементов α[i] массива данных α, где i = [1..Length(α)].

CheckSum – контрольная сумма массива α.

MaxVal – максимально возможное числовое значение CheckSum.

Тогда контрольной суммой массива α будет являться величина CheckSum, полученная путем деления с остатком суммы всех элементов

массива Sum на максимально возможное числовое значение контрольной суммы, увеличенное на единицу или:

CheckSum = Sum mod (MaxVal+1) .

Использование метода контрольных сумм применяется до сих пор в некоторых протоколах передачи данных.

Более совершенным способом контроля целостности данных является, так называемый, метод “циклического контрольного кода”(cyclic redundancy check – CRC). Алгоритм широко используется в аппаратных устройствах (дисковые контроллеры, сетевые адаптеры и др.) для верификации неизменности входной и выходной информации, а также во многих программных продуктах для выявления ошибок при передаче данных по каналам связи. В основе метода CRC лежит понятие полинома или многочлена. Каждый бит некоторого блока данных соответствует одному из коэффициентов двоичного полинома. Например, полином шестнадцатеричного числа 7A (двоичная запись – 1111010) будет выглядеть следующим образом:

A(x) = 1*x6+1*x5+1*x4+1*x3+0*x2+1*x1+0*x0 = x6+x5+x4+x3+x

Таким образом, любой блок данных представляет собой последовательность битов, которую можно представить в виде двоичного полинома A(x). Для вычисления контрольного кода необходим еще один полином G(x), называемый порождающим полиномом. Для каждой реализации алгоритма контроля CRC порождающий полином выбирается заранее произвольным образом. Например, для контроллеров гибких магнитных дисков порождающий полином G(x) = x16+x12+x5+1.

Пусть R(x) – некий полином. R(x) называется контрольным кодом полинома A(x) при порождающем полиноме G(x), если R(x) является остатком от деления полинома A(x)*xr на G(x), где r – степень полинома G(x).

R(x) = (A(x)*xr) mod G(x).

Так же, как и для контрольных сумм, контрольный код не занимает много места (обычно 16/32 бита), однако вероятность обнаружения ошибки существенно выше. Например, в отличие от контрольных сумм метод CRC сможет обнаружить перестановку двух байт либо добавление единицы к одному и вычитание единицы из другого.

Существенно более высокой надежности, чем при методе «циклического контрольного кода», можно достичь, используя однонаправленные функции «хэширования». Термин «однонаправленный» означает следующее:

Пусть имеется некая функция f и произвольный набор данных A.

Пусть результатом применения функции f к A является набор данных B (хэш).

$f(A) = B$.

Функция f является однонаправленной, если не существует такой функции g, что

$g(B) = A$,

либо такую функцию g крайне сложно построить.

Коллизией называется ситуация, когда разным наборам входных блоков данных соответствует один хэш. Важная отличительная особенность хороших алгоритмов хэширования заключается в том, что генерируемые с его помощью значения настолько уникальны и трудноповторимы, что задача нахождения коллизий является чрезвычайно тяжелой как по ресурсоемкости, так и по производительности. Вышесказанное можно записать следующим образом:

Пусть $f(A)=B$. Не существует такого A’ либо его крайне сложно найти, что $f(A')=B$. Чем больше длина хэша, тем труднее найти соответствующий набор входных данных. Среди алгоритмов хэширования наибольшей известностью пользуются:

алгоритм MD5 (длина хэша – 128 бит), автор Ron Rivest, создатель алгоритма шифрования с открытым ключом RSA;

алгоритм SHA–1 (длина хэша – 160 бит), созданный усилиями специалистов Национального института по стандартизации и технологиям (NIST) и Агентства национальной безопасности (NSA).

Также стоит отметить российский стандарт на функцию хэширования ГОСТ Р34.11–94.

Лекция 15. Методы и средства обеспечения информационной безопасности от угрозы отказа доступа к информации

Защита от сбоев программно–аппаратной среды

Поскольку одной из основных задач АС является своевременное обеспечение пользователей системы необходимой информацией (сведениями, данными, управляющими воздействиями и т.п.), то угроза отказа доступа к информации применительно к АС может еще рассматриваться как угроза отказа в обслуживании или угроза отказа функционирования. В свою очередь, создание и эксплуатация АС тесным образом связаны с проблемой обеспечения надежности, важность которой возрастает по мере увеличения сложности и стоимости разработки, а также характера возможных последствий, которые для управляющих критических систем могут быть катастрофическими. К неправильному функционированию АС приводят ошибки в ПО или отказ аппаратуры. В связи с этим вводят понятие надежности ПО, под кото рым понимается свойство объекта сохранять во времени значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, ремонта, хранения и транспортировки.

Несмотря на явное сходство в определениях надежности для аппаратных средств и ПО, фактически между этими надежностями сохраняются принципиальные различия. Программа в большинстве случаев не может отказать случайно. Ошибки в ПО, допущенные при его создании, зависят от технологии, организации и квалификации исполнителей и в принципе не являются функцией времени. Причиной отказов, возникающих из–за этих ошибок и фиксируемых как случайный процесс, является не время функционирования системы, а набор входных данных, сложившихся к моменту отказа.

Угроза отказа функционирования АС может быть вызвана как целенаправленными действиями злоумышленников, так и недостаточной надежностью входящей в состав АС аппаратуры и ПО. При обеспечении защиты АС от угрозы отказа функционирования обычно делают следующие допущения. Считается, что надежность аппаратных компонентов достаточно высока, и в практическом плане этой составляющей в общей надежности АС можно пренебречь. Более того, темпы морального старения вычислительной техники значительно опережают темпы ее физического старения, и замена вычислительной техники, как правило, происходит до ее выхода из строя. В настоящее время (при условии соблюдения правил эксплуатации) практически не рассматривается возможность потери данных вследствие утери МНИ функциональных свойств. Таким образом, надежность функционирования АС может быть сведена к надежности функционирования входящего в ее состав программного обеспечения. Другое допущение связано с тем, что принято не различать природу причин сбоев и отказов работы АС, т.е. для надежности функционирования АС неважно, вызваны ли они действиями злоумышленника или связаны с ошибками разработки.

Существуют два основных подхода к обеспечению защиты ПО АС от угрозы отказа функционирования – предотвращение неисправностей и отказоустойчивость.

Отказоустойчивость предусматривает, что оставшиеся ошибки ПО обнаруживаются во время выполнения программы и парируются за счет использования программной, информационной и временной избыточности. Предотвращение неисправностей связано с анализом природы ошибок, возникающих на разных фазах создания ПО, и причин их возникновения.

Обеспечение отказоустойчивости ПО АС

Невозможность обеспечить в процессе создания АС ее абсолютную защищенность от угрозы отказа функционирования даже при отсутствии злоумышленных воздействий заставляет искать дополнительные методы и средства повышения безопасности функционирования ПО на этапе эксплуатации. Для этого разрабатываются и применяются методы оперативного обнаружения дефектов при исполнении программ и искажений данных введением в них временной, информационной и программной избыточности. Эти же виды избыточности используются для оперативного восстановления искаженных программ и предотвращения возможности развития угроз до уровня, нарушающего безопасность АС.

Для обеспечения высокой надежности и безопасности функционирования АС необходимы вычислительные ресурсы для максимально быстрого обнаружения проявления дефектов, возможно точной классификации типа уже имеющихся и вероятных последствий искажений, а также для автоматизированных мероприятий, обеспечивающих быстрое восстановление нормального функционирования АС. Неизбежность ошибок в сложных АС, искажений исходных данных и других аномалий приводит к необходимости

регулярной проверки состояния и процесса исполнения программ, а также сохранности данных. В процессе проектирования требуется разрабатывать надежные и безопасные программы и базы данных, устойчивые к различным возмущениям и способные сохранять достаточное качество результатов во всех реальных условиях функционирования. В любых ситуациях прежде всего должны исключаться катастрофические последствия дефектов и длительные отказы или в максимальной степени смягчаться их влияние на результаты, выдаваемые пользователю.

Временная избыточность состоит в использовании некоторой части производительности компьютера для контроля исполнения программ и восстановления (рестарта) вычислительного процесса. Для этого при проектировании АС должен предусматриваться запас производительности, который затем будет использоваться системами контроля и для повышения надежности и безопасности функционирования. Значение временной избыточности зависит от требований к безопасности функционирования или обработки информации и находится в пределах от 5...10% производительности до трех–четырехкратного дублирования в мажоритарных вычислительных комплексах.

Информационная избыточность состоит в дублировании накопленных исходных и промежуточных данных, обрабатываемых программами. Избыточность используется для сохранения достоверности данных, которые в наибольшей степени влияют на нормальное функционирование АС и требуют значительного времени на восстановление. Такие данные обычно характеризуют некоторые интегральные сведения о внешнем управляющем процессе; в случае их разрушения может прерваться процесс управления внешними объектами или обработки их информации, отражающийся на безопасности АС.

Программная избыточность используется для контроля и обеспечения достоверности наиболее важных решений по управлению и обработке информации. Она заключается в сопоставлении результатов обработки одинаковых исходных данных разными программами и исключении искажения результатов, обусловленных различными аномалиями. Программная избыточность необходима также для реализации средств автоматического контроля и восстановления данных с использованием информационной избыточности и для функционирования всех средств защиты, имеющих временную избыточность.

Последовательный характер исполнения программ центральным процессором приводит к тому, что средства оперативного программного контроля включаются после выполнения прикладных и сервисных программ. Поэтому средства программного контроля обычно не могут обнаруживать возникновение искажения вычислительного процесса или данных (первичную ошибку) и фиксируют, как правило, только последствия первичного искажения (вторичную ошибку). Результаты первичного искажения в ряде случаев могут развиваться во времени и принимать катастрофический характер отказа при увеличении времени запаздывания в обнаружении последствий первичной ошибки.

Обеспечение отказоустойчивости ПО АС применимо в основном к прикладному программному обеспечению, так как в этом случае реализация задачи контроля возлагается на операционную систему. Что же касается самой операционной системы, то данный подход здесь практически не работает, так как для нее потребуется своя контролирующая операционная «сверхсистема», которую также надо контролировать, и т.д. Поэтому для операционных систем применяют методы предотвращения неисправностей в ПО.

Предотвращение неисправностей в ПО АС

В настоящее время в разных странах и фирмах отработаны технологии создания, развития и применения программ для компьютеров на основе формализованных моделей жизненного цикла программ различных классов и назначения. В модели жизненный цикл структурируется рядом крупных фаз или этапов, каждый из которых характеризуется достаточно определенными целями и результатами. Так как основные промежуточные и конечные цели создания и применения программ одного класса достаточно близки, то и модели жизненного цикла для аналогичных типов программных средств в значительной степени подобны. Главные различия заключаются в выделении наиболее важных процессов, а также способов их группирования и отображения. При этом важную роль играют классы и параметры программ, которые (иногда неявно) определяют первоначальное формирование моделей жизненного цикла.

Защита семантического анализа и актуальности информации

На уровне представления информации защиту от угрозы отказа доступа к информации (защиту семантического анализа*)* можно рассматривать как противодействие сопоставлению используемым синтаксическим конструкциям (словам некоторого алфавита, символам и т.п.) определенного смыслового содержания. В большей степени эта задача относится к области лингвистики, рассматривающей изменение значения слов с течением времени, переводу с иностранного языка и другим аналогичным научным и прикладным областям знаний.

В качестве примера нарушения доступности информации можно привести сообщение времен Петра I о том, что переправа войск через реку осуществлялась на самолетах. Истинный смысл сообщения заключается в том, что переправа войск проходила не на летательных аппаратах (иначе сообщение было бы исторически неверно), а на небольших плотах.

В этом примере защита информации осуществляется использованием факта «самолет–небольшой плот (устар.)». Если потенциальный злоумышленник не знает этот факт, для него не будет доступен смысл сообщения.

Применительно к АС задача защиты от угрозы доступности информации может рассматриваться как использование для обработки файла данных программ, обеспечивающих воспроизведение данных в том виде, как они были записаны.

Рассмотрим, например, файл, содержащий текстовую информацию и данные о ее оформлении (выделение курсивом, подчеркивание и т.п.). Если для воспроизведения выбрать более простой редактор, или редактор, не поддерживающий выбранный тип разметки, выделение определенных слов пропадет, а значит, будет утрачена часть информации, которая закладывалась в оформление текста.

На уровне содержания защита информации от угрозы доступности обеспечивается защитой *актуальности информации* или легализацией полученных сведений или данных.

Предположим, что некто имеет возможность доступа к технической подготовке некой гипотетической базе данных, содержащей нормативные акты. Для своевременности обновления базы данных информация, содержащая новое постановление или другой нормативный акт, поступает до момента опубликования в источниках, вводящих в силу данный акт. Если это лицо решит воспользоваться полученной информацией, путем доступа к тексту до его официальной публикации, то он не сможет подтвердить обоснованность своих действий до вступления нормативного акта в силу.

Применительно к АС защита содержания информации от угрозы блокировки доступа (отказа функционирования) означает юридическую обоснованность обработки и использования информации, хранящейся в АС.

Р а з д е л 5. Архитектура безопасности взаимодействия открытых систем

Лекция 16. Архитектура безопасности и сервисы безопасности взаимодействия открытых систем

Структура семиуровневой модели взаимодействия открытых систем

Логически сеть существует на уровне передачи пакетов данных. Для того, чтобы два абонента сети смогли «понимать» друг друга и «разговаривать» друг с другом, они должны использовать одинаковый формат передаваемых в пакетах данных.

Решение этой проблемы привело к созданию протоколов – наборов соглашений и правил по методам передачи данных, их пакетированию и адресации.

Для стандартизации обмена данными была разработана модель взаимодействия открытых систем OSI. Эталонная модель OSI, иногда называемая стеком OSI, представляет собой семиуровневую сетевую иерархию, разработанную Международной организацией по стандартам (International Standardization Organization – ISO).

Эта модель содержит в себе по сути две различных модели:

- горизонтальную модель на базе протоколов, обеспечивающую механизм взаимодействия программ и процессов на различных машинах;
- вертикальную модель на основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине.

Рассмотрим структуру эталонной модели взаимодействия открытых систем, представленную на рис. 10.

Рис. 10. Эталонная модель взаимодействия открытых систем OSI

Уровень 1, физический

Физический уровень получает пакеты данных от вышележащего канального уровня и преобразует их в оптические или электрические сигналы, соответствующие 0 и 1 бинарного потока. Эти сигналы посылаются через среду передачи на приемный узел.

Механические и электрические/оптические свойства среды передачи определяются на физическом уровне и включают:

тип кабелей и разъемов ;

разводку контактов в разъемах;

схему кодирования сигналов для значений 0 и 1.

Уровень 2, канальный

Канальный уровень обеспечивает создание, передачу и прием кадров данных. Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов. Спецификации IEEE 802.x делят канальный уровень на два подуровня: управление логическим каналом (LLC) и управление доступом к среде (MAC). LLC обеспечивает обслуживание сетевого уровня, а подуровень MAC регулирует доступ к разделяемой физической среде.

Уровень 3, сетевой

Сетевой уровень отвечает за деление пользователей на группы. На этом уровне происходит маршрутизация пакетов на основе преобразования MAC–адресов в сетевые адреса. Сетевой уровень обеспечивает также прозрачную передачу пакетов на транспортный уровень.

Уровень 4, транспортный

Транспортный уровень делит потоки информации на достаточно малые фрагменты (пакеты) для передачи их на сетевой уровень.

Уровень 5, сеансовый

Сеансовый уровень отвечает за организацию сеансов обмена данными между оконечными машинами. Протоколы сеансового уровня обычно являются составной частью функций трех верхних уровней моде***ли.***

Уровень 6, уровень представления

Уровень представления отвечает за возможность диалога между приложениями на разных машинах. Этот уровень обеспечивает преобразование данных (кодирование, компрессия и т.п.) прикладного уровня в поток информации для транспортного уровня. Протоколы уровня представления обычно являются составной частью функций трех верхних уровней модели.

Уровень 7, прикладной

Прикладной уровень отвечает за доступ приложений в сеть. Задачами этого уровня является перенос файлов, обмен почтовыми сообщениями и управление сетью.

Концепция сервисов безопасности

Впервые в наиболее полном виде концепция сервисов безопасности была изложена в 1989 г. в Международном стандарте ISO|IEC 7498–2 «Базовая эталонная модель взаимодействия открытых систем. Часть 2: Архитектура безопасности». В 1991 г. этот стандарт был повторен в «Рекомендации X.800: Архитектура безопасности взаимодействия открытых систем для применений МККТТ».

В ней рассмотрены основные (базовые) сервисы безопасности для случая взаимодействия двух систем, и описаны основные механизмы, обеспечивающие эти услуги. Указано также их желательное расположение в эталонной семиуровневой модели взаимодействия открытых систем (см. табл. 7).

Таблица 7.

Сервисы (услуги безопасности)	**Механизмы защиты**							
	Шифование	Цифовая подпись	Контроль доступа	Целостность	Аутентификация	Заполнене трафика	Управление маршрутизацией	Нотариальное заверение
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Аутентификация получателя	3,4	3,4	–	–	3,4	–	–	–
Аутентификация источника данных	3,4	3,4,7	–	–	–	–	–	–
Управление доступом	–	–	3,4,7	–	–	–	–	–
Конфиденциальность соединения	2,3,4,6,7	–	–	–	–	–	3	–
Конфиденциальность без установления соединения	2,3,4,6,7	–	–	–	–	–	–	–
Конфиденциальность выделенного поля данных	6,7	–	–	–	–	–	–	–
Конфиденциальность трафика	1,6	–	–	–	–	3,7	3	–
Целостность соединения без восстановления	3,4,7	–	3,4,7	–	–	–	–	–
Целостность соединения с восстановлением	4,7	–	4,7	–	–	–	–	–
Целостность выделенного поля в режиме с восстановлением соединения	7	–	7	–	–	–	–	–

Окончание табл. 7

1	2	3	4	5	6	7	8	9
Целостность блока данных без установления соединения	3,4,7	3,4,7	–	3,4,7	–	–	–	–
Доказательство источника	–	7	–	7	–	–	–	7
Доказательство доставки	–	7	–	7	–	–	–	7

Для построения защищенных распределенных систем современные стандарты определяют и ряд других сервисов безопасности, например, туннелирование, межсетевое экранирование и др. Практически все сервисы могут быть реализованы только с помощью криптографических методов.

Идентификация / аутентификация

Здесь имеются в виду две разные вещи: аутентификация сторон (криптографические протоколы идентификации) и аутентификация источника данных (установление авторства документа, обычно решается с помощью цифровой подписи).

Конфиденциальность

Это традиционно криптографический сервис, основанный на применении шифрования.

Контроль целостности

Основан на применении специальных криптографических контрольных сумм – имитовставок. В современных системах контроль целостности должен распространяться не только на отдельные порции данных, аппаратные или программные компоненты. Он обязан

охватывать распределенные конфигурации, защищать от несанкционированной модификации потоки данных.

Протоколирование / аудит

Протоколирование/аудит обеспечивают анализ последствий нарушения информационной безопасности и выявление злоумышленников. Такой аудит называют пассивным. Активный аудит направлен на выявление подозрительных действий в реальном масштабе времени. Важным элементом современной трактовки протоколирования/аудита является протокол автоматизированного обмена информацией о нарушениях безопасности между корпоративными системами, подключенными к одной внешней сети.

Межсетевое экранирование

Экранирование как сервис безопасности выполняет следующие функции: разграничение межсетевого доступа путем фильтрации передаваемых данных; преобразование передаваемых данных.

Преобразование передаваемых данных может затрагивать как служебные поля пакетов, так и прикладные данные. В первом случае обычно имеется в виду трансляция адресов, помогающая скрытъ топологию защищаемой системы и существование некоторых объектов доступа. Преобразование данных, как правило, состоит в шифровании.

Туннелирование

Туннелирование, как и экранирование, можно рассматривать как самостоятельный сервис безопасности. Его суть состоит в том, чтобы «упаковать» передаваемую порцию данных вместе со служебными полями в новый «конверт». Данный сервис может применяться для обеспечения конфиденциальности и целостности всей передаваемой порции, включая служебные поля. Туннелирование может применяться как на сетевом, так и на прикладном уровнях. Комбинация

туннелирования и шифрования позволяет реализовать виртуальные частные сети.

Если рассмотреть механизмы, применяемые для реализации перечисленных сервисов, то мы также убеждаемся в том, что криптографические механизмы играют определяющую роль.

Действительно, механизмы шифрования и цифровой подписи и удостоверения целостности основаны на использовании криптографических схем. Механизм контроля доступа реализует идентификацию, проверку полномочий пользователя и разрешение или отказ в доступе к объекту. Для этого могут использоваться различные средства: списки полномочий, системы идентификации, специальные режимы и особенности работы, метки, временные ограничения и выделенные маршруты. Все эти средства могут быть реализованы на основе схемы управления криптографическими ключами, дающими право доступа к соответствующей информации (например, Kerberos, KryptoKnight и др.).

Механизмы аутентификации взаимодействующих сторон также используют криптографические протоколы аутентификации. Для защиты паролей используют криптографические схемы. Схемы «рукопожатия» основаны на односторонних криптографических хэш–функциях. Наиболее стойкие протоколы аутентификации основаны на криптографических алгоритмах идентификации, использующих технику «запрос–ответ».

Механизм заполнения трафика применяется для сокрытия передаваемой информации в общем потоке передаваемых данных. Наиболее эффективным способом заполнения трафика является шифрование всего трафика, включая заполняющую паузы информацию, единым криптографическим способом.

Механизм управления маршрутизацией позволяет при обнаружении воздействия на передаваемую информацию изменить маршрут на более безопасный, обеспечивающий конфиденциальность и целостность передаваемой информации.

Механизм нотариального заверения основан на введении третьей доверенной стороны, участвующей во взаимодействии двух сторон, позволяющей удостоверить источник и получателя данных, время сеанса связи и т.п. Наиболее безопасными при таком взаимодействии являются криптографические трехсторонние протоколы.

Криптографические методы дают наиболее безопасные реализации сервисов безопасности, однако при их использовании стоимость услуги получается более высокой, так как они связаны с необходимостью реализации системы управления ключами. В открытой сетевой среде между сторонами идентификации/аутентификации не существует доверенного маршрута. Это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить прямое взаимодействие, т. е. защиту от пассивного и активного прослушивания сети: перехвата, изменения и/или воспроизведения данных. Передача паролей в открытом виде является нежелательной. При этом не спасает положение и шифрование паролей, так как оно не защищает от воспроизведения. Нужны более сложные протоколы аутентификации. Надежная идентификация затруднена не только из–за сетевых угроз, но и по целому ряду причин. Во–первых, почти все аутентификационные сущности можно узнать, украсть или подделать. Во–вторых, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно

вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто–то может подсмотреть за вводом данных. В–третьих, чем надежнее средство защиты, тем оно дороже. Современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. Единый вход в сеть – это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации. Необходимо отметить, что сервис идентификации / аутентификации может стать объектом атак на доступность. Если система сконфигурирована так, что после определенного числа неудачных попыток устройство ввода идентификационной информации (такое, например, как терминал) блокируется, то злоумышленник может остановить работу легального пользователя буквально несколькими нажатиями клавиш.

В этой связи рассмотрим систему Kerberos – программный продукт, разработанный в середине 1980–х годов в Массачусетском технологическом институте. Kerberos предназначен для решения следующей задачи. Имеется открытая (незащищенная) сеть, в узлах которой сосредоточены субъекты – пользователи, а также клиентские и серверные программные системы. Каждый субъект обладает секретным ключом. Чтобы субъект C мог доказать свою подлинность субъекту S (без этого S не станет обслуживать C), он должен не только назвать себя, но и продемонстрировать знание секретного ключа. C не может просто послать S свой секретный ключ, во–первых, потому, что сеть открыта (доступна

для пассивного и активного прослушивания), а, во–вторых, потому, что S не знает (и не должен знать) секретный ключ C. Требуется менее прямолинейный способ демонстрации знания секретного ключа.

Система Kerberos представляет собой доверенную третью сторону (то есть сторону, которой доверяют все), владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности.

Чтобы с помощью Kerberos получить доступ к S (обычно это сервер), C (как правило – клиент) посылает Kerberos запрос, содержащий сведения о нем (клиенте) и о запрашиваемой услуге. В ответ Kerberos возвращает так называемый билет, зашифрованный секретным ключом сервера, и копию части информации из билета, зашифрованную секретным ключом клиента. Клиент должен расшифровать вторую порцию данных и переслать ее вместе с билетом серверу. Сервер, расшифровав билет, может сравнить его содержимое с дополнительной информацией, присланной клиентом. Совпадение свидетельствует о том, что клиент смог расшифровать предназначенные ему данные (ведь содержимое билета никому, кроме сервера и Kerberos, недоступно), то есть продемонстрировал знание секретного ключа. Значит, клиент – именно тот, за кого себя выдает. Подчеркнем, что секретные ключи в процессе проверки подлинности не передавались по сети (даже в зашифрованном виде) – они только использовались для шифрования. Как организован первоначальный обмен ключами между Kerberos и субъектами и как субъекты хранят свои секретные ключи – вопрос отдельный.

Проиллюстрируем описанную процедуру на рис 11.

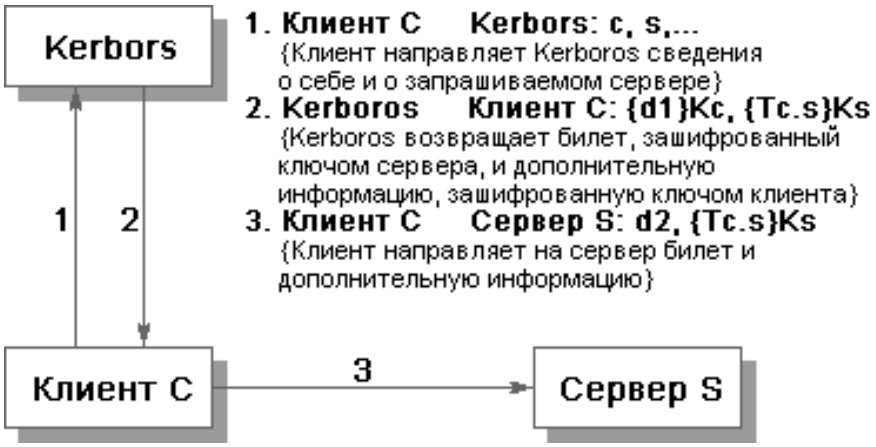

Рис. 11. Проверка сервером S подлинности клиента C

Здесь c и s – сведения (например, имя), соответственно, о клиенте и сервере; d1 и d2 – дополнительная (по отношению к билету) информация; Tc.s – билет для клиента C на обслуживание у сервера S; Kc и Ks – секретные ключи клиента и сервера; {info}K – информация info, зашифрованная ключом K.

Идентификация/аутентификация с помощью биометрических данных

Биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик.

К числу физиологических характеристик принадлежат особенности отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п. К поведенческим характеристикам относятся динамика подписи (ручной), стиль работы с клавиатурой.

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются и результат

обработки (называемый биометрическим шаблоном) заносится в базу данных (исходные данные, такие, как результат сканирования пальца или роговицы, обычно не хранятся). В дальнейшем для идентификации (и одновременно аутентификации) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными.

Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных.

Необходимо учитывать, что биометрия подвержена тем же угрозам, что и другие методы аутентификации.

Во–первых, биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения. А, как известно, за время пути данные могут быть искажены или перехвачены.

Во–вторых, биометрические методы не более надежны, чем база данных шаблонов.

В–третьих, следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в «полевых» условиях, когда, например, к устройству сканирования роговицы могут поднести муляж и т.п. В–четвертых, биометрические данные человека меняются, так что база шаблонов нуждается в сопровождении, что создает определенные проблемы и для пользователей, и для администраторов.

Но главная опасность состоит в том, что любая «пробоина» для биометрии оказывается фатальной. Пароли, при всей их ненадежности, в крайнем случае, можно сменить. Утерянную аутентификационную карту можно аннулировать и завести новую. Палец же, глаз или голос изменить

нельзя. Если биометрические данные окажутся скомпрометированы, придется, как минимум, производить существенную модернизацию всей системы.

Лекция 17. Протоколы сетевой безопасности (часть 1)

Понятие корпоративной сети

Корпоративные сети называют также сетями масштаба предприятия, что соответствует дословному переводу термина «enterprise–wide networks», используемого в англоязычной литературе для обозначения этого типа сетей. Сети масштаба предприятия (корпоративные сети) объединяют большое количество компьютеров на всех территориях отдельного предприятия. Они могут быть сложно связаны и покрывать город, регион или даже континент. Число пользователей и компьютеров может измеряться тысячами, а число серверов – сотнями, расстояния между сетями отдельных территорий могут оказаться такими, что становится необходимым использование глобальных связей (рис. 12.)

Для соединения удаленных локальных сетей и отдельных компьютеров в корпоративной сети применяются разнообразные телекоммуникационные средства, в том числе телефонные каналы, радиоканалы, спутниковая связь. Корпоративную сеть можно представить в виде «островков локальных сетей», плавающих в телекоммуникационной среде. Непременным атрибутом такой сложной и крупномасштабной сети является высокая степень гетерогенности – нельзя удовлетворить потребности тысяч пользователей с помощью однотипных программных и аппаратных средств, что является также характерной особенностью АСТНК. В корпоративной сети обязательно будут использоваться различные типы компьютеров – от мэйнфреймов до

персоналок, несколько типов операционных систем и множество различных приложений. Неоднородные части корпоративной сети должны работать как единое целое, предоставляя пользователям по возможности прозрачный доступ ко всем необходимым ресурсам.

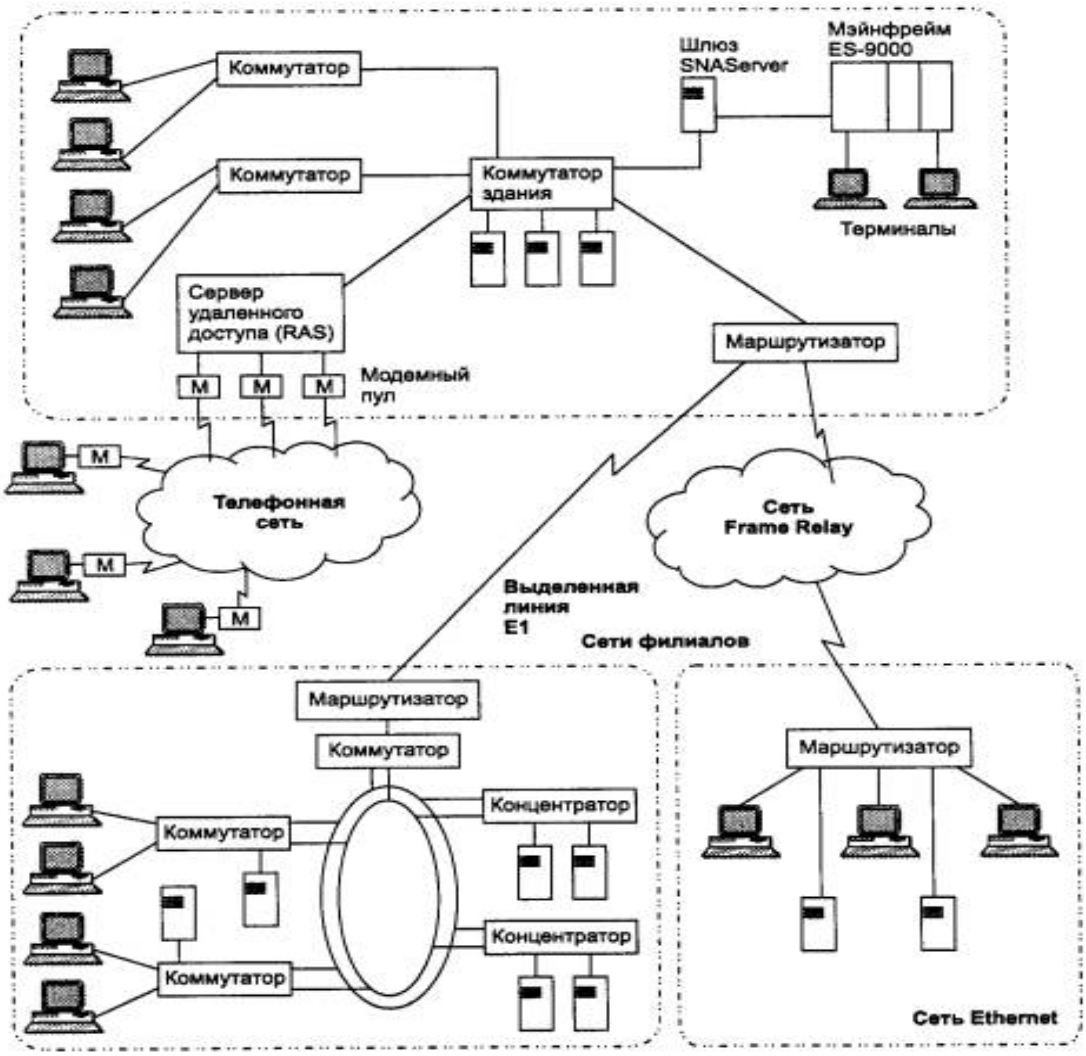

Рис.12.Пример корпоративной сети

При каждом переходе на следующий уровень сложности компьютерное оборудование сети становится все более разнообразным, а географические расстояния увеличиваются, делая достижение целей ИБ более сложным; более проблемным и дорогостоящим становится управление такими соединениями.

Появление корпоративных сетей – это хорошая иллюстрация известного философского постулата о переходе количества в качество. При объединении отдельных сетей крупного предприятия, имеющего филиалы в разных городах и даже странах, в единую сеть многие количественные характеристики объединенной сети превосходят некоторый критический порог, за которым начинается новое качество. В этих условиях существующие методы и подходы к решению традиционных задач сетей меньших масштабов для корпоративных сетей оказались непригодными. На первый план вышли задачи и проблемы информационной безопасности корпоративных сетей. По сети циркулирует все возрастающее количество данных, и сеть должна обеспечивать их безопасность и защищенность наряду с доступностью.

Задачи протоколов сетевой безопасности

Для того чтобы успешно внедрять и поддерживать различные механизмы информационной безопасности, оценивать системы перед выбором при приобретении, беседовать на одном языке с коллегами–профессионалами и понимать, о чем пишут в специальной литературе, необходимо иметь представление о том, какие способы защиты существуют, и, возможно, являются отраслевым стандартом в вопросах защиты информации.

Одним из видов таких стандартов являются различные протоколы безопасности. Протокол – это набор общепризнанных и поддерживаемых правил и форматов взаимодействия.

Перед тем, как применить какие–либо механизмы безопасности к объекту или субъекту, необходимо его однозначно идентифицировать (то есть узнать его системно–информационное наименование и убедиться, что оно реально соответствует объекту/субъекту), или, иначе говоря, аутентифицировать.

Поэтому первая задача протоколов безопасности — аутентификация удаленного объекта или субъекта (пользователя, системы или процесса), Практически все протоколы несут в себе аутентификацию, как одну из функций, но есть ряд протоколов предназначенных специально для аутентификации (PAP, CHAP и их подвиды; RADIUS, TACACS, Kerberos, S/Key).

Следующая задача протоколов безопасности — обеспечение защиты информации при прохождении по каналам связи, т. е. согласование ключей шифрования, шифрование данных в точке отправления, расшифрование в точке получения. Говоря о подобных протоколах, следует понимать область их приложения, относительно модели OSI или TCP/IP. Это важно учитывать при выборе конкретной модели безопасности, так как необходимо знать, какая часть информации остается видимой после криптографической обработки (адреса отправителя и получателя, другая служебная информация).

Например, протоколы прикладного уровня (механизмы шифрования в рамках конкретного бизнес–приложения или стандартные протоколы прикладного уровня, такие как SHTTP) оставляют в открытом, нешифрованном виде всю информацию, которая необходима для работы нижних уровней (номера портов, IP–адреса, последовательные номера пакетов и т. п.). Следует помнить, что эта информация остается видимой и, если покидает в таком виде локальную сеть, то дает возможному злоумышленнику некоторые дополнительные сведения о топологии сети (по адресам), о работающих приложениях (по портам) и т. д.

Протоколы транспортного уровня (SSL, Secure Shell, SOCKS) скрывают картину работы отдельных приложений, но оставляют информацию для сетевого уровня. Многие протоколы сетевого или подсетевого уровня (IPSec, PPTP) могут скрывать:

- либо только данные, пришедшие от протокола верхнего уровня (транспортного), оставляя видимыми адреса отправителя и получателя и некоторую другую информацию;
- либо полностью инкапсулировать все данные сетевого уровня, выставляя новые заголовки и окончания пакетов; такой режим работы часто еще называют туннелированием и именно он участвует в построении виртуальных частных сетей (англ. virtual private network — VPN).

Некоторые протоколы известны не только своей функциональной нагрузкой, но и задачами, которые они решают. Скажем, SSL — это де–факто сложившийся стандарт защиты интернет–соединений, в том числе при использовании систем оплаты по пластиковым картам. Сервер протокола SOCKS, обеспечивающий защиту данных между отправителем и получателем, выступает как шлюз–посредник приложений (англ. application–level proxy). Kerberos популярен как система, позволяющая пользователю аутентифицировать себя (например, вводить пароль) лишь однажды, при входе в систему, а далее получать прозрачный доступ (в рамках своих прав) ко всем ресурсам сети — механизм получил специальное название SSO — single sign–on—"один вход".

Существуют дополнительные протоколы, ориентированные на выполнение специальных задач, такие как X.509 — протокол цифровых сертификатов, указывающий, каким образом субъекты, использующие в открытой сети механизмы асимметричной криптографии, должны распространять свои открытые ключи через центры сертификации (CA — certification authority). LDAP (Lightweight Directory Access Protocol) — протокол, регулирующий доступ к данным об объектах и субъектах данной зоны управления (домена, службы каталога и т. п.).

При анализе безопасности конкретной системы необходимо выяснить, какие механизмы защиты она использует (идентификацию,

аутентификацию, защищенный обмен данными и/или управляющими сообщениями, регулирует доступ и т. д.), выяснить, на основе каких протоколов работают соответствующие механизмы, и далее делать вывод об их сильных или слабых сторонах.

Система одноразовых паролей S/Key

Система одноразовых паролей предназначена для защиты от случаев, когда злоумышленник «прослушивает» сеть, пытаясь перехватить пароль (или соответствующее ему выражение, например, значение хэф–функции) для дальнейшего но использования. В системе S/Key [RFC–1760] парольная фраза пересылается по сети только однажды и после этого больше не используется, что делает описанную атаку бессмысленной. При этом сама парольная фраза никогда не пересылается. Пароль, вводимый пользователем называется секретом, чтобы не путать его далее с самим одноразовым паролем.

Данная система основана на клиент/серверном подходе. Клиент генерирует одноразовый пароль по схеме, сервер верифицирует его.

Использование одноразового пароля происходит в три фазы:

- подготовительная – сбор данных для ввода;
- генерационная – многократное применение хэш–функции к данным;
- выывод – 64–битовый одноразовый пароль выводится в виде, удобном для восприятия пользователем.

Первоначально клиент и сервер должны быть сконфигурированы для использования единого секрета, т. е. он должен присутствовать и у клиента, и у сервера. Далее, для создания уникальности одноразового пароля, клиент и сервер должны определить случайное число и число итераций применения хэш–функции. Эти значения сервер в ответ на

запрос об аутентификации (пакет инициализации) может выслать клиенту в открытом виде (plaintext), они не являются секретными.

Протоколы удаленного доступа

К настоящему времени разработано несколько протоколов удаленного доступа. Основные из них – следующие:

SLIP (Serial Line Interface Protocol) – протокол взаимодействия с последовательной линией, который применялся с начала 80–х гг в сетях Unix,

RAS (Remote Access Service) – служба удаленного доступа, которая обеспечивает связь компьютеров под управлением операционных систем из клана Windows,

ARAP (Apple Remote Access Protocol) – протокол удаленного доступа фирмы Apple, предназначенный для организации удаленного доступа в сетях на базе протокола AppleTalk.

Наиболее распространен протокол **PPP** (Point–to–Point Protocol) – протокол "Точка–точка". Это группа протоколов, которая является стандартом Интернет. Основная задача ее – формирование кадров для передачи пакетов сетевого уровня через линию передачи данных. Метод формирования кадров, используемый PPP, обеспечивает одновременную работу через звено передачи данных нескольких протоколов сетевого уровня. Расширяемый протокол **LCP** (Link Control Protocol) – протокол управления звеном входит в состав PPP и позволяет ему функционировать в линиях передачи данных разных типов. Он позволяет согласовывать размеры пакета, потребовать проведения аутентификации системы на другой стороне линии, определить, функционирует ли звено передачи данных и при необходимости разорвать его. Протоколы семейства **NCP** (Network Control Protocol) – протоколы управления сетью также входят в PPP и предназначены для конфигурирования различных протоколов сетевого уровня, для назначения адресов. Каждый из

протоколов этого семейства предназначен для настройки и обслуживания одного из протоколов сетевого уровня, например, для настройки параметров протокола IP предназначен протокол IPCP.

Протоколы аутентификации удаленного доступа

Протоколы аутентификации удаленного доступа имеют ряд особенностей:

- возможность аутентификации удаленного компьютера до конфигурирования и начала работы протоколов сетевого и транспортного уровней, что не позволяет злоумышленнику обмениваться данными с компьютерами локальной сети до завершения фазы аутентификации;
- возможность аутентификации сервера удаленного доступа удаленным компьютером (взаимная аутентификация), что позволяет удаленному компьютеру убедиться в том, что он установил соединение с подлинным, а не подложным сервером удаленного доступа. Исключить риск использования злоумышленником полученной от удаленного компьютера секретной информации (пароля), которая может быть использована злоумышленником при обращении к подлинному серверу удаленного доступа, т.о. устраняется риск, возникающий при получении злоумышленником доступа к линии передачи данных;
- возможность проведения аутентификации в процессе работы соединения, что устраняет риск перехвата установленного звена передачи данных после проведения аутентификации между удаленным компьютером и сервером удаленного доступа;
- применение схемы аутентификации, исключающей необходимость обмена незашифрованной секретной информацией по линии передачи данных, что исключает перехват паролей;
- защита от повторного использования перехваченных данных для подложной аутентификации;

• возможность переключения на другие протоколы аутентификации удаленного доступа, что позволяет провести аутентификацию в случае, если удаленный компьютер или сервер удаленного доступа не поддерживают данный протокол аутентификации.

В настоящее время только семейство протоколов PPP включает в свой состав протоколы аутентификации, удовлетворяющие всем этим требованиям или их большинству. В процессе конфигурирования, поддержки и разрыва звена связи протокол PPP проходит через последовательность фаз. Эта последовательность приведена на рис. 13, где в скобках указаны английские названия фаз работы протокола PPP.

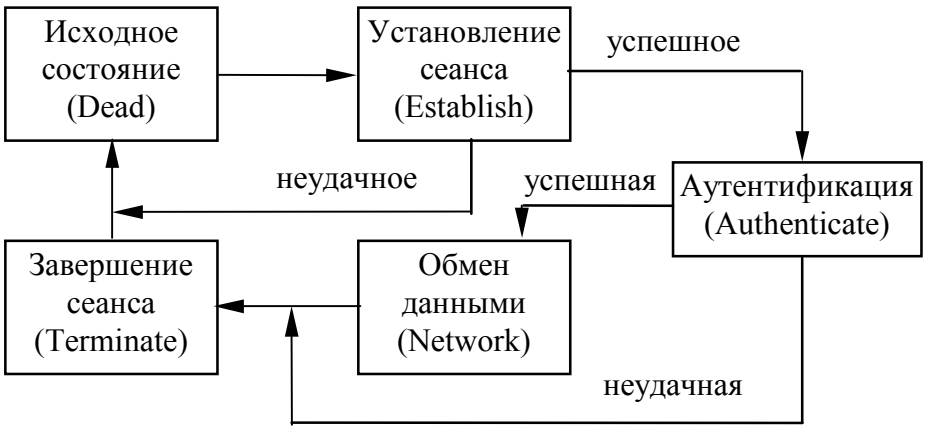

Рис. 13 Последовательность фаз работы протоколов семейства PPP

Для того, чтобы передавать данные через линию передачи данных, системы на обеих сторонах линии должны произвести обмен пакетами LCP. На этом этапе происходит настройка параметров, которые не зависят от отдельного протокола сетевого уровня. В тех случаях, когда перед настройкой параметров протоколов сетевого уровня требуется провести аутентификацию системы на противоположной стороне звена передачи данных, протокол PPP переходит в фазу аутентификации. Аутентификация должна начинаться сразу после установления звена

передачи данных, однако определение качества звена может продолжаться параллельно.

Фаза аутентификации не является обязательной и в общем случае может отсутствовать. Это означает, что в тех случаях, когда такая аутентификация все же требуется, программное обеспечение удаленного доступа на этапе установления звена передачи данных должно явно указать это. Такое указание может быть сделано любой из сторон, участвующих в соединении (как вызывающей, так и вызываемой). Если другая сторона не поддерживает предложенный протокол аутентификации, то программное обеспечение в зависимости от реализации или от его настройки может либо отказаться от установления соединения, разорвав только что установленное звено передачи данных, либо предложить аутентификацию с использованием другого протокола. Переход к фазе настройки протоколов сетевого уровня может произойти только после успешного завершения фазы аутентификации.

Протокол PPP предусматривает, что в процессе установления соединения по требованию любой из взаимодействующих систем может быть использован один из двух стандартных протоколов аутентификации. Это протокол аутентификации по паролю PAP и протокол аутентификации "вызов–отклик" CHAP. Выбор одного из этих протоколов зависит от их поддержки клиентом и сервером и от того, какую политику аутентификации выберет каждый из них.

Протокол аутентификации PAP

Протокол PAP (Password Authentication Protocol) обеспечивает простейший метод аутентификации. Он использует двухзвенную процедуру обмена пакетами. Эта процедура может отрабатываться только после установления звена передачи данных. После того, как фаза установления звена передачи данных завершена, пара значений, состоящая из идентификатора и пароля, передается по звену до тех пор,

пока аутентификация не будет подтверждена или звено не будет разорвано.

PAP не является защищенным протоколом аутентификации. Пароль передается по звену передачи данных "открытым текстом", и не существует защиты от перехвата и повторного использования пакетов, так же как и от попыток подбора пароля. Протокол предусматривает, что в том случае, если программное обеспечение использует протокол аутентификации, более защищенный, чем PAP, то оно должно предлагать использовать его в первую очередь.

В процессе аутентификации участвуют две системы. Одна из них (как правило, удаленный компьютер), чья подлинность проверяется, передает через линию передачи данных сведения, которые являются секретными и позволяют установить подлинность удаленного компьютера. Проверяющая система (как правило, сервер удаленного доступа) сравнивает эти сведения с хранящимися в базе данных управления доступом. Если они совпадают, то аутентификация считается успешно завершившейся, и пользователю удаленного компьютера предоставляется доступ к сети.

Протокол Secure–HTTP

Secure–HTTP — протокол, разработанный для обеспечения безопасности сообщений при использовании протокола HTTP и облегченной интеграции с приложениями, ориентированными на HTTP. Сохраняя все характеристики HTTP, протокол позволяет производить аутентификацию, шифрование, электронно–цифровую подпись сообщений в любой комбинации. При этом протокол поддерживает как криптографическую схему с открытыми ключами, так и симметричную схему шифрования. Протокол поддерживает гибкое определение алгоритмов шифрования с помощью возможности, называемой

переговоры о параметрах (англ. opnw. negotiation). В ней определяются три составляющих протокола:

Транзакционный модуль— т.е. будет ли запрос и/или ответ зашифрован и/или подписан.

Криптографические алгоритмы— какой алгоритм будет использоваться для шифрования (в документе указаны алгоритмы DES и RC2) и электронно–цифровой подписи (указаны RSA и DSA).

Выбор сертификата — какой из цифровых сертификатов использовать.

Следует учесть, что как протокол прикладного уровня он защищает html–документы, но оставляет открытой информацию нижележащих уровней. Это, по–видимому, одна из причин, по которой на практике S–HTTP используется не очень широко, гораздо реже, чем протоколы безопасности транспортного уровня. Поэтому слегка коснемся особенностей его реализации.

Формирование сообщения требует наличия трех составляющих.

1. Собственно сообщение формата HTTP или другие данные.

2. Криптографические предпочтения получателя и ключевая информация.

3. Криптографические предпочтения отправителя и ключевая информация.

Для создания сообщения отправитель должен произвести интеграцию криптографических предпочтений своих и получателя и, сформировав список криптографических опций, применить его с использованием соответствующей ключевой информации.

Восстановление сообщения (в HTTP формат) требует наличия четырех составляющих.

1. Собственно S–HTTP сообщение.

2. Определенные получателем ранее криптографические предпочтения и ключевая информация.

3. Текущие криптографические предпочтения получателя и ключевая информация.

4. Определенные отправителем ранее криптографические предпочтения и ключевая информация.

Для восстановления сообщения получатель, считывая заголовки, определяет, какие криптографические преобразования были произведены, и производит обратные или восстановительные преобразования на основе ключевой информации.

Отметим, что для обеспечения криптографической защиты могут быть использованы механизмы общего распределенного секрета (вводом пароля вручную или с использованием технологии Kerberos) и обмен открытыми ключами. Возможно использование сессионного ключа с помощью предварительных защищенных транзакций или иным способом.

Формат сообщения включает строку запроса, строку статуса, заголовок протокола, содержание и опции формата инкапсуляции.

Самым высоким уровнем модели OSI, на котором возможно формирование защищенных виртуальных каналов, является пятый – сеансовый. При построении защищенных виртуальных сетей на сеансовом уровне появляется возможность криптографической защиты информационного обмена, включая аутентификацию, а также реализации ряда функций посредничества между взаимодействующими сторонами.

Действительно, сеансовый уровень модели OSI отвечает за установку логических соединений и управление ими. Поэтому существует возможность применения на этом уровне программ–посредников, проверяющих допустимость запрошенных соединений и обеспечивающих выполнение других функций защиты межсетевого взаимодействия. Протоколы формирования защищенных виртуальных

каналов на сеансовом уровне прозрачны для прикладных протоколов защиты, а также высокоуровневых протоколов предоставления различных сервисов (протоколов HTTP, FTP, POPS, SMTP и др.).

Однако на сеансовом уровне начинается непосредственная зависимость от приложений, реализующих высокоуровневые протоколы. Поэтому реализация протоколов защиты информационного обмена, соответствующих данному уровню, в большинстве случаев требует внесения изменений в высокоуровневые сетевые приложения.

Для защиты информационного обмена на сеансовом уровне широкое распространение получил протокол SSL. Для выполнения на сеансовом уровне функций посредничества между взаимодействующими сторонами организацией IETF в качестве стандарта принят протокол SOCKS.

Лекция 18. Протоколы сетевой безопасности (часть 2)

Протокол SSL

Протокол SSL (Secure Socket Layer) был разработан компанией Netscape Communications для реализации защищенного обмена информацией в клиент–серверных приложениях. В настоящее время SSL применяется в качестве протокола защищенного канала, работающего на сеансовом уровне модели OSI. Этот протокол использует криптографические методы защиты информации для обеспечения безопасности обмена данными. SSL выполняет все функции по созданию защищенного канала между двумя абонентами сети, включая их взаимную аутентификацию, обеспечение конфиденциальности, целостности и аутентичности передаваемых данных. Ядром протокола

является технология комплексного использования асимметричных и симметричных криптосистем.

Взаимная аутентификация обеих сторон в SSL выполняется путем обмена цифровыми сертификатами открытых ключей пользователей (клиента и сервера), заверенными цифровой подписью специальных сертификационных центров. Протокол SSL поддерживает сертификаты, соответствующие общепринятому стандарту X.509, а также стандарты инфраструктуры открытых ключей PKI, с помощью которой организуется выдача и проверка подлинности сертификатов.

Конфиденциальность обеспечивается шифрованием передаваемых сообщений с использованием симметричных сессионных ключей, которыми стороны обмениваются при установлении соединения. Сессионные ключи передаются также в зашифрованном виде; при этом они шифруются с помощью открытых ключей, извлеченных из сертификатов абонентов. Подлинность и целостность циркулирующей информации обеспечиваются за счет формирования и проверки электронной цифровой подписи.

В качестве алгоритмов асимметричного шифрования используются RSA и алгоритм Диффи–Хеллмана. Допустимые алгоритмы симметричного шифрования – RC2, RC4, DES, а также 3DES. Для вычисления хэш–функций могут применяv4ться стандарты MD5 и SHA–1. В протоколе SSL версии 3.0 набор криптографических алгоритмов является расширяемым.

Согласно протоколу SSL криптозащищенные туннели создаются между конечными точками виртуальной сети. В качестве инициаторов каждого защищенного туннеля выступают клиент и сервер, функционирующие на компьютерах в конечных точках туннеля (рис.14).

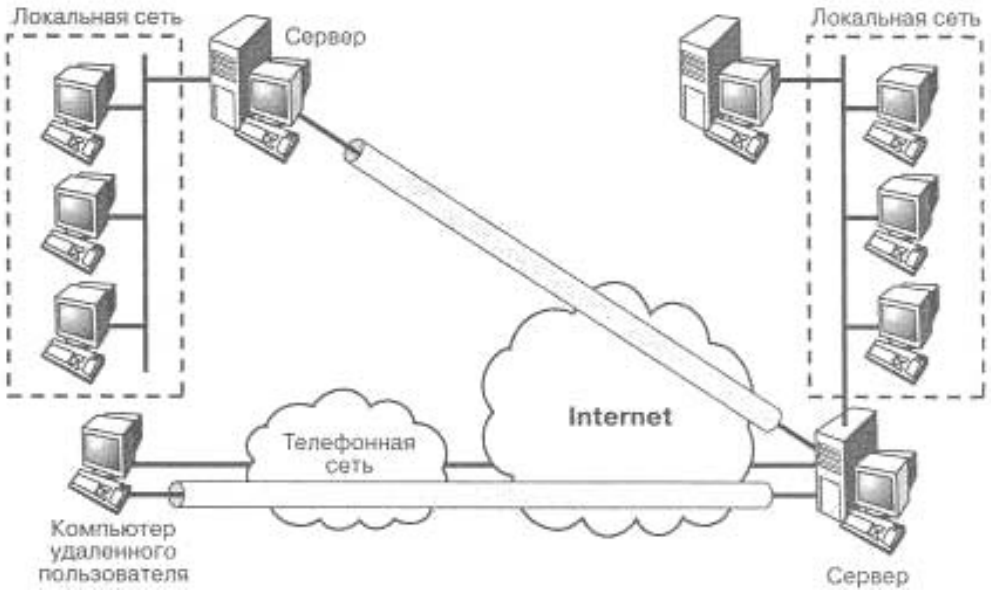

Рис. 14. Криптозащищенные туннели, сформированные на основе протокола SSL

Протокол SSL предусматривает следующие этапы взаимодействия клиента и сервера при формировании и поддержке защищаемого соединения:

- установление SSL–сессии;
- защищенное взаимодействие.

В процессе установления SSL–сессии решаются следующие задачи:

- аутентификация сторон;
- согласование криптографических алгоритмов и алгоритмов сжатия, которые будут использоваться при защищенном информационном обмене;
- формирование общего секретного мастер–ключа;
- генерация на основе сформированного мастер–ключа общих секретных сеансовых ключей для криптозащиты информационного обмена.

Процедура установления SSL–сессии, называемая также процедурой рукопожатия, отрабатывается перед непосредственной защитой информационного обмена и выполняется по протоколу начального приветствия (Handshake Protocol), входящему в состав протокола SSL.

При установлении повторных соединений между клиентом и сервером стороны могут, по взаимному соглашению, формировать новые сеансовые ключи на основе «старого» общего «секрета» (данная процедура называется «продолжением» SSL–сессии).

Соответствие между открытыми ключами и их владельцами устанавливается с помощью цифровых сертификатов, выдаваемых специальными центрами сертификации. Сертификат представляет собой блок данных, содержащий следующую информацию:

- имя центра сертификации;
- имя владельца сертификата;
- открытый ключ владельца сертификата;
- срок действия сертификата;
- идентификатор и параметры криптоалгоритма, который должен использоваться при обработке сертификата;
- цифровую подпись центра сертификации, заверяющую все данные в составе сертификата.

Цифровая подпись центра сертификации в составе сертификата обеспечивает достоверность и однозначность соответствия открытого ключа и его владельца. Центр сертификации исполняет роль нотариуса, заверяющего подлинность открытых ключей, что позволяет их владельцам пользоваться услугами защищенного взаимодействия без предварительной личной встречи. Одним из таких центров в Internet является компания Verisign, учрежденная фирмой RSA Data Security Inc., при участии компаний Visa, IBM, Netscape, Microsoft и Oracle.

Протокол SSL поддерживается программным обеспечением серверов и клиентов, выпускаемых ведущими западными компаниями. Однако в нашей стране существуют обстоятельства, препятствующие распространению данного протокола и принятию его в качестве базового для реализации приложений, требующих защищенного информационного взаимодействия участвующих сторон.

К числу существенных недостатков протокола SSL относится тот факт, что практически все продукты, поддерживающие SSL, реализованы в США и из–за экспортных ограничений доступны лишь в усеченном варианте (с длиной сеансового ключа 40 бит для алгоритмов симметричного шифрования и 512 бит для алгоритма RSA, используемого на этапе установления SSL–сессии), чего на сегодняшний день явно недостаточно. При нынешнем уровне развития вычислительной техники это позволяет проводить на данный протокол криптоаналитические атаки методом «грубой силы».

Ограничения на длину допустимых ключей шифрования относятся и к криптографическим модулям популярных Web–навигаторов – Netscape Navigator и Netscape Communicator компании Netscape, а также Internet Explorer от Microsoft.

Следует отметить, что последние экспортные релизы этих продуктов все же поддерживают ряд алгоритмов с достаточной длиной ключа, но с особыми ограничениями. Например, экспортная версия Netscape Communicator 4.0 содержит исполняемый код алгоритмов RC (128 бит) и 3DES (168 бит). Однако он задействуется только при особых условиях. Экспортный Netscape устанавливает соединение, защищенное стойкой криптографией, только с серверами, входящими в определенный список, поддерживаемый сертификатором VeriSign Inc. За пределами США VeriSign предоставляет такие права лишь серверам лицензированных банков. Подобные ограничения содержит и экспортный

Internet Explorer. Возникают также трудности создания и использования национальных центров сертификации.

Недостатки SSL и TLS проявляются и в том, что для транспортировки своих сообщений эти протоколы используют всего один протокол сетевого уровня – IP и, следовательно, могут работать только в IP–сетях. Кроме того, применение на практике защитных свойств SSL/TLS не в полной мере прозрачно для прикладных протоколов.

Еще одна негативная особенность SSL — возобновляемые сессии, суть которых заключается в том, что если клиент и сервер разорвали соединение, они могут возобновить его, проведя минимальный обмен данными, и использовать старый параметр Session ID. Злоумышленник, скомпрометировав одну из предыдущих сессий, может провести с сервером процедуру ее восстановления. Как следствие, будут скомпрометированы все последующие данные, передаваемые в текущей сессии.

Кроме того, в SSL для аутентификации и шифрования используются одинаковые ключи, что при определенных условиях может привести к потенциальной уязвимости. Подобное решение дает возможность собрать больше статистического материала, чем при аутентификации и шифровании разными ключами. Как и другие программные продукты, SSL подвержен атакам, связанным с недоверенной программной средой, внедрением программ–закладок и др.

Протокол SOCKS

Протокол SOCKS, автором которого является Давид Коблас (David Coblas), известен с 1990 года. Этот протокол организует процедуру взаимодействия клиент–серверных приложений на сеансовом уровне модели OSI через сервер–посредник или proxy–сервер.

В общем случае программы–посредники, которые традиционно используются в межсетевых экранах, могут выполнять следующие функции:

- идентификацию и аутентификацию пользователей;
- криптозащиту передаваемых данных;
- разграничение доступа к ресурсам внутренней сети;
- разграничение доступа к ресурсам внешней сети;
- фильтрацию и преобразование потока сообщений, например, поиск вирусов и прозрачное шифрование информации;
- трансляцию внутренних сетевых адресов для исходящих потоков сообщений.

Сначала протокол SOCKS разрабатывался только для перенаправления запросов к серверам со стороны клиентских приложений, а также возврата этим приложениям полученных ответов. Перенаправление запросов и ответов между клиент–серверными приложениями уже позволяет реализовать функцию трансляции сетевых IP–адресов NAT (Network Address Translation). Замена у исходящих пакетов внутренних IP–адресов отправителей одним IP–адресом шлюза позволяет скрыть топологию внутренней сети от внешних пользователей и тем самым усложнить задачу несанкционированного доступа. Трансляция сетевых адресов помимо повышения безопасности позволяет расширить внутреннее адресное пространство сети за счет возможности поддержки собственной системы адресации.

На основе протокола SOCKS могут быть реализованы и другие функции посредничества по защите сетевого взаимодействия. Например, протокол SOCKS может применяться для контроля над направлениями информационных потоков и разграничения доступа в зависимости от атрибутов пользователей и информации. Эффективность использования

протокола SOCKS для выполнения функций посредничества обеспечивается его ориентацией на сеансовый уровень модели OSI. По сравнению с посредниками прикладного уровня на сеансовом достигаются более высокое быстродействие и независимость от высокоуровневых протоколов (HTTP, FTP, POP3, SMTP и др.).

Кроме того, протокол SOCKS не привязан к протоколу IP и не зависит от операционных систем. Например, для обмена информацией между клиентскими приложениями и посредником может использоваться протокол IPX.

Благодаря протоколу SOCKS межсетевые экраны и виртуальные частные сети могут организовать безопасное взаимодействие и обмен информацией между разными сетями. Протокол SOCKS позволяет реализовать безопасное управление этими системами на основе унифицированной стратегии. Следует отметить, что на основе протокола SOCKS могут создаваться защищенные туннели для каждого приложения и сеанса в отдельности.

Согласно спецификации протокола SOCKS различают *SOCKS–сервер,* который целесообразно устанавливать на шлюз (межсетевой экран) сети, и *SOCKS–клиент,* который устанавливают на каждый пользовательский компьютер. SOCKS–сервер обеспечивает взаимодействие с любым прикладным сервером от имени соответствующего этому серверу прикладного клиента. SOCKS–клиент предназначен для перехвата всех запросов к прикладному серверу со стороны клиента и передачи их SOCKS–серверу. Следует отметить, что SOCKS–клиенты, выполняющие перехват запросов клиентских приложений и осуществляющие взаимодействие с SOCKS–сервером, могут быть встроены в универсальные клиентские программы. SOCKS–серверу известно о графике на уровне сеанса (сокета), поэтому он может осуществлять тщательный контроль и, в частности, блокировать работу

конкретных приложений пользователей, если они не имеют необходимых полномочий на информационный обмен.

В настоящее время протокол SOCKS версии 5 одобрен организацией IETF в качестве стандарта Internet и включен в RFC 1928.

Общая схема установления соединения по протоколу SOCKS выглядит следующим образом:

- клиент, желающий установить связь с каким–либо сервером в сети, соединяется вместо этого с SOCKS–сервером (специализированным proxy–сервером) и посылает ему запрос с сообщением IP–адреса и порта удаленного сервера, с которым ему необходимо связаться;
- SOCKS–сервер соединяется с удаленным сервером–адресатом;
- клиент и удаленный сервер взаимодействуют друг с другом по цепочке соединений, SOCKS–сервер просто ретранслирует данные.

Протокол SOCKS 5 является существенным развитием четвертой версии. Он реализует следующие возможности:

- предусмотрена аутентификация пользователей, от имени которых обращаются SOCKS–клиенты. SOCKS–сервер может согласовывать с SOCKS–клиентом способ аутентификации. Она делает возможным разграничение доступа к компьютерным ресурсам. Допускается также двусторонняя аутентификация, то есть пользователь может, в свою очередь, убедиться, что соединился с нужным SOCKS–сервером;
- допускается использование доменных имен: SOCKS–клиент может передавать SOCKS–серверу не только IP–адрес компьютера, с которым необходимо установить соединение, но и его DNS–имя;
- поддерживается не только протокол TCP, но и протокол UDP.

Общая схема установления соединения по протоколу SOCKS версии 5 может быть описана следующим образом:

- запрос прикладного клиента, желающего установить соединение с каким–либо прикладным сервером в сети, перехватывается установленным на этом же компьютере SOCKS–клиентом;
- соединившись с SOCKS–сервером, SOCKS–клиент сообщает ему идентификаторы всех методов аутентификации, которые он поддерживает;
- SOCKS–сервер решает, каким методом аутентификации воспользоваться (если SOCKS–сервер не поддерживает ни один из методов аутентификации, предложенных SOCKS–клиентом, соединение разрывается);
- при поддержке каких–либо предложенных методов аутентификации SOCKS–сервер в соответствии с выбранным методом аутентифицирует пользователя, от имени которого выступает SOCKS–клиент. В случае безуспешной аутентификации SOCKS–сервер разрывает соединение;
- после успешной аутентификации SOCKS–клиент передает SOCKS–сервер DNS–имя или IP–адрес запрашиваемого прикладного сервера в сети, и далее SOCKS–сервер на основе имеющихся правил разграничения доступа принимает решение об установлении соединения с этим прикладным сервером;
- в случае установления соединения прикладной клиент и прикладной сервер взаимодействуют друг с другом по цепочке соединений, в которой SOCKS–сервер ретранслирует данные, а также может выполнять функции посредничества по защите сетевого взаимодействия; например, если в ходе аутентификации SOCKS–клиент и SOCKS–сервер обменялись сеансовым ключом, то весь трафик между ними может шифроваться.

Аутентификация пользователя, выполняемая SOCKS–сервером, может основываться на цифровых сертификатах в формате X.509 или

паролях. Для шифрования графика между SOCKS–клиентом и SOCKS–сервером используются протоколы, ориентированные на сеансовый или более низкие уровни модели OSI. Кроме аутентификации пользователей, трансляции IP–адресов и криптозащиты графика SOCKS–сервер выполняет также следующие функции:

- разграничение доступа к ресурсам внутренней сети;
- разграничение доступа к ресурсам внешней сети;
- фильтрацию потока сообщений, например динамический поиск вирусов;
- регистрацию событий и реагирование на задаваемые события;
- кэширование данных, запрашиваемых из внешней сети.

Протокол SOCKS осуществляет встроенную поддержку популярных Web–навигаторов Netscape Navigator и Netscape Communicator компании Netscape, а также Internet Explorer компании Microsoft.

Специальные программы, называемые соксификаторами, дополняют клиентские приложения поддержкой протокола SOCKS. К таким программам относится, например, NEC SocksCap и др. При установке соксификатор внедряется между пользовательскими приложениями и стеком коммуникационных протоколов. Далее в процессе работы он перехватывает коммуникационные вызовы, формируемые приложениями, и перенаправляет их в случае надобности на SOCKS–сервер. При отсутствии нарушений установленных правил безопасности работа SOCKS клиента совершенно прозрачна для клиентских приложений и пользователей.

Таким образом, для формирования защищенных виртуальных сетей по протоколу SOCKS в точке сопряжения каждой локальной сети с Internet на компьютере–шлюзе устанавливается SOCKS–сервер, а на рабочих станциях в локальных сетях и на компьютерах удаленных

пользователей – SOCKS–клиенты. По существу, SOCKS–сервер можно рассматривать как межсетевой экран (рис. 15).

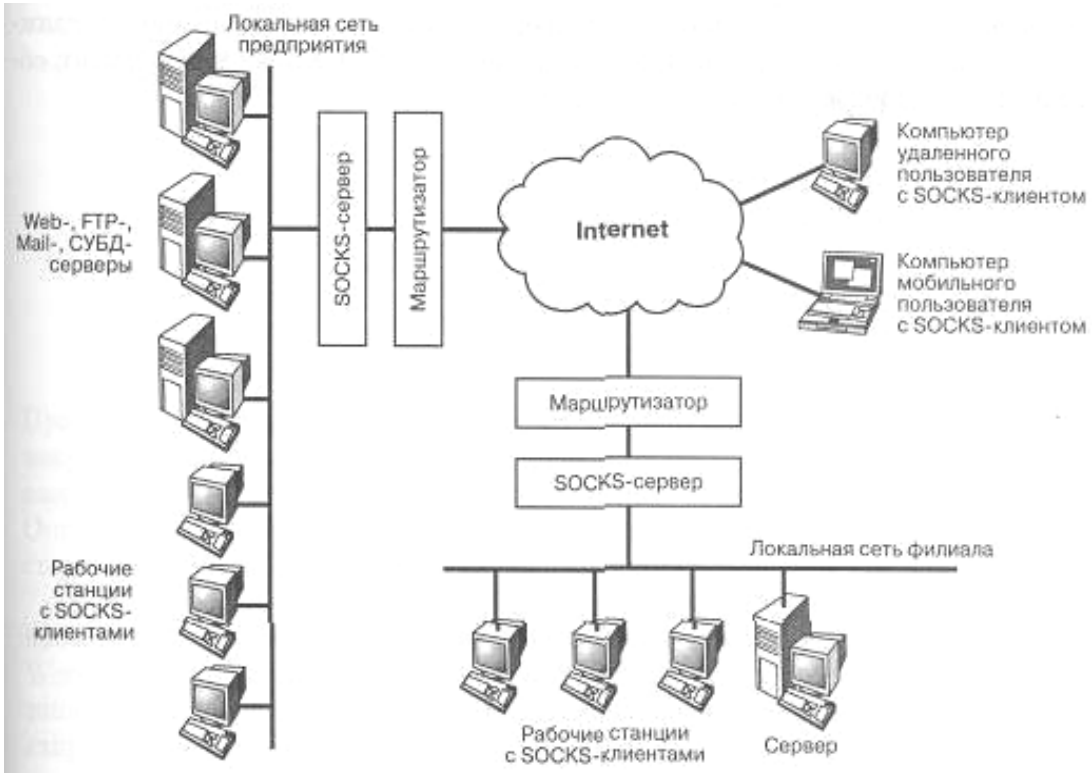

Рис. 15. Схема взаимодействия по протоколу SOCKS

Удаленные пользователи могут подключаться к Internet любым способом – по коммутируемой или выделенной линии. При попытке пользователя защищенной виртуальной сети установить соединение с каким–либо прикладным сервером SOCKS–клиент начинает взаимодействовать с SOCKS–сервером. По завершении первого этапа взаимодействия пользователь будет аутентифицирован, а проверка правил доступа покажет, имеет ли он право соединиться с конкретным серверным приложением, функционирующим на компьютере с указанным адресом. Дальнейшее взаимодействие может происходить по криптографически защищенному каналу.

Помимо задачи защиты локальной сети от несанкционированного доступа на SOCKS–сервер может возлагаться контроль доступа пользователей этой локальной сети к открытым ресурсам Internet (Telnet, WWW, SMTP, POP и др.). Доступ полностью авторизован, так как идентифицируются и аутентифицируются конкретные пользователи, а не компьютеры, с которых они входят в сеть. Правила доступа могут запрещать или разрешать соединения с конкретными ресурсами Internet в зависимости от полномочий конкретного сотрудника. Действие правил доступа может определяться и другими параметрами, например методом аутентификации или временем суток. В дополнение к функциям разграничения доступа могут выполняться регистрация событий и реагирование на задаваемые события. Для достижения более высокой степени безопасности сетевого взаимодействия серверы локальной сети, к которым разрешен доступ со стороны Internet, должны быть выделены в отдельный подсоединяемый к SOCKS–серверу сегмент, образующий защищаемую открытую подсеть.

Лекция 19. Обеспечение безопасности локальных вычислительных систем при подключении к глобальным сетям с использованием криптографических протоколов

Общая характеристика стека протоколов TCP/IP

Одним из важных составных элементов системы информационной безопасности компьютерной сети АСТНК является система безопасности сетевых коммуникаций. Оценка безопасности коммуникаций базируется на изучении возможностей используемых протоколов обмена данными по защите данных от модификации и несанкционированного просмотра.

Выбор для исследований стека протоколов *TCP/IP* обусловлен широким распространением сетей данной архитектуры и объединением их в глобальную сеть *Internet.* Сеть построена в соответствии с четырехуровневой моделью *DARPA.* Структурная схема модели приведена на рис.16.

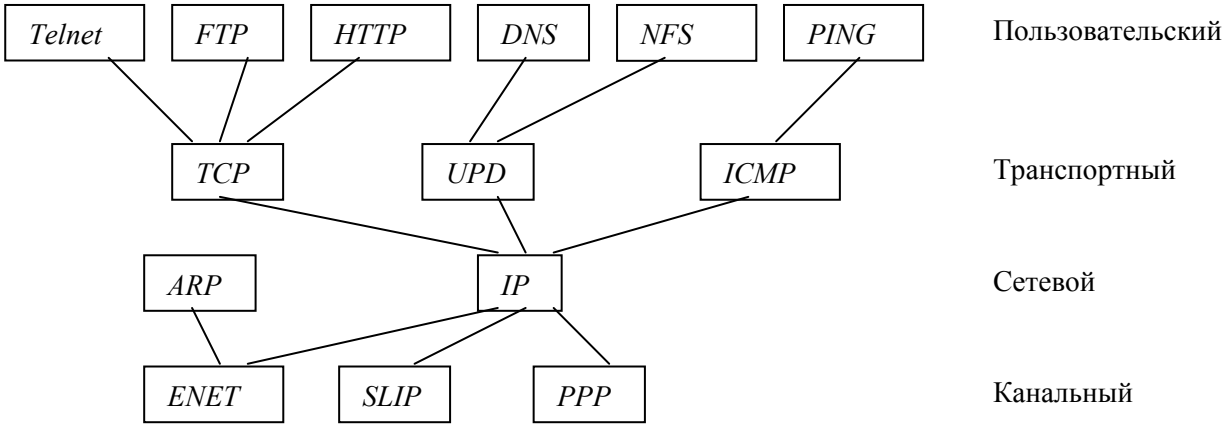

Рис. 16. Структурная схема четырехуровневой модели *DARPA.*

Известно, что ни один из уровней *TCP/IP* своими стандартными средствами не обеспечивает защиты от просмотра нарушителем передаваемой по сети информации.

Особенности размещения криптографических протоколов на различных уровнях в сетях на базе протокола TCP/IP

В стеке коммуникационных протоколов *TCP/IP* различают физический, или канальный, сетевой (Интернет), транспортный и прикладной уровни.

Криптографические средства можно размещать на всех уровнях.. Все зависит от требуемых услуг безопасности и окружения. Располагая криптографические средства на низком уровне, мы тем самым при минимуме криптографических средств автоматически получаем высокую

степень совместимости и большое удобство при использовании самых различных приложений и прикладных программ.

Наоборот, при размещении криптографических средств на высоком уровне мы сталкиваемся с необходимостью учета индивидуальных особенностей большого спектра различных протоколов высокого уровня, имеющих свою специфику, что приводит к целому ряду ограничений и требований, которые необходимо соблюдать при использовании таких криптографических средств.

Рассмотрим отдельно каждый из уровней.

Физический, или канальный уровень.

Шифрование трафика (соединения) на физическом уровне осуществляется с помощью скремблеров, шифрующих модемов, специализированных канальных адаптеров.

Достоинства: простота применения, аппаратная реализация, полное закрытие трафика, прозрачность шифрования.

Недостатки: негибкость решения (фиксированный тип канала, фиксированная производительность), сложность адаптации к етевой топологии, низкая совместимость, высокая стоимость.

Стандартные реализации канального уровня не предусматривают использования надежных методов идентификации и защиты информации от несанкционированного просмотра. В стандартном режиме идентификация–аутентификация абонентов осуществляется только по сетевым (MAC) адресам при использовании сред передачи информации с собственной адресацией (таких, как *Ethernet)*. Средств защиты от просмотра нет.Для защиты информации на канальном уровне предложены протоколы, использующие криптографические механизмы защиты информации. Наиболее известными являются *PPTP* (совместная разработка фирм

Microsoft, 3COM и др.) Фирмой *Cisco Systems* разработаны протоколы *L2F* и *L2TP,* однако, они еще не окончательно стандартизованы.

Сетевой уровень

Подсети взаимодействуют между собой через маршрутизаторы. Поскольку маршрутизация производится на сетевом уровне (модуль *IP),* наличие транспортного и прикладного уровней на данных устройствах необязательно. Таким образом, защищенными от НСД, осуществляемого путем просмотра сетевого трафика, могут быть только протоколы, использующие шифрование передаваемых данных. При этом необходимо, чтобы эти протоколы использовали методы идентификации–аутентификации, не зависящие от средств идентификации *TCP/IP.*

Для защиты информации криптографическими методами был разработан протокол *IPSec.* Протокол предусматривает использование многих алгоритмов шифрования, ни один из которых не является доверенным. Отсюда следует, что использование стандартных средств защиты на сетевом уровне не может в достаточной степени защитить информацию, поскольку использование сертифицированных алгоритмов приводит к изменению стандартов.

Тем не менее, на сетевом уровне можно построить систему прозрачного шифрования информации с использованием отечественных алгоритмов с необходимой стойкостью.

В этом случае необходимо заменить или усилить только один *IP*–модуль. Основное преимущество такого расположения криптографических механизмов заключается в том, что *IP* уровень является стандартным для всех интернет–сетей и любое приложение будет работать стандартным образом. Необходимо только модифицировать *TCP/IP–модуль.*

Это позволяет строить закрытые виртуальные защищенные сети на базе открытых глобальных сетей.

Примеры протоколов сетевого уровня: IPSP/IKMP (IP Secure Protocol/Internet Key Management Protocol), IOST/MKMP (Secure Tunnel Protocol/Modular Key Management Protocol), SKIP, Photurus, SKEME, ISAKMP, OAKLEY.

Транспортный уровень

К транспортному уровню TCP/IP относятся User Datagram Protocol (UDP) I и Transmission Control Protocol (TCP).

Основной функцией протоколов транспортного уровня *UDP* является мультиплексирование–демультиплексирование пакетов, проходящих с сетевого уровня на пользовательский и обратно. Модуль UDP может не контролировать целостность пакетов, хотя такая возможность предусмотрена.

Модуль TCP осуществляет контроль доставки информации и контроль ее целостности. Протокол TCP не содержит никаких механизмов защиты информации от несанкционированного просмотра и надежной идентификации–аутентификации. Для защиты обмена информацией на транспортном уровне обычно используются протоколы SSH (Secure Shell), SSL (Secure Socket Layer) и его более новая версия TLS (Transport Layer Security Protocol), PCT (Private Communication Technology). Эти протоколы с точки зрения четырехуровневой модели DARPA расположены между прикладным и транспортным уровнями. В силу наличия незащищенных каналов воздействия на модуль TCP данный протокол не в полной мере обеспечивает безопасность информации при активном воздействии нарушителя на защищенные хосты, хотя и защищает информацию от просмотра непосредственно в канале.

Известно, что безопасность сетевого уровня может быть основана на базе протоколов типа «точка – точка», что означает, что закрытые каналы связи могут быть установлены между прикладными процессами и что эти каналы

могут быть использованы для передачи аутентификационной и конфиденциальной информации. (это очень удобно для применения в электронной коммерции).

Отметим, что пользователям для применения этих средств не нужно ничего знать ни о технических подробностях и особенностях обеспечения безопасности на транспортном уровне, ни о том, как он функционирует. (Именно так и сделано, например, в Netscape Navigator.)

Расположение криптографических средств на этом уровне позволяет так же, как и на сетевом уровне, строить закрытые виртуальные сети на базе открытых глобальных сетей.

Прикладной уровень

Стандартные средства прикладного уровня не предусматривают защиты информации от несанкционированного просмотра. Идентификация–аутентификация абонентов осуществляется по IP – адресам получателя и отправителя и портам отправителя и получателя.

При расположении криптографических средств на прикладном уровне не требуется никаких модификаций ни для программного TCP/IP – модуля, ни для сетевого программного интерфейса. Все модификации ограничены прикладным уровнем. Это означает, что, во–первых, прикладные протоколы должны быть модифицированы так, чтобы они обеспечивали услуги безопасности, и, во–вторых, что сами прикладные программы, использующие эти протоколы, должны быть также, соответственно, модифицированы.

Таким образом, безопасность прикладного уровня сосредоточена на прикладном уровне. Это и является основным преимуществом такого решения, так как все более нижние уровни не нуждаются в модификациях. Этот подход оказывается очень удобным для применений в тех сетях, где сетевая инфраструктура не может быть модифицирована.

Для защиты информации криптографическими методами на прикладном уровне используются протоколы Secure Telnet, Secure FTP, Secure RPC Authentication, PEM (Privacy Enhanced Mail), Secure MIME (S/MIME), Secure http и другие.

Для безопасного администрирования (при отсутствии выделенного канала) обычно используется протокол SSH. Для защиты электронных транзакций широко применяется протокол SET (Secure Electronic Transaction*)*.

Для управления ключами и шифрования информации применяется протокол SKIP (Simple Key management for Internet Protocol) или протокол удаленной аутентификации с одновременным распределением ключей *Kerberos.*

Общим у всех перечисленных протоколов является использование всех уровней стека TCP/IP.

Выше прикладного уровня

Данный подход основан на том, что все прикладные данные заранее преобразуются таким образом, чтобы они могли быть переданы непосредственно с помощью существующего протокола прикладного уровня и чтобы при этом были реализованы необходимые службы и обеспечивался необходимый уровень безопасности.

Примеры: PGP, средства криптографической защиты документов Microsoft Office.

Необходимо отметить , что в условиях активного воздействия на защищаемые хосты никакие меры, за исключением использования технологии VPN на сетевом уровне, в общем случае не дают гарантий защиты информации от навязывания и несанкционированного просмотра. Поэтому рассмотрим эту технологию более подробно.

Построение замкнутых подсетей (VPN) с гарантированной надежностью защиты

Таким образом, установлено что встроенные на различных уровнях семейства протоколов *TCP/IP* штатные средства протокола не обеспечитвают защиту ни от навязывания ложной информации, ни от перлюстрации информации при передаче ее в глобальных сетях в условиях активного НСД. Более того, поскольку ПО современных сетевых ОС практически никогда не бывает доверенным, использование различных средств защиты информации методами шифрования, в общем случае, никогда не обеспечивает заранее заданный уровень доверия к степени защищенности информации.

Отметим, что речь идет о задаче построения системы, стойкость которой к удаленному НСД определяется стойкостью используемой криптосхемы.

Пусть Ω обозначает объединение всех подсетей сети Internet. Каждая подсеть состоит из непустого множества хостов, один хост также может рассматриваться как подсеть. Пример включения двух подсетей в Internet изображен на рис. 16.

Пусть любые хосты, входящие в подсети множества Ω, могут обмениваться между собой информацией по сети. Назовем потоком информации между хостами A и B множество пакетов, передаваемых по сети от хоста A хосту B и обратно.

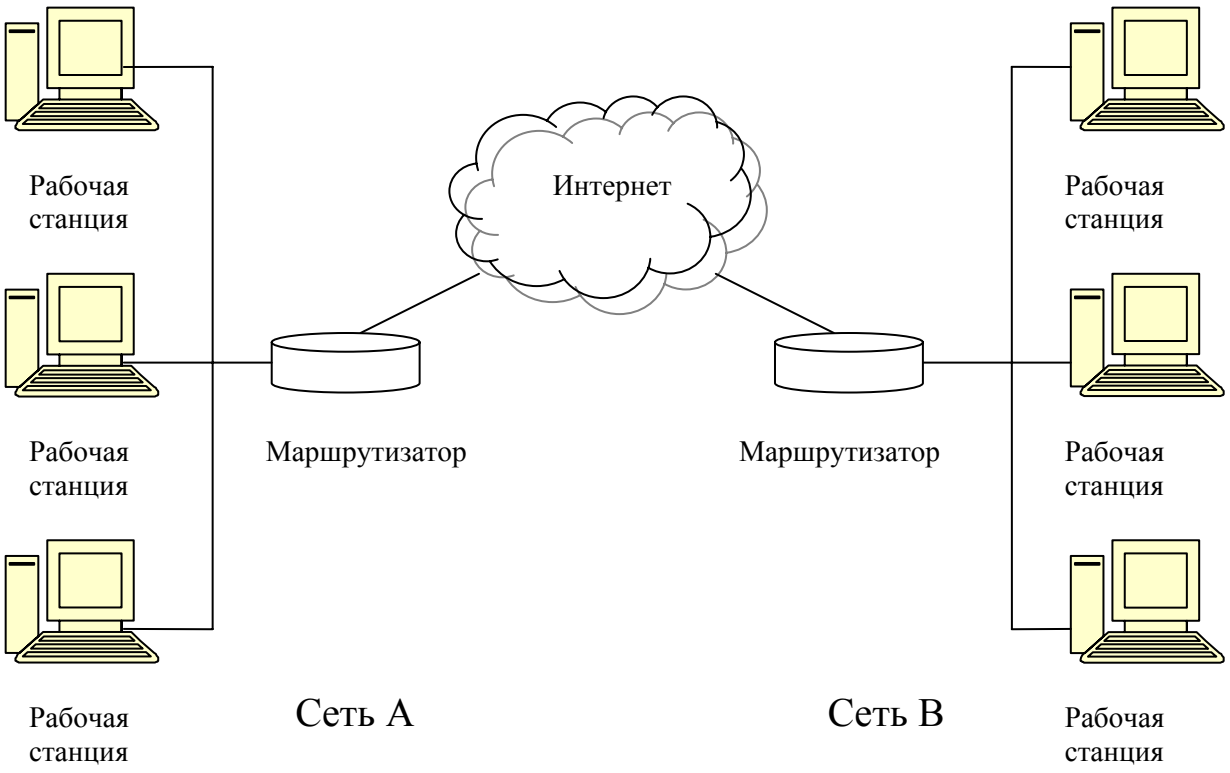

Рис. 16. Включение двух сетей к Internet.

Выберем две подсети A и B из Ω. Пусть эти подсети обмениваются информацией через Internet. Обозначим через I(A) поток информации, порождаемый подсетью A. Обозначим I(A–>B) поток информации из подсети A в подсеть B. В данных обозначениях:

$I(A \cup B) = I(A) \cup I(B);$ (1)

$I(A) = \cup_{a \in A} I(a);$ (2)

$I(A \cap B) = I(A) \cap I(B)$ (3)

$I(A,B) = I(A \text{–>} B) \cup I(B \text{–>} A)$ (4)

$I(A) = \cup_{A \in \Omega} I(A,B)$ (5)

Формула (4) описывает качественный состав потока информации между подсетями A и B.

Определение 1. Множество подсетей назовем информационно замкнутым (ИЗ), если хосты этого множества подсетей могут обмениваться

информацией только между собой. Остальные множества назовем информационно открытыми (ИО).

Из определения 1 следует,что ИЗ–множество подсетей $\Psi \subset \Omega$ должно обладать следующими свойствами:

- для любого $g \notin \Psi$ и любого $h \in \Psi$, $I(g,h) = I(h,g) = \varnothing$;
- должно быть исключено использование внутренними хостами внешних информационных ресурсов.

Для обеспечения информационного замыкания подсети А необходимо закрыть информационные потоки, выходящие из этой подсети в открытую сеть, а также исключить получение и обработку информации из незакрытых потоков, исходящих от внешних узлов сети. Для закрытия информационных потоков необходимо использовать шифрование с заданной стойкостью, так как другие маскирующие преобразования, не зависящие от секретного ключа, потенциально могут быть раскрыты противником.

Взяв за основу схему взаимодействия подсистем четырехуровневой модели DARPA, найдем в ней уровень, наиболее приемлемый для внедрения процедуры шифрования потоков передаваемой информации.

Утверждение 1. Для построения надежной системы защиты информации с использованием шифрования, удовлетворяющей постановке задачи, необходимо встроить модуль шифрования информации на сетевом уровне.

Доказательство. Рассмотрим четырехуровневую модель построения стека протоколов TCP–IP. Рассмотрим подробнее достоинства и недостатки встраивания систем шифрования на каждом уровне в отдельности.

Канальный уровень. Основным достоинством построения такой системы защиты будет прозрачность (это основное требование и оно здесь выполнено) системы защиты относительно любых протоколов прикладного уровня.

Недостатками будут:

- необходимость дублирования системы шифрования для всех типов протоколов канального уровня, используемых на данном хосте;
- защита информации только в рамках одного сегмента сети.

Сетевой уровень. Размещение системы шифрования на сетевом уровне имеет один недостаток – открытость канального уровня для атак извне. Достоинствами размещения системы шифрования на сетевом уровне являются:

- прозрачность для протоколов верхнего уровня;
- защищенность транспортного и прикладного уровней данного хоста (вообще говоря, наличие этих уровней необязательно);
- простота анализа ПО (сетевой уровень самый простой);
- возможность автоматического гарантирования отсутствия путей обхода шифрующего модуля.

Транспортный уровень. В рамках данного стека протоколов из свойств функций, реализованных на транспортном уровне, следует, что:

- для закрытия всех потоков информации необходимо дублировать систему шифрования (для *TCP* и *UDP* отдельно);
- модуль *TCP* имеет большую сложность. В силу этой причины, проверка соответствия реализованной криптосхемы, интерфейсов криптографического модуля и доказательство отсутствия путей обхода системы шифрования становятся сложной проблемой;
- не все сетевые устройства содержат транспортный уровень.
- сетевой уровень открыт для атак извне;
- необходимость сильной модификации модуля сетевого уровня для построения системы прозрачной защиты подсетей.

Это недостатки. Достоинства:

гарантирование доставки информации, что приводит к экономии ключей шифрования;

- прозрачность зашиты для приложений прикладного уровня, функционирующих на данном хосте.

Прикладной уровень. При размещении системы шифрования на прикладном уровне возможны два варианта:

- система защищает только одно приложение;
- система стоит «на проходе», то есть представляет собой proxy–сервер, осуществляющий шифрование информации.

Ясно, что в первом случае не обеспечивается прозрачность для любых приложений, а во втором – появляются пути обхода, наличие которых зависит от администрирования системы.

Отсюда следует, что для построения системы защиты, обладающей заданными свойствами системы защиты информации, необходимо встроить систему шифрования на сетевом уровне.

Лекция 20. Синтез защищенных виртуальных систем. Описание протокола IPsec. Назначение протокола Ipsec

Протокол IPsec

Протокол IPsec был создан Группой разработки технологий Интернет (Internet Engineering Task Force, IETF, тематическая группа по безопасности IP, IP Security Working Group) как базовый протокол обеспечения безопасности данных на уровне IP–соединений.

IPsec обеспечивает аутентификацию абонентов и управление удаленным доступом, аутентификацию, конфиденциальность и целостность данных, защиту от анализа и воспроизведения трафика.

IPsec может быть применен для создания сквозных защищенных каналов между произвольными IP–хостами и/или группами хостов (т.н. транспортный режим), защищенных каналов между шлюзами отдельных подсетей (туннельный режим) и виртуальных закрытых сетей (Virtual Private Network, VPN), обеспечивающих безопасность и конфиденциальность взаимодействия отдельных фрагментов или подсетей территориально распределенной VPN, связанных между собой не напрямую, а через другие сети. Для каждого IP–соединения, то есть для каждой пары IP–адресов респондентов (отправителя и получателя), или для групп IP–адресов, задается своя политика безопасности, определяющая принципы применения IPsec и набор входящих в его состав средств обеспечения безопасности соединения и защиты данных. При реализации протокола IPsec в сетевой архитектуре появляется единый защищенный канал, через который проходит трафик всех без исключения сетевых приложений или сервисов.

Архитектура IPsec

Архитектура и спецификации протокола IPsec описаны в документах тематической группы IETF по безопасности IP. Основными составляющими IPsec, согласно, являются протокол аутентификации AH (Authentication Header) и протокол инкапсулирующей защиты данных ESP (Encapsulating Security Payload). Эти протоколы составляют «видимую», интерфейсную часть IPsec. Для решения задач защиты данных AH и ESP используют криптографические алгоритмы аутентификации и шифрования, которые с точки зрения архитектуры IPsec являются ее внутренними элементами. Протоколы AH и ESP обеспечивает аутентификацию и криптографическую защиту передаваемых по сети данных, но не имеют собственных средств установления защищенных соединений и согласования параметров

сессии по открытым каналам связи. Для согласования параметров сессии (т.е. выбора алгоритмов аутентификации и шифрования, их параметров и режимов, и обмена ключами) применяются протоколы управления ключами, входящими в состав системы IKE (Internet Key Exchange). В определенном смысле данные протоколы являются внешними по отношению к архитектуре IPsec, но без их участия на этапе установления соединения функционирование IPsec невозможно.

Роль общего фундамента в архитектуре IPsec играет так называемый домен интерпретации (Domain Of Interpretation, DOI) – специальная база данных, хранящая стандартные идентификаторы всех зарегистрированных протоколов, алгоритмов шифрования и аутентификации и режимов их применения. Данные DOI используются всеми протоколами, входящими в состав IPsec и IKE.

Инфраструктура функционально полной IPsec–системы выглядит следующим образом (рис 17).

Инфраструктура IPsec включает протоколы аутентификации и защиты данных (AH, ESP), систему установления и согласования параметров соединений (IKE) со входящими в ее состав протоколами управления ключами (ISAKMP и OAKLEY), базу предопределенных стандартных констант (DOI), базу контекстов защиты (SA, Security Association), согласованных на этапе установления соединения и определяющих режимы применения протоколов AH и ESP для защиты передаваемых данных, и базу политик безопасности (SPD, Security Policy Database), управляющую IPsec–системой в целом. Кроме того, для аутентификации участников информационного обмена используется внешняя система цифровых сертификатов (X.509 Certificate Authority, CA).

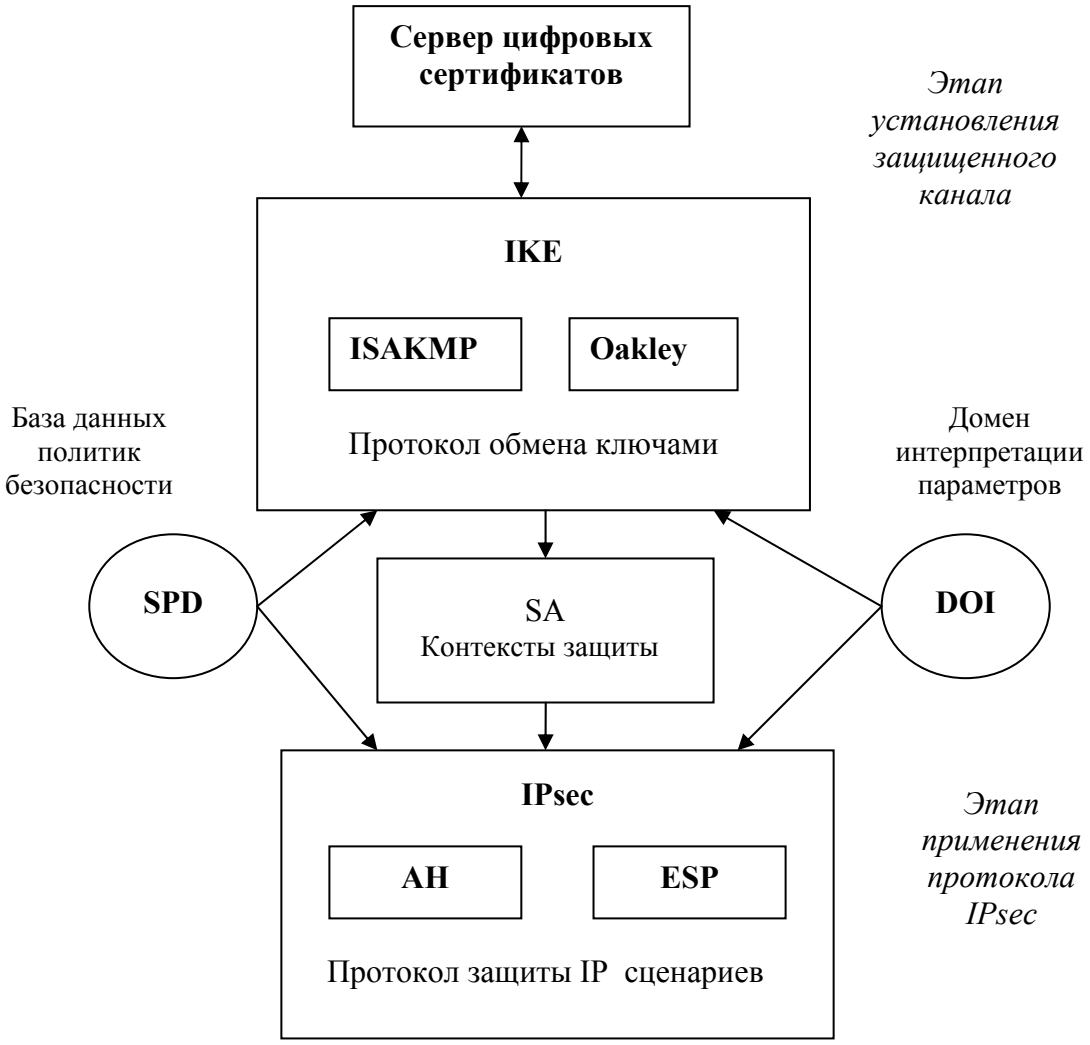

Рис. 17. Инфраструктура IPsec–системы

Несмотря на структурную сложность IPsec–системы, логика ее работы достаточно проста. Функционирование IPsec–системы начинается после получения запроса на установление защищенного IPsec–соединения и состоит из двух фаз, или этапов – подготовительного и целевого применения:

Подготовительный (установление защищенного канала). Посредством применения системы управления ключами IKE согласовывается состав, режимы применения и параметры протоколов IPsec и создаются соответствующие контексты защиты SA. В ходе функционирования IKE использует справочную информацию домена интерпретации DOI и цифровые сертификаты абонентов, полученные от сервера CA. Установление

защищенного канала осуществляется в строгом соответствии с правилами, определенными в базе политик безопасности SPD для данного IP–соединения.

Целевого применения. Протокол IPsec применяется для защиты входящего и исходящего трафика данного IP–соединения в соответствии с согласованными контекстами защиты SA. Защита трафика также осуществляется в строгом соответствии с правилами, определенными в базе политик безопасности SPD для данного IP–соединения.

Рассмотрим далее назначение каждого элемента и его роль в функционировании IPsec–системы в деталях.

Система управления ключами IKE (Internet Key Exchange)

IPsec использует гибкий механизм установления защищенных каналов и управления ключами, называемый IKE (Internet Key Exchange), включающий в себя протокол согласования параметров сессии и управления ключами ISAKMP (Internet Security Association and Key Management Protocol) и произвольный протокол обмена ключами (Key Determination Protocol), в качестве которого де–факто выступает протокол OAKLEY. Применение IKE позволяет участникам информационного обмена проверить аутентичность респондентов, согласовать все необходимые параметры IPsec–сессии, договориться об общих применяемых алгоритмах аутентификации и шифрования и обменяться ключами до того, как будет начат обмен данными. Основное назначение IKE – установление защищенного соединения между участниками информационного обмена, а результат его применения –выработка соответствующего контекста защиты SA (Security Association), определяющие состав и режимы применения протоколов IPsec (AH и/или ESP) и содержащего все параметры, необходимые для их работы.

Функционирование IKE начинается при получении им запроса на установление соединения, также называемого запросом SA, от

приложения или сервиса верхнего уровня. Выработка SA проходит в две фазы. На первой фазе происходит взаимная аутентификация респондентов и создание (с использованием протокола Диффи–Хеллмана) временного защищенного канала ISAKMP с выработкой контекста защиты, специфичного для данного протокола (т.е. ISAKMP SA). На второй фазе данный канал используется непосредственно для выбора протоколов (AH и/или ESP), соответствующих алгоритмов аутентификации и шифрования, обмена ключами и согласования других параметров IPsec, и формирования контекста безопасности для избранного протокола (AH SA или ESP SA).

Для решения задач аутентификации и настройки алгоритмов обмена ключами на этапе установления защищенного соединения между участниками информационного обмена IKE использует их цифровые сертификаты (X.509 Digital Certificates), полученные от внешнего сервера С А.

Домен интерпретации DOI (Domain of Interpretation)

Домен интерпретации DOI – специальная база данных, содержащая полный набор предопределенных зарегистрированных параметров протокола IPsec, представленных стандартными идентификаторами [79]. DOI содержит идентификаторы протоколов управления ключами (IKE и ISAKMP) аутентификации и инкапсулирующей защиты данных (AH и ESP), применяемых ими алгоритмов аутентификации и шифрования, перечень которых будет приведен далее, и опциональных алгоритмов компрессии данных IP–пакетов. Кроме того, DOI определяет синтаксис контекстов защиты SA.

В составе IPsec–системы DOI является общей справочной базой данных, которая используется для выработки контекстов защиты SA протоколом ISAKMP для их последующего применения в процессе функционирования IPsec–системы.

База данных политик безопасности SPD (Security Policy Database)

База данных политик безопасности SPD – элемент IPsec–системы, позволяющий управлять ее функционированием. SPD определяет правила применения IPsec–системы и требования по обеспечению безопасности. Конкретно, она задает политики безопасности при установлении защищенного соединения (Connection management SPD) и политики защиты IP–трафика (Traffic SPD) для определенных IP адресов, т.е. отдельных хостов, шлюзов или маршрутизаторов, или групп IP адресов, т.е. сетей. Тем самым SPD предопределяет состав и позволяет управлять протоколами и алгоритмами защиты, которые будут использоваться для обеспечения безопасного сетевого взаимодействия с конкретными респондентами.

В соответствии с определенными в SPD правилами, к каждому IP–пакету может быть применено одно из следующих действий:

- IP–пакет может быть передан далее после обработки протоколом Ipsec;
- IP–пакет может быть передан далее без изменений (т.е. пропущен) IP–пакет может быть уничтожен.

База данных политик безопасности создается и поддерживается специалистами по безопасности. SPD является сугубо специфичной для каждой реализации IPsec–системы. Ее содержимое зависит от целевого назначения элемента вычислительной сети с установленной IPsec–системой (оконечный хост, межсетевой экран, шлюз или маршрутизатор). Полнота, сбалансированность SPD, ее соответствие решаемым системой задачам являются ключевыми показателями, предопределяющими эффективность функционирования IPsec–системы в целом.

Контекст защиты SA (Security Associations)

Контекст защиты SA представляет собой формализованную запись, определяющую способы обеспечения безопасности при информационном обмене между респондентами. SA содержит все необходимые для этого данные – идентификаторы протоколов и алгоритмов (являющиеся зарегистрированными в DOI идентификаторами), ключи или материал для их генерации и другие параметры. Контексты защиты автоматически генерируются при установлении защищенного соединения системой управления ключами IKE, либо могут быть заданы вручную. Каждый контекст защиты имеет уникальный идентификатор, состоящий из трех полей:

- индекс параметров безопасности ;
- IP–адрес получателя;
- идентификатор протокола безопасности.

Контекст защиты SA включает в себя идентификатор протокола безопасности и поэтому является специфичным для каждого протокола. В IPsec–системе есть три зарегистрированных в DOI протокола – ISAKMP, AH и ESP и, соответственно, существует три вида контекстов защиты – ISAKMP SA, AH SA, ESP SA. Для каждого соединения с использованием перечисленных протоколов должен иметься в наличии соответствующий контекст защиты.

Далее, каждый контекст защиты определяет способ защиты трафика только в одном направлении, заданном IP–адресом получателя. Это означает, что SA является однонаправленным. Для обеспечения безопасности двунаправленного соединения необходимо иметь два отдельных контекста защиты, которые, однако, могут быть одинаковыми и отличаться только направлением (IP–адресом получателя). Таким образом, двум респондентам для обеспечения безопасности трафика в обоих направлениях с применением одновременно протоколов AH и ESP

потребуется по четыре контекста защиты каждому (и еще столько же контекстов защиты протокола ISAKMP должно было быть временно создано для установления защищенного канала на этапе выработки AH SA и ESP SA).

Индекс параметров безопасности SPI применяется для обеспечения уникальности каждого контекста защиты, например, в случае наличия двух одинаковых по протоколу безопасности и IP–адресу получателя контекстов защиты, использующих разные алгоритмы аутентификации или шифрования или разные их ключи.

Контексты защиты SA хранятся в специальной базе данных – SAD (Security Association Database), которая пополняется новыми записями протоколом IKE и используется протоколами AH и ESP.

Связки контекстов защиты и селекторы контекстов защиты

Каждый отдельный контекст защиты определяет единственный протокол защиты – AH или ESP, но никак не оба сразу. В определенных ситуациях требуется, чтобы для защиты трафика по некоторым IP–соединениям использовались сразу несколько протоколов, причем комбинация их применения может быть достаточно сложной (например, трафик между рабочими станциями разных сетей, проходящий через шлюз данной сети, может требовать применения разных контекстов защиты внутри сетей и между ними). Для обеспечения возможности комбинированного применения протоколов AH и ESP в разных режимах контексты защиты объединяются в т.н. связки (SA–bundle). В соответствии с наличием двух режимов применения протоколов IPsec – туннельного и транспортного, которые рассматриваются ниже, имеется два способа связывания контекстов защиты – транспортная связка и повторное туннелирование. Транспортная связка используется на конечных точках соединения и позволяет применять для защиты трафика

сразу оба протокола, AH и ESP (в транспортном режиме). Повторное туннелирование позволяет выполнять многократное применение протоколов AH и ESP к уже защищенному в туннельном режиме трафику.

Необходимость использования связок контекстов защиты зависит от особенностей топологии сети и определяется зафиксированными в политике безопасности требованиями по защите трафика конкретных IP–соединений. Селекторы контекстов защиты предоставляют средство связывания базы данных политик безопасности и контекстов защиты и позволяют выполнить «тонкую настройку» протоколов защиты трафика. Селектор SA содержит следующие поля:

- IP–адрес отправителя и получателя;
- имя объекта (имя пользователя или хоста в DNS или X.500 формате);
- параметр, определяющий уровень критичности данных (sensitivity level);
- идентификатор протокола транспортного уровня (TCP или UDP):
- номера TCP/UDP портов соединения (отправителя и получателя).

Используя механизм селекторов, база данных политик безопасности (те ее части, которые относятся к управлению обработкой входящего и исходящего трафика) может определить, какой из трех возможных способов обработки должен быть применен к IP–пакету: выполнение IPsec–обработки, передача пакета без изменений или его уничтожение. Кроме того, наличие информации о портах теоретически позволяет увязать способ применения протокола IPsec с приложением–источником и приложением–приемником данных.

Функционирование протокола IPsec

Ядром IPsec–системы является протокол IPsec (IP Security Protocol), обеспечивающий защиту сетевого трафика, а именно аутентификацию отправителя и аутентификацию, конфиденциальность и целостность данных IP–пакетов, циркулирующих между связанными по IPsec–протоколу респондентами. В процессе функционирования IPsec руководствуется требованиями политики безопасности SPD, информацией домена интерпретации DOI и задействует тот или иной механизм обеспечения безопасности в соответствии с контекстом защиты SA, предварительно установленным для данного соединения системой IKE.

IPsec не является протоколом как таковым. Фактически, это набор из двух протоколов – AH и ESP, каждый из которых выполняет определенные функции по защите IP–пакетов. Вкратце, AH предназначен для обеспечения аутентификации, а ESP – конфиденциальности данных. Оба протокола также имеют средства контроля целостности IPsec–пакетов и защиты от воспроизведения трафика.

Режимы применения протокола IPsec

В зависимости от типа соединения (хост–хост, хост–шлюз, шлюз–шлюз) каждый из протоколов, AH и ESP, может применяться в одном из двух режимов – транспортном или туннельном. Транспортный режим применяется для защиты трафика между двумя конечными точками соединения (т.е. для соединений хост–хост). Точнее, в данном режиме осуществляется только защита передаваемых данных – адреса респондентов не скрываются и передаются в открытом виде (Рис. 18).

Туннельный режим применяется в случае, когда оба респондента не являются конечными точками соединения, например, между шлюзами, маршрутизаторами или межсетевыми экранами (Рис. 19.).

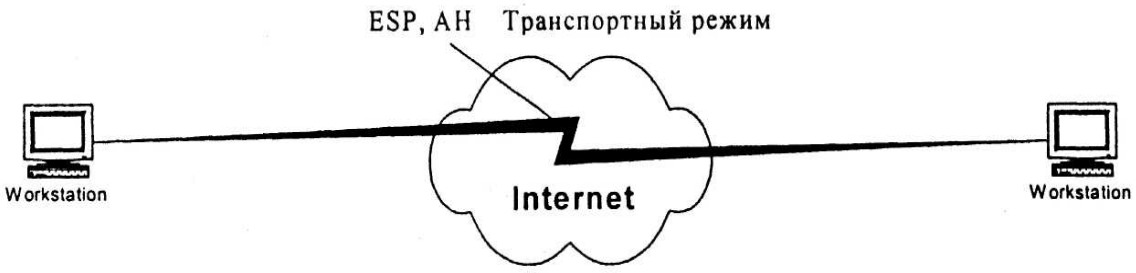

Рис. 18. Применение IPsec в транспортном режиме.

Рис. 19. Применение IPsec в туннельном режиме.

Кроме защиты данных туннельный режим предусматривает сокрытие реальных адресов респондентов, что обеспечивается замещением исходного заголовка IP–пакета заголовком IPsec.

Оригинальный заголовок передается в составе данных IPsec–пакета в зашифрованном виде и восстанавливается на конечной точке туннельного IPsec–соединения. Тем самым, перехват IPsec–трафика между шлюзами не позволяет восстановить архитектуру расположенной за ними сети, проследить реальный маршрут IP–пакета и установить адреса респондентов.

Протоколы AH и ESP могут применяться по отдельности либо в определенной комбинации в соответствии с требованиями по безопасности (для этого применяются связки SA).

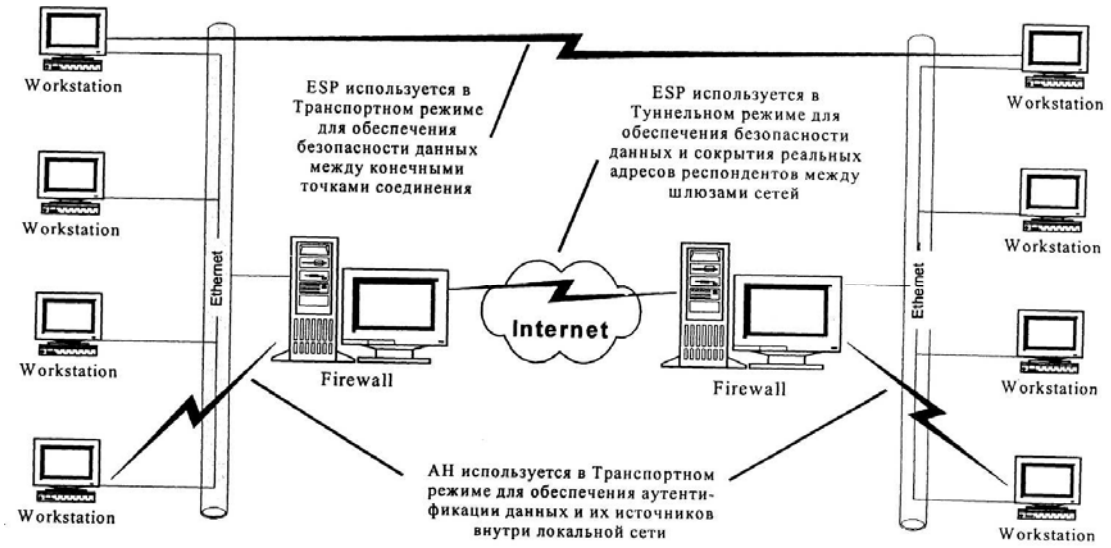

Рис. 20. Пример комбинированного применения протоколов AH и ESP в туннельном и транспортном режимах.

Наличие возможностей комбинированного применения протоколов AH и ESP в разных режимах (транспортном или туннельном) предоставляет широкие возможности для создания как универсальных, так и специализированных решений по обеспечению безопасности данных в информационно–вычислительной сети.

Возможные варианты комбинированного применения протоколов IPsec в туннельном и транспортном режиме показаны на рис. 20.

Р а з д е л 6. Обеспечение информационной безопасности АСТНК на основе принципа гарантированного результата

Лекция 21. Синтез модели внутреннего нарушителя

Определение модели нарушителя и обоснование его стратегии на основе принципа гарантированного результата

Разработка модели внутреннего нарушителя основана на применении принципа гарантированного результата.

Определение 1. *Программой–нарушителем* (ПН) будем называть программу или процесс, осуществляющий несанкционированное воздействие на процессы в ПО ПЭВМ.

Определение 2. Модель нарушителя (МН) для случая логического НСД назовем ЛМН. При этом под логическим НСД понимается НСД на основе ПН.

Структура модели включает следующие разделы:

1. ПО и аппаратура ПЭВМ обладает следующими свойствами:

1.1 специальной аппаратной поддержки работы ПН в аппаратуре ПЭВМ нет;

1.2 ПН. в программном обеспечении нет;

1.3 *BIOS* ПЭВМ аппаратно гарантированно защищен от перезаписи;

1.4 расширения *BIOS* ПЭВМ аппаратно защищены от перезаписи;

1.5 информация на диске защищена методом стойкого шифрования;

2. Нарушителю известны:

2.1 тип используемого оборудования;

2.2 система защиты информации;

3. Нарушитель обладает:

3.1 всеми исходными текстами ПО (включая и средства защиты), работающего на данной ПЭВМ;

3.2 полной технологической документацией на атакуемый комплекс;

3.3 рабочим экземпляром комплекса;

4. Нарушитель имеет возможность:

4.1 получить доступ к включенной ПЭВМ на неограниченное время под контролем легальных пользователей;

4.2 получить доступ к выключенной ПЭВМ па неограниченное время;

4.3 получить бесконтрольный доступ к включенной незаблокированной ПЭВМ на короткое время, достаточное для запуска одной программы со съемного накопителя;

5. Нарушитель не может:

5.1 получить доступ к включенной незаблокированной ПЭВМ на длительное время, достаточное для хищения всей обрабатываемой информации;

5.2 получать кратковременный доступ к незаблокированной включенной ПЭВМ в любое удобное для себя время;

5.3 бесконтрольно вскрывать корпус ПЭВМ;

6. Нарушитель не имеет:

6.l) ключевой информации (включая пароли пользователей);

6.2) конкретной открытой информации, обрабатываемой на данной ПЭВМ.

Ясно, что при выполнении условий ЛМН и при условии абсолютной лояльности и «законопослушности» пользователей единственным путем получения защищаемой информации будет внедрение ПН, осуществляющих компрометацию ключевой информации пользователей.

Рассмотрим различные задачи, возникающие при защите ПЭВМ от внедрения ПН.

Прежде всего следует выделить:

1) построение системы защиты от занесения ПН;

2) построение системы защиты от воздействия (уже занесенной) ПН.

Для задач *первого типа* направления поиска решений могут быть следующие:

- создание средств, предотвращающих занесение ПН;
- создание средств, обнаруживающих факт занесения ПН.

Все методы, связанные с решениями задач *второго типа,* опираются на свойства самой операционной системы и выходят за рамки постановки задачи синтеза .

Рассмотрим основные методы решения задач *первого типа.*

ПН могут быть занесены в ПО локальных станций двумя различными способами во время следующих операций, всегда выполняемых ПЭВМ:

a) во время начальной загрузки – загрузкой другой ОС со съемного накопителя или подключением жесткого диска атакуемой ПЭВМ к машине нарушителя;

b) после загрузки ОС – во время сеанса работы оператора на ПЭВМ под управлением штатной ОС.

Защита от занесения ПН в случае (a) осуществляется организационно–техническими мерами (установка замка на съемные накопители, опечатывание корпуса, установка на него датчиков сигнализации и т.д.), что выходит за рамки постановки задачи, поскольку модель нарушителя предполагает невозможность вскрытия корпуса и установки дополнительных устройств нарушителем (условие 5.3).

Защита от занесения ПН в случае (b) решается с помощью систем обнаружения атак. До перезагрузки операционной системы действие ПН может быть полностью скрытым. Защита ПО от занесения ПН зависит от встроенных в ОС механизмов разграничения доступа. При этом на степень защищенности информации влияют такие трудно учитываемые факторы, как возможные ошибки администрирования систем безопасности, установка дополнительного оборудования с драйверами сторонних фирм и т.д.

Поэтому средства, непосредственно защищающие ПО от внедрения ПН, не рассматриваются.

Для упрощения дальнейших рассуждений будем в дальнейшем рассматривать случай отсутствия в штатной ОС любых средств ограничения доступа и защиты информации.

Определим цели и возможности нарушителя. Нарушитель может быть:

- легальным пользователем ПЭВМ;
- пользователем, не допущенным к работе на данной ПЭВМ.

В первом случае полагаем, что целью «легального нарушителя» является доступ к информации других пользователей (случай хищения собственной информации тривиален, и защита от него осуществляется организационно–техническими мерами). Второй случай рассматривается с самого начала. Таким образом, эти оба случая сводятся к рассмотрению действий нарушителя в рамках ЛМН.

Перечислим возможные воздействия нарушителя на работу локальной станции в рамках ЛМН и укажем результат такого воздействия. При этом предполагаем, что конечной целью воздействия нарушителя на ПЭВМ будет получение закрытой информации,

записанной на жестком диске ПЭВМ. В рамках ЛМН действия нарушителя могут быть направлены:

1. на разрушение ПЭВМ (вызов неисправностей путем электромагнитного облучения, физического и электрического воздействия и т.п.);
2. на несанкционированное получение информации, без изменения ПО (запуск ПЭВМ в обход системы защиты или путем загрузки другой ОС со съемных магнитных носителей);
3. на занесение ПН.

Рассмотрим подробнее перечисленные выше типы воздействий.

Результат воздействий первого типа может привести к разрушению ПЭВМ. В то же время работа ПЭВМ во время различных неразрушающих физических воздействий зависит в первую очередь от свойств используемой в ПЭВМ элементной базы и класса защищенности ПЭВМ от физических воздействий. В меньшей степени поведение ПЭВМ в нештатных ситуациях зависит от наличия или отсутствия недокументированных возможностей, оставленных систем отладки, занесенных ПН, и используемого штатного ПО. Более того, например, воздействие электромагнитных излучений на ПЭВМ может привести к снижению напряжения питания или появлению пульсаций в различных цепях. Такое воздействие делает поведение ПО ПЭВМ непредсказуемым. Можно предположить, что воздействие этого типа может привести к активизации защитного ПО (например, реакция на перегрев процессора приводит к ускорению вращения вентиляторов). Таким образом, помимо систем обеспечения работоспособности ПЭВМ возможна активизация иных ПН, занесенных, например, в процедуры обработки аварийных ситуаций. Защита от физических воздействий может быть только аппаратная (экранирование и заземление корпуса ПЭВМ, помещение

рабочего места в экранированную камеру, использование сканирующих приемников, управляющих включением шумовых генераторов и т. д.), поэтому рассмотрение этих ситуаций выходит за рамки данной работы.

Защита от воздействий второго типа строится на использовании аппаратных средств: замков на дисководы и т.д., с обязательной реализацией организационных мероприятий, поскольку из военного дела известно, что ни одно укрепление не выстоит долго, если его никто не будет защищать. Рассмотрение таких способов защиты выходит за рамки курса ИБ АСТНК.

В связи с этим необходим анализ третьего типа воздействий.

Рассмотрим классификация ПН по характеру воздействия:

- целевые ПН – ориентированы на нарушение работы конкретных модулей, осуществляющих защитные функции или взаимодействующих с системами защиты;
- обучающиеся ПН – реализуют механизм внедрения целевых ПН в ПО защищаемого комплекса. Эти ПН могут, например, ожидать получения кода целевой ПН по сети или из другого канала ввода информации и помещать их в заранее выбранное место ПО ПЭВМ.

Комбинации указанных свойств ПН не рассматриваем, поскольку:

- целевые – обучающиеся ПН, в рамках предложенной классификации, представляются в виде комбинации элементов классов 1 и 2;
- нецелевые – необучающиеся ПН являются деструкторами. Такие ПН уничтожают информацию, делая ее недоступной ни легальному пользователю, ни нарушителю.

Заметим, что «мастер – пароли», «люки» и наличие отладочных модулей относятся к ПН 1–го типа. К ПН второго типа относятся, например, программы, осуществляющие динамическое обновление ПО ОС *Windows*. Защититься от занесения ПН 2–го типа не всегда возможно.

Дело в том, что такого рода программы могут быть внедрены разработчиками непосредственно в ядро ОС. Собственно, наличие такого рода ПН не опасно, поскольку они не оказывают непосредственного воздействия на обработку информации. Тем не менее результат работы этих ПН – внедрение целевых ПН (типа 1) – уже опасен. При этом ПН второго типа может маскировать свою работу, используя всю мощь средств ОС. Назовем сеансом работы оператора (пользователя) период работы пользователя на ПЭВМ между двумя ближайшими по времени холодными (производится либо выключением питания ПЭВМ, либо нажатием кнопки «Reset»*)* перезагрузками. Постоянным воздействием на вычислительную среду (ПВ) назовем действие занесенной посредством осуществления ЛНСД или УНСД ПН в течение более одного сеанса работы оператора на локальной станции.

По типу воздействия на ПО ПЭВМ. ПН можно разбить на два класса:

- временного воздействия (ВВ) – занесение ПН и ее воздействие на ПО происходит в течение одного сеанса работы на ПЭВМ (например, в период между загрузками локальной станции или в период одной смены оператора);
- постоянного воздействия (ПВ).

По условиям ЛМН (5.1 и 5.2) использование ПН типа ВВ неэффективно. Дело в том, что защита ПО от занесения ПН типа ВВ целиком зависит от работы средств разграничения доступа используемой ОС. Поскольку мы рассматриваем незащищенное ПО, защиты от ПН типа ВВ нет. Вместе с тем отметим, что для ПН типа ВВ характерно то, что они, как правило, самоуничтожаются во время или по окончании сеанса работы оператора на ЭВМ. Таким образом, использование ПН типа ВВ требует их многократного внедрения (противоречие условию 5.2 ЛМН).

В дальнейшем будем рассматривать только ПН типа ПВ. Поскольку мы предположили отсутствие штатных средств разграничения доступа к информации используемой ОС, способы внедрения ПН этого класса не имеют значения. Будем считать, что:

- у нарушителя нет доступа к незашифрованной закрытой информации непосредственно в момент ее обработки легальным пользователем;
- легальные пользователи правильно осуществляют уничтожение остаточной информации.

В условиях ЛМН противник не имеет ключей шифрования и конкретной открытой информации, обрабатываемой данным комплексом. Поэтому для получения интересующей противника информации ему необходимо получить открытую и/или ключевую информацию. Оба типа информации можно получить либо методами криптоанализа зашифрованной информации, либо методами ЛНСД (путем занесения ПН с целью получения интересующих сведений). Использование методов криптоанализа является отдельной областью исследований, и в данном разделе не рассматривается.

Атаки на программные и программно–аппаратные средства защиты информации

По определению нарушитель действует в рамках ЛМН, поэтому целевых закладок типа ПВ в ПО рабочей станции нет. Задача нарушителя – внедрить целевую закладку, обеспечивающую получение нарушителем открытой информации или ключей шифрования. Эта задача может быть решена следующей атакой целевой ПН:

- создать ПН, внедряемую в драйвер, осуществляющий шифрование информации. Функционирование данной ПН может, например, сводиться к сохранению пароля пользователя или другой информации в свободных областях на жестком диске;

- внедрить эту ПН в ПО атакуемой машины;
- получить требуемую для взлома информацию методами атака путем подмены программы шифрования:
- ЛНСД;
- создать ПН, являющуюся драйвером, осуществляющим шифрование информации более слабым алгоритмом;
- заменить на атакуемой машине исходный драйвер на вновь созданный;
- регулярно получать информацию путем вскрытия слабого шифра.

Теперь рассмотрим возможность проведения атак на систему. Воздействие ПН непосредственно на алгоритм шифрования, реализованный внутри платы, невозможно. Однако, можно воздействовать на программный интерфейс с платой шифрования таким образом, что открытая информация вообще не попадет в плату, а, подвергшись легкой маскировке, будет воспринята остальными частями программного комплекса как закрытая. Таким образом, атаки на программные и программно–аппаратные системы шифрования проводятся по аналогичным сценариям.

Покажем, что с точки зрения защиты установленных средств шифрования наиболее опасным классом атак являются ПН для оказания ПВ. По условиям ЛМН для защиты информации методом шифрования наиболее опасным типом атаки является занесение ПН, осуществляющих ПВ. Докажем существование ПН типа ПВ, факт внедрения которой не обнаруживается чисто программными средствами контроля целостности.

Утверждение . Существует универсальная обучающаяся ПН типа ПВ, блокирующая работу любых программных средств защиты.

Доказательство. Рассмотрим продукт фирмы VMashine, названный Vmashine. Детальное описание и собственно программу можно найти в

Internet (www.vmware.com). Это программа, запускающаяся как приложение под управлением ОС LINUX. После старта эта программа создает виртуальную машину, работающую под управлением ОС LINUX. При этом сама программа VMashine осуществляет обращение к периферийным устройствам ПЭВМ через драйверы ОС LINUX (в силу архитектуры ОС семейства UNIX иначе не бывает). На созданную таким образом виртуальную машину можно установить любую другую ОС, например, Windows NT, LINUX или FreeBSD. Заметим, что все вышеперечисленные ОС работают в защищенном режиме микропроцессора. Более того, ядро этих ОС может работать только в нулевом кольце защиты (с максимальным уровнем привилегий). На самом деле в этом режиме работает только ядро основной ОС (в нашем случае LINUX). Отсюда следует, что запущенная под управлением VMashine вторая ОС получает доступ к ресурсам ПЭВМ под контролем первой ОС и при этом нормально работает.

Очевидно, что созданная по аналогии с VMashine обучающаяся ПН сделает недействительными любые способы контроля, встроенные в запускаемую под ней ОС, в случае, если получит управление до старта систем контроля целостности.

Следствие. Существует обучающаяся ПН, блокирующая работу программно–аппаратных средств контроля целостности и/или шифрования, при условии получения управления до старта систем контроля целостности, как программной, так и аппаратной реализаций функций контроля целостности.

Таким образом, можно эмулировать как наличие любых устройств, так и их отсутствие. Особо отметим, что исследуемая ПН получают управление до старта программных и активизации программно–аппаратных средств защиты.

Назовем электронным замком (ЭЗ) программный или программно–аппаратный комплекс, разрешающий загрузку ОС на ПЭВМ пользователям, прошедшим идентификацию–аутентификацию, и блокирующий загрузку ОС на ПЭВМ при неудачной идентификации–аутентификации.

Поэтому необходимо рассматривать только защиту от воздействия ПН на этапе начальной загрузки, так как на последующих этапах, после успешного занесения ПН, любые защитные системы могут оказаться неэффективными.

Защититься от занесения целевых ПН типа ПВ можно с помощью различных средств проверки целостности ПО. Основной принцип работы средств проверки целостности ПО заключается в вычислении контрольной суммы для всех основных фрагментов ПО с помощью некоторой криптографической хеш–функции, зависящей от секретного ключа.

Уточним цели дальнейших исследований, ими будут:

1) построение архитектуры системы защиты от действия закладок типа ПВ (в рамках ЛМН);

2) доказательство независимости функционирования системы защиты с предложенной архитектурой от воздействия целевых и обучающихся закладок;

3) доказательство существования такой системы защиты.

Очевидно, что единственным способом выявления факта занесения ПН в ПО является проверка ПО на целостность. Известно, что для контроля целостности используют два типа криптографических методов: цифровая подпись и имитовставка. Для определенности будем в дальнейшем предполагать, что для проверки целостности ПО используется имитовставка.

Определение. Назовем уровнем защищенности от НСД величину, равную сложности преодоления нарушителем системы защиты.

Для систем защиты от ЛНСД ПЭВМ с ЭЗ уровень защищенности равен сложности преодоления нарушителем создаваемой ЭЗ защиты. Ясно, что этот показатель, в свою очередь, зависит от стойкости используемой криптосхемы.

Утверждение . В условиях ЛМН для достижения наперед заданного уровня защищенности выявления факта занесения ПН типа ПВ необходимо и достаточно, чтобы все зарезервированные области, конфигурационные файлы и исполняемый код до момента старта ПО с перезаписываемых областей памяти были проверены на целостность с помощью криптографической хэш–функции, обеспечивающей заданный уровень выявления изменений проверяемых объектов.

Следствие. Контроль целостности необходимо проводить на этапе начальной загрузки при инициализации расширений BIOS ПЭВМ.

Рассмотрим алгоритм загрузки IBM–совместимой ПЭВМ. После включения питания (или нажатия кнопки «Reset»), как правило, реализуются следующие шаги:

1) тестирование регистров микропроцессора;
2) проверка контрольной суммы ROM BIOS;
3) проверка и инициализация таймеров;
4) проверка и инициализация контроллера DMA;
5) проверка регенерации памяти;
6) тестирование 64К байт нижней памяти;
7) загрузка векторов прерывания и стека в нижнюю область памяти;
8) инициализация видеоконтроллера;
9) тестирование полного объема ОЗУ;
10) тестирование клавиатуры;
11) тестирование CMOS памяти и часов;
12) инициализация COM и LPT портов;

13) инициализация и тест контроллеров НГМД и НЖМД;

14) сканирование области дополнительного ROM и инициализация найденных расширений BIOS;

15) настройка Р–п–Р устройств;

16) вызов процедуры Bootstrap;

16.1) поиск активного устройства (то есть устройства, содержащего загрузчик);

16.2) передача управления считанному с активного устройства загрузчику.

Отметим, что все команды, выполняющиеся на этапах 1–16, записаны в микросхемы ПЗУ или FLASH, расположенные внутри корпуса ПЭВМ. Поэтому ПН можно занести в ПО только программными способами.

Отсюда следует, что процедуру проверки можно:

1) встроить в BIOS ПЭВМ (проводить между пунктами 15 и 16);

2) разместить на плате расширения BIOS. Из описания выполнения пункта 16 ясно, что проверку следует проводить непосредственно на фазе выполнения процедуры инициализации BIOS EXTENTI0N.

Других мест для размещения процедуры проверки целостности нет. Для обеспечения проведения надежного контроля целостности его следует проводить с использованием криптографической хеш–функции с заданным уровнем надежности.

Пусть ПЭВМ защищена электронным замком, работающим на этапе инициализации расширений BIOS. Тогда в условиях ЛМН для обеспечения заранее заданного уровня надежности при проверке целостности необходимо и достаточно, чтобы при работе электронного замка последовательно выполнялись следующие действия:

1) проводилась идентификация – аутентификация пользователя;

2) проверялась целостность объектов из рассмотренного списка с использованием криптографической хеш–функции, обеспечивающей заданный уровень выявления изменений проверяемых объектов.

Идентификация – аутентификация пользователя происходит при вводе ключей до последующей проверки целостности. Таким образом, идентификация – аутентификация необходима для предотвращения доступа к информации со стороны нарушителя типа «легальный пользователь». ПО BIOS и BIOS EXTENTION (в том числе и ПО ЭЗ) недоступны нарушителю для модификации. По условиям ЛМН BIOS и BIOS EXTENTION ПЭВМ защищены от перезаписи. Поэтому в условиях ЛМН противник не может изменить последовательность начальной загрузки. Проведение аутентификации и идентификации позволяет использовать ПЭВМ только легальным пользователям.

Лекция 22. Усложненная модель внутреннего нарушителя для реализации логического несанкционированного доступа

Усиленный структурный вариант логической модели нарушителя

Рассмотрим пример синтеза усложненной модели внутреннего нарушителя. Принцип гарантированного результата в решении задачи разработки систем защиты информации обусловливает процедуру усиления возможностей нарушителя для реализации ЛНСД путем наделения его максимальными возможностями для достижения целей. Таким образом, разработчик должен получить решение для наиболее неблагоприятных факторов, имеющих место при создании структурного варианта модели внутреннего нарушителя.

Структура модели внутреннего нарушителя

Определение. Усиленную модель внутреннего нарушителя для случая ЛНСД назовем УМН. Она включает следующие условия:

- ПО и аппаратура ПЭВМ обладают следующими свойствами:
- в аппаратуре ПЭВМ могут присутствовать аппаратные закладки;
- в программном обеспечении могут присутствовать ПЗ, оказывающие постоянное воздействие;
- BIOS ПЭВМ аппаратно гарантированно не защищен от перезаписи;
- расширения BIOS ПЭВМ аппаратно не защищены от перезаписи;
- информация на диске не защищена методом стойкого шифрования;

Нарушителю известны:

- тип используемого оборудования;
- система защиты информации;

нНрушитель обладает:

- всеми исходными текстами ПО (включая и средства защиты), работающего на данной ПЭВМ;
- полной технологической документацией на атакуемый комплекс;
- рабочим экземпляром комплекса;
- нарушитель имеет возможность:
- перехватывать, подменять и удалять передаваемые по телекоммуникациям данные;
- имитировать терминалы;
- получить доступ к включенной ПЭВМ на неограниченное время под контролем легальных пользователей;
- получить доступ к включенной незаблокированной ПЭВМ на ограниченное время, достаточное для хищения всей обрабатываемой информации;
- получить доступ к выключенной ПЭВМ на неограниченное время;

- получить бесконтрольный доступ к включенной незаблокированной ПЭВМ на короткое время, достаточное для запуска одной программы со съемного накопителя;
- получать кратковременный доступ к незаблокированной включенной ПЭВМ в любое удобное для себя время;
- осуществлять атаку путем всевозможного сочетания функций вызова и команд, заложенных в криптографическом интерфейсе, вместе с подачей на вход произвольных наборов данных с целью получения доступа к ключам;
- кратковременно вскрывать корпус ПЭВМ;

Нарушитель не может:

- нарушить целостность технических устройств, выполняющих криптографические функции;
- преодолеть средства физической защиты устройства CF для считывания хранящегося там долговременного ключа;
- быть «офицером безопасности» или любым другим лицом, имеющим доступ по долгу службы к паролям или компонентам секретных ключей;

Нарушитель не имеет:

- ключевой информации.

Понятно, что приведенная модель нарушителя описывает крайнюю ситуацию, в которой противник обладает почти максимальными возможностями для осуществления своих замыслов. Такая ситуация может возникнуть при неправильной системе организационно–технических мероприятий либо, если нарушителем является один из сотрудников обслуживающего технического персонала.

Пример программно–аппаратного решения обеспечения ИБ с учетом усиленной модели внутреннего нарушителя

Система безопасности транзакций *TSS (Transaction Security System)* предназначена для обеспечения безопасности банковских рабочих мест с учетом сложной распределенной архитектуры информационной системы банка.

Для стандартизации основных криптографических функций, выполняемых аппаратными устройствами, и определения порядка их взаимодействия в рамках системы TSS разработана системная криптографическая архитектура SCA (System Cryptographic Architecture). Архитектура SCA исходит из модели нарушителя, которым может быть лицо, являющееся техническим специалистом или обслуживающим персоналом банка. Поэтому злоумышленник обладает значительными возможностями по доступу к компьютеру и обрабатываемой информации. Целью нарушителя является овладение неизвестным ему главным ключом конкретного компьютера (терминала, хоста). Основное требование к системе безопасности состоит в том, что принятые меры должны быть достаточны для противодействия угрозам со стороны одного лица, какими бы полномочиями это лицо ни обладало.

Будем исходить из самой неблагоприятной ситуации, когда нарушитель может вскрыть корпус компьютера и устанавить программно–аппаратные закладки. В этом случае информация, подлежащая шифрованию, очевидно, будет ему доступна.

Архитектура криптоадаптера

Для обеспечения требований архитектуры SCA недостаточно чисто программных решений. Необходимо обязательное использование аппаратных устройств, осуществляющих защиту ключей в системах шифрования и реализующих криптоалгоритмы. Разработка технических

устройств в системе TSS осуществляется в соответствии с принципами общей криптографической архитектуры CCA (Common Cryptographic Architecture), являющейся составной частью SCA. Базовый принцип CCA: секретная информация в открытом виде может находиться только в защищенной зоне внутри аппаратного устройства. Базовый принцип предусматривает специальные требования к интерфейсам технических устройств:

- интерфейс обращения к устройству должен быть стандартизован;
- интерфейс обращения к устройству должен быть строго ограничен;
- доступ к интерфейсу должен определяться уровнем полномочий пользователя;
- интерфейс не должен допускать выхода ключевой информации в открытом виде при любом сочетании набора допустимых команд.

Для реализации этого принципа средства, выполняющие криптографические функции, размещаются в защищенной области специального аппаратного устройства – криптоадаптера. Основным назначением криптоадаптера, обозначаемого в дальнейшем CF (crypto facility), служит:

- хранение главного ключа в физически защищенной памяти;
- выполнение криптографических функций по шифрованию и расшифрованию данных;
- шифрование и перешифрование ключей.

Главное требование к этому устройству заключается в реализации базового принципа: *ни один из ключей, используемых в системе, не должен появляться вне этого устройства в незашифрованном виде.*

При этом обеспечивается защита от физического проникновения и попыток считывания памяти (через электрическое взаимодействие, рентгеновское излучение, электронное просвечивание, химическое

воздействие и т.п.). В случае физического проникновения или попыток считывания памяти происходит автоматическое обнуление памяти.

Для реализации устройства CF используется следующий подход:

- ввод в систему главного ключа осуществляется со специального считывающего устройства непосредственно в CF, минуя остальные устройства компьютера;
- генерацию и хранение ключей (в зашифрованном виде) можно осуществлять вне устройства *CF*. В самом устройстве должен храниться только один главный ключ;
- в самом устройстве наряду с защищенной памятью должен быть реализован защищенный криптопроцессор, способный выполнять все необходимые криптографические операции;
- внутренние команды управления криптопроцессором должны быть недоступны извне; обращение к CF извне осуществляется только в соответствии со специальным интерфейсом, включающим ограниченный набор команд–инструкций;
- данный интерфейс должен включать и поддерживать только такие инструкции, при которых выполняется указанное выше главное требование к CF.

Внутренний интерфейс

Основной проблемой при создании такого устройства является разработка специального интерфейса для обращения к CF извне со стороны операционной системы и прикладных программ, выполняемых на компьютере. Необходимо выбрать набор команд–инструкций, описывающий этот интерфейс, таким образом, чтобы они, с одной стороны, позволяли выполнять все необходимые криптографические операции по шифрованию и расшифрованию различных массивов данных, а с другой

стороны, позволяли осуществлять перешифрование ключей с одного ключа на другой без раскрытия самих ключей.

Заметим, что концепция главного ключа предполагает наличие в системе достаточно большого числа ключей, которые предназначаются для различных целей. Помимо первичных ключей, которые могут использоваться в качестве сеансовых, коммуникационных, файловых ключей и т.п., в ней предусмотрены вторичные ключи, предназначенные для шифрования первичных ключей (вторичные коммуникационные, вторичные файловые и т.п.). Ключевая система предполагает хранение в открытом виде в защищенной области криптоадаптера только главного (мастер) ключа. Все остальные ключи хранятся в незащищенных областях в зашифрованном виде. Для этого используют ключи шифрования ключей (вторичные ключи). В открытом виде ключи могут присутствовать только внутри защищенной области и только в момент выполнения соответствующих криптографических функций.

Введем обозначения:

K_{MH} – главный ключ (хост–) компьютера;

K_{SC} – вторичный ключ для шифрования коммуникационных ключей;

K_{SF} – вторичный ключ для шифрования файлов;

K_N – вторичный ключ;

K – первичный ключ.

Будем считать, что все ключи в системе, предназначенные для выполнения операций шифрования и расшифрования каких–либо данных при внутреннем использовании, хранятся в компьютере в зашифрованном на главном ключе виде $Ек_{MH}(K)$. При этом их генерация изначально осуществляется в таком же виде $RN= Ек_{MH}(K)$. Для этого необходимы следующие три команды.

1. Макроинструкция ЕМК (encipher–under–master–key) имеет вид

$EMK(K) = Ек_{МН}(K)$.

Заметим, что одновременное наличие обратной команды в том же устройстве недопустимо, так как ее выполнение приведет к появлению в открытом виде ключа К.

2. Макроинструкция ECPH (encipher) имеет вид:

$ECPH(Ек_{МН}(K),data)=E_K(data)$.

3. Макроинструкция DCPH (decipher) имеет вид;

$DCPH(Ек_{МН}(K), E_K(data))= data$.

Заметим, что операция ЕМК не может быть применена к главному ключу $К_{МН}$, иначе можно применить операцию DCPH для расшифрования любого ключа.

В связи с тем, что все первичные ключи должны храниться в зашифрованном на вторичных ключах виде, необходимо предусмотреть еще две команды.

4. Макроинструкция RFMK (reencipher–from–master–key) имеет вид:

$RFMK\ (Ек_{МН1}(K_N),\ Ек_{МН}(K)) = Ек_N(K)$.

5. Макроинструкция RTMK (reencipher–to–master–key) имеет вид:

$RTMK\ (Ек_{МН2}(K_N), Ек_N(K)) = Ек_{МН}(K)$.

В данном случае для шифрования вторичных ключей вместо главного ключа $К_{МН}$ используются два производных от него ключа $К_{МН1}$ и $К_{МН2}$, которые получаются из главного ключа инверсией некоторых бит ключа по заранее оговоренному правилу.

Ключ $К_{МН1}$ используется для шифрования при хранении тех вторичных ключей, которые применяются в макроинструкции RFMK для перешифрования с главного ключа на текущий вторичный ключ K_N. Тем самым макроинструкция RFMK переводит зашифрованный ключ из разряда «внутренний», то есть предназначенный для внутреннего

использования, в разряд «внешний», т. е. предназначенный для внешнего использования или хранения.

Ключ $К_{МН2}$ используется для шифрования при хранении тех вторичных ключей, которые применяются в макроинструкции RTMK для перешифрования с текущего вторичного ключа K_N на главный ключ. Тем самым макроинструкция RTMK переводит зашифрованный ключ из разряда «внешний» в разряд «внутренний», т. е. предназначенный для внутреннего использования при шифровании и расшифровании с помощью операций ECPH и DCPH.

Эти два ключа введены в связи с необходимостью развести операции RFMK и RTMK таким образом, чтобы они не были взаимно обратными на одном компьютере и имели разные входные параметры. В противном случае в системе будут храниться вторичные ключи, зашифрованные на главном ключе, т. е. записи вида $Ек_{МН}(К)$, к которым вместе с $Ек_N(К)$ можно применять операцию DCPH для расшифрования ключа К.

Данного набора операций достаточно для организации закрытой передачи информации по сети, содержащей несколько компьютеров.

Лекция 23. Структурно–временная модель внешнего нарушителя

Подсистема защиты информации типовой АС

Традиционно функции защиты информации в АС при обработке информации реализуются системой защиты информации(СЗИ), входящей в АС в качестве подсистемы. При этом используемые в настоящее время СЗИ в функциональном смысле, являются однотипными. К основным функциям системы типовой СЗИ относятся:

- идентификация и аутентификация пользователя;

- паролирование входа;
- накопление, хранение и обработка информации в преобразованном (шифрованном) виде;
- «прозрачная» защита информации на уровне логического устройства ЭВМ, логического диска, каталогов и шаблонов файлов;
- управление доступом;
- мандатный принцип контроля доступа;
- регистрация и учет событий;
- объединение пользователей в группы с общими файлами;
- защита файлов пользователей на чтение, запись, удаление, переименование, изменение, создание с тем же именем;
- запрет на запуск программ с дискет;
- контроль целостности программного обеспечения;
- работа пользователя в привычной среде;
- индивидуальная и групповая настройка;
- сигнализация об эталонном изменении целостности ЭВМ.

Процесс функционирования типовой СЗИ состоит в решении последовательности сервисных задач в соответствии с поступающими в ходе работы АС запросами на те или иные действия с информацией.

При обмене данными функции защиты информации реализуются за счет применения специальных методов приема–передачи информации, среди которых наиболее эффективными являются методы с применением многоосновных кодовых конструкций, а также методы приема–передачи с псевдослучайной последовательностью рабочих частот.

Этапы несанкционированного доступа к информации в АС

Анализ известных данных о способах доступа внешнего нарушителя к информации в компьютерных системах дает возможность установить обобщенную схему несанкционированного доступа к информации в АС с целью противоправного манипулирования данными и программами. Такая схема включает три взаимосвязанных этапа:

- этап исследования механизма доступа к информации в АС;
- этап исследования основных подсистем СЗИ;
- этап несанкционированного копирования, модификации и удаления информации в АС.

Этап исследования механизма доступа к информации в АС

На первом этапе осуществляется исследование СЗИ с целью изучения механизма организации процесса идентификации и аутентификации пользователей и разграничения доступа к информации подсистемами обеспечения санкционированного доступа к информации и разграничения доступа к вычислительным ресурсам АС. Объектом такого исследования являются идентификационные таблицы, пароли и коды, используемые для регистрации пользователей и их допуска к информационным ресурсам АС. Этап реализуется путем внедрения специальных программных средств в РВС АСУ. Эти средства контролируют прерывания от устройств ввода паролей, копируя таким образом пароли доступа в АСУ, и пересылают эти копии на указанный абонентский пункт сети. Этап завершается самоуничтожением этих программ. Длительность этапа исследования механизма доступа определяется организацией порядка доступа, используемыми методами паролирования и составляет величину порядка 1–5 минут.

При этом следует иметь ввиду, что длительность всех этапов и отдельных фаз этапов, реализуемых непосредственно вредоносными

программами без участия злоумышленника, определяется активным периодом действия вредоносной программы, т.е. временным интервалом от момента инициализации ее функций до момента самоуничтожения.

Этап исследования основных подсистем СЗИ

Главной задачей второго этапа является исследование основных подсистем СЗИ: подсистемы преобразования информации, подсистемы поддержания целостности вычислительной среды, подсистемы закрытия и подсистемы регистрации. Работа других подсистем СЗИ на данном этапе не исследуется.

Задачи этого этапа реализуются несколькими фазами.

В первой фазе, на основе полученной информации о паролях доступа к АСУ, разрабатываются способы преодоления (вскрытия) СЗИ, создаются и тестируются программы контроля работы подсистем СЗИ.

Во второй фазе осуществляется проникновение в распределенную вычислительную сеть АС программ контроля работы подсистем СЗИ под именами и с полномочиями реальных пользователей. Эти программы перехватывают и копируют (с последующей пересылкой по назначению) всю информацию, с которой работают эти подсистемы. При исследовании подсистемы преобразования информации в СЗИ возможно копирование программ этой подсистемы. Фаза завершается самоуничтожением программ контроля работы подсистем СЗИ. Длительность данной фазы определяется периодом реализации функций основных подсистем СЗИ и составляет величину порядка 3–10 минут.

В третьей фазе производится анализ полученных данных о работе подсистем СЗИ и дисассемблирование полученных копий средств преобразования информации (при наличии таких копий), либо синтез алгоритмов работы этих средств по имеющейся информации об исходных данных и результатах работы.

На основе этой информации разрабатываются программы отключения или видоизменения защитных механизмов СЗИ и программы манипулирования данными в АС.

Этап несанкционированного копирования, модификации и удаления информации в АСУ

На третьем этапе осуществляется преодоление СЗИ и, в зависимости от преследуемых целей, копирование, модификация или удаление информации в АС.

Также как и на втором этапе задачи третьего этапа реализуются несколькими фазами.

Первая фаза состоит в отключении или видоизменении защитных механизмов СЗИ при помощи соответствующих программ.

Во второй фазе осуществляется вход в СЗИ программ манипулирования информацией в АС под именами и с полномочиями реальных пользователей.

В третьей фазе осуществляется поиск необходимых файлов, информационных массивов, программ и их фрагментов.

В четвертой фазе, в случае, если цель — искажение информации, производится модификация либо удаление, как целых файлов, так и отдельных информационных массивов или программ, а в отдельных случаях — лишь их фрагментов. Если цель — копирование информации, то производится копирование файлов. Фаза завершается самоуничтожением программ искажения информации.

В пятой фазе программой копирования информации осуществляется пересылка скопированных данных на требуемый абонентский пункт вычислительной сети АС. Фаза завершается самоуничтожением программ копирования информации.

Длительность этапа несанкционированного манипулирования информацией определяется особенностями организации хранения информации,

ее шифрования, логической и физической структурой файлов данных и составляет величину порядка 10–15 минут.

Основные характеристики вредоносных программ

Очевидно,что основную функциональную нагрузку при реализации несанкционированного проникновения в АС несут вредоносные программы.

При проектировании таких программ соблюдаются ряд положений компьютерной вирусологии, основными из которых являются:

- обеспечение живучести;
- самоуправляемость;
- комбинируемость свойств.

Свойство живучести вредоносных программ обеспечивается тремя механизмами: самодублированием, ассоциированием с другими программами и самомодификацией структуры.

Самодублирование вредоносной программы представляет собой процесс воспроизведения своего собственного кода в оперативной или внешней памяти компьютера.

Ассоциирование вредоносной программы с другой программой представляет собой процесс интеграции своего кода либо его части в код другой программы таким образом, чтобы при некоторых условиях управление передалось на вредоносную программу.

Самомодификация структуры вредоносной программы представляет собой процесс воспроизведения изоморфного собственному кода программы в оперативной или внешней памяти компьютера.

В соответствии с положениями компьютерной вирусологии свойством самодублирования обладают вирусы, разрабатываемые по репликативной технологии, свойством ассоциирования – вирусы

разрабатываемые по технологии stealth («невидимка»), а свойством самомодификации – по технологии phantom («призрак»).

Наибольшую вероятность обнаружения антивирусными средствами имеют разрушающие программы, разрабатываемые по репликативной технологии, а наименьшую–разрабатываемые по технологии phantom («призрак»).

Самоуправляемость обеспечивает вредоносной программе условия, в соответствии с которыми она всегда получает управление на себя, т.е. процессор должен начать выполнять команды, относящиеся к коду разрушающей программы раньше команд любой прикладной или системной программы.

Такими условиями являются следующие:

- вредоносная программа должна находиться в оперативной памяти до начала работы программы, которая является целью воздействия, и, следовательно, должна быть загружена раньше или одновременно с основной;
- вредоносная программа должна активизироваться по некоторому общему как для себя, так и для остальных программ событию, т.е. при выполнении ряда условий в программно–аппаратной среде управление должно быть передано на вредоносную программу.

Это достигается путем анализа и обработки вредоносной программой общих относительно вредоносной и прикладной программ воздействий на вычислительный процесс (выделенных прерываний, операций с портами и т.д.). В качестве выделенных прерываний используются:

- прерывания от клавиатуры;
- прерывания при работе с накопителями;
- прерывания от внешних устройств;

- прерывания от таймера компьютера;
- прерывания операционной системы (прерывания при работе с файлами и запуске исполняемых модулей).

Типы вирусных программ

Особенности воздействия вредоносных программ зависят от степени воплощения комбинаций свойств пяти стандартных типов компьютерных вирусов: «классический » , т«программная закладка», «программный червь», «логическая бомба» и «логический люк».

Средства второго, третьего и четвертого типа относятся к вирусным программам класса «троянский конь». Их отличительной особенностью является доминирование механизма ассоциирования с другими программами. Программные средства данного класса являются жестко функциональными и учитывают особенности вычислительной среды, в которой функционируют.

Классический тип

Средства первого типа представляют собой компьютерные вирусы, разрабатываемые по традиционной технологии как программы с доминированием механизма самодублирования. Их особенностью является ненаправленность на конкретные программы и данные и отсутствие каких либо ограничений на условия применения. Вредоносные воздействия таких программ сводятся к искажению информации и нарушению сеансов работы вычислительной сети. Эти средства представляют опасность, в основном, для абонентских пунктов сети, т.к. распространяются с потоком передаваемых файлов и инфицируют программное обеспечение абонентского пункта путем использования его ресурсов (запуска инфицированных программ в оперативной памяти) при реализации удаленного доступа к ресурсам вычислительной сети.

Программная закладка

Средства второго типа могут проявлять себя в определенных условиях (по времени, ключевым сообщениям и т.д.) и предназначены для копирования конфиденциальной информации, паролей и ключей. По методу, месту внедрения и применения выделяются следующие группы средств данного типа:

- закладки, код которых ассоциирован с программами игрового и развлекательного назначения;
- закладки, код которых ассоциирован с прикладными программами общего назначения (клавиатурные и экранные драйверы, программы тестирования компьютера, утилиты и оболочки типа Norton);
- закладки, код которых ассоциирован с программами базовой системы ввода–вывода операционной системы.

Программный червь

Средства третьего типа также могут проявлять себя в определенных условиях и предназначены для направленного искажения информации, засылки сообщений не по адресу или блокировки приема и передачи сообщений.

Основными путями проникновения вредоносных программ в АСУ являются:

- заражение программного обеспечения абонентских пунктов путем нерегламентированных действий пользователей (в основном путем запуска посторонних программ);
- умышленное внедрение в программное обеспечение абонентских пунктов путем их ассоциирования с выполняемыми программными модулями или программами начальной загрузки, либо использование в виде отдельных программных модулей;

- передача с пересылаемыми файлами на другие абонентские пункты и заражение его программного обеспечения после пользования зараженными программами;
- распространение внутри абонентских пунктов, объединенных в локальную вычислительную сеть;
- внедрение в программное обеспечение абонентских пунктов при запуске программ с удаленного абонентского пункта;
- внедрение при разрешении записи с удаленного терминала;
- внедрение в пересылаемые файлы на коммуникационные машины и серверы локальных сетей.

Основными функциями вредоносных программ являются:

- исследовавние систем защиты информации, перехват паролей и шифров обрабатываемых данных;
- разрушение данных и программ АСУ;
- копирование, искажение и навязывание ложной информации через коммуникационные фрагменты сети;
- имитация посылки сообщений на локальные фрагменты сети;
- имитация удаленного доступа к ресурсам локальных фрагментов сети;
- копирование, навязывание, искажение информации в пределах локальных фрагментов сети при передаче по собственным линиям связи.

Основное их назначение – разрушение функций самоконтроля или изменение алгоритмов функционирования программ системы разграничения доступа пользователей к ресурсам вычислительной сети, уничтожение или компрометации данных о полномочиях пользователей, нарушение работы всей сети в целом и систем разграничения доступа в частности. При этом информация для их работы

должна предоставляться средствами типа «программная закладка». По методу и месту внедрения и применения выделяются следующие группы средств данного типа:

- программы, код которых ассоциирован с программами начальной загрузки, находящихся в Master Boot Record или Boot – секторах активных разделов;
- программы, код которых ассоциирован с программами загрузки драйверов операционной системы, командного интерпретатора, сетевых драйверов.

Логическая бомба

Средства четвертого типа нацелены на проникновение в системы разграничения доступа пользователей к ресурсам вычислительной сети с целью перехвата информации от подсистем СЗИ. По методу и месту внедрения и применения выделяются следующие группы средств данного типа:

- программы–имитаторы, имитирующие программы ввода конфиденциальной информации, совпадающие с реальными программами лишь по внешним признакам;
- неинтегрированные программы, т.е. программы, содержащие лишь свой собственный код (внедряемые в пакетные файлы типа .bat).

Логический люк

Отличительной особенностью средств пятого типа является доминирование механизма самомодификации структуры, что обеспечивает таким программам возможность длительного пребывания в вычислительной среде за счет низкой вероятности обнаружения антивирусными программами. Такие программы могут проявлять только в условиях и на фоне работы программ манипулирования данными и

ориентированы на направленную модификацию или копирование данных в информационных массивах.

Объектами воздействия вредоносных программ в АСУ являются данные и программы абонентских пунктов, коммутационных машин и серверов ЛВС.

Основными последствиями проникновения вредоносных программ в распределенную вычислительную сеть АС являются:

1. Для абонентских пунктов сети:

- искажение (разрушение) файлов и системных областей операционной системы;
- уменьшение скорости работы, неадекватная реакция на команды пользователя;
- вмешательство в процесс обмена сообщениями по сети путем непрерывной посылки хаотических сообщений;
- блокирование принимаемых или передаваемых сообщений, их искажение;
- имитация физических сбоев;
- имитация пользовательского интерфейса или приглашений ввода паролей с целью их запоминания;
- накопление обрабатываемой и конфиденциальной информации в скрытых областях внешней памяти;
- анализ кодов оперативной памяти с целью выявления ключевых таблиц или фрагментов ценной информации;
- искажение программ и данных в оперативной памяти ЭВМ.

2. Для серверов локальных сетей:

- искажение информации проходящей через сервер (при обмене между абонентскими пунктами);

- сохранение проходящей информации в скрытых областях внешней памяти;
- искажение или уничтожение собственной информации сервера (в частности идентификационных таблиц) и тем самым нарушение работы локальной сети;
- внедрение разрушающих программ в файлы пересылаемые внутри локальной сети или на удаленные абонентские пункты.

3. Для коммуникационных машин:

- разрушение собственного программного обеспечения коммуникационной машины и вывод из строя коммуникационного узла вместе со всеми присоединенными абонентскими пунктами;
- засылка пакетов не по адресу, потеря пакетов, неверная сборка пакетов, подмена пакетов;
- контроль активности абонентов коммуникационной машины для получения косвенных данных о характере информации, которой обмениваются абоненты сети.

В таблице 8 приведены данные о свойствах вредоносных программ применительно к различным этапам обобщенной стратегии проникновения в АС.

Структурно–временные особенности применения вредоносных программ приводят к необходимости рассматривать в качестве объекта оптимизации процесс функционирования АС в условиях воздействия таких программ.

Таблица 8.

Этап	Проявляемые свойства	Объекты воздействия	Длительность
Первый этап	«Программная закладка»	Идентификационные таблицы, пароли	1–5 минут
Второй этап			
Фаза 1	«Программная закладка», «Логический люк»	Подсистема преобразования информации, подсистема поддержания целостности вычислительной среды, подсистема закрытия и подсистема регистрации	3–10 минут
Третий этап			
Фаза 1	«Программный червь»	Подсистема обеспечения санкционированного доступа СРВ	10–20 минут
Фаза 2	«Логическая бомба»	Подсистема разграничения доступа СЗИ	
Фаза 3	«Логический люк»	Информационные массивы АС	
Фаза 4	«Классические» вирусы, «Программный червь»	Информационные массивы АС	
Фаза 5	«Логический люк»	Информационные массивы АС	

Это приводит к необходимости ориентироваться на разработку и использование программных методов защиты информации с целью противодействия такого типа угрозам в АСТНК.

Р а з д е л 7. Управление информационной безопасностью АСТНК

Лекция 24. Аудит рисков информационной безопасности АСТНК

Термины и определения

Ресурс (Asset). В широком смысле это все, что представляет ценность с точки зрения организации и является объектом защиты. В узком смысле ресурс — часть информационной системы. В прикладных методах анализа рисков обычно рассматриваются следующие классы ресурсов:

- оборудование (физические ресурсы);
- информационные ресурсы (базы данных, файлы, все виды документации);
- программное обеспечение (системное, прикладное, утилиты, другие вспомогательные программы);
- сервис и поддерживающая инфраструктура (обслуживание СВТ, энергоснабжение, обеспечение климатических параметров и т.п.).

Информационная Безопаснсоть (ИБ) (Information Security) — защищенность ресурсов ИС от факторов, представляющих угрозу для:

- конфиденциальности;
- целостности;
- доступности.

Угроза (Threat) — совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности.

Уязвимость (Vulnerability) — слабость в системе защиты, которая делает возможной реализацию угрозы.

Анализ рисков — процесс определения угроз, уязвимостей, возможного ущерба, а также контрмер.

Базовый уровень безопасности (Baseline Security) — уровень, соответствующий критериям CCTA Baseline Security Survey. Обязательный минимальный уровень защищенности для информационных систем государственных учреждений Великобритании.

Методы данного класса применяются в случаях, когда к информационной системе не предъявляется повышенных требований в области информационной безопасности.

Риск нарушения ИБ (Security Risk) — возможность реализации угрозы.

Оценка рисков (Risk Assessment) — идентификация рисков, выбор параметров для их описания и получение оценок по этим параметрам.

Управление рисками (Risk Management) — процесс определения контрмер в соответствии с оценкой рисков.

Система управления ИБ (Information Security Management System) — комплекс мер, направленных на обеспечение режима ИБ на всех стадиях жизненного цикла ИС.

Класс рисков — множество угроз ИБ, выделенных по определенному признаку (например, относящихся к определенной подсистеме или типу

Аудит представляет собой независимую экспертизу отдельных областей функционирования организации. Аудит безопасности информационных систем является одной из составляющих ИТ аудита.

Цели аудита ИБ АСТНК

Целями проведения аудита безопасности являются:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;

- оценка текущего уровня защищенности ИС;
- локализация узких мест в системе защиты ИС;
- оценка соответствия ИС существующим стандартам в области информационной безопасности;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Этапность работ по проведению аудита безопасности информационных систем

Аудит проводится не по инициативе аудитора, а по инициативе руководства компании, которое в данном вопросе является основной заинтересованной стороной. Поэтому на этапе инициирования процедуры аудита должны быть решены следующие организационные вопросы: права и обязанности аудитора должны быть четко определены и документально закреплены в его должностных инструкциях, а также в положении о внутреннем (внешнем) аудите; аудитором должен быть подготовлен и согласован руководством план проведения аудита.

На этапе инициирования процедуры аудита должны быть определены границы проведения обследования. Одни информационные подсистемы компании не являются достаточно критичными и их можно исключить из границ проведения обследования. Другие подсистемы могут оказаться недоступными для аудита из–за соображений конфиденциальности.

Границы проведения обследования определяются в следующих категориях:

1. Список обследуемых физических, программных и информационных ресурсов.

2. Площадки (помещения), попадающие в границы обследования.

3. Основные виды угроз безопасности, рассматриваемые при проведении аудит.

4. Организационные (законодательные, административные и процедурные), физические, программно–технические и прочие аспекты обеспечения безопасности, которые необходимо учесть в ходе проведения обследования, и их приоритеты (в каком объеме они должны быть учтены). План и границы проведения аудита обсуждается на рабочем собрании, в котором участвуют аудиторы, руководство компании и руководители структурных подразделений.

Этап сбора информации аудита, является наиболее сложным и длительным. Это связано с отсутствием необходимой документации на информационную систему и с необходимостью плотного взаимодействия аудитора со многими должностными лицами организации.

Получение информации об организации, функционировании и текущем состоянии ИС осуществляется аудитором в ходе специально организованных интервью с ответственными лицами компании, путем изучения технической и организационно–распорядительной документации, а также исследования ИС с использованием специализированного программного инструментария.

Используемые аудиторами методы анализа данных определяются выбранными подходами к проведению аудита, которые могут существенно различаться.

Первый подход, самый сложный, базируется на анализе рисков. Опираясь на методы анализа рисков аудитор определяет для обследуемой ИС индивидуальный набор требований безопасности, в наибольшей степени учитывающий особенности данной ИС, среды ее функционирования.

Второй подход, самый практичный, опирается на использование стандартов информационной безопасности. Стандарты определяют

базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики. Стандарты могут определять разные наборы требований безопасности, в зависимости от уровня защищенности ИС, который требуется обеспечить, ее принадлежности (коммерческая организация, либо государственное учреждение), а также назначения (финансы, промышленность, связь и т.п.).

Анализ рисков – первый этап построения любой системы информационной безопасности. Он включает в себя мероприятия по обследованию безопасности ИС, с целью определения того какие ресурсы и от каких угроз надо защищать, а также в какой степени те или: иные ресурсы нуждаются в защите. Определение набора адекватных контрмер осуществляется в ходе управления рисками.

Риск определяется вероятностью причинения ущерба и величиной ущерба, наносимого ресурсам ИС, в случае осуществления угрозы безопасности.

Анализ рисков состоит в том, чтобы выявить существующие риски и оценить их величину (дать им качественную, либо количественную оценку).

Третий подход, наиболее эффективный, предполагает комбинирование первых двух. Базовый набор требований безопасности, предъявляемых к ИС, определяется стандартом. Дополнительные требования, в максимальной степени учитывающие особенности функционирования данной ИС, формируются на основе анализа рисков.
Обычно выделяют следующие фазы управления рисками ИБ:

- идентификация ключевых ресурсов ИС;
- определение важности тех или иных ресурсов для организации;

- идентификация существующих угроз безопасности и уязвимостей ,делающих возможным осуществление угроз;
- вычисление рисков, связанных с осуществлением угроз безопасности.

Ресурсы разделяют на следующие категории:

- информационные ресурсы;
- программное обеспечение;
- технические средства (серверы, рабочие станции, активное сетевое оборудование и т. п.);
- людские ресурсы.

Важность (или стоимость) ресурса определяется величиной ущерба, наносимого в случае нарушения конфиденциальности, целостности или доступности этого ресурса.

Определение величины риска

Величина риска определяется на основе стоимости ресурса, вероятности осуществления угрозы и величины уязвимости по следующей формуле:

Риск = (стоимость ресурса * вероятность угрозы) / величина уязвимости.

Под уязвимостями обычно понимают свойства ИС, делающие возможным успешное осуществление угроз безопасности.

Задача управления рисками заключается в выборе обоснованного набора контрмер, позволяющих снизить уровни рисков до приемлемой величины. Стоимость реализации контрмер должна быть меньше величины возможного ущерба. Разница между стоимостью реализации контрмер и величиной возможного ущерба должна быть обратно пропорциональна вероятности причинения ущерба.

Аудит базового уровня информационной безопасности

В последнее время появились национальные и ведомственные стандарты, в которых определены требования к базовому уровню безопасности информационных технологий.

Британские стандарты BS7799. Документ "BS7799: Управление ИБ" состоит из двух частей.

В частиас 1: «Практические рекомендации» определяются и рассматриваются следующие аспекты ИБ:

- политика безопасности;
- организация защиты;
- классификация и управление информационными ресурсами;
- управление персоналом;
- физическая безопасность;
- администрирование компьютерных систем и сетей;
- управление доступом к системам;
- разработка и сопровождение систем;
- проверка системы на соответствие требованиям ИБ;

Часть 2: «Спецификации системы», рассматривает эти же аспекты с точки зрения сертификации информационной системы на соответствие требованиям стандарта.

Базовые требования в области ИБ в США. В США имеется похожий по подходу и степени подробности документ «Руководство по политике безопасности для автоматизированных информационных систем», в котором рассмотрены:

- общие положения политики безопасности;
- поддержание безопасности на протяжении жизненного цикла;
- минимальные (базовые) требования в области ИБ.

Германский стандарт BSI «Руководство по защите информационных технологий для базового уровня.

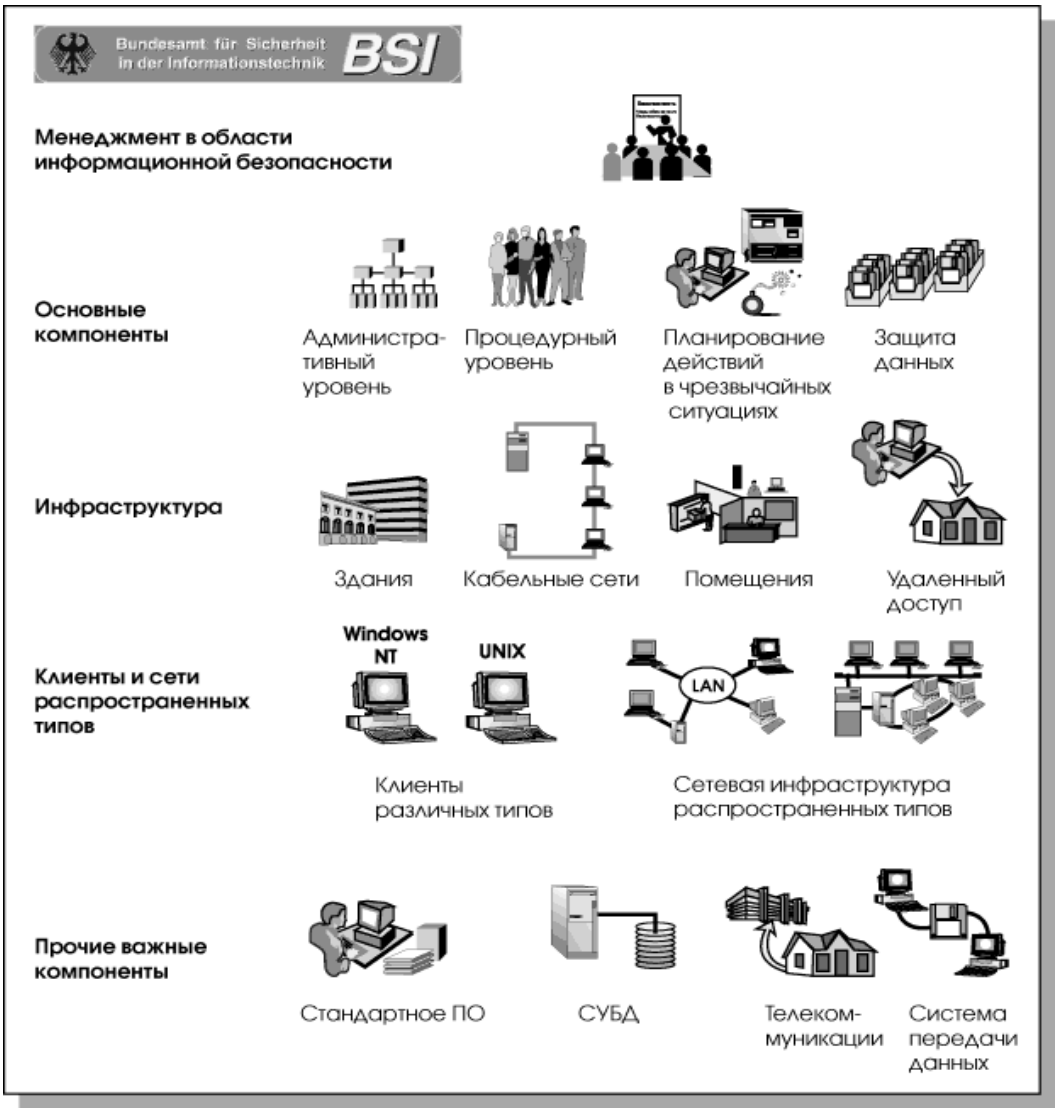

Рисунок 21. Германский стандарт BSI. Общая структура документа.

Общая структура документа приведена на рис.21.

Можно выделить следующие блоки:

- Методология управления ИБ (организация менеджмента в области ИБ).
- Компоненты информационных технологий:

  – основные компоненты (организационный уровень ИБ);

  – процедурный уровень, организация защиты данных, планирование действий в чрезвычайных ситуациях:

– инфраструктура (здания, помещения, кабельные сети, организация удаленного доступа);

– клиентские компоненты различных типов (DOS, Windows, UNIX, мобильные компоненты, прочие типы);

– сети различных типов (соединения "точка–точка", сети Novell NetWare, сети с ОС UNIX и Windows, разнородные сети):

– элементы систем передачи данных (электронная почта, модемы, межсетевые экраны и т.д.);

– телекоммуникации (факсы, автоответчики, интегрированные системы на базе ISDN, прочие телекоммуникационные системы);

– стандартное ПО;

– базы данных.

- Каталоги угроз безопасности и контрмер (около 600 наименований в каждом каталоге). Каталоги структурированы следующим образом.

Угрозы по классам:

– форсмажорные обстоятельства;

– недостатки организационных мер;

– ошибки человека;

– технические неисправности;

– преднамеренные действия.

Контрмеры по классам:

– улучшение инфраструктуры;

– административные контрмеры;

– процедурные контрмеры;

– программно–технические контрмеры;

– уменьшение уязвимости коммуникаций;

– планирование действий в чрезвычайных ситуациях.

Все компоненты рассматриваются по следующему плану: общее описание, возможные сценарии угроз безопасности (перечисляются применимые к данной компоненте угрозы из каталога угроз безопасности), возможные контрмеры (перечисляются возможные контрмеры из каталога контрмер).

Построение модели информационной технологии

Между ресурсами, очевидно, существуют взаимосвязи. Например, выход из строя какого–либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи необходимо учитывать, для чего строится модель организации с точки зрения ИБ.

Эта модель обычно строится следующим образом. Для выделенных ресурсов определяется их ценность как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т.д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации. а основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер должны являться рекомендации по проведению регулярных проверок эффективности системы защиты.

Инструментальные средства аудита рисков ИБ

Применение каких–либо инструментальных средств не является обязательным, однако оно позволяет уменьшить трудоемкость проведения анализа рисков и выбора контрмер. В настоящее время на рынке есть около десятка программных продуктов для анализа и

управления рисками базового уровня безопасности. Демо–версии некоторых продуктов доступны по Интернет. При выполнении полного анализа рисков приходится решать ряд сложных проблем:

- Как определить ценность ресурсов?
- Как составить полный список угроз ИБ и оценить их параметры?
- Как правильно выбрать контрмеры и оценить их эффективность?
- Для решения этих проблем существуют специально разработанные инструментальные средства, построенные с использованием структурных методов системного анализа и проектирования (SSADM — Structured Systems Analysis and Design).

В настоящее время на рынке присутствует несколько программных продуктов этого класса. Наиболее популярный из них, CRAMM.

Целью разработки этого метода являлось создание формализованной процедуры, позволяющей:

- убедиться, что требования, связанные с безопасностью, полностью проанализированы и документированы;
- избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков;
- оказывать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем;
- обеспечить проведение работ в сжатые сроки;
- автоматизировать процесс анализа требований безопасности;
- представить обоснование для мер противодействия;
- оценивать эффективность контрмер, сравнивать различные варианты контрмер;
- генерировать отчеты.

В настоящее время CRAMM является, судя по количеству ссылок в Интернете, самым распространенным методом анализа и контроля рисков.

Анализ рисков включает в себя идентификацию и вычисление уровней (мер) рисков на основе оценок, присвоенных ресурсам, угрозам и уязвимостям ресурсов.

Контроль рисков состоит в идентификации и выборе контрмер, позволяющих снизить риски до приемлемого уровня.

Этот метод, должен гарантировать, что защита охватывает всю систему и существует уверенность в том, что:

- все возможные риски идентифицированы;
- уязвимости ресурсов идентифицированы и их уровни оценены;
- угрозы идентифицированы и их уровни оценены;
- контрмеры эффективны;
- расходы, связанные с ИБ, оправданы.

Исследование ИБ системы с помощью CRAMM проводится в три стадии.

Стадия 1: анализируется все, что касается идентификации и определения ценности ресурсов системы. В конце стадии 1 заказчик исследования будет знать, достаточно ли ему существующей традиционной практики или он нуждается в проведении полного анализа безопасности.

Стадия 2: рассматривается все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. В конце стадии 2 заказчик получает идентифицированные и оцененные уровни рисков для своей системы.

Стадия 3**:** поиск адекватных контрмер. По существу – это поиск варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика.

Лекция 25. Управление рисками информационной безопасности

Формальная постановка проблемы оценки информационных рисков

Анализ существующих подходов к проблеме оценки информационных рисков показывает, что этот вопрос в большей степени является открытым, так как сама эта проблемная область еще плохо формализована и изучена. Модели этой проблемной области очень грубы, дают, как правило, качественные оценки, достоверность которых не всегда очевидна. Это связано с огромной сложностью самой проблемы и с зависимостью ее от чисто субъективных факторов.

Для описания таких моделей используется различный математический аппарат: методы субъективной вероятности, нечеткие множества, нейронные сети и т.д. Подобные модели являются средством уменьшения степени неопределенности при выборе возможных вариантов решений. Также проблемную область оценки информационных рисков можно описать в виде семантической модели, общий вид которой представлен на рис. 22.

В рамках рассматриваемой модели выделяют четыре проблемные подобласти. Первая из них (φ_1) связана с установлением соответствия между существующими информационными объектами и теми информационными рисками, которые определены для АСТНК. В рамках этой подобласти описывается степень влияния информационного объекта, его значимость с точки зрения тех информационных рисков, которые присуще АСТНК. Фактически здесь специфицируется связь между служебной информацией, обрабатываемой в АСТНК, и теми последствиями, к которым может привести нарушение характеристик качества обработки этой служебной информации в части ее доступности, целостности и конфиденциальности.

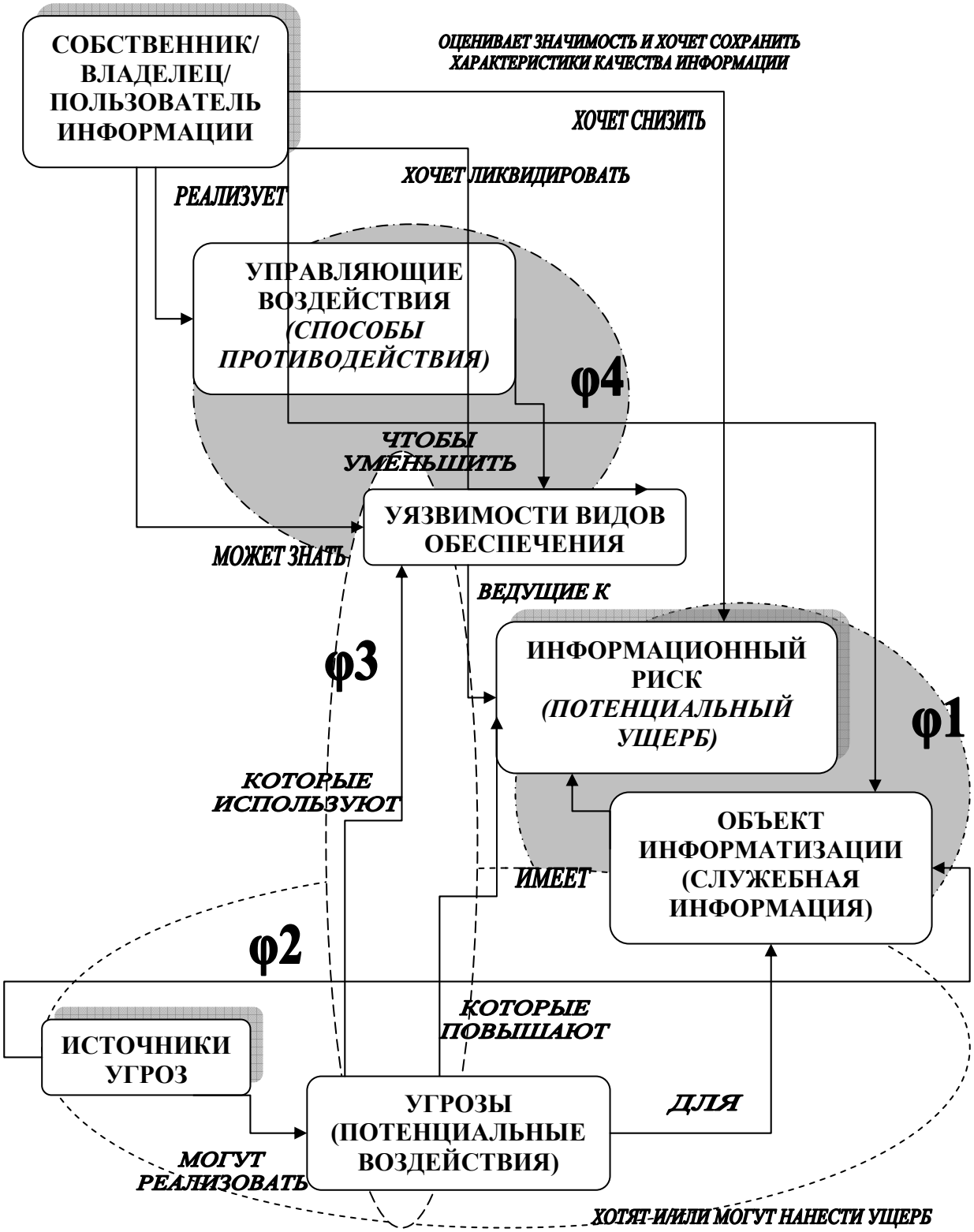

Рис 22. Семантическая модель проблемной области оценки информационных рисков

Так например, нарушение конфиденциальности информации о допустимых финансовых условиях для одной из сторон в рамках некоторой коммерческой операции может привести к тому, что противоположная сторона в рамках этой операции изначально будет ориентироваться на эти допустимые условия и экономический эффект этой коммерческой операции уже будет предопределен еще до начала обсуждения условий ее реализации.

Вторая подобласть (φ_2) связана со степенью значимости угроз для конкретных информационных объектов. В рамках этой подобласти описывается степень влияния тех или иных угроз (потенциальных воздействий) на конкретные информационные объекты. Фактически здесь специфицируется уровень критичности тех или иных воздействий на качество служебной информации, обрабатываемой в АСТНК.

Так например, задержка загрузки информации в базу данных АСТНК в одном случае не является значимой угрозой (регламент ее обработки допускает это), а в другом случае это может негативно сказаться на своевременности

представления информации ЛПР.

Третья подобласть (φ_3) связана со значимостью реализации угроз посредством использования конкретных уязвимостей в АСТНК с точки зрения определенных информационных рисков. В рамках этой подобласти описывается критичность использования той или иной уязвимости АСТНК при реализации конкретной угрозы для конкретного информационного риска. Фактически здесь специфицируется возможность материализации определенного события риска за счет использования слабых мест АСТНК при реализации конкретного воздействия на обрабатываемую служебную информацию.

Так, например, несанкционированная возможность работы на РМ (рабочем месте) проблемно–тематического аналитика не позволит

модифицировать первичную базу данных (нарушить целостность), так как эта операция может быть осуществлена только с РМ аналитика–технолога, но позволит получить обобщенную и агрегированную информацию в рамках некоторой регламентной задачи (нарушение конфиденциальности).

И, наконец, четвертая подобласть (φ_4) связана с эффективностью различных механизмов противодействия угрозам, используемым в АСТНК. В рамках этой подобласти описывается эффективность мер, направленных на снижение объективных, субъективных и случайных уязвимостей. Эти механизмы могут быть связаны с информационным, программным, техническим, инженерно–физическим, кадровым и организационно–нормативным обеспечением функционирования АСТНК. Механизмы противодействия могут касаться как самой АСТНК, так и внешней среды ее функционирования.

Например, снижение количества семантических и синтаксических ошибок, которые могут возникнуть (нарушение достоверности) при вводе информации в корпоративную базу данных АСТНК, может быть достигнуто как за счет повышения квалификации соответствующих групп пользователей, так и за счет повышения функциональных возможностей средств автоматического контроля корректности вводимых данных.

В соответствии с этой семантической моделью были введены показатели:

$G = \{G_i\}$, $(i = 1,\ldots,I)$ – множество угроз;

$R = \{\langle E_j, Q_j \rangle\}$, $(j = 1,\ldots,J)$ – множество рисков;

$U = \{U_d\}$, $(d = 1,\ldots,D)$ – множество уязвимостей;

$S = \{S_k\}$, $(k = 1,\ldots,K)$ – множество источников угроз;

$O = \{O_b\}$, $(b = 1,\ldots,B)$ – множество объектов воздействия;

$Z = \{\langle F_n, C_n \rangle\}$, (n = 1,…,N) – множество способов противодействия.

Где E_j – событие риска, Q_j – величина ущерба,

F_n – реализуемая функция, C_n – –стоимость реализации.

В соответствии с проблемными подобластями семантической модели определим для этих множеств следующие отображения:

$O \times R \xrightarrow{\varphi 1} A$, где A – множество чисел от 0 до 1, определяющих степень;

обусловленности рисков существующим множеством объектов;

$S \times G \times O \xrightarrow{\varphi 2} V$, где V – множество чисел от 0 до 1, определяющих степень критичности угроз множеству объектов;

$G \times U \times R \xrightarrow{\varphi 3} P$, где P – множество пар чисел $\left\langle P^{(E)}, P^{(Q)} \right\rangle$, определяющих потенциал рисков при наличии множества угроз и множества уязвимостей, таких, что $0 \le P^{(E)} \le 1$, $P^{(Q)} \ge 0$; $Z \times U \xrightarrow{\varphi 4} M$, где M – множество чисел от 0 до 1, определяющих степень доступности уязвимостей в условиях применения множества способов противодействия.

С точки зрения задачи снижения информационных рисков необходимо было осуществить оптимизацию использования средств противодействия в части минимизации уязвимостей АСТНК. Значимость конкретных процессов обработки информации определяет необходимость принятия тех или иных мер по снижению информационных рисков. Эти меры должны реализовываться через придание этим процессам обработки информации определенных свойств и включением в них соответствующих средств противодействия уязвимостям. Применяемые меры и реализуемые средства должны быть адекватными возможным угрозам и реализовывать

предписания регламента обработки информации, устанавливаемые нормативно–правовыми документами АСТНК. Недостаточность мер может повлечь за собой высокий уровень остаточного информационного риска. Излишние меры, в свою очередь, связаны с избыточными затратами финансовых, материальных и людских ресурсов, могут привести к ухудшению функциональных характеристик системы обработки информации. Реализация функций по снижению информационных рисков предполагает декомпозицию этих функций на группы (возможно с дублированием), обеспечением которых должны заниматься соответствующие средства, реализованные в виде взаимосвязанной (многоконтурной и многоуровневой) подсистемы элементов различной природы в рамках АСТНК.

Таким образом, можно сформулировать оптимизационная задачу следующего вида:

$$\min_{Z} \max_{G} P_{\Sigma},$$

где $P\Sigma$ – консолидированный риск по оцениваемому множеству информационных объектов АСТНК. При этом должны учитываться ограничения на потенциальные возможности наступления определенных событий риска, максимально допустимый для АСТНК ущерб и приемлемую (заданную) стоимость методов противодействия. Ущерб от наступления событий риска может выражаться в денежном выражении, в трудоемкости процессов по ликвидации их последствий, некоторых условных единицах, характеризующих степень негативных последствий. Стоимость методов противодействия может выражаться в денежном выражении, в трудоемкости поддержания процессов по снижению информационных рисков, в объемно–временных затратах средств противодействия в системе.

Таким образом, в основе процессов консолидации/декомпозиции информационных рисков лежит архитектура АСТНК, которая позволяет связать элементы системы, потенциальные угрозы нарушения характеристик качества СОИ и информационные риски (φ1×φ2).

Структура деревьев угроз

Для моделирования процесса консолидации/декомпозиции можно использовать специальные конструкции – деревья угроз. В корне дерева помещается угроза, соотнесенная с совокупностью угроз меньшего уровня абстракции. Составляющие угрозы образуют листья дерева угроз. Объединение деревьев приводит к образованию структуры частичного порядка – решетка угроз. В этой структуре максимальными элементами являются угрозы, а именно, угрозы нарушения целостности, доступности и конфиденциальности информации. Для построения таких деревьев предлагается использовать три структурные абстракции: обобщение, агрегация, ассоциация. Они позволяют соответственно специфицировать отношения «тип – подтип», «целое – часть», «совокупность – элемент». Структуру типа «угроза» можно представить как агрегат и/или ассоциацию базовых типов «угроза», а сам агрегат/ассоциация может служить объектом обобщения (классификации). Классификация типов «угроза» может быть выражена иерархией обобщений, элементы которой могут представлять собой иерархию агрегаций и/или ассоциаций. Применяя подход «снизу вверх», абстракцию можно представить как процесс синтеза консолидированных угроз из более простых угроз. С другой стороны, аналитический подход «сверху – вниз» дает возможность, начав с консолидированных угроз, путем их декомпозиции прийти к уровню «элементарных» угроз. Подход «сверху – вниз» применяют с целью понять сложные угрозы и связь между ними, а подход «снизу – вверх» – для конструирования консолидированных угроз. Оба подхода

применяются одновременно. Путем использования указанных абстракций проблематика оценки информационных рисков может быть разложена на небольшие, осмысленные понятия, которые поддаются оценке и для которых могут быть определены различного рода шкалы и меры. Необходимо отметить, что рассматриваемые структурные абстракции напрямую связаны с процедурными абстракциями, широко используемыми в технологии программирования различных процессов. Такими процедурными абстракциями являются: порядок, отбор и повторение. Агрегирование соответствует порядку, т.е. процедуре sequence. Операция над агрегатом вырождается в последовательность операций над каждым компонентом. Обобщение соответствует отбору, т.е. процедуре if_then_else. Операция над обобщением вырождается в операцию над некоторой обобщенной категорией. Ассоциация соответствует повторению, т.е. процедуре while_do или for_each. Операция над набором вырождается в операцию, которая применяется к каждому члену набора. Эти три формы процедурных абстракций могут быть использованы для описания всех примитивно рекурсивных функций, для которых решаются вопросы их эффективной вычислимости.

Таким образом, обобщение реализует логику «ИЛИ» для составляющих ее элементов. Это означает, что корневая угроза соотносится с любой из угроз–листьев этого дерева (рис 23), т.е. угроза G_0 может быть реализована при условии реализации хотя бы одной из угроз G_1, G_2, G_3.

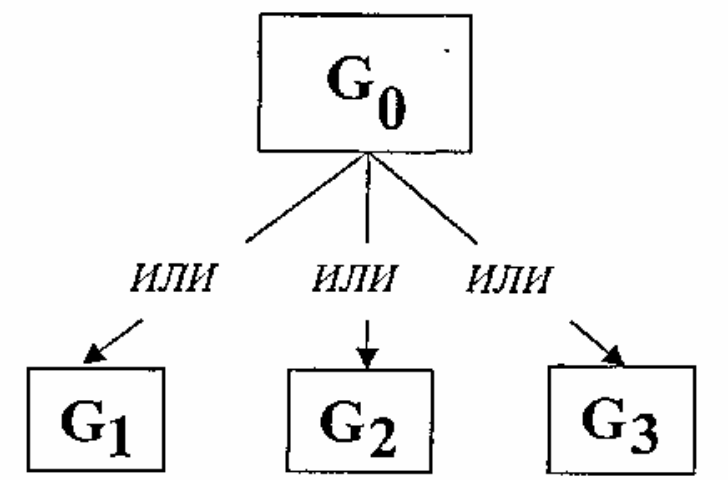

Рис 23. Пример дерева угрозы – обобщения

Агрегация реализует логику «И» для составляющих ее элементов. Это означает, что корневая угроза соотносится со всей совокупности угроз–листьев этого дерева (рис 24), которые реализуются в определенной последовательности, т.е. угроза G_0 может быть реализована при условии реализации всех угроз в установленном порядке от G_1 до G_3.

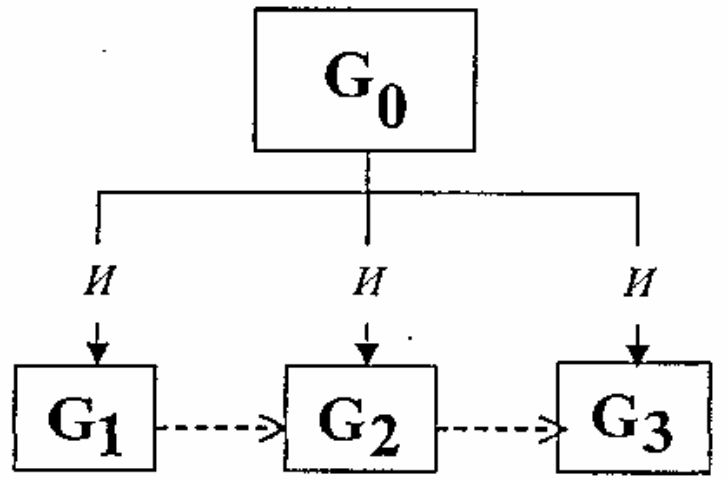

Рис 24. Пример дерева угрозы – агрегация.

Ассоциация реализует логику «И» для составляющих ее элементов. Это означает, что корневая угроза соотносится со всей совокупностью угроз листьев этого дерева (рис 25), которые реализуются в произвольной последовательности, т.е. угроза G_0 может быть реализована при условии реализации всех угроз G_1, G_2, G_3 в произвольном порядке.

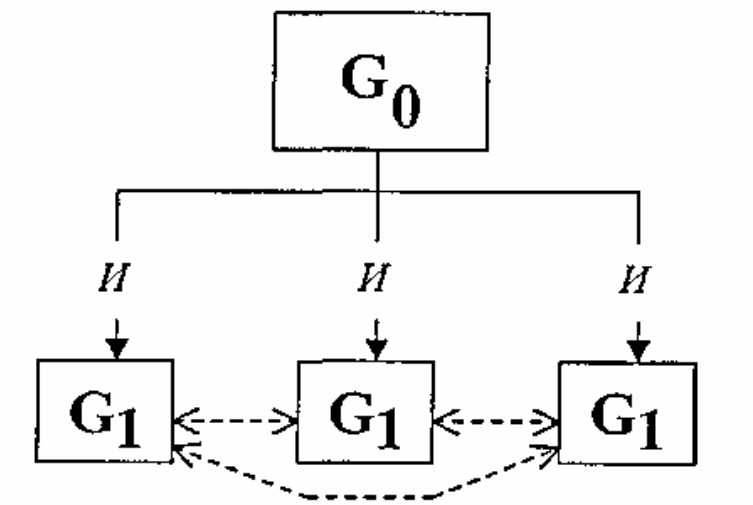

Рис 25. Пример дерева угрозы – ассоциация.

В качестве примеров таких консолидированных угроз можно привести следующие:

1. Угроза–обобщение. Угроза несанкционированного ознакомления с информацией (G_0) может быть реализована либо путем несанкционированного доступа к информации в момент ее передачи (G_1), либо путем несанкционированного прочтения информации в момент ее визуализации (G_2), либо путем несанкционированного доступа к файловой системе (G_3).

2. Угроза–агрегация. Угроза несанкционированного доступа к информации (G_0) может быть реализована только в следующей последовательности: несанкционированное проникновение на территорию объекта информатизации (G_1), несанкционированное подключение к сети (G_2), несанкционированный доступ к файловой системе (G_3).

3. Угроза–ассоциация.Угроза несанкционированного уничтожения информации (G_0) может быть реализована на следующей совокупности угроз, реализованных в произвольной последовательности: уничтожение информации в базе данных (G_1), уничтожение информации в файлах резервных копий (G_2), уничтожение информации на бумажных носителях(G_3).

Представленные методы консолидации и декомпозиции угроз имеют следующие положительные моменты:

1. В рамках данных методов для каждой конкретной АСТНК могут быть заданы три типа отношений между угрозами на различных уровнях системы, что позволяет связать семантику информационных процессов объекта информатизации с конкретной технической реализацией АСТНК.

2. Введенные абстракции позволяют задать на множестве угроз различных уровней АСТНК отношение частичного порядка, которое дает возможность представления совокупности этих угроз в виде структуры типа решетка. Для структур подобного типа существуют формальные алгоритмы для исследования свойств объектов, представленных в виде такой структуры. Так, например, становится возможным проанализировать целостность и непротиворечивость определенного множества угроз, соответствие их структуре АСТНК.

3. Синтезируя указанную структуру, описывающую связность угроз различных уровней абстракции, можно выделять значимые пути, которые и будут определять наиболее критичные элементы АСТНК с точки зрения их потенциала риска.

4. На основании решетки угроз становится возможным осуществлять как качественный анализ информационных рисков, так и получать числовые оценки этих рисков в случае определения на этой решетке системы шкал и мер.

Технология управления рисками затрагивает все этапы жизненного цикла АСТНК и состоит из этапов, приведенных в табл. 9.

Таблица. 9

Фаза жизненного цикла информационной технологии	Соответствие фазе управления рисками
1.Предпроектная стадияАСТНК. Определение целей и задач их документирование.	Выявление основных классов рисков для данной АСТНК, вытекающих из целей и задач, концепция обеспечения ИБ
2. Проектирование АСТНК	Выявление рисков, специфичных дляданнойАСТНК (вытекающих из особенностей архитектуры АСТНК)
3.Создание АСТНК (поставка элементов, монтаж, настройка и конфигурирование)	До начала функционирования должны быть идентифицированы и приняты во внимания все классы рисков
4. Функционирование АСТНК	Периодическая идентификация, анализ, мониторинг,реализация контрмер, связанныхс изменениями внешних условий и в конфигурации АСТНК
5. Прекращение функционирования АСТНК.	Соблюдение требований информационной безопасности по отношению к выводимым информационным ресурсам

СПИСОК ОБЯЗАТЕЛЬНОЙ ЛИТЕРАТУРЫ

Раздел 1. Сущность, задачи и организационно-правовые основы проблемы информационной безопасности АСТНК

Безопасность России. Правовые, социально-экономические и научно-технические аспекты. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. МГФ «Знание», 2005. Стр. 71-99, стр. 255-298, стр. 464-482.

Раздел 2. Основные теоретические результаты в области теории информационной безопасности

Безопасность России. Правовые, социально-экономические и научно-технические аспекты. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. МГФ «Знание», 2005. Стр. 350-406.

П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков.

Теоретические основы компьютерной безопасности. М.: Радио и связь, 2000. Стр. 89-115, стр. 118-149.

Раздел 3. Критерии и спецификации безопасности автоматизированных систем и информационных технологий

П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков.

Теоретические основы компьютерной безопасности. М.: Радио и связь, 2000. Стр.149-148.

Раздел 4. Организационно-режимные меры и программно-аппаратные средства обеспечения конфиденциальности, целостности и доступа к информации

П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков.

Теоретические основы компьютерной безопасности. М.: Радио и связь, 2000. Стр. 27-87.

Раздел 5. Архитектура безопасности взаимодействия открытых систем

П.Н. Девянин, А.М. Ивашко, А.С. Першаков, В. Г. и др. Программно-аппаратные средства защиты от несанкционированного доступа к

компьютерным криптографическим системам обработки информации. Учеб. пособ. МИЭМ, 2004.Стр.6-8, стр. 81-186.

Зима В.Н.,Молдовян А.А. и др. Безопасность глобальных сетевых технологий. - Спб.: БХВ-Петербург,2000. Стр.199-299.

Раздел 6. Обеспечение информационной безопасности АСТНК на основе принципа гарантированного результата

П.Н. Девянин, А.М. Ивашко, А.С. Першаков, В. Г. и др. Программно-аппаратные средства защиты от несанкционированного доступа к компьютерным криптографическим системам обработки информации. Учеб. пособ. МИЭМ, 2004. Стр.26-56.

Раздел 7. Управление информационной безопасностью АСТНК

Петренко С.А., Симонов С.В. Управление информационными рисками.

М.: Компания АйТи; ДМК Пресс.2004. Стр101-155.

СПИСОК ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

Раздел 1. Сущность, задачи и организационно-правовые основы проблемы информационной безопасности АСТНК.

Научные и методологические проблемы информационной безопасности.

(Сб. статей) Под общ. ред. В. П. Шерстюка. – М.: МЦНМО, 2004.

Шерстюк В.П. Актуальные проблемы обеспечения информационной безопасности. Военная мысль. 2003, № 5.

Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации. - М. : Издательская группа ЮРИСТ, 2001.

Е.Б. Белов. Правовое обеспечение информационной безопасности.М: Радио и связь,2001.

Раздел 2. Основные теоретические результаты в области теории информационной безопасности

Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: издатель Молгачева С.В. 2001.

Раздел 3. Критерии и спецификации безопасности автоматизированных систем и информационных технологий

Голдовский И. Н. Безопасность платежей в Интернете. Спб-ПитерБ, 2001. Стр. 222-237.

Раздел 4 .Организационно-режимные меры и программно-аппаратные средства обеспечения конфиденциальности, целостности и доступа к информации

Мишин А.Ю. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита в сетях. М : Радио и связь.2001.

А.В. Петраков. Основы практической защиты информации.-- М.: Радио и связь. 2000.

Раздел 5. Архитектура безопасности взаимодействия открытых систем.

Галатенко В.А. Современная трактовка сервисов безопасности - Jet-Info, 1999, 5.

Браун С. Виртуальные частные сети. М.: Лорт,2001.

.Давыдова В.А. и др. Новые средства криптографической защиты информации. - М: Изд. МИФИ, 1996, 132 стр.

Варфоломеев А.В. и др. Управление ключами в системах защиты информации в банковских технологиях. - М: Изд. МИФИ, 1996.

Кабатянский А.Г. Математика разделения секрета// Математическое просвещение – 1998,Сер. , Вып. 2.

Диффи У. Хелманн М. Защищенность и имитостойкость. Введение в криптографию.//ТИИЭР, 1979, Т67, №3.

Пярин. А В. Генерация, распределение и использование криптографических ключей // Защита информации .-1992 т.1,стр. 114 - 152.

Саломаа. А В. Криптография с открытым ключом. М. : Мир, 1996.

Березин А. С. и др. Построение корпоративных защищенных виртуальных частных сетей.// Конфидент. Защита информации - №1, 2001. Стр.54-61.

Раздел 6. Обеспечение информационной безопасности АСТНК на основе принципа гарантированного результата.

Першаков. А С. О возможности гарантированной защиты информации в недоверенной среде.// Проблемы информационной безопасности-1999, т.1. Стр. 63 - 69.

Раздел 7. Управление информационной безопасностью АСТНК.

Проблемы управления информационной безопасностью. Под ред. Д.С. Черешкина Д.С. ИСА РАН,2002.

Медведовский И.Д. Руководство по управлению информационными рисками корпоративных информационных систем. Internet\Intranet, Domina Security, 2002.

ОПИСАНИЕ КУРСА И ПРОГРАММА

Цель и задачи курса.

Целью курса является изучение современных научных принципов, моделей, методов и средств обеспечения информационной безопасности в автоматизированных системах транснациональных корпораций (АСТНК), составляющих ядро мировой экономической системы и национальных экономик.

Задачами курса в ходе изучения дисциплины является овладение студентами следующими знаниями:

- Структура теории информационной безопасности (структура понятия «обеспечение информационной безопасности», основные понятия, определения, принципиальные особенности постановки проблемы и решения задач обеспечения информационной безопасности АСТНК).
- Организационно-правовые основы в сфере информационной безопасности АСТНК. Доктрина информационной безопасности Российской Федерации.
- Классификация угроз нарушения информационной безопасности АСТНК, источники, риски и формы атак на информацию.
- Понятие политики безопасности, доступа и монитора безопасности.
- Основные типы политики безопасности.
- Формальные описания и базовые принципы описания основных моделей безопасности.
- Методы и средства обеспечения информационной безопасности от угроз нарушения конфиденциальности , целостности и отказа доступа к информации.

- Стандарты и спецификации информационной безопасности.
- Архитектура и классификация основных сервисов безопасности открытых систем.
- Безопасность глобальных сетевых технологий.
- Синтез защищенных виртуальных сетей.
- Синтез моделей внутренних нарушителей, реализующих стратегию логического несанкционированного доступа к информации.
- Обобщенная модель стратегии удаленного логического несанкционированного доступа к информации.
- Аудит рисков информационной безопасности для решения задач управления информационной безопасностью АСТНК

Область знаний, в которой широко используются современные механизмы обеспечения информационной безопасности, включает сферу управления большими социально-экономическими системами.

Курс предназначен для обучения в магистратуре.

Данная дисциплина предназначена для подготовки специалистов по магистерской программе «Обеспечение информационной безопасности автоматизированных систем », может быть выбрана курсом по выбору по магистерским программам «Интеллектуалоные системы», «Разработка и применение нанотехнологий на базе проектирования и управления системами качества промышленных предприятий».

Курс является теоретическим, но предполагает получение практических знаний по синтезу компьютерных стеганографических систем обеспечения конфиденциальности информации, виртуальных защищенных сетей и разработке формальных моделей внутренних нарушителей а также организации и проведения аудита рисков информационной безопасности.

Инновационность курса по:

- содержанию

В курсе впервые реализуется системное описание актуальной проблемы обеспечения информационной безопасности АСТНК, используются современные научные результаты для постановки и решения задач управления информационной безопасностью АСТНК.

- методике преподавания

Системная организация наиболее актуальных Интернет – ресурсов, привлекаемых в процессе проведения семинарских занятий, и выполнения курсовой работы в рамках данной магистерской программы.

- литературе

Используются учебники признанных специалистов в отдельных аспектах проблемы обеспечения информационной безопасности, научные статьи и результаты диссертационных работ, выполненных в ведущих отечественных научных школах по проблеме информационной безопасности.

- организации учебного процесса

Введена курсовая работа по исследованию компьютерных стеганографических систем, реализация которой связана с использованием открытых сетей.

Структура курса : 72 часа (2 кредита)

Лекции:	50 часов
Семинары:	10 часов
Курсовая работа:	6 часов
Лабораторная работа:	6 часов

Темы лекций:

Лекция 1. (2 часа)

Место и роль информационной безопасности в общей совокупности проблем современного этапа развития глобальной и национальной экономических систем.

Лекция 2. (2 часа)

Структура категории « информационная безопасность». Введение в основы информационной безопасности АСТНК.

Лекция 3. (2 часа)

Организационно-правовые основы информационной безопасности АСТНК. Защита коммерческой тайны, интеллектуальной собственности.

Лекция 4. (2 часа)

Классификации угроз и методов обеспечения информационной безопасности.

Лекция 5 . (2 часа)

Информационные воздействия и несанкционированный доступ. Каналы несанкционированного доступа. Анализ причин нарушений информационной безопасности АСТНК.

Лекция 6. (2 часа)

Политика безопасности и основные типы политик безопасности.

Лекция 7. (2 часа)

Основные определения и базовые принципы построения формальных моделей политик безопасности.

Лекция 8. (2 часа)

Дискреционная модель Харрисона-Рузо-Ульмана разграничения, управления и контроля за распространением прав доступа. Критерий безопасности.

Типизованная матрица доступа.

Лекция 9. (2 часа)

Классическая мандатная модель политики безопасности Белла-Лападулы, особенности и области применения. Критерий безопасности.

Лекция 10. (2 часа)

Ролевая модель управления доступом. Формальные модели ролевой политики безопасности. Критерий безопасности.

Лекция 11. (2 часа)

Стандарты и спецификации информационной безопасности автоматизированных систем.

Лекция 12. (2 часа)

Федеральные критерии безопасности информационных технологий. Понятия продукта информационных технологий, профиля защиты, плана защиты.

Лекция 13. (2 часа)

Методы и средства обеспечения информационной безопасности от угрозы нарушения конфиденциальности информации.

Лекция 14. (2 часа)

Методы и средства обеспечения информационной безопасности от угрозы нарушения целостности информации.

Лекция 15. (2 часа)

Методы и средства обеспечения информационной безопасности от угрозы отказа доступа к информации.

Лекция 16. (2 часа)

Архитектура безопасности и сервисы безопасности взаимодействия открытых систем.

Лекция 17. (2 часа)

Протоколы сетевой безопасности (часть 1).

Лекция 18. (2 часа)

Протоколы сетевой безопасности (часть 2).

Лекция 19. (2 часа)

Обеспечение безопасности локальных вычислительных систем при подключении к глобальным сетям с использованием криптографических протоколов.

Лекция 20. (2 часа)

Синтез защищенных виртуальных систем.

Лекция 21. (2 часа)

Синтез модели внутреннего нарушителя.

Лекция 22. (2 часа)

Усложненная модель внутреннего нарушителя для реализации логического несанкционированного доступа.

Лекция 23. (2 часа)

Структурно-временная модель внешнего нарушителя.

Лекция 24. (2 часа)

Аудит рисков информационной безопасности АСТНК.

Лекция 25. (2 часа)

Управление рисками информационной безопасности.

Темы семинарских занятий:

1. Криптографические преобразования на основе методы замены и перестановок – 2 часа.
2. Стеганографические методы обеспечения конфиденциальности информации – 2 часа.
3. Архитектура IPsec-системы – 2 часа.
4. Элементы компьютерной вирусологии – 2 часа.
5. Формализованный процесс управления рисками информационной безопасности – 2 часа.

Курсовая работа – 6 часов.

Тема курсовой работы:

Исследование устойчивости к информационным атакам стеганографической системы с шифрованием.

Лабораторная работа – 6 часов.

Тема лабораторной работы:

Разработка метода шифрования на основе алгоритма Виженера.

Описание системы контроля знаний

В курсе «Обеспечение информационной безопасности автоматизированных систем транснациональных корпораций» предусматривается цикл лекций, семинарские занятия, лабораторная и курсовая работа.

В систему контроля знаний входит: контроль посещения лекций, активность работы на семинарских занятиях, контроль выполнения лабораторных работ, контроль поэтапного выполнения курсовой работы. Особо ценится своевременное выполнение лабораторной работы, качество выполнения курсовой работы, и итоговое испытание.

Промежуточная аттестация студентов проводится в конце каждого месяца, и результаты размещаются на учебном портале.

Балльная структура оценки:

Посещение лекций и семинаров: 0- 20 баллов

Лабораторные работа: 0 - 35 баллов

Курсовая работа: 0 - 25 баллов

Итоговое испытание: 0 - 20 баллов

Всего - 100 баллов

Шкала оценок:

Баллы за семестр	Автоматическая Оценка	Баллы за экзамен	Общая сумма баллов	Итоговая оценка
91 - 100	5	-	100	5
76 - 90	4	0 - 20	76-90 91 – 110	4 5
55 - 75	3	0 - 20	36 – 75 76 – 90 91 - 95	3 4 5
35 - 54	-	0 - 20	55 - 74	3
< 35	-	-	< 35	2

Студенты, получившие положительные оценки по результатам работы в семестре, но претендующие на получение более высокой оценки, могут участвовать в сдаче экзаменов в период сессии. Количество баллов за экзамен от 0 до 20 баллов.

Студенты, набравшие в течение семестра 35-55 баллов, обязаны пройти итоговую семестровую аттестацию в установленном порядке. Студенты, не выполнившие программу изучаемой дисциплины и не набравшие 35 баллов,

не допускаются до прохождения итоговой семестровой аттестации. Студенты, набравшие на экзамене менее 5 баллов, получают оценку «неудовлетворительно» независимо от числа набранных в семестре баллов.

Правила выполнения письменных работ (курсовых, лабораторных):

Задания на выполнение лабораторной и курсовой работ предлагается студентам в начале учебного семестра. Лабораторная и курсовая работа выполняется и сдается в срок, указанный в календарном плане.

Требования к оформлению работ: полуторный интервал, кегль — 14, цитирование и сноски в соответствии с принятыми стандартами, правильность грамматики, орфографии, синтаксиса.

Курсовая работа должна содержать обзорную часть проблемы, иметь четкую постановку задачи, содержать результаты исследования индивидуальных аудио и видео объектов.

Текст отчета о лабораторной работе должен содержать краткую теоретическую и развернутую практическую части, с подробными комментариями ко всем этапам исследования, объем не менее —15 страниц.

Академическая этика

В содержание курса включаются оригинальные научные и методические разработки автора УМК. Привлеченные материалы в содержание курса будут иметь ссылку на соответствующие источники. Это касается и источников, найденных в интернете – указывается полный адрес сайта. В конце работы дается полный список всех источников.

ПРОГРАММА КУРСА

Раздел I. Сущность, задачи и организационно-правовые основы проблемы информационной безопасности АСТНК.

Структура понятия «информационная безопасность» и основные определения. Доктрина информационной безопасности Российской Федерации. Источники угроз информационной безопасности АСТНК. Общие методы обеспечения информационной безопасности: правовые, организационно-технические, экономические. Основные национальные и международные законодательные и нормативные документы в сфере информационной безопасности. Особенности деятельности по обеспечению информационной безопасности АСТНК. Категории государственной и коммерческой тайны. Анализ и классификация возможных угроз информационной безопасности АСТНК. Основные методы реализации угроз информационной безопасности. Причины, виды и каналы утечки информации.

Раздел 2. Основные теоретические результаты в области теории информационной безопасности

Понятие политики безопасности и основные типы политик безопасности . Классификация основных формальных моделей политик безопасности. .Базовые принципы построения формальных моделей управления разграничения и контроля доступа к информации .Дискреационная модель матрицы прав доступа Харрисона-Рузо-Ульмана и ее модификации. Классическая мандатная модель Белла-Лападула. Ролевая модель политики безопасности. Задачи реализации и контроля выполнения правил политики безопасности.

Раздел 3. Критерии и спецификации безопасности автоматизированных систем и информационных технологий.

Нормативные документы Гостехкомиссии Российской Федерации. Структура требований к автоматизированным системам и средствам вычислительной техники. Критерии безопасности компьютерных систем МО США. Структура требований. Классы защищенности. Интерпретации и развитие «Оранжевой книги». Европейские критерии безопасности информационных технологий. Функциональные критерии. Критерии адекватности. Единые критерии безопасности информационных технологий. Определение продукта информационных технологий. Структуры профиля и плана защиты.

Раздел 4.Организационно-режимные меры и программно-аппаратные средства обеспечения конфиденциальности, целостности и доступа к информации.

Основные задачи обеспечения информационной безопасности от реализации угроз нарушения конфиденциальности, целостности и отказа в доступе к информации. Организационно-режимные и организационно-технологические меры обеспечения информационной безопасности. Идентификация и аутентификация. Парольные системы. Подходы к обоснованию выбора парольных систем. Методы аутентификации. Хранение и передача пароля по сети. Криптография и стеганография – основные методы обеспечения конфиденциальности информации. Целостность данных в автоматизированных системах. Модель контроля целостности данных. Обеспечение целостности информации на уровне содержания. Обеспечение отказоустойчивости программно-аппаратной среды.

Раздел 5. Архитектура безопасности взаимодействия открытых систем.

Классификация сервисов безопасности. Рекомендации по позиционированию сервисов безопасности по уровням эталонной модели

взаимодействия открытых систем. Основные протоколы сетевой безопасности. Криптографические средства сервисов безопасности.

Криптографические протоколы сетевой безопасности. Основные схемы генерации, распространения, хранения и удаления криптографических ключей. Безопасность локальных вычислительных систем при подключении к глобальным сетям с использованием криптографических протоколов. Архитектура IPsec-системы. Синтез виртуальных сетей на основе протокола IPsec.

Раздел 6. Обеспечение информационной безопасности АСТНК на основе принципа гарантированного результата

Постановка задачи синтеза модели внутреннего нарушителя, реализующего стратегию логического несанкционированного доступа. Методология синтеза моделей внутренних нарушителей. Формализованные модели внутреннего нарушителя. Сценарный анализ стратегий внутреннего нарушителя. Обоснование выбора метода обеспечения информационной безопасности с учетом ограничений модели внутреннего нарушителя. Обобщенная структурно-временная стратегия внешнего нарушителя. Элементы теории компьютерной вирусологии.

Раздел 7.Управление информационной безопасностью АСТНК

Актуальность решения проблемы аудита и управления рисками информационной безопасности. Постановка задачи аудита и страхования рисков безопасности АСТНК. Формализация процесса анализа и мониторинга рисков информационной безопасности. Методы вычисления рисков информационной безопасности Корпоративные методики процедур аудита рисков информационной
безопасности.

Список обязательной литературы.

Раздел 1. Сущность, задачи и организационно-правовые основы проблемы информационной безопасности АСТНК.

Безопасность России. Правовые, социально-экономические и научно-технические аспекты. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. МГФ «Знание», 2005. стр.71-99, стр.255-298, стр.464-482.

Раздел 2. Основные теоретические результаты в области теории информационной безопасности.

Безопасность России. Правовые, социально-экономические и научно-технические аспекты. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. МГФ «Знание», 2005. стр.350-406.

П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков.

Теоретические основы компьютерной безопасности. Москва. Радио и связь. 2000г. стр89-115, стр.118-149.

Раздел 3. Критерии и спецификации безопасности автоматизированных систем и информационных технологий.

П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков.

Теоретические основы компьютерной безопасности. Москва. Радио и связь. 2000г. стр.149-148.

Раздел 4. Организационно-режимные меры и программно-аппаратные средства обеспечения конфиденциальности, целостности и доступа к информации.

П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков.

Теоретические основы компьютерной безопасности. Москва. Радио и связь. 2000г.стр.27-87.

Раздел 5. Архитектура безопасности взаимодействия открытых систем.

П.Н. Девянин, А.М. Ивашко, А.С. Першаков, В. Г. и др.

Программно-аппаратные средства защиты от несанкционированного доступа к компьютерным криптографическим системам обработки информации. Учебное пособие. МИЭМ, 2004г.,стр.6-8..стр. 81-186.

Зима В.Н.,Молдовян А.А. и др. Безопасность глобальных сетевых технологий. - Спб.: БХВ-Петербург,2000.,стр.199-299.

Раздел 6. Обеспечение информационной безопасности АСТНК на основе принципа гарантированного результата.

П.Н. Девянин, А.М. Ивашко, А.С. Першаков, В. Г. и др.

Программно-аппаратные средства защиты от несанкционированного доступа к компьютерным криптографическим системам обработки информации. Учебное пособие. МИЭМ, 2004г., стр.26-56.

Раздел 7. Управление информационной безопасностью АСТНК.

Петренко С.А., Симонов С.В. Управление информационными рисками.

М.: Компания АйТи; ДМК Пресс.2004. стр101-155.

Список дополнительной литературы:

Раздел 1. Сущность, задачи и организационно-правовые основы проблемы информационной безопасности АСТНК.

Научные и методологические проблемы информационной безопасности.

(Сб. статей) Под общей редакцией В. П. Шерстюка-М: МЦНМО,2004.

Шерстюк В.П. Актуальные проблемы обеспечения информационной безопасности. -Военная мысль.2003,№5.

Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации. -М. : Издательская группа ЮРИСТ,2001.

Е.Б. Белов . Правовое обеспечение информационной безопасности.-М: Радио и связь.2001.

Раздел 2. Основные теоретические результаты в области теории информационной безопасности.

А.Ю. Щербаков Введение в теорию и практику компьютерной безопасности.- М: издатель Молгачева С.В.2001.

Раздел 3. Критерии и спецификации безопасности автоматизированных систем и информационных технологий.

И. Голдовский. Безопасность платежей в Интернете.-Спб-ПитерБ 2001. стр222-237.

Раздел 4.Организационно-режимные меры и программно-аппаратные средства обеспечения конфиденциальности, целостности и доступа к информации.

А.Ю. Мишин и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита в сетях.- М: Радио и связь.2001.

А.В. Петраков. Основы практической защиты информации.-М:. Радио и связь. 2000.

Раздел 5. Архитектура безопасности взаимодействия открытых систем.

В.А. Галатенко . Современная трактовка сервисов безопасности- Jet-Info, 1999,5.

Браун С. Виртуальные частные сети. - М: Лорт.2001.

Е.В.Давыдова и др. Новые средства криптографической защиты информации- М: Изд. МИФИ,1996.-132 стр.

А.В. Варфоломеев и др. Управление ключами в системах защиты информации в банковских технологиях.- М: Изд. МИФИ. 1996.

А.Г. Кабатянский .Математика разделения секрета// Математическое просвещение – 1998-Сер –Вып 2.

Диффи У. Хелманн М. Защищенность и имитостойкость. Введение в криптографию.//ТИИЭР.1979-Т67-№3.

А.В. Пярин Генерация, распределение и использование криптографических ключей // Защита информации .-1992 т.1-стрю114-152.

А. Саломаа. Криптография с открытым ключом. М:- Мир,1996.

А.С.Березин и др. Построение корпоративных защищенных виртуальных частных сетей.// Конфидент. Защита информации -№1-2001.с.54-61.

Раздел 6. Обеспечение информационной безопасности АСТНК на основе принципа гарантированного результата.

А.С. Першаков О возможности гарантированной защиты информации в недоверенной среде.// Проблемы информационной безопасности-1999 т.1.стр63-69.

Раздел 7. Управление информационной безопасностью АСТНК.

Проблемы управления информационной безопасностью. Под ред. Д.С. Черешкина. ИСА РАН,2002.

И.Д. Медведовский. Руководство по управлению информационными рисками корпоративных информационных систем. Internet\Intranet.-Domina Security, 2002.