Министерство образования и науки Российской Федерации

**Орский гуманитарно-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования «Оренбургский государственный университет»**

В. С. Богданова, О. В. Пергунова

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИЯХ ПРОМЫШЛЕННОСТИ

Электронное учебное пособие

Орск 2016

ISBN 978-5-8424-0837-5

УДК 004
ББК 66.2(2Рос)
Б73

Научный редактор

***Сурина Е. Е.**, кандидат экономических наук, доцент, заведующий кафедрой программного обеспечения Орского гуманитарно-технологического института (филиала) ОГУ*

Рецензенты:

***Жантлисова Е. А.,** кандидат экономических наук, доцент, заведующий кафедрой гуманитарных и социально-экономических наук Новотроицкого филиала ФГАОУ ВО «Национальный исследовательский технологический университет «МИСиС»*

***Пузикова Е. А.**, кандидат экономических наук, доцент, главный специалист по логистике и внешнеэкономической деятельности ООО «Даэрс-финанс»*

Б73 Богданова, В. С. Обеспечение информационной безопасности на предприятиях промышленности : [Электронное учебное пособие] / В. С. Богданова, О. В. Пергунова. – Орск : Издательство Орского гуманитарно-технологического института (филиала) ОГУ, 2016 – ISBN 978-5-8424-0837-5. Режим доступа: http://library.ogti.ru/global/metod/metod2016_11_06.pdf

В учебном пособии достаточно полно освещены теоретические вопросы обеспечения информационной безопасности на промышленном предприятии. Рассмотрены уровни защиты компьютерной информации: законодательный, технический, программный и организационный.

Учебное пособие может быть использовано студентами направлений подготовки 09.03.01 «Информатика и вычислительная техника», профиль Программное обеспечение вычислительной техники и автоматизированных систем при освоении дисциплины «Основы информационной безопасности»; 09.03.03 «Прикладная информатика», профиль Прикладная информатика в экономике при освоении дисциплин «Безопасность информационных систем и баз данных», «Экономика защиты информации», «Математические основы криптографии».

Подключение к сети Интернет на скорости не ниже 64 кбит/сек, современный браузер с надстройкой для чтения формата PDF (Portable Document Format) и/или возможностью скачивания файла для последующего открытия с помощью программ для просмотра файлов в формате PDF.

Программные средства, использованные при подготовке электронного издания: Microsoft Word 2013, Adobe Acrobat pro 10.

Редактор
Е. В. Кондаева

Редактор 2 категории
Г. А. Чумак

Технический редактор
Ю. И. Базлин

Утверждено редакционно-издательским советом Орского гуманитарно-технологического института (филиала) ОГУ в качестве электронного учебного пособия 18 сентября 2016.

Объем издания – 1,3 мБ.

Издательство Орского гуманитарно-технологического института (филиала) федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет»

462403, г. Орск Оренбургской обл., пр. Мира, 15А

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В Доктрине информационной безопасности Российской Федерации термин «информационная безопасность» используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В Законе Российской Федерации «Об участии в международном информационном обмене» информационная безопасность определяется аналогичным образом как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

В данном учебном пособии наше внимание будет сосредоточено на хранении, обработке и передаче информации вне зависимости от того, на каком языке (русском или каком-либо ином) она закодирована, кто или что является ее источником и какое психологическое воздействие она оказывает на людей. Поэтому термин «информационная безопасность» будет использоваться в узком смысле, так, как это принято, например, в англоязычной литературе.

Под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный, с методологической точки зрения, подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Вернуться к содержанию

1. ОСНОВНЫЕ ПОНЯТИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Под **информацией**, применительно к задаче ее защиты, понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. В зависимости от формы представления информация может быть разделена на речевую, телекоммуникационную и документированную.

Речевая информация возникает в ходе ведения в помещениях разговоров, работы систем связи, звукоусиления и звуковоспроизведения. **Телекоммуникационная** информация циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче. К **документированной** информации, или документам, относят информацию, представленную на материальных носителях вместе с идентифицирующими ее реквизитами.

К **информационным процессам** относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Под **информационной системой** понимают упорядоченную совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы.

Информационными ресурсами называют документы и массивы документов, существующие отдельно или в составе информационных систем.

Процесс создания оптимальных условий для удовлетворения информационных потребностей граждан, организаций, общества и государства в целом называют информатизацией.

Информационные системы, технологии и средства их обеспечения могут быть объектами собственности физических и юридических лиц, государства. Собственником информационной системы, технологии и средств их обеспечения признается физическое или юридическое лицо, на средства которого эти объекты произведены, приобретены или получены в порядке наследования, дарения или иным законным способом.

Информацию разделяют на открытую и ограниченного доступа. К информации ограниченного доступа относятся государственная тайна и конфиденциальная информация. В соответствии с российским законодательством к конфиденциальной относится следующая информация:

– служебная тайна (врачебная, адвокатская, тайна суда и следствия и т. д.);

– коммерческая тайна;

– персональные данные (сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность).

Информация является одним из объектов гражданских прав, в том числе и прав собственности, владения и пользования. **Собственник** информационных ресурсов, систем и технологий – это субъект с полномочиями владения, пользования и распоряжения указанными объектами. **Владельцем** информационных ресурсов, систем и технологий является субъект с полномочиями владения и пользования указанными объектами. Под **пользователем** информации будем понимать субъекта, обращающегося к информационной системе за получением необходимой ему информации и пользующегося ею.

К **защищаемой** относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Защитой информации называют деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Под **утечкой** понимают неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками. **Разглашение** – это доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации в сети Интернет). **Несанкционированный доступ** – получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней.

Целью защиты информации является предотвращение ущерба собственнику, владельцу или пользователю информации. Под **эффективностью защиты информации** понимают степень соответствия результатов защиты информации поставленной цели. **Объектом защиты** может быть информация, ее носитель или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью.

Под качеством информации понимают совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации. Одним из показателей качества информации является ее **защищенность** – поддержание на заданном уровне тех параметров информации, которые характеризуют установленный статус ее хранения, обработки и использования.

Основными характеристиками защищаемой информации являются конфиденциальность, целостность и доступность. **Конфиденциальность информации** – это известность ее содержания только субъектам, имеющим соответствующее полномочие. Конфиденциальность является субъективной характеристикой информации, связанной с объективной необходимостью защиты законных интересов одних субъектов от других.

Шифрованием информации называют процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов. Результат шифрования информации называют **шифротекстом** или **криптограммой**. Обратный процесс восстановления информации из шифротекста называют **расшифрованием** информации. Алгоритмы, используемые при шифровании и расшифровании информации, обычно не являются конфиденциальными, а конфиденциальность шифротекста обеспечивается использованием при шифровании дополнительного параметра, называемого **ключом шифрования**. Знание ключа шифрования позволяет выполнить правильное расшифрование шифротекста.

Целостностью информации называют неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения. Целостность является частью более широкой характеристики информации – ее достоверности, включающей помимо целостности еще полноту и точность отображения предметной области.

Хешированием информации называют процесс ее преобразования в хеш – значение фиксированной длины (дайджест). Одним из применений хеширования является обеспечение целостности информации.

Под **доступностью** информации понимают способность обеспечения беспрепятственного доступа субъектов к интересующей их информации. **Отказом в обслуживании** называют состояние информационной системы, при котором блокируется доступ к некоторому ресурсу. Совокупность информационных ресурсов и системы формирования, распространения и использования информации называют **информационной средой** общества.

Под **информационной безопасностью** понимают состояние защищенности информационной среды, обеспечивающее ее формирование и развитие.

Политика безопасности – это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.

Вернуться к содержанию

2. АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Особенности административного уровня защиты информации

К административному уровню информационной безопасности (ИБ) относятся действия общего характера, предпринимаемые руководством организации.

Главная цель мер административного уровня – сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы (ИС) организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т. п.

Термин «политика безопасности» является не совсем точным переводом английского словосочетания «security policy», однако в данном случае калька лучше отражает смысл этого понятия, чем лингвистически более верные «правила безопасности». Мы будем иметь в виду не отдельные правила или их наборы (такого рода решения выносятся на процедурный уровень), а стратегию организации в области ИБ. Для выработки стратегии и проведения ее в жизнь нужны, несомненно, политические решения, принимаемые на самом высоком уровне.

Под политикой безопасности понимается совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.

Такая трактовка, конечно, гораздо шире, чем набор правил разграничения доступа («Оранжевая книга»).

ИС организации и связанные с ней интересы субъектов – это сложная система, для рассмотрения которой необходимо применять объектно-ориентированный подход и понятие уровня детализации. Целесообразно выделить три таких уровня.

Чтобы рассматривать ИС предметно, с использованием актуальных данных, следует составить карту ИС. Эта карта должна быть изготовлена в объектно-ориентированном стиле, с возможностью варьировать не только уровень детализации, но и видимые грани объектов. Техническим средством составления, сопровождения и визуализации подобных карт может служить свободно распространяемый каркас какой-либо системы управления.

Вернуться к содержанию

2.2. Политика безопасности

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и исходят от руководства организации. Примерный список подобных решений может включать в себя следующие элементы:

– решение сформировать или пересмотреть комплексную программу обеспечения ИБ, назначение ответственных за продвижение программы;

– формулировка целей, которые преследует организация в области ИБ, определение общих направлений в достижении этих целей;

– обеспечение базы для соблюдения законов и правил;

– формулировка административных решений по тем вопросам реализации программы ИБ, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками

своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

• вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;

• организационный, содержащий описание подразделений, комиссий, групп и так далее, отвечающих за работы в области информационной безопасности;

• классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;

• штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т. п.);

• раздел, освещающий вопросы физической защиты;

• управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;

• раздел, описывающий правила разграничения доступа к производственной информации;

• раздел, характеризующий порядок разработки и сопровождения систем;

• раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;

• юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем. Примеры таких вопросов – отношение к передовым (но, возможно, недостаточно проверенным) технологиям, доступ в Internet (как совместить свободу доступа к информации с защитой от внешних угроз?), использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т. д.

Политика среднего уровня должна для каждого аспекта освещать следующие темы:

Описание аспекта. Например, если рассмотреть применение пользователями неофициального программного обеспечения (ПО), последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

Область применения. Следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, пользующихся портативными и домашними компьютерами и вынужденных переносить информацию на производственные машины?

Позиция организации по данному аспекту. Продолжая пример с неофициальным программным обеспечением, можно представить себе позиции полного запрета, выработки процедуры приемки подобного ПО и т. п. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще, стиль документов, определяющих политику безопасности (как и их перечень), в разных организациях может сильно отличаться.

Роли и обязанности. В «политический» документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

Законопослушность. Политика должна содержать общее описание запрещенных действий и наказаний за них.

Точки контакта. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно «точкой контакта» служит определенное должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Она включает в себя два аспекта – цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведем несколько примеров вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

- Кто имеет право доступа к объектам, поддерживаемым сервисом?
- При каких условиях можно читать и модифицировать данные?
- Как организован удаленный доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. Ее цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жесткие правила могут мешать работе пользователей, вероятно, их придется часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного вопроса.

Вернуться к содержанию

2.3. Программа безопасности

После того, как сформулирована политика безопасности, можно приступать к составлению программы ее реализации и собственно к реализации.

Чтобы понять и реализовать какую-либо программу, ее нужно структурировать по уровням, обычно в соответствии со структурой организации. В простейшем и самом распространенном случае достаточно двух уровней – верхнего, или центрального, который охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. У этой программы следующие главные цели:

• управление рисками (оценка рисков, выбор эффективных средств защиты);

• координация деятельности в области информационной безопасности, пополнение и распределение ресурсов;

• стратегическое планирование;

• контроль деятельности в области информационной безопасности.

В рамках программы верхнего уровня принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, и необходимо иметь четкую политику отслеживания и внедрения новых средств.

Контроль деятельности в области безопасности имеет двустороннюю направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать защитные меры с учетом изменения обстановки.

Следует подчеркнуть, что программа верхнего уровня должна занимать строго определенное место в деятельности организации, она должна официально приниматься и поддерживаться руководством, а также иметь определенный штат и бюджет.

Цель программы нижнего уровня – обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие следует использовать механизмы защиты; закупаются и устанавливаются технические средства; выполняется повседневное администрирование; отслеживается состояние слабых мест и тому подобное, обычно за программу нижнего уровня отвечают администраторы сервисов.

Вернуться к содержанию

2.4. Синхронизация программы безопасности с жизненным циклом систем

Если синхронизировать программу безопасности нижнего уровня с жизненным циклом защищаемого сервиса, можно добиться большего эффекта с меньшими затратами. Программисты знают, что добавить новую возможностью к уже готовой системе на порядок сложнее, чем изначально спроектировать и реализовать ее, то же справедливо и для ИБ.

В жизненном цикле информационного сервиса можно выделить следующие этапы:

Инициация. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.

Закупка. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.

Установка. Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.

Эксплуатация. На данном этапе сервис не только работает и администрируется, но и подвергается модификации.

Выведение из эксплуатации. Происходит переход на новый сервис.

Рассмотрим действия, выполняемые на каждом этапе более подробно.

На этапе инициации оформляется понимание того, что необходимо приобрести новый или значительно модернизировать существующий сервис; определяется, какими характеристиками и какой функциональностью он должен обладать; оцениваются финансовые и иные ограничения.

С точки зрения безопасности, важнейшим действием здесь является оценка критичности как самого сервиса, так и информации, которая с его помощью будет обрабатываться. Требуется сформулировать ответы на следующие вопросы:

• Какого рода информация предназначается для обслуживания новым сервисом?

• Каковы возможные последствия нарушения конфиденциальности, целостности и доступности этой информации?

• Каковы угрозы, по отношению к которым сервис и информация будут наиболее уязвимы?

• Есть ли какие-либо особенности нового сервиса (например, территориальная распределенность компонентов), требующие принятия специальных процедурных мер?

• Каковы характеристики персонала, имеющие отношение к безопасности (квалификация, благонадежность)?

• Каковы законодательные положения и внутренние правила, которым должен соответствовать новый сервис?

Результаты оценки критичности являются отправной точкой в составлении спецификаций. Кроме того, они определяют ту меру внимания, которую служба безопасности организации должна уделять новому сервису на последующих этапах его жизненного цикла.

Этап закупки – один из самых сложных. Нужно окончательно сформулировать требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика, и к квалификации, которой должен обладать персонал, использующий или обслуживающий закупаемый продукт. Все эти сведения оформляются в виде спецификации, куда входят не только аппаратура и программы, но и документация, обслуживание, обучение персонала. Разумеется, особое внимание должно уделяться вопросам совместимости нового сервиса с существующей конфигурацией. Подчеркнем также, что нередко средства безопасности являются необязательными компонентами коммерческих продуктов, и нужно проследить, чтобы соответствующие пункты не выпали из спецификации.

Когда продукт закуплен, его необходимо установить. Несмотря на кажущуюся простоту, установка является очень ответственным делом. Во-первых, новый продукт следует сконфигурировать. Как правило, коммерческие продукты поставляются с отключенными средствами безопасности; их необходимо включить и должным образом настроить. Для большой организации, где много пользователей и данных, начальная настройка может стать весьма трудоемким и ответственным делом.

Во-вторых, новый сервис нуждается в процедурных регуляторах. Следует позаботиться о чистоте и охране помещения, о документах, регламентирующих использование сервиса, о подготовке планов на случай экстренных ситуаций, об организации обучения пользователей и т. п.

После принятия перечисленных мер необходимо провести тестирование. Его полнота и комплексность могут служить гарантией безопасности эксплуатации в штатном режиме.

Период эксплуатации самый длительный и сложный. С психологической точки зрения, наибольшую опасность в это время представляют незначительные изменения в конфигурации сервиса, в поведении пользователей и администраторов. Если безопасность не поддерживать, она ослабевает. Пользователи не столь ревностно выполняют должностные инструкции, администраторы менее тща-

тельно анализируют регистрационную информацию. То один, то другой пользователь получает дополнительные привилегии. Кажется, что в сущности ничего не изменилось; на самом же деле от былой безопасности не осталось и следа.

Для борьбы с эффектом медленных изменений приходится прибегать к периодическим проверкам безопасности сервиса. Разумеется, после значительных модификаций подобные проверки являются обязательными.

При выведении из эксплуатации затрагиваются аппаратно-программные компоненты сервиса и обрабатываемые им данные. Аппаратура продается, утилизируется или выбрасывается. Только в специфических случаях необходимо заботиться о физическом разрушении аппаратных компонентов, хранящих конфиденциальную информацию. Программы, вероятно, просто стираются, если иное не предусмотрено лицензионным соглашением.

При выведении данных из эксплуатации их обычно переносят на другую систему, архивируют, выбрасывают или уничтожают. Если архивирование производится с намерением впоследствии прочитать данные в другом месте, следует позаботиться об аппаратно-программной совместимости средств чтения и записи. Информационные технологии развиваются очень быстро, и через несколько лет устройств, способных прочитать старый носитель, может просто не оказаться. Если данные архивируются в зашифрованном виде, необходимо сохранить ключ и средства расшифровки. При архивировании и хранении архивной информации нельзя забывать о поддержании конфиденциальности данных.

Вернуться к содержанию

3. УПРАВЛЕНИЕ РИСКАМИ

3.1. Основные понятия и определения

Управление рисками рассматривается нами на административном уровне ИБ, поскольку только руководство организации способно выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

Вообще говоря, управление рисками, равно как и выработка собственной политики безопасности, актуально только для тех организаций, информационные системы которых и/или обрабатываемые данные можно считать нестандартными. Обычную организацию вполне устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или, вообще, без всякого анализа рисков (особенно это верно с формальной точки зрения, в свете проанализированного нами ранее российского законодательства в области ИБ). Можно провести аналогию между индивидуальным строительством и получением квартиры в районе массовой застройки. В первом случае необходимо принять множество решений, оформить большое количество бумаг, во втором достаточно определиться лишь с несколькими параметрами. Более подробно данный аспект рассмотрен в статье Сергея Симонова «Анализ рисков, управления рисками» (Jet Info, 1999, 1).

Использование информационных систем связано с определенной совокупностью рисков. Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая (пере)оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

С количественной точки зрения, уровень риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимые места), а также величины возможного ущерба.

Таким образом, суть мероприятий по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми). Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

• (пере)оценка (измерение) рисков;

• выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия:

• ликвидация риска (например, за счет устранения причины);

• уменьшение риска (например, за счет использования дополнительных защитных средств);

• принятие риска (и выработка плана действия в соответствующих условиях);

• переадресация риска (например, путем заключения страхового соглашения).

Процесс управления рисками можно разделить на следующие этапы:

1. Выбор анализируемых объектов и уровня детализации их рассмотрения.
2. Выбор методологии оценки рисков.
3. Идентификация активов.
4. Анализ угроз и их последствий, выявление уязвимых мест в защите.
5. Оценка рисков.
6. Выбор защитных мер.
7. Реализация и проверка выбранных мер.
8. Оценка остаточного риска.

Этапы 6-й и 7-й относятся к выбору защитных средств (нейтрализации рисков), остальные – к оценке рисков.

Уже перечисление этапов показывает, что управление рисками – процесс циклический. По существу, последний этап – это оператор конца цикла, предписывающий вернуться к началу. Риски нужно контролировать постоянно, периодически проводя их переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую деятельность.

Управление рисками, как и любую другую деятельность в области информационной безопасности, необходимо интегрировать в жизненный цикл ИС. Тогда эффект оказывается наибольшим, а затраты – минимальными. Ранее мы определили пять этапов жизненного цикла. Кратко опишем, что может дать управление рисками на каждом из них.

На этапе инициации известные риски следует учесть при выработке требований к системе вообще и средствам безопасности в частности.

На этапе закупки (разработки) знание рисков поможет выбрать соответствующие архитектурные решения, которые играют ключевую роль в обеспечении безопасности.

На этапе установки выявленные риски следует учитывать при конфигурировании, тестировании и проверке ранее сформулированных требований, а полный цикл управления рисками должен предшествовать внедрению системы в эксплуатацию.

На этапе эксплуатации управление рисками должно сопровождать все существенные изменения в системе.

При выведении системы из эксплуатации управление рисками помогает убедиться в том, что миграция данных происходит безопасным образом.

Вернуться к содержанию

3.2. Подготовительные этапы управления рисками

Выбор анализируемых объектов и уровня детализации их рассмотрения – первый шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру; однако, если организация крупная, всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил. В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приближенностью итоговой оценки. Если важных сервисов все еще много, выбираются те из них, риски для которых заведомо велики или неизвестны.

Мы уже указывали на целесообразность создания карты информационной системы организации. Для управления рисками подобная карта особенно важна, поскольку она наглядно показывает, какие сервисы выбраны для анализа, а какими пришлось пренебречь. Если ИС меняется, а карта поддерживается в актуальном состоянии, то при переоценке рисков сразу станет ясно, какие новые или существенно изменившиеся сервисы нуждаются в рассмотрении.

Вообще говоря, уязвимым является каждый компонент информационной системы – от сетевого кабеля, который могут прогрызть мыши, до базы данных, которая может быть разрушена из-за неумелых действий администратора. Как правило, в сферу анализа невозможно включить каждый винтик и каждый байт. Приходится останавливаться на некотором уровне детализации, опять-таки отдавая себе отчет в приближенности оценки. Для новых систем предпочтителен детальный анализ; старая система, подвергшаяся небольшим модификациям, может быть проанализирована более поверхностно.

Очень важно выбрать разумную методологию оценки рисков. Целью оценки является получение ответа на два вопроса: приемлемы ли существующие риски, и если нет, то какие защитные средства стоит использовать. Значит, оценка должна быть количественной, допускающей сопоставление с заранее вы-

бранными границами допустимости и расходами на реализацию новых регуляторов безопасности. Управление рисками – типичная оптимизационная задача, и существует довольно много программных продуктов, способных помочь в ее решении (иногда подобные продукты просто прилагаются к книгам по информационной безопасности).

Принципиальная трудность, однако, состоит в неточности исходных данных. Можно, конечно, попытаться получить для всех анализируемых величин денежное выражение, высчитать все с точностью до копейки, но большого смысла в этом нет. Практичнее пользоваться условными единицами. В простейшем и вполне допустимом случае можно пользоваться трехбалльной шкалой.

При идентификации активов, то есть тех ресурсов и ценностей, которые организация пытается защитить, следует, конечно, учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как репутация организации. Отправной точкой здесь является представление о миссии организации, то есть об основных направлениях деятельности, которые желательно (или необходимо) сохранить в любом случае. Выражаясь объектно-ориентированным языком, следует в первую очередь описать внешний интерфейс организации, рассматриваемой как абстрактный объект.

Одним из главных результатов процесса идентификации активов является получение детальной информационной структуры организации и способов ее (структуры) использования. Эти сведения целесообразно нанести на карту ИС в качестве граней соответствующих объектов.

Информационной основой сколько-нибудь крупной организации является сеть, поэтому в число аппаратных активов следует включить компьютеры (серверы, рабочие станции, ПК), периферийные устройства, внешние интерфейсы, кабельное хозяйство, активное сетевое оборудование (мосты, маршрутизаторы и т. п.). К программным активам, вероятно, будут отнесены операционные системы (сетевая, серверные и клиентские), прикладное программное обеспечение, инструментальные средства, средства управления сетью и отдельными системами. Важно зафиксировать, где (в каких узлах сети) хранится программное обеспечение и из каких узлов оно используется. Третьим видом информационных активов являются данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, способы доступа к ним. Все это важно для оценки последствий нарушений информационной безопасности.

Управление рисками – процесс далеко не линейный. Практически все его этапы связаны между собой, и по завершении почти любого из них может возникнуть необходимость возврата к предыдущему. Так, при идентификации активов может оказаться, что выбранные границы анализа следует расширить, а степень детализации – увеличить. Особенно труден первичный анализ, когда многократные возвраты к началу неизбежны.

Вернуться к содержанию

3.3. Основные этапы управления рисками

Этапы, предшествующие анализу угроз, можно считать подготовительными, поскольку, строго говоря, они напрямую с рисками не связаны. Риск появляется там, где есть угрозы.

Краткий перечень наиболее распространенных угроз был рассмотрен нами ранее. К сожалению, на практике угроз гораздо больше, причем далеко не все из них носят компьютерный характер. Так, вполне реальной угрозой является наличие мышей и тараканов в занимаемых организацией помещениях. Первые могут повредить кабели, вторые вызвать короткое замыкание. Как правило, наличие той или иной угрозы является следствием пробелов в защите информационной системы, которые, в свою очередь, объясняются отсутствием некоторых сервисов безопасности или недостатками в реализующих их защитных механизмах. Опасность прогрызания кабелей возникает не просто там, где есть мыши, она связана с отсутствием или недостаточной прочностью защитной оболочки.

Первый шаг в анализе угроз – их идентификация. Рассматриваемые виды угроз следует выбирать исходя из соображений здравого смысла (исключив, например, землетрясения, однако не забывая о возможности захвата организации террористами), но в пределах выбранных видов провести максимально подробный анализ.

Целесообразно выявлять не только сами угрозы, но и источники их возникновения – это поможет в выборе дополнительных средств защиты. Например, нелегальный вход в систему может стать следствием воспроизведения начального диалога, подбора пароля или подключения к сети неавторизованного оборудования. Очевидно, для противодействия каждому из перечисленных способов нелегального входа нужны свои механизмы безопасности.

После идентификации угрозы необходимо оценить вероятность ее осуществления. Допустимо использовать при этом трехбалльную шкалу (низкая (1), средняя (2) и высокая (3) вероятность).

Кроме вероятности осуществления, важен размер потенциального ущерба. Например, пожары бывают нечасто, но ущерб от каждого из них, как правило, велик. Тяжесть ущерба также можно оценить по трехбалльной шкале.

Оценивая размер ущерба, необходимо иметь в виду не только непосредственные расходы на замену оборудования или восстановление информации, но и более отдаленные, такие как подрыв репутации, ослабление позиций на рынке и т. п. Пусть, например, в результате дефектов в управлении доступом к бухгалтерской информации сотрудники получили возможность корректировать данные о собственной заработной плате.

Следствием такого состояния дел может стать не только перерасход бюджетных или корпоративных средств, но и полное разложение коллектива, грозящее развалом организации.

Уязвимые места обладают свойством притягивать к себе не только злоумышленников, но и сравнительно честных людей. Не всякий устоит перед искушением немного увеличить свою зарплату, если есть уверенность, что это сойдет с рук. Поэтому, оценивая вероятность осуществления угроз, целесообразно исходить не только из среднестатистических данных, но учитывать также специфику конкретных информационных систем. Если в подвале дома, занимаемого организацией, располагается сауна, а сам дом имеет деревянные перекрытия, то вероятность пожара, к сожалению, оказывается существенно выше средней.

После того, как накоплены исходные данные и оценена степень неопределенности, можно переходить к обработке информации, то есть собственно к оценке рисков. Вполне допустимо применить такой простой метод, как умножение вероятности осуществления угрозы на предполагаемый ущерб. Если для вероятности и ущерба использовать трехбалльную шкалу, то возможных произведений будет шесть: 1, 2, 3, 4, 6 и 9. Первые два результата можно отнести к низкому риску, третий и четвертый – к среднему, два последних – к высокому, после чего появляется возможность снова привести их к трехбалльной шкале. По этой шкале и следует оценивать приемлемость рисков. Правда, граничные случаи, когда вычисленная величина совпала с приемлемой, целесообразно рассматривать более тщательно из-за приближенного характера результата.

Если какие-либо риски оказались недопустимо высокими, необходимо их нейтрализовать, реализовав дополнительные меры защиты. Как правило, для ликвидации или нейтрализации уязвимого места, сделавшего угрозу реальной, существует несколько механизмов безопасности, различных по эффективности и стоимости. Например, если велика вероятность нелегального входа в систему, можно потребовать, чтобы пользователи выбирали длинные пароли (скажем, не

менее восьми символов), задействовать программу генерации паролей или закупить интегрированную систему аутентификации на основе интеллектуальных карт. Если есть вероятность умышленного повреждения сервера баз данных, что может иметь серьезные последствия, можно врезать замок в дверь серверной комнаты или поставить около каждого сервера по охраннику.

Оценивая стоимость мер защиты, приходится, разумеется, учитывать не только прямые расходы на закупку оборудования и/или программ, но и расходы на внедрение новинки и, в частности, обучение и переподготовку персонала. Эту стоимость также можно оценить по трехбалльной шкале и затем сопоставить ее с разностью между вычисленным и допустимым риском. Если по этому показателю новое средство оказывается экономически выгодным, его можно взять на заметку (подходящих средств, вероятно, будет несколько). Однако если средство окажется дорогим, его не следует сразу отбрасывать, памятуя о приближенности расчетов.

Выбирая подходящий способ защиты, целесообразно учитывать возможность экранирования одним механизмом обеспечения безопасности сразу нескольких прикладных сервисов. Так поступили в Массачусетском технологическом институте, защитив несколько тысяч компьютеров сервером аутентификации Kerberos.

Важным обстоятельством является совместимость нового средства со сложившейся организационной и аппаратно-программной структурой, с традициями организации. Меры безопасности, как правило, носят недружественный характер, что может отрицательно сказаться на энтузиазме сотрудников. Порой сохранение духа открытости важнее минимизации материальных потерь. Впрочем, такого рода ориентиры должны быть расставлены в политике безопасности верхнего уровня.

Можно представить себе ситуацию, когда для нейтрализации риска не существует эффективных и приемлемых по цене мер. Например, компания, базирующаяся в сейсмически опасной зоне, не всегда может позволить себе строительство защищенной штаб-квартиры. В таком случае приходится поднимать планку приемлемого риска и переносить центр тяжести на смягчение последствий и выработку планов восстановления после аварий, стихийных бедствий и иных происшествий. Продолжая пример с сейсмоопасностью, можно рекомендовать регулярное тиражирование данных в другой город и овладение средствами восстановления первичной базы данных.

Как и всякую иную деятельность, реализацию и проверку новых регуляторов безопасности следует предварительно планировать. В плане необходимо

учесть наличие финансовых средств и сроки обучения персонала. Если речь идет о программно-техническом механизме защиты, нужно составить план тестирования (автономного и комплексного).

Когда намеченные меры приняты, необходимо проверить их действенность, то есть убедиться, что остаточные риски стали приемлемыми. Если это на самом деле так, значит, можно спокойно намечать дату ближайшей переоценки. В противном случае придется проанализировать допущенные ошибки и провести повторный сеанс управления рисками немедленно.

Вернуться к содержанию

4. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И КРИТЕРИИ КЛАССИФИКАЦИИ УГРОЗ

Угроза – это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку, — злоумышленником. Потенциальные злоумышленники называются источниками угрозы.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется окном опасности, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Если речь идет об ошибках в ПО, то окно опасности «открывается» с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда – недель), поскольку за это время должны произойти следующие события:

• должно стать известно о средствах использования пробела в защите;

• должны быть выпущены соответствующие заплаты;

• заплаты должны быть установлены в защищаемой ИС.

Мы уже указывали, что новые уязвимые места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат – как можно более оперативно.

Отметим, что некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Рассмотрим наиболее распространенные угрозы, которым подвержены современные информационные системы. Иметь представление о возможных угрозах, а также об уязвимых местах, которые эти угрозы обычно эксплуатируют,

необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности. Слишком много мифов существует в сфере информационных технологий (вспомним все ту же «Проблему 2000»), поэтому незнание в данном случае ведет к перерасходу средств и, что еще хуже, к концентрации ресурсов там, где они не особенно нужны, за счет ослабления действительно уязвимых направлений.

Подчеркнем, что само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать – вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Мы попытаемся взглянуть на предмет с точки зрения типичной (на наш взгляд) организации. Впрочем, многие угрозы (например, пожар) опасны для всех.

Угрозы можно классифицировать по нескольким критериям:

• по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;

• по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

• по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);

• по расположению источника угроз (внутри/вне рассматриваемой ИС).

В качестве основного критерия мы будем использовать первый (по аспекту ИБ), привлекая при необходимости остальные.

Вернуться к содержанию

4.1. Угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь – следствие непреднамеренных ошибок.

Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе.

Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками – максимальная автоматизация и строгий контроль.

Другие угрозы доступности классифицируем по компонентам ИС, на которые нацелены угрозы:

• отказ пользователей;

• внутренний отказ информационной системы;

• отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

• нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);

• невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т. п.);

• невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т. п.).

Основными источниками внутренних отказов являются:

• отступление (случайное или умышленное) от установленных правил эксплуатации;

• выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала;

• ошибки при (пере)конфигурировании системы;

• отказы программного и аппаратного обеспечения;

• разрушение данных;

• разрушение или повреждение аппаратуры;

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

• нарушение работы систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;

• разрушение или повреждение помещений;

• невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности.

Весьма опасны так называемые «обиженные» сотрудники, нынешние и бывшие. Как правило, они стремятся нанести вред организации, например:

• испортить оборудование;

• встроить логическую бомбу, которая со временем разрушит программы и/или данные;

• удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа к информационным ресурсам аннулировались.

Опасны, разумеется, стихийные бедствия и события, воспринимаемые как стихийные бедствия: пожары, наводнения, землетрясения, ураганы. По статистике, на долю огня, воды и тому подобных «злоумышленников» приходится 13% потерь, нанесенных ИС.

Угрозы доступности могут выглядеть грубо – как повреждение или даже разрушение оборудования. Такое повреждение может вызываться естественными причинами. К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов, и случаи выгорания оборудования не редкость.

В принципе, мощный кратковременный импульс, способный разрушить данные на магнитных носителях, можно сгенерировать и искусственным образом – с помощью так называемых высокоэнергетических радиочастотных пушек. Но, наверное, в наших условиях подобную угрозу следует все же признать надуманной.

Действительно опасны протечки водопровода и отопительной системы. Часто организации, чтобы сэкономить на арендной плате, снимают помещения в домах старой постройки, делают косметический ремонт, но не меняют ветхие трубы. Автору довелось быть свидетелем ситуации, когда прорвало трубу с горячей водой и системный блок компьютера (это была рабочая станция производства Sun Microsystems) оказался заполнен кипятком. Когда кипяток вылили, а компьютер просушили, он возобновил нормальную работу, но лучше таких опытов не ставить...

Летом, в сильную жару, норовят сломаться кондиционеры, установленные в серверных залах, набитых дорогостоящим оборудованием. В результате значительный ущерб наносится и репутации, и кошельку организации.

Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные

носители зачастую хранят небрежно (к этому мы еще вернемся при обсуждении угроз конфиденциальности), не обеспечивая их защиту от вредного воздействия окружающей среды. И, когда требуется восстановить данные, оказывается, что эти самые носители никак не желают читаться.

Перейдем теперь к угрозам доступности, которые будут похитрее засоров канализации. Речь пойдет о программных атаках на доступность.

В качестве средства вывода системы из штатного режима эксплуатации может использоваться агрессивное потребление ресурсов (обычно полосы пропускания сетей, вычислительных возможностей процессора или оперативной памяти). По расположению источника угрозы такое потребление подразделяется на локальное и удаленное. При просчетах конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Простейший пример удаленного потребления ресурсов – атака, получившая наименование «SYN-наводнение». Она представляет собой попытку переполнить таблицу «полуоткрытых» TCP-соединений сервера (установление соединений начинается, но не заканчивается). Такая атака, по меньшей мере, затрудняет установление новых соединений со стороны легальных пользователей, то есть сервер выглядит как недоступный.

По отношению к атаке «Papa Smurf» уязвимы сети, воспринимающие ping-пакеты с широковещательными адресами. Ответы на такие пакеты «съедают» полосу пропускания.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме – как скоординированные распределенные атаки, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание. Временем начала «моды» на подобные атаки можно считать февраль 2000 года, когда жертвами оказались несколько крупнейших систем электронной коммерции (точнее – владельцы и пользователи систем). Отметим, что если имеет место архитектурный просчет в виде разбалансированности между пропускной способностью сети и производительностью сервера, то защититься от распределенных атак на доступность крайне трудно.

Для выведения систем из штатного режима эксплуатации могут использоваться уязвимые места в виде программных и аппаратных ошибок. Например, известная ошибка в процессоре Pentimn 1 дает возможность локальному пользователю путем выполнения определенной команды «подвесить» компьютер, так что помогает только аппаратный RESET.

Программа «Teardrop» удаленно «подвешивает» компьютеры, эксплуатируя ошибку в сборке фрагментированных IP-пакетов.

Вернуться к содержанию

4.2. Вредоносное программное обеспечение

Одним из опаснейших способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения.

Мы выделим следующие грани вредоносного ПО:

• вредоносная функция;

• способ распространения;

• внешнее представление.

Часть, осуществляющую разрушительную функцию, будем называть «бомбой» (хотя, возможно, более удачными терминами были бы «заряд» или «боеголовка»). Вообще говоря, спектр вредоносных функций неограничен, поскольку «бомба», как и любая другая программа, может обладать сколь угодно сложной логикой, но обычно «бомбы» предназначаются для:

• внедрения другого вредоносного ПО;

• получения контроля над атакуемой системой;

• агрессивного потребления ресурсов;

• изменения или разрушения программ и/или данных.

По механизму распространения различают:

• вирусы – код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;

• «черви» – код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. «Черви», напротив, ориентированы в первую очередь на путешествия по сети.

Иногда само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией. Например, «черви» «съедают» полосу пропускания сети и ресурсы почтовых систем. По этой причине для атак на доступность они не нуждаются во встраивании специальных «бомб».

Вредоносный код, который выглядит как функционально полезная программа, называется троянским. Например, обычная программа, будучи пораженной вирусом, становится троянской; порой троянские программы изготавливают

вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке.

Отметим, что данные нами определения и приведенная классификация вредоносного ПО отличаются от общепринятых. Например, в ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» содержится следующее определение:

«Программный вирус – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах».

На наш взгляд, подобное определение неудачно, поскольку в нем смешаны функциональные и транспортные аспекты.

Окно опасности для вредоносного ПО появляется с выпуском новой разновидности «бомб», вирусов и/или «червей» и перестает существовать с обновлением базы данных антивирусных программ и наложением других необходимых заплат.

По традиции из всего вредоносного ПО наибольшее внимание общественности приходится на долю вирусов. Однако до марта 1999 года с полным правом можно было утверждать, что, «несмотря на экспоненциальный рост числа известных вирусов, аналогичного роста количества инцидентов, вызванных ими, не зарегистрировано. Соблюдение несложных правил «компьютерной гигиены» практически сводит риск заражения к нулю. Там, где работают, а не играют, число зараженных компьютеров составляет лишь доли процента».

В марте 1999 года, с появлением вируса «Melissa», ситуация кардинальным образом изменилась. «Melissa» – это макровирус для файлов MS-Word, распространяющийся посредством электронной почты в присоединенных файлах. Когда такой (зараженный) присоединенный файл открывают, он рассылает свои копии по первым 50 адресам из адресной книги Microsoft Outlook. В результате почтовые серверы подвергаются атаке на доступность.

В данном случае нам хотелось бы отметить два момента.

1. Как уже говорилось, пассивные объекты отходят в прошлое; так называемое активное содержимое становится нормой. Файлы, которые по всем признакам должны были бы относиться к данным (например, документы в форматах MS-64гс1 или Postscript, тексты почтовых сообщений), способны содержать интерпретируемые компоненты, которые могут запускаться неявным образом при

открытии файла. Как и всякое в целом прогрессивное явление, такое «повышение активности данных» имеет свою оборотную сторону (в рассматриваемом случае – отставание в разработке механизмов безопасности и ошибки в их реализации). Обычные пользователи еще нескоро научатся применять интерпретируемые компоненты «в мирных целях» (или хотя бы узнают об их существовании), а перед злоумышленниками открылось, по существу, неограниченное поле деятельности. Как ни банально это звучит, но если для стрельбы по воробьям выкатывается пушка, то пострадает, в основном, стреляющий.

2. Интеграция разных сервисов, наличие среди них сетевых, всеобщая связность многократно увеличивают потенциал для атак на доступность, облегчают распространение вредоносного ПО (вирус «Melissa» – классический тому пример). Образно говоря, многие информационные системы, если не принять защитных мер, оказываются «в одной лодке» (точнее – в корабле без переборок), так что достаточно одной пробоины, чтобы «лодка» тут же пошла ко дну.

Как это часто бывает, вслед за «Melissa» появилась на свет целая серия вирусов, «червей» и их комбинаций: «Explorer.zip» (июнь 1999), «Bubble Boy» (ноябрь 1999), «ILOVEYOU» (май 2000) и т. д. Не то что бы от них был особенно большой ущерб, но общественный резонанс они вызвали немалый.

Активное содержимое, помимо интерпретируемых компонентов документов и других файлов данных, имеет еще одно популярное обличье: так называемые мобильные агенты. Это программы, которые загружаются на другие компьютеры и там выполняются. Наиболее известные примеры мобильных агентов – Java-апплеты, загружаемые на пользовательский компьютер и интерпретируемые Internet-навигаторами. Оказалось, что разработать для них модель безопасности, оставляющую достаточно возможностей для полезных действий, не так-то просто; еще сложнее реализовать такую модель без ошибок. В августе 1999 года стали известны недочеты в реализации технологий ActiveX и Java в рамках Microsoft Internet Explorer, которые давали возможность размещать на Web-серверах вредоносные апплеты, позволяющие получать полный контроль над системой-визитером.

Для внедрения «бомб» часто используются ошибки типа «переполнение буфера», когда программа, работая с областью памяти, выходит за границы допустимого и записывает в нужные злоумышленнику места определенные данные. Так действовал еще в 1988 году знаменитый «червь Морриса»; в июне 1999 года хакеры нашли способ использовать аналогичный метод по отношению к Mi-

crosoft Internet Information Server (IIS), чтобы получить контроль над Web-сервером. Окно опасности охватило сразу около полутора миллионов серверных систем.

Не забыты современными злоумышленниками и испытанные троянские программы. Например, «троянцы» Back Orifice и Netbus позволяют получить контроль над пользовательскими системами с различными вариантами MS-Windows.

Таким образом, действие вредоносного ПО может быть направлено не только против доступности, но и против других основных аспектов информационной безопасности.

Вернуться к содержанию

4.3. Угрозы целостности

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги. По данным газеты USA Today, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере 882 миллионов долларов. Можно предположить, что реальный ущерб был намного больше, поскольку многие организации, по понятным причинам, скрывают такие инциденты; не вызывает сомнений, что в наши дни ущерб от такого рода действий вырос многократно.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних.

Ранее мы проводили различие между статической и динамически целостностью. С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

- ввести неверные данные;
- изменить данные.

Иногда изменяются содержательные данные, иногда – служебная информация. Потенциально уязвимы, с точки зрения нарушения целостности, не только данные, но и программы.

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений. Соответствующие действия в сетевой среде называются активным прослушиванием.

Вернуться к содержанию

4.4. Угрозы конфиденциальности

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (пароли пользователей) не относятся к определенной предметной области, в ИС она играет техническую роль, но ее раскрытие особенно опасно, так как чревато получением несанкционированного доступа ко всей информации, в том числе и предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и, вообще, нетехнический характер.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем. Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке. И дело здесь не в организованности людей, а в изначальной непригодности парольной схемы.

Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена необходимая защита. Угроза же состоит в том, что кто-то откажется узнать секреты, которые сами просятся в руки. Для атаки могут использоваться разные технические средства (подслушивание, прослушивание).

Еще один пример изменения, о котором часто забывают, – хранение данных на резервных носителях. Для защиты данных на основных носителях применяются развитые системы управления доступом; копии же нередко просто лежат в шкафах, и получить доступ к ним могут многие.

Перехват данных – очень серьезная угроза, и если конфиденциальность, действительно, является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например, на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных. Часто ноутбуки оставляют без присмотра на работе или в автомобиле, иногда просто теряют.

Опасной нетехнической угрозой конфиденциальности являются методы морально-психологического воздействия, такие как маскарад – выполнение действий под видом лица, обладающего полномочиями для доступа к данным (см., например, статью Айрэ Винклера «Задание: шпионаж» в Jet Info, 1996, 19).

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например, системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т. д. Другой пример – нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Таковы основные угрозы, которые наносят наибольший ущерб субъектам информационных отношений.

Вернуться к содержанию

5. ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Основные классы мер процедурного уровня

Мы приступаем к рассмотрению мер безопасности, которые ориентированы на людей, а не на технические средства. Именно люди формируют режим информационной безопасности, и они же оказываются главной угрозой, поэтому «человеческий фактор» заслуживает особого внимания.

В российских компаниях накоплен богатый опыт регламентирования и реализации процедурных (организационных) мер, однако дело в том, что они пришли из «докомпьютерного» прошлого, поэтому требуют переоценки.

Следует осознать ту степень зависимости от компьютерной обработки данных, в которую попало современное общество. Без всякого преувеличения можно сказать, что необходима информационная гражданская оборона. Спокойно, без нагнетания страстей, нужно разъяснять обществу не только преимущества, но и опасности, связанные с использованием информационных технологий. Акцент следует делать не на военной или криминальной стороне дела, а на гражданских аспектах, связанных с поддержанием нормального функционирования аппаратного и программного обеспечения, то есть концентрироваться на вопросах доступности и целостности данных.

На процедурном уровне можно выделить следующие классы мер:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Вернуться к содержанию

5.2. Управление персоналом

Управление персоналом начинается с приема нового сотрудника на работу и даже раньше – с составления описания должности. Уже на данном этапе желательно подключить к работе специалиста по информационной безопасности для определения компьютерных привилегий, ассоциируемых с должностью. Существует два общих принципа, которые следует иметь в виду:

- разделение обязанностей;
- минимизация привилегий.

Принцип разделения обязанностей предписывает так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс. Например, нежелательна ситуация, когда крупные платежи от имени организации выполняет один человек. Надежнее поручить одному сотруднику оформление заявок на подобные платежи, а другому – заверять эти заявки. Другой пример – процедурные ограничения действий суперпользователя. Можно искусственно «расщепить» пароль суперпользователя, сообщив первую его часть одному сотруднику, а вторую – другому. Тогда критически важные действия по администрированию ИС они смогут выполнить только вдвоем, что снижает вероятность ошибок и злоупотреблений.

Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа очевидно – уменьшить ущерб от случайных или умышленных некорректных действий.

Предварительное составление описания должности позволяет оценить ее критичность и спланировать процедуру проверки и отбора кандидатов. Чем ответственнее должность, тем тщательнее нужно проверять кандидатов: навести о них справки, быть может, побеседовать с бывшими сослуживцами и т. д. Подобная процедура может быть длительной и дорогой, поэтому нет смысла дополнительно усложнять ее. В то же время неразумно и совсем отказываться от предварительной проверки, чтобы случайно не принять на работу человека с уголовным прошлым или психическим заболеванием.

Когда кандидат определен, он, вероятно, должен пройти обучение; по крайней мере, его следует подробно ознакомить со служебными обязанностями, а также с нормами и процедурами информационной безопасности. Желательно, чтобы меры безопасности были им усвоены до вступления в должность и до заведения его системного счета с входным именем, паролем и привилегиями.

С момента заведения системного счета начинается его администрирование, а также протоколирование и анализ действий пользователя. Постепенно изменяется окружение, в котором работает пользователь, его служебные обязанности и т. п. Все это требует соответствующего изменения привилегий. Техническую сложность представляют временные перемещения пользователя, выполнение им обязанностей взамен сотрудника, ушедшего в отпуск, и иные обстоятельства, когда полномочия нужно сначала предоставить, а через некоторое время взять обратно. В такие периоды профиль активности пользователя резко меня-

ется, что создает трудности при выявлении подозрительных ситуаций. Определенную аккуратность следует соблюдать и при выдаче новых постоянных полномочий, не забывая ликвидировать старые права доступа.

Ликвидация системного счета пользователя, особенно в случае конфликта между сотрудником и организацией, должна производиться максимально оперативно (в идеале – одновременно с извещением о наказании или увольнении). Возможно и физическое ограничение доступа к рабочему месту. Разумеется, если сотрудник увольняется, у него нужно принять все его компьютерное хозяйство и, в частности, криптографические ключи, если использовались средства шифрования.

К управлению сотрудниками примыкает администрирование лиц, работающих по контракту (например, специалистов фирмы-поставщика, помогающих запустить новую систему). В соответствии с принципом минимизации привилегий, им нужно выделить ровно столько прав, сколько необходимо, и изъять эти права сразу по окончании контракта. Проблема, однако, состоит в том, что на начальном этапе внедрения «внешние» сотрудники будут администрировать «местных», а не наоборот. Здесь на первый план выходит квалификация персонала организации, его способность быстро обучаться, а также оперативное проведение учебных курсов. Важны и принципы выбора деловых партнеров.

Иногда внешние организации принимают на обслуживание и администрирование ответственные компоненты компьютерной системы, например, сетевое оборудование. Нередко администрирование выполняется в удаленном режиме. Вообще говоря, это создает в системе дополнительные уязвимые места, которые необходимо компенсировать усиленным контролем средств удаленного доступа или, опять-таки, обучением собственных сотрудников,

Мы видим, что проблема обучения – одна из основных с точки зрения информационной безопасности. Если сотрудник не знаком с политикой безопасности своей организации, он не может стремиться к достижению сформулированных в ней целей. Не зная мер безопасности, он не сможет их соблюдать. Напротив, если сотрудник знает, что его действия протоколируются, он, возможно, воздержится от нарушений.

Вернуться к содержанию

5.3. Физическая защита и поддержание работоспособности

Безопасность информационной системы зависит от окружения, в котором она функционирует. Необходимо принять меры для защиты зданий и прилегающей территории, поддерживающей инфраструктуры, вычислительной техники, носителей данных.

Основной принцип физической защиты, соблюдение которого следует постоянно контролировать, формулируется как «непрерывность защиты в пространстве и времени». Ранее мы рассматривали понятие окна опасности. Для физической защиты таких окон быть не должно.

Мы кратко рассмотрим следующие направления физической защиты:

- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры;
- защита от перехвата данных;
- защита мобильных систем.

Меры физического управления доступом позволяют контролировать и при необходимости ограничивать вход и выход сотрудников и посетителей. Контролироваться может все здание организации, а также отдельные помещения, например, те, где расположены серверы, коммуникационная аппаратура и т. п.

При проектировании и реализации мер физического управления доступом целесообразно применять объектный подход. Во-первых, определяется периметр безопасности, ограничивающий контролируемую территорию. На этом уровне детализации важно продумать внешний интерфейс организации – порядок входа/выхода штатных сотрудников и посетителей, вноса/выноса техники. Все, что не входит во внешний интерфейс, должно быть инкапсулировано, то есть защищено от нелегальных проникновений.

Во-вторых, производится декомпозиция контролируемой территории, выделяются (под)объекты и связи (проходы) между ними. При такой более глубокой детализации следует выделить среди подобъектов наиболее критичные, с точки зрения безопасности, и обеспечить им повышенное внимание. Декомпозиция должна быть семантически оправданной, обеспечивающей разграничение разнородных сущностей, таких как оборудование разных владельцев или персонал, работающий с данными разной степени критичности. Важно сделать так, чтобы посетители, по возможности, не имели непосредственного доступа к компьютерам или, в крайнем случае, позаботиться о том, чтобы от окон и дверей не просматривались экраны мониторов и принтеры. Необходимо, чтобы посетителей по внешнему виду можно было отличить от сотрудников. Если отличие состоит в том, что посетителям выдаются идентификационные карточки, а сотрудники ходят «без опознавательных знаков», злоумышленнику достаточно снять карточку, чтобы его считали «своим». Очевидно, соответствующие карточки нужно выдавать всем.

Средства физического управления доступом известны давно. Это охрана, двери с замками, перегородки, телекамеры, датчики движения и многое другое. Для выбора оптимального (по критерию стоимость/эффективность) средства целесообразно провести анализ рисков (к этому мы еще вернемся). Кроме того, есть смысл периодически отслеживать появление технических новинок в данной области, стараясь максимально автоматизировать физическую защиту.

Более подробно данная тема рассмотрена в статье В. Барсукова «Физическая защита информационных систем» (Jet Info, 1997, 1).

Профессия пожарного – одна из древнейших, но пожары по-прежнему случаются и наносят большой ущерб. Мы не собираемся цитировать параграфы противопожарных инструкций или изобретать новые методы борьбы с огнем – на это есть профессионалы. Отметим лишь необходимость установки противопожарной сигнализации и автоматических средств пожаротушения. Обратим также внимание на то, что защитные меры могут создавать новые слабые места. Если на работу взят новый охранник, это, вероятно, улучшает физическое управление доступом. Если же он по ночам курит и пьет, то ввиду повышенной пожароопасности подобная мера защиты может только навредить.

К поддерживающей инфраструктуре можно отнести системы электро-, водо- и теплоснабжения, кондиционеры и средства коммуникаций. В принципе, к ним применимы те же требования целостности и доступности, что и к информационным системам. Для обеспечения целостности нужно защищать оборудование от краж и повреждений. Для поддержания доступности следует выбирать оборудование с максимальным временем наработки на отказ, дублировать ответственные узлы и всегда иметь под рукой запчасти.

Отдельную проблему составляют аварии водопровода. Они происходят нечасто, но могут нанести огромный ущерб. При размещении компьютеров необходимо принять во внимание расположение водопроводных и канализационных труб и постараться держаться от них подальше.

Сотрудники должны знать, куда следует обращаться при обнаружении протечек.

Перехват данных (о чем мы уже писали) может осуществляться самыми разными способами. Злоумышленник может подсматривать за экраном монитора, читать пакеты, передаваемые по сети, производить анализ побочных электромагнитных излучений и наводок (ПОМИН) и т. д. Остается уповать на повсеместное использование криптографии (что, впрочем, сопряжено у нас в стране со множеством технических и законодательных проблем), стараться макси-

мально расширить контролируемую территорию, разместившись в тихом особнячке, поодаль от других домов, пытаться держать под контролем линии связи (например, заключать их в надувную оболочку с обнаружением прокалывания), но самое разумное, вероятно, – постараться осознать, что для коммерческих систем обеспечение конфиденциальности является все-таки не главной задачей.

Желающим подробнее ознакомиться с вопросом мы рекомендуем прочитать статью В. Барсукова «Блокирование технологических каналов утечки информации» (Jet Info, 1998, 5-6).

Мобильные и портативные компьютеры – заманчивый объект кражи. Их часто оставляют без присмотра, в автомобиле или на работе, и похитить такой компьютер совсем несложно. Мы настоятельно рекомендуем шифровать данные на жестких дисках таких компьютеров.

Вообще говоря, при выборе средств физической защиты следует производить анализ рисков. Так, принимая решение о закупке источника бесперебойного питания, необходимо учесть качество электропитания в здании, занимаемом организацией (впрочем, почти наверняка оно окажется плохим), характер и длительность сбоев электропитания, стоимость доступных источников и возможные потери от аварий (поломка техники, приостановка работы организации и т. п.) (см. также статью В. Барсукова «Защита компьютерных систем от силовых деструктивных воздействий» в Jet Info, 2000, 2). В то же время во многих случаях решения очевидны. Меры противопожарной безопасности обязательны для всех организаций. Стоимость реализации многих мер (например, установка обычного замка на дверь серверной комнаты) либо мала, либо хоть и заметна, но все же явно меньше, чем возможный ущерб. В частности, имеет смысл регулярно копировать большие базы данных.

Нечаянные ошибки системных администраторов и пользователей грозят повреждением аппаратуры, разрушением программ и данных, в лучшем случае они создают бреши в защите, которые делают возможной реализацию угроз.

Можно выделить следующие направления повседневной деятельности:

– поддержка пользователей;

– поддержка программного обеспечения;

– конфигурационное управление;

– резервное копирование;

– управление носителями;

– документирование;

– регламентные работы.

Поддержка пользователей подразумевает, прежде всего, консультирование и оказание помощи при решении разного рода проблем.

Поддержка ПО – одно из важнейших средств обеспечения целостности информации. Обычно контроль достигается комбинированием средств физического и логического управления доступом, а также использованием утилит проверки и обеспечения целостности.

Конфигурационное управление позволяет контролировать и фиксировать изменения, вносимые в программную конфигурацию. Прежде всего, необходимо застраховаться от случайных или непродуманных модификаций, уметь, как минимум, возвращаться к прошлой, работающей, версии. Фиксация изменений позволит легко восстановить текущую версию после аварии.

Лучший способ уменьшить количество ошибок в рутинной работе – максимально автоматизировать ее. Правы те «ленивые» программисты и системные администраторы, которые, окинув взглядом море однообразных задач, говорят: «Я ни за что не буду делать этого; я напишу программу, которая сделает все за меня». Автоматизация и безопасность зависят друг от друга; тот, кто заботится в первую очередь об облегчении своей задачи, на самом деле оптимальным образом формирует режим информационной безопасности.

Резервное копирование необходимо для восстановления программ и данных после аварий. И здесь целесообразно автоматизировать работу, как минимум сформировав компьютерное расписание создания полных и инкрементальных копий, а как максимум – воспользовавшись соответствующими программными продуктами (см., например, Jet Info, 2000, 12). Нужно также наладить размещение копий в безопасном месте, защищенном от несанкционированного доступа, пожаров, протечек, то есть от всего, что может привести к краже или повреждению носителей. Целесообразно иметь несколько экземпляров резервных копий и часть из них хранить вне территории организации, защищаясь таким образом от крупных аварий и аналогичных инцидентов.

Время от времени в тестовых целях следует проверять возможность восстановления информации с копий.

Управлять носителями необходимо для обеспечения физической защиты и учета дискет, лент, печатных выдач и т. п. Управление носителями должно обеспечивать конфиденциальность, целостность и доступность информации, хранящейся вне компьютерных систем. Под физической защитой здесь понимается не только отражение попыток несанкционированного доступа, но и предохранение от вредных влияний окружающей среды (жары, холода, влаги, магнетизма).

Управление носителями должно охватывать весь жизненный цикл – от закупки до выведения из эксплуатации.

Документирование – неотъемлемая часть информационной безопасности. В виде документов оформляется почти все – от политики безопасности до журнала учета носителей. Важно, чтобы документация была актуальной, отражала именно текущее состояние дел, причем в непротиворечивом виде.

К хранению одних документов (содержащих, например, анализ уязвимых мест системы и угроз) применимы требования обеспечения конфиденциальности, к другим, таким как план восстановления после аварий, – требования целостности и доступности (в критической ситуации план необходимо найти и прочитать).

Регламентные работы – очень серьезная угроза безопасности. Сотрудник, осуществляющий регламентные работы, получает исключительный доступ к системе, и на практике очень трудно проконтролировать, какие именно действия он совершает. Здесь на первый план выходит степень доверия к тем, кто выполняет работу.

Вернуться к содержанию

5.4. Реагирование на нарушения режима безопасности и планирование восстановительных работ

Программа безопасности, принятая организацией, должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима информационной безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.

Реакция на нарушения режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- выявление нарушителя;
- предупреждение повторных нарушений.

В организации должен быть человек, доступный 24 часа в сутки (лично, по телефону, пейджеру или электронной почте), который отвечает за реакцию на нарушения. Все должны знать координаты этого человека и обращаться к нему при первых признаках опасности. В общем, как при пожаре, нужно знать, куда звонить и что делать до приезда пожарной команды.

Важность быстрой и скоординированной реакции можно продемонстрировать на следующем примере. Пусть локальная сеть предприятия состоит из двух сегментов, администрируемых разными людьми. Далее, пусть в один из сегментов был внесен вирус. Почти наверняка через несколько минут (или, в крайнем

случае, несколько десятков минут) вирус распространится и на другой сегмент. Значит, меры нужно принять немедленно. «Вычищать» вирус необходимо одновременно в обоих сегментах; в противном случае сегмент, восстановленный первым, заразится от другого, а затем вирус вернется и во второй сегмент.

Нередко требование локализации инцидента и уменьшения наносимого вреда вступает в конфликт с желанием выявить нарушителя. В политике безопасности организации приоритеты должны быть расставлены заранее. Поскольку, как показывает практика, выявить злоумышленника очень сложно, на наш взгляд, в первую очередь следует заботиться об уменьшении ущерба.

Чтобы найти нарушителя, нужно заранее выяснить контактные координаты поставщика сетевых услуг и договориться с ним о самой возможности и порядке выполнения соответствующих действий. Более подробно данная тема рассматривается в статье Н. Браунли и Э. Гатмэна «Как реагировать на нарушения информационной безопасности (И.С 2350, BCP 21)» (Jet Info, 2000, 5).

Чтобы предотвратить повторные нарушения, необходимо анализировать каждый инцидент, выявлять причины, накапливать статистику. Каковы источники вредоносного ПО? Какие пользователи имеют обыкновение выбирать слабые пароли? На подобные вопросы и должны дать ответ результаты анализа.

Необходимо отслеживать появление новых уязвимых мест и, как можно быстрее, ликвидировать ассоциированные с ними окна опасности. Кто-то в организации должен курировать этот процесс, принимать краткосрочные меры и корректировать программу безопасности для принятия долгосрочных мер.

Ни одна организация не застрахована от серьезных аварий, вызванных естественными причинами, действиями злоумышленника, халатностью или некомпетентностью. В то же время у каждой организации есть функции, которые руководство считает критически важными, они должны выполняться несмотря ни на что. Планирование восстановительных работ позволяет подготовиться к авариям, уменьшить ущерб от них и сохранить способность к функционированию хотя бы в минимальном объеме.

Отметим, что меры информационной безопасности можно разделить на три группы, в зависимости от того, направлены ли они на предупреждение, обнаружение или ликвидацию последствий атак. Большинство мер носит предупредительный характер. Оперативный анализ регистрационной информации и некоторые аспекты реагирования на нарушения (так называемый активный

аудит) служат для обнаружения и отражения атак. Планирование восстановительных работ, очевидно, можно отнести к последней из трех перечисленных групп.

Процесс планирования восстановительных работ можно разделить на следующие этапы:

• выявление критически важных функций организации, установление приоритетов;

• идентификация ресурсов, необходимых для выполнения критически важных функций;

• определение перечня возможных аварий;

• разработка стратегии восстановительных работ;

• подготовка к реализации выбранной стратегии;

• проверка стратегии.

Планируя восстановительные работы, следует отдавать себе отчет в том, что полностью сохранить функционирование организации не всегда возможно. Необходимо выявить критически важные функции, без которых организация теряет свое лицо, и даже среди критичных функций расставить приоритеты, чтобы как можно быстрее и с минимальными затратами возобновить работу после аварии.

Идентифицируя ресурсы, необходимые для выполнения критически важных функций, следует помнить, что многие из них имеют некомпьютерный характер. На данном этапе желательно подключать к работе специалистов разного профиля, способных в совокупности охватить все аспекты проблемы. Критичные ресурсы обычно относятся к одной из следующих категорий:

• персонал;

• информационная инфраструктура;

• физическая инфраструктура.

Составляя списки ответственных специалистов, следует учитывать, что некоторые из них могут непосредственно пострадать от аварии (например, от пожара), кто-то может находиться в состоянии стресса, часть сотрудников, возможно, будет лишена возможности попасть на работу (например, в случае массовых беспорядков). Желательно иметь некоторый резерв специалистов или заранее определить каналы, по которым можно на время привлечь дополнительный персонал.

Информационная инфраструктура включает в себя следующие элементы:

• компьютеры;

• программы и данные;

• информационные сервисы внешних организаций;

• документацию.

Нужно подготовиться к тому, что на «запасном аэродроме», куда организация будет эвакуирована после аварии, аппаратная платформа может отличаться от исходной. Соответственно, следует продумать меры поддержания совместимости по программам и данным.

Среди внешних информационных сервисов для коммерческих организаций, вероятно, важнее всего получить оперативную информацию и связь с государственными службами, курирующими данный сектор экономики.

Документация важна хотя бы потому, что не вся информация, с которой работает организация, представлена в электронном виде. Скорее всего, план восстановительных работ напечатан на бумаге.

К физической инфраструктуре относятся здания, инженерные коммуникации, средства связи, оргтехника и многое другое. Компьютерная техника не может работать в плохих условиях, без стабильного электропитания и т. п.

Анализируя критичные ресурсы, целесообразно учесть временной профиль их использования. Большинство ресурсов требуется постоянно, но в некоторых нужда может возникать только в определенные периоды (например, в конце месяца или года при составлении отчета).

При определении перечня возможных аварий нужно попытаться разработать их сценарии. Как будут развиваться события? Каковы могут оказаться масштабы бедствия? Что произойдет с критичными ресурсами? Например, смогут ли сотрудники попасть на работу? Будут ли выведены из строя компьютеры? Возможны ли случаи саботажа? Будет ли работать связь? Пострадает ли здание организации? Можно ли будет найти и прочитать необходимые бумаги?

Стратегия восстановительных работ должна базироваться на наличных ресурсах и быть не слишком накладной для организации. При разработке стратегии целесообразно провести анализ рисков, которым подвергаются критичные функции, и попытаться выбрать наиболее экономичное решение.

Стратегия должна предусматривать не только работу по временной схеме, но и возвращение к нормальному функционированию.

Подготовка к реализации выбранной стратегии состоит в выработке плана действий в экстренных ситуациях и по их окончании, а также в обеспечении некоторой избыточности критичных ресурсов. Последнее возможно и без большого расхода средств, если заключить с одной или несколькими организациями

соглашения о взаимной поддержке в случае аварий: те, кто не пострадал, предоставляют часть своих ресурсов во временное пользование менее удачливым партнерам.

Избыточность обеспечивается также мерами резервного копирования, хранением копий в нескольких местах, представлением информации в разных видах (на бумаге и в файлах) и т. д.

Имеет смысл заключить соглашение с поставщиками информационных услуг о первоочередном обслуживании в критических ситуациях или заключать соглашения с несколькими поставщиками. Правда, эти меры могут потребовать определенных расходов.

Проверка стратегии производится путем анализа подготовленного плана, принятых и намеченных мер.

Вернуться к содержанию

6. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Под **угрозой** безопасности информации в компьютерной системе (КС) понимают событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой информации.

Уязвимость информации – это возможность возникновения на какомлибо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

Атакой на КС называют действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости. Иначе говоря, атака на КС является реализацией угрозы безопасности информации в ней.

Угрозы информационной безопасности могут быть разделены на угрозы, не зависящие от деятельности человека (**естественные угрозы** физических воздействий на информацию стихийных природных явлений), и угрозы, вызванные человеческой деятельностью (**искусственные угрозы**), которые являются гораздо более опасными.

Искусственные угрозы, исходя из их мотивов, разделяются на **непреднамеренные** (случайные) и **преднамеренные** (умышленные).

К непреднамеренным угрозам относятся:

- ошибки в проектировании КС;
- ошибки в разработке программных средств КС;
- случайные сбои в работе аппаратных средств КС, линий связи, энергоснабжения;
- ошибки пользователей КС;
- воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.

К умышленным угрозам относятся:

- несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);
- несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.

В зависимости от целей преднамеренных угроз безопасности информации в КС угрозы могут быть разделены на основные группы:

- угроза нарушения целостности, то есть преднамеренного воздействия на информацию, хранящуюся в КС или передаваемую между КС;
- угроза нарушения доступности информации, то есть отказа в обслуживании, вызванного преднамеренными действиями одного из пользователей КС (нарушителя), при котором блокируется доступ к некоторому ресурсу КС со стороны других пользователей КС (постоянно или на больший период времени).

Поскольку наиболее опасные угрозы информационной безопасности вызваны преднамеренными действиями нарушителя, которые в общем случае являются неформальными, проблема защиты информации относится к формально не определенным проблемам. Отсюда следуют два основных вывода:

- надежная защита информации в КС не может быть обеспечена только формальными методами (например, только программными и аппаратными средствами);
- защита информации в КС не может быть абсолютной.

При решении задачи защиты информации в КС необходимо применять так называемый системно-концептуальный подход. В соответствии с ним решение задачи должно подразумевать:

- целевую системность, при которой защищенность информации рассматривается как составная неотъемлемая часть ее качества;
- пространственную системность, предполагающую взаимосвязанность защиты информации во всех элементах КС;
- организационную системность, предполагающую единство организации всех работ по защите информации в КС и управление ими.

Концептуальность подхода к решению задачи защиты информации в КС предусматривает ее решение на основе единой концепции (совокупности научно обоснованных решений, необходимых и достаточных для оптимальной организации защиты информации в КС).

Обеспечение информационной безопасности КС является непрерывным процессом, целенаправленно проводимым на всех этапах ее жизненного цикла с комплексным применением всех имеющихся методов и средств.

Существующие методы и средства защиты информации можно подразделить на четыре основные группы:

- методы и средства организационно-правовой защиты информации;
- методы и средства инженерно-технической защиты информации;
- криптографические методы и средства защиты информации;
- программно-аппаратные методы и средства защиты информации.

- *Вернуться к содержанию*

7. ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К методам и средствам организационной защиты информации относятся организационно-технические и организационно правовые мероприятия, проводимые в процессе создания и эксплуатации КС для обеспечения защиты информации. Эти мероприятия должны проводиться при строительстве или ремонте помещений, в которых будет размещаться КС; проектировании системы, монтаже и наладке ее технических и программных средств; испытаниях и проверке работоспособности КС.

Основные свойства методов и средств организационной защиты:

- обеспечение полного или частичного перекрытия значительной части каналов утечки информации (например, хищения или копирования носителей информации);
- объединение всех используемых в КС средств в целостный механизм защиты информации.

Методы и средства организационной защиты информации включают в себя:

- ограничение физического доступа к объектам КС и реализацию режимных мер;
- ограничение возможности перехвата побочных электромагнитных излучений и наводок;
- разграничение доступа к информационным ресурсам и процессам КС (установка правил разграничения доступа, шифрование информации при ее хранении и передаче, обнаружение и уничтожение аппаратных и программных закладок);
- резервное копирование наиболее важных с точки зрения утраты массивов документов;
- профилактику заражения компьютерными вирусами.

Перечислим основные виды мероприятий, которые должны проводиться на различных этапах жизненного цикла КС:

1) **на этапе создания КС**: при разработке ее общего проекта и проектов отдельных структурных элементов – анализ возможных угроз и методов их нейтрализации; при строительстве и переоборудовании помещений – приобретение сертифицированного оборудования, выбор лицензированных организаций; при разработке математического, программного, информационного и лингвисти-

ческого обеспечения – использование сертифицированных программных и инструментальных средств; при монтаже и наладке оборудования – контроль за работой технического персонала; при испытаниях и приемке в эксплуатацию – включение в состав аттестационных комиссий сертифицированных специалистов;

2) **в процессе эксплуатации КС** – организация пропускного режима, определение технологии автоматизированной обработки документов, организация работы обслуживающего персонала, распределение реквизитов разграничения доступа пользователей к элементам КС (паролей, ключей, карт и т. п.), организация ведения протоколов работы КС, контроль выполнения требований служебных инструкций и т. п.;

3) **мероприятия общего характера** – подбор и подготовка кадров, организация плановых и предупреждающих проверок средств защиты информации, планирование мероприятий по защите информации, обучение персонала, участие в семинарах, конференциях и выставках по проблемам безопасности информации и т. п.

Основой проведения организационных мероприятий является использование и подготовка законодательных и нормативных документов в области ИБ, которые на правовом уровне должны регулировать доступ к информации со стороны потребителей. В российском законодательстве позже, чем в законодательстве других развитых стран, появились необходимые правовые акты.

Можно выделить четыре уровня правового обеспечения ИБ. **Первый уровень** образуют международные договоры, к которым присоединилась Российская Федерация, и федеральные законы России:

- международные (всемирные) конференции об охране промышленной собственности, охране интеллектуальной собственности, авторском праве;
- Конституция Российской Федерации (статья 23 определяет право граждан на тайну переписки, телефонных, телеграфных и иных сообщений);
- Гражданский кодекс Российской Федерации (в статье 139 устанавливается право на возмещение убытков от утечки с помощью незаконных методов информации, относящейся к служебной и коммерческой тайне);
- Уголовный кодекс Российской Федерации (статья 272 устанавливает ответственность за неправомерный доступ к компьютерной информации, статья 273 – создание, использование и распространение вредоносных программ для ЭВМ, статья 274 – за нарушение правил эксплуатации ЭВМ, систем и сетей);

- Федеральный закон «Об информации, информатизации и защите информации» от 20.02.95 № 24 – ФЗ (статья 10 устанавливает разнесение информационных ресурсов по категориям доступа: открытая информация, государственная тайна, конфиденциальная информация, статья 21 определяет порядок защиты информации);
- Федеральный закон «О государственной тайне» от 21.07.93 № 5485-1 (статья 5 устанавливает перечень сведений, составляющих государственную тайну; статья 8 – степени секретности сведений и грифы секретности их носителей; «особой важности», «совершенно секретно» и «секретно»; статья 20 – органы по защите государственной тайны для координации деятельности этих органов; статья 28 – порядок сертификации средств защиты информации, относящейся к государственной тайне);
- Федеральные законы «О лицензировании отдельных видов деятельности» от 08.08.2001 № 128-ФЗ, «О связи» от 16.02.95 № 15-ФЗ, «Об электронной цифровой подписи» от 10.01.02 № 1-ФЗ, «Об авторском праве и смежных правах» от 09.07.93 № 5351-1, «О правовой охране программ для ЭВМ и баз данных» от 23.09.92 № 3523-1.

Второй уровень правового обеспечения ИБ составляют подзаконные акты, к которым относятся указы Президента Российской Федерации и постановления Правительства Российской Федерации, а также письма Высшего Арбитражного Суда Российской Федерации и постановления пленумов Верховного Суда Российской Федерации.

Третий уровень правового обеспечения ИБ составляют государственные стандарты в области защиты информации, руководящие документы, нормы, методики и классификаторы, разработанные соответствующими государственными органами.

Четвертый уровень правового обеспечения ИБ образуют локальные нормативные акты, положения, инструкции, методические рекомендации и другие документы по комплексной защите информации в КС конкретной организации. К таким нормативным документам относятся:

- приказ об утверждении перечня сведений, составляющих коммерческую тайну предприятия;
- трудовые и гражданско-правовые договоры (подряда, поручения, комиссии и т. п.), в которые включены пункты об обязанности возмещения ущерба за разглашение сведений, составляющих коммерческую тайну предприятия и др.

- *Вернуться к содержанию*

8. ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Под инженерно-техническими средствами защиты информации понимают физические объекты, механические, электрические и электронные устройства, элементы конструкции зданий, средства пожаротушения и другие средства, обеспечивающие:

- защиту территории и помещений КС от проникновения нарушителей;
- защиту аппаратных средств КС и носителей информации от хищения;
- предотвращение возможности удаленного (из-за пределов охраняемой территории) видеонаблюдения (подслушивания) за работой персонала и функционированием технических средств КС;
- предотвращение возможности перехвата ПЭМИН, вызванных работающими техническими средствами КС и линиями передачи данных;
- организацию доступа в помещения КС сотрудников;
- контроль над режимом работы персонала КС;
- контроль над перемещением сотрудников КС в различных производственных зонах;
- противопожарную защиту помещений КС;
- минимизацию материального ущерба от потерь информации, возникших в результате стихийных бедствий и техногенных аварий.

Важнейшей составной частью инженерно-технических средств защиты информации являются технические средства охраны, которые образуют первый рубеж защиты КС и являются необходимым, но недостаточным условием сохранения конфиденциальности и целостности информации в КС.

Вернуться к содержанию

9. ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К аппаратным средствам защиты информации относятся электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие некоторые функции обеспечения ИБ. Критерием отнесения устройства к аппаратным, а не к инженерно-техническим средствам защиты является обязательное включение в состав технических средств КС.

К основным аппаратным средствам защиты информации относятся:

- устройства для ввода идентифицирующей пользователя информации;
- устройства для шифрования информации;
- устройства для воспрепятствования несанкционированному включению рабочих станций и серверов.

Примеры вспомогательных аппаратных средств защиты информации:

- устройства уничтожения информации на магнитных носителях;
- устройства сигнализации о попытках несанкционированных действий пользователей КС

Под программными средствами защиты информации понимают специальные программы, включаемые в состав программного обеспечения КС исключительно для выполнения защитных функций.

К основным программным средствам защиты информации относятся:

- программы идентификации и аутентификации пользователей КС;
- программы разграничения доступа пользователей к ресурсам КС;
- программы шифрования информации;
- программы защиты информационных ресурсов от несанкционированного изменения, использования и копирования.

Под идентификацией, применительно к обеспечению ИБ КС, понимают однозначное распознавание уникального имени субъекта КС. Аутентификация означает подтверждение того, что предъявленное имя соответствует данному субъекту.

Примеры вспомогательных программных средств защиты информации:

- программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т. п.);
- программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий;
- программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации);

- программы текстового контроля защищенности КС и др.

К преимуществам программных средств защиты информации относятся:

- простота тиражирования;
- гибкость (возможность настройки на различные условия применения, учитывающие специфику угроз ИБ конкретных КС);
- простота применения – одни программные средства, например шифрования, работают в «прозрачном» (незаметном для пользователя) режиме, а другие не требуют от пользователя никаких новых навыков;
- практически неограниченные возможности их развития путем внесения изменений для учета новых угроз безопасности информации;

К недостаткам программных средств защиты информации относятся:

- снижение эффективности КС за счет потребления ее ресурсов, требуемых для функционирования программ защиты;
- более низкая производительность (по сравнению с выполняющими аналогичные функции аппаратными средствами защиты, например шифрования);
- возможность злоумышленного изменения программных средств защиты в процессе эксплуатации КС.

Вернуться к содержанию

10. ТРЕБОВАНИЯ К КОМПЛЕКСНЫМ СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ

Поскольку потенциальные угрозы безопасности информации весьма многообразны, цели защиты информации могут быть достигнуты только путем создания комплексной системы защиты информации (КСЗИ), под которой понимается совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации в КС.

Основные требования к комплексной системе защиты информации:

- разработка на основе положений и требований существующих законов, стандартов и нормативно-методических документов по обеспечению ИБ;
- использование комплекса программно-технических средств и организационных мер для защиты КС;
- надежность, производительность, конфигурируемость;
- экономическая целесообразность (поскольку стоимость КСЗИ включается в стоимость КС, стоимость средств защиты не должна быть выше возможного ущерба от потери информации);
- выполнение на всех этапах ЖЦ обработки информации в КС (в том числе при проведении ремонтных и регламентных работ);
- возможность совершенствования;
- обеспечение разграничения доступа к конфиденциальной информации с отвлечением нарушителя на ложную информацию (обеспечение не только пассивной, но и активной защиты);
- взаимодействие с незащищенными КС по установленным для этого правилам разграничения доступа;
- обеспечение проведения учета и расследования случаев нарушения безопасности информации в КС;
- сложная для пользователя;
- возможность оценки эффективности ее применения.

Впервые основные категории требований к защищенности КС были сформулированы в документе Министерства обороны США «Trusted Computer System Evaluation Criteria» («Критерии оценки безопасности компьютерных систем», или «Оранжевая книга»), в 1985 г. В этом документе предложены три основные категории требований.

1. Политика:

- наличие явной и хорошо определенной политики обеспечения безопасности;
- использование маркировки объектов в КС для управления доступом к ним.

2. Подотчетность:

- индивидуальная идентификация субъектов КС;
- сохранение и защита информации аудита.

3. Гарантии:

- включение в состав КС программно-аппаратных средств для получения гарантий выполнения требований категорий 1 и 2;
- постоянная защищенность средств обеспечения безопасности информации в КС от их преодоления и (или) несанкционированного изменения.

В «Оранжевой книге» были введены семь классов защищенности КС – от минимальной защиты (класс D1) до верифицированной (формально доказанной) защиты (класс A1). Требования «Оранжевой книги» явились первой попыткой создать единый стандарт безопасности КС, рассчитанный на проектировщиков, разработчиков (программистов), пользователей подобных систем и специалистов по их сертификации.

Отличительной чертой этого стандарта является ориентация на государственные (в первую очередь военные) организации и операционные системы.

В 1992 г. Гостехкомиссия России опубликовала первый комплект руководящих документов по защите средств вычислительной техники (СВТ) и автоматизированных систем (АС) от несанкционированного доступа.

СВТ не решают непосредственно прикладных задач, а используются в качестве элементов АС. Примерами СВТ являются плата расширения BIOS с соответствующим аппаратным и программным интерфейсом для аутентификации пользователей АС или программа «прозрачного» шифрования информации на жестком диске.

В руководящих документах Гостехкомиссии России определены семь классов защищенности СВТ от несанкционированного доступа к обрабатываемой (сохраняемой, передаваемой) с помощью этих средств информации (наиболее защищенным является первый класс).

АС рассматривается как комплекс СВТ и имеет дополнительные характеристики: полномочия пользователей, модель нарушителя, технология обработки информации. Типичным примером АС является многопользовательская и многозадачная ОС.

В руководящих документах Гостехкомиссии России определены девять классов защищенности АС от несанкционированного доступа, которые объединены в три группы:

- однопользовательские АС с информацией, размещенной на носителях одного уровня конфиденциальности (класс 3Б и 3А);
- многопользовательские АС с одинаковыми полномочиями пользователей и информацией на носителях разного уровня конфиденциальности (классы 2Б и 2А);
- многопользовательские АС с разными полномочиями пользователей и информацией разного уровня конфиденциальности (в порядке возрастания защищенности от класса 1Д до класса 1А).

Под несанкционированным доступом к информации в руководящих документах Гостехкомиссии России понимается доступ к информации, нарушающий установленные правила разграничения доступа и использующий штатные возможности СВТ и АС. Руководящие документы Гостехкомиссии России, подобно «Оранжевой книге», ориентированы прежде всего на применение в КС силовых структур Российской Федерации.

Дальнейшее развитие стандартов в области ИБ КС привело к появлению европейских «Критериев оценки безопасности ИТ» (Information Technology Security Evaluation Criteria), американских «Федеральных критериев БИТ», канадских «Критериев оценки безопасности компьютерных продуктов» и завершилось на сегодняшний день принятием «Общих критериев оценки безопасности ИТ».

«Общие критерии оценки безопасности ИТ» адресованы трем группам специалистов (пользователям, разработчикам и экспертам по классификации КС) и представляют собой новый межгосударственный уровень в стандартизации безопасности ИТ.

В Российской Федерации «Общие критерии оценки безопасности ИТ» изданы в качестве ГОСТ (ГОСТ РИСО/МЭК 15408 – 2001 «Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ»).

В «Общих критериях оценки безопасности ИТ» предложена система функциональных требований к защищенным КС и критерии их независимого ражирования.

Иначе говоря, в этих стандартах не устанавливается линейная шкала уровней безопасности КС, характерная для «Оранжевой книги». Это объясняется тем, что для одних КС наиболее важным требованием является идентификация и

аутентификация пользователей, а для других – реализация конкретной политики разграничения доступа к ресурсам или обеспечение доступности информации.

Вернуться к содержанию

11. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

11.1. Аутентификация пользователей на основе паролей и модели «рукопожатия»

При выборе паролей пользователи КС должны руководствоваться двумя, по сути взаимоисключающими, правилами – пароли должны трудно подбираться и легко запоминаться.

Сложность выбираемых пользователями КС паролей должна определяться администратором при реализации установленной для данной системы политики безопасности. Другими параметрами политики учетных записей при использовании парольной аутентификации должны быть:

- максимальный срок действия пароля;
- несовпадение пароля с логическим именем пользователя, под которым он зарегистрирован в КС;
- неповторяемость паролей одного пользователя.

Требование неповторяемости паролей может быть реализовано двумя способами. Во-первых, можно установить минимальный срок действия пароля. Во-вторых, можно вести список уже использовавшихся данным пользователем паролей.

К сожалению, обеспечить реальную уникальность каждого вновь выбираемого пользователем пароля с помощью приведенных выше мер практически невозможно.

Обеспечить приемлемую степень сложности паролей и их реальную уникальность можно путем назначения паролей всем пользователям администратором КС с одновременным запретом на изменение пароля самим пользователем. Для генерации паролей администратор при этом может использовать программный генератор, позволяющий создавать пароли различной сложности.

Однако при таком способе назначения паролей возникают проблемы, связанные с необходимостью создания защищенного канала для передачи пароля от администратора к пользователю, трудность проверки сохранения пользователем не им выбранного пароля только в своей памяти и потенциальной возможностью администратора, знающего пароли всех пользователей, злоупотребления своими полномочиями. Поэтому наиболее целесообразным является выбор пароля пользователем на основе установленных администратором правил с возможностью задания администратором нового пароля пользователю в случае, если тот забыл свой пароль.

Еще одним аспектом политики учетных записей пользователей КС должно стать определение противодействия системы попыткам подбора паролей.

Могут применяться следующие правила:

- ограничение числа попыток входа в систему;
- скрытие логического имени последнего работавшего пользователя;
- учет всех попыток входа в систему в журнале аудита.

Реакцией системы на неудачную попытку входа пользователя могут быть:

- блокировка учетной записи, под которой осуществляется попытка входа, при превышении максимально возможного числа попыток;
- нарастающее увеличение временной задержки перед предоставлением пользователю следующей попытки входа.

Постоянная блокировка учетной записи, под которой осуществляется попытка входа, при обнаружении попытки подбора пароля менее целесообразна, поскольку она позволит нарушителю намеренно заблокировать работу в КС легального пользователя.

При любой реакции системы на попытку подбора пароля необходимо в настройках параметров политики учетных записей обеспечить сброс значения счетчика попыток входа в систему под конкретной учетной записью через заданный промежуток времени, иначе значения счетчика будут суммироваться для разных сеансов работы пользователя.

При первоначальном вводе или смене пароля пользователя обычно применяются два классических правила:

- символы вводимого пароля не отображаются на экране
- для подтверждения правильности ввода пароля этот ввод повторяется дважды.

Одним из следствий первого правила является нецелесообразность назначения пользователю пароля системой, поскольку в этом случае пароль должен быть выведен пользователю в открытом виде или записан на специальном носителе.

Однако отказ от отображения символов вводимого пароля может создать проблему, так как увеличивается вероятность того, что случайная ошибка, допущенная при вводе пароля, останется незамеченной, а это может привести к блокировке учетной записи легального пользователя. Поэтому, если вход пользователя в КС происходит в защищенном помещении, в которое не могут попасть посторонние лица, от правила скрытия символов вводимого пароля можно и отказаться.

Очевидно, что в базе данных учетных записей пользователей КС пароли не могут храниться в открытом виде. Для хранения паролей возможно их предварительное шифрование или хеширование.

Несмотря на то, что с помощью применения перечисленных выше правил парольную аутентификацию можно сделать более безопасной, она все-таки остается весьма уязвимой. Для ее усиления могут использоваться так называемые одноразовые пароли. Недостатками схемы одноразовых паролей являются организация защищенного хранения длинного списка паролей и неясность с номером следующего пароля, если после ввода предыдущего пароля из списка вход пользователя в систему не был осуществлен из-за сбоя в работе КС.

Но в любом варианте парольной аутентификации подтверждение подлинности пользователя осуществляется на основе ввода им некоторой конфиденциальной информации, которую можно подсмотреть, выманить, подобрать, угадать и т. д. Рассмотрим аутентификацию пользователей на основе модели «рукопожатия», во многом свободной от указанных недостатков.

Примеры:

1. Система предлагает пользователю ответить при регистрации его в КС на несколько вопросов, имеющих частично объективное и частично вымышленное содержание (например, «девичья фамилия вашей матери», «где находится такой-то клуб» и т. д.). При входе в систему пользователю предлагается ответить на другой список вопросов, среди которых есть некоторые из заданных ему при регистрации.

2. Аутентификация на основе модели «рукопожатия». При регистрации в КС пользователю предлагается набор небольших изображений (пиктограмм), среди которых он должен выбрать заданное число картинок. При последующем входе в систему ему выводится другой набор изображений, часть из которых он видел при регистрации. Для правильной аутентификации пользователь должен отметить те картинки, которые он выбрал при регистрации.

Вернуться к содержанию

11.2. Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью

К основным биометрическим характеристикам пользователей КС, которые могут применяться при их аутентификации, относятся:

- отпечатки пальцев;
- геометрическая форма рук;
- узор радужной оболочки глаза;

- рисунок сетчатки глаза;
- геометрическая форма и размеры лица;
- тембр голоса;
- геометрическая форма и размеры уха и др.

Наиболее распространенными являются программно-аппаратные средства аутентификации пользователей по их отпечаткам пальцев. Для считывания этих отпечатков обычно применяются оснащенные специальными сканерами клавиатуры и мыши. Наличие достаточно больших банков данных с отпечатками пальцев граждан является основной причиной достаточно широкого применения подобных средств аутентификации в государственных структурах, а также в крупных коммерческих организациях. Недостатком таких средств является потенциальная возможность применения отпечатков пальцев пользователей для контроля над их частной жизнью.

Если, по объективным причинам, получение четкого отпечатка пальца невозможно, то может применяться аутентификация по геометрической форме руки пользователя. В этом случае сканеры могут быть установлены на стене помещения.

Наиболее достоверными, но и более дорогостоящими являются средства аутентификации пользователей, основанные на характеристиках глаза. Вероятность повторения этих признаков оценивается 10^{-78}.

Наиболее дешевыми, но и менее достоверными являются средства аутентификации, основанные на геометрической форме и размере лица пользователя или на тембре его голоса, что позволяет использовать эти средства и для аутентификации при удаленном доступе пользователей КС.

Общим недостатком средств аутентификации пользователей КС по их биометрическим характеристикам является их более высокая стоимость по сравнению с другими средствами аутентификации, что обусловлено, в первую очередь, необходимостью приобретения дополнительных аппаратных средств. Способы аутентификации, основанные на особенностях клавиатурного почерка и росписи мышью пользователей, не требуют применения специальной аппаратуры.

Общей особенностью способов аутентификации, основанных на клавиатурном почерке и росписи мышью является нестабильность их характеристик у одного и того же пользователя, которая может быть вызвана:

1) естественными изменениями, связанными с улучшением навыков пользователя по работе с клавиатурой и мышью или, наоборот, с их ухудшением из-за старения организма;

2) изменениями, связанными с ненормальным физическим или эмоциональным состоянием пользователя.

Изменения характеристик пользователя, вызванные причинами первого рода, не являются скачкообразными, поэтому могут быть нейтрализованы изменениями эталонных характеристик после каждой успешной аутентификации пользователя.

Изменения характеристик пользователя, вызванные причинами второго рода, могут быть скачкообразными и привести к отклонению его попытки входа в КС. Однако эта особенность аутентификации на основе клавиатурного почерка и росписи мышью может стать и достоинством, если речь идет о пользователях КС военного, энергетического и финансового назначения.

Перспективным направлением развития способов аутентификации пользователей КС, основанных на их личных особенностях, может стать подтверждение подлинности пользователя на основе его знаний и навыков, характеризующих уровень образования и культуры.

Вернуться к содержанию

12. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Криптография – область знаний, изучающая тайнопись и методы ее раскрытия. Криптография – раздел математики. До недавнего времени все исследования в этой области были закрытыми, но в последние несколько лет стало появляться все больше публикаций в открытой печати. Смягчение секретности объясняется тем, что стало уже невозможным скрывать накопленное количество информации. С другой стороны, криптография все больше используется в гражданских отраслях, что требует раскрытия сведений. Цель криптографической системы заключается в том, чтобы зашифровать осмысленный исходный текст (или открытый), получив совершенно бессмысленный, на взгляд, шифрованный текст.

Получатель, которому он предназначен, должен быть способен расшифровать этот шифр-текст, восстановив, таким образом, соответствующий ему открытый текст.

Информацию нужно защищать в тех случаях, когда есть опасение, что она станет доступной посторонним людям, которые могут обратить ее во вред пользователю. Между людьми происходит интенсивный обмен информацией, причем часто на большие расстояния. Для обеспечения такого обмена информацией существуют различные виды технических средств связи: телеграф, телефон, радио, телевидение, интернет. Нередко возникает необходимость в обмене между удаленными пользователями не просто информацией, а защищаемой информацией.

В этом случае незаконный пользователь может попытаться перехватить информацию из общедоступного технического канала связи. Опасаясь этого, законные пользователи должны принять дополнительные меры для защиты своей информации. Разработкой таких мер защиты занимаются криптография и стеганография.

Криптография – это наука о методах преобразования (шифрования) информации с целью ее защиты от незаконного пользователя.

Стеганография – это набор средств и методов скрытия фактов передачи сообщения.

Шифр – это способ преобразования информации с целью ее защиты от незаконных пользователей.

Центральным понятием криптографии является понятие стойкости шифра. Получение строгих доказуемых оценок стойкости конкретного шифра – нерешенная проблема. Это объясняется отсутствием необходимых материальных результатов. Поэтому стойкость конкретного шифра оценивается путем всевозможных его вскрытий и зависит от квалификации криптоаналитиков. Процедуру атаки на шифр иногда называют проверкой стойкости. Под стойкостью шифра понимают способность шифра противостоять всевозможным атакам на него. Важным этапом для проверки стойкости шифра является продумывание различных предполагаемых возможностей, с помощью которых противник может атаковать шифр.

Криптосистема – это завершенная комплексная модель, способная производить двусторонние преобразования над данными произвольного объема и подтверждать время отправки сообщения, обладающая механизмом преобразования паролей и ключей.

Таким образом, криптосистема выполняет три основные функции:

1) усиление защищенности данных;
2) облегчение работы с криптоалгоритмом со стороны человека;
3) обеспечение совместимости потоков данных.

Конкретная программная реализация криптосистемы называется криптопакетом.

Любой шифр может быть скрыт, если в этом есть необходимость и информация, которую предполагается получить, стоит затраченных средств, усилий и времени.

Раскрытием криптосистемы называется результат работы криптоаналитика, приводящий к возможности эффективного раскрытия любого зашифрованного с помощью данной криптосистемы открытого текста. Широко известным примером криптосистемы является «шифр Цезаря», который представляет собой простую замену каждой буквы открытого текста третьей следующей за ней буквой алфавита.

Типы шифров

Все методы шифров можно разделить на две группы:

1) шифры с секретным ключом;
2) шифры с открытым ключом.

Первый характеризуется наличием некоторой информации (секретного ключа), обладание которой дает возможность как шифровать, так и расшифровывать сообщения. Поэтому они именуются также одноключевыми. Шифры с открытым ключом подразумевают наличие двух ключей: открытого и закрытого.

Один используется для шифровки, другой – для расшифровки сообщений. Эти шифры называют двухключевыми.

Шифр с секретным ключом

Этот тип шифра подразумевает наличие некоторой информации, обладание которой позволяет как расшифровывать, так и зашифровывать сообщения. С одной стороны, недостаток такой схемы в том, что необходимо кроме открытого канала для передачи шифрограммы, наличие секретного канала – для передачи ключа. Кроме того, при утечке информации о ключе невозможно доказать, от кого из двух корреспондентов произошла утечка. С другой стороны, среди шифров именно этой группы есть единственная в мире схема шифровки, обладающая теоретической стойкостью.

Шифры с открытым ключом

Открытый ключ публикуется, то есть доводится до сведения всех желающих, секретный ключ хранится у его владельца и является залогом секретности сообщений. Суть метода в том, что зашифрованная с помощью секретного ключа информация может быть расшифрована лишь при помощи открытого, и наоборот. Ключи генерируются парами и имеют однозначное соответствие друг другу. Причем из одного ключа невозможно вычислить другой, и наоборот. Характерной особенностью шифров этого типа, выгодно отличающих их от шифров с секретным ключом, является то, что секретный ключ известен одному человеку, в то время как в первой схеме он должен быть известен, по крайней мере, двоим. Это дает такие преимущества:

1. Не требуется защищенный канал для пересылки секретного ключа, так как связь по открытому каналу.

2. наличие двух ключей позволяет использовать данную шифровальную схему в двух режимах:

а) секретная связь;

б) цифровая подпись.

Все государства уделяют пристальное внимание вопросам криптографии. Объясняется такая политика теми особенностями, которые имеет криптография в плане ее доступности использования и трудности преодоления.

Криптография, в отличие от мер физической защиты, обладает тем уникальным свойством, что при правильном выборе метода затраты на обеспечение защиты информации меньше затрат на преодоление этой защиты. Так как обыкновенный человек может себе позволить такую крепкую защиту, которую не в силах преодолеть государство со всей его финансовой и технической мощью.

Сертификация и стандартизация криптосистемы

Криптосистема не может считаться надежной, если не известен полностью алгоритм ее работы. Зная алгоритм, можно проверить, устойчива ли защита. Однако проверить это может лишь специалист. Для неспециалиста доказательством надежности может служить мнение независимых экспертов. Отсюда и возникла система сертификации. Ей подлежат все системы защиты информации, чтобы ими могли официально пользоваться предприятия и учреждения. Использовать несертифицированные системы не запрещено, но в таком случае не гарантировано, что она окажется достаточно надежной. У нас единственным органом уполномоченным проводить сертификацию, является Федеральное агентство правительственной связи и информации при президенте Российской Федерации.

Вернуться к содержанию

13. ОСНОВНЫЕ ПОНЯТИЯ КРИПТОЛОГИИ. СИММЕТРИЧНЫЕ И АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Назовем открытым текстом (plaintext) информацию, содержание которой может быть понятно любому субъекту. Под шифрованием понимается процесс преобразования открытого текста в шифротекст (cipher text) или криптограмму с целью сделать его содержание непонятным для посторонних лиц:

$$C = E_k(P),$$

где C – шифротекст;

E – функция шифрования;

k – ключ шифрования (дополнительный параметр функции шифрования);

P – открытый текст.

Очевидно, что без введения ключа шифрования применение одной и той же функции шифрования к одному и тому же открытому тексту приводило бы всегда к получению одного и того же шифротекста. В этом случае защищенность шифротекста целиком и полностью определялась бы неизвестностью для посторонних функции шифрования, что практически невозможно обеспечить (особенно при современном уровне развития информационных технологий).

Под расшифрованием понимается процесс обратного преобразования шифротекста в открытый текст:

$$P = D_{k'}(C),$$

где D – функция расшифрования;

k' – ключ расшифрования (дополнительный параметр функции расшифрования).

Совокупность реализуемых функциями E и D алгоритмов, множества возможных ключей, множества возможных открытых текстов и шифротекстов принято называть **криптосистемой**. Если при шифровании и расшифровании используются одни и те же ключи (k = k'), то такую криптосистему называют симметричной. Очевидно, что ключ шифрования (он же – ключ расшифрования) в этом случае должен быть секретным.

Если при шифровании и расшифровании используются различные ключи, то такую криптосистему называют асимметричной.

В этом случае один из этих ключей должен оставаться секретным (secret key), а другой может быть открытым (public key). Поэтому асимметричные криптосистемы иногда называют криптосистемами с открытым ключом.

Науку о защите информации с помощью шифрования называют криптографией (криптография в переводе означает «загадочное письмо или тайнопись»). Криптография известна из глубокой древности, а одним из первых ее методов следует, по-видимому, считать создание письменности.

Процесс получения открытого текста из шифротекста без знания ключа расшифрования называют обычно дешифрованием (или взломом шифра), а науку о методах дешифрования – криптоанализом. Совместным изучением методов криптографии и криптоанализа занимается криптология.

Характеристика надежности шифротекста от вскрытия называется криптостойкостью. Криптостойкость шифра может оцениваться двумя величинами:

• минимальным объемом шифротекста, статистическим анализом которого можно его вскрыть и получить открытый текст без знания ключа;

• числом MIPS-часов или MIPS-лет – временем работы условного криптаналитического компьютера производительностью один миллион операций в секунду, необходимым для вскрытия шифротекста.

Очевидным правилом при выборе криптосистемы для защиты конфиденциальной информации в КС должно быть следующее: ценность конфиденциальной информации должна быть ниже стоимости вскрытия ее шифротекста нарушителем.

При разработке криптографических алгоритмов широко применяются вычисления в кольце вычетов по модулю. Это вызвано следующими причинами:

• выполнение обратных вычислений (логарифмирования, извлечения корня, разложения на сомножители) гораздо более трудоемко, чем прямые вычисления (возведение в степень или умножение), что соответствует требованию существенно большей трудоемкости дешифрования без знания ключа по сравнению с расшифрованием по известному ключу;

• при вычислениях по модулю ограничивается диапазон возможных значений для всех промежуточных величин и результата (например: a^{25} {mod n} = ((((a^{2}a)^2)^2)^2) a {mod n}).

Криптография применяется пр :

• защите конфиденциальности информации, передаваемой по открытым каналам связи;

• аутентификации (подтверждении подлинности) передаваемой информации;

• защите конфиденциальной информации при ее хранении на открытых носителях;

• обеспечении целостности информации (защите информации от внесения несанкционированных изменений) при ее передаче по открытым каналам связи или хранении на открытых носителях;

• обеспечении неоспоримости передаваемой по сети информации (предотвращении возможного отрицания факта отправки сообщения);

• защите программного обеспечения и других информационных ресурсов от несанкционированного использования и копирования.

Хеширование – процесс преобразования исходного текста M произвольной длины в хеш-значение (дайджест или образ) H(M) фиксированной длины. К функциям хеширования предъявляются следующие требования:

• постоянство длины хеш-значения независимо от длины исходного текста:

$$\forall M \ \mathrm{Length}[H(M)] = \mathrm{const};$$

• полная определенность (для двух одинаковых исходных текстов должно получаться одно и то же хеш-значение):

$$\forall M = M_2 \ H(M_1) = H(M_2);$$

• необратимость (невозможность восстановления исходного текста по его хеш-значению):

$$\neg\exists \, H^{-1}(H(M)) = M;$$

• стойкость к взлому (практическая невозможность подбора другого исходного текста для известного хеш-значения):

$$\neg\exists \, M' \neq M \ H(M') = H(M).$$

К основным применениям хеширования при обеспечении информационной безопасности КС относятся:

• защита парольной и иной идентифицирующей пользователей КС информации;

• создание дайджеста файла или электронного сообщения, применяемого в системах электронной цифровой подписи.

Вернуться к содержанию

13.1. Способы создания симметричных криптосистем. Абсолютно стойкий шифр

К основным способам симметричного шифрования относятся перестановки, подстановки и гаммирование. При использовании перестановки биты (или символы) открытого текста переставляются в соответствии с задаваемым ключом шифрования правилом:

$$\forall i, 1 \le i \le n C_i = P_{k[i]},$$

где $P = \{P_1, P_2, ...P_i, ...P_n\}$ – открытый текст;

n – длина открытого текста;

$C = \{C_1, C_2, ..., C_i, ..., C_n\}$ – шифротекст;

$k = \{k_1, k_{2,} ..., k_i, ...k_n\}$ – ключ шифрования.

При расшифровании применяется обратная перестановка:

$$\forall i, 1 \le i \le n P_{k[i]} = C_i.$$

Очевидно, что при шифровании перестановкой ключ должен удовлетворять условию:

$$\forall k_i \in k 1 \le k_i \le n \wedge \forall k_i, k_j \in k, k_i \ne k_j.$$

Пример. Пусть надо зашифровать слово «связной» (n = 7), с помощью ключа k = {4, 2, 1, 7, 6, 3, 5}. В результате шифрования мы получаем шифротекст «звсйоян».

Если длина ключа меньше длины открытого текста, то можно разбить открытый текст на блоки, длина которых равна длине ключа, и последовательно применить ключ перестановки к каждому блоку открытого текста. Если длина открытого текста не кратна длине ключа, то последний блок может быть дополнен пробелами или нулями.

Можно использовать и другой прием. После разбиения открытого текста длиной n на блоки, длина которых равна длине ключа m, открытый текст записывается в таблицу с числом столбцов, равным длине ключа (каждый блок открытого текста записывался в столбец таблицы). Число строк таблицы в этом

случае будет равно наименьшему целому числу, не меньшему n/m. Затем столбы полученной таблицы переставляются в соответствии с ключом перестановки, а шифротекст считывается из строк таблицы последовательно.

Пример. Необходимо зашифровать открытый текст: «связной прилетает в пятницу» (n = 27), – с помощью ключа перестановки k = (3, 5, 4, 2, 1) (m = 5). После разбиения открытого текста на блоки и занесения его в таблицу размером 6 строк и 5 столбцов получаем:

с	й	е	в	и
в		т		ц
я	п	а	п	у
з	р	е	я	
н	и	т	т	
о	л		н	

После применения ключа перестановки к столбцам таблицы получаем:

е	и	в	й	с
т	ц			в
а	у	п	п	я
е		я	р	з
т		т	и	н
		н	л	о

После считывания текста по строкам таблицы получаем окончательный шифротекст: «еивйстц вауппяе ярзт тин нло».

При расшифровании шифротекст записывается в таблицу того же размера по строкам, затем происходит обратная перестановка столбцов в соответствии с ключом, после чего расшифрованный текст считывается из таблицы по столбцам.

Если в качестве ключа перестановки используется последовательность не цифр, а произвольных символов (например, пароль пользователя КС), то его необходимо предварительно преобразовать в последовательность целых чисел от единицы до m (m – длина ключа):

1) символы ключа сортируются в лексикографическом порядке;

2) каждый символ исходного ключа заменяется целым числом, равным номеру его позиции в отсортированном ключе.

Приведем пример функций на языке С, выполняющих шифрование и расшифрование перестановкой заданной строки символов максимальной длины MAXLEN (в этом примере открытый текст не разбивается на блоки):

```
#include <stdlib.h>
#include <string.h>
. . .
// функция, используемая при сортировке символов ключа
int It(const void *a, const void *b)
{
if (*(char*)a<*(char *)b) return –1;
else if(*(char*)a==*(char*)b) return 0;
else return 1;
}
/*функция шифрования открытого текста str длиной n по ключу key с записью полученного шифротекста в res*/
void Crypt(const char *str,const char *key,char *res, unsigned n)
{
char tmp[MAXLEN];//отсортированный ключ
/*выравнивание длин открытого текста и ключа: усечение или дополнение пробелами ключа */
if (n<strlen(key)) strncpy(tmp,key,n);
else strcpy(tmp,key);
while (strlen(tmp)<n)
strcat(tmp,” ”,1);
char Key[MAXLEN];//преобразованный ключ
strcpy(Key,tmp);
//сортировка символов ключа
qsort(tmp,n,sizeof(char),It);
unsigned Perm[MAXLEN]; // ключ перестановки
//цикл шифрования
for (unsigned i=0;i<n;i++)
{ //получение очередного элемента ключа перестановки
Perm[i]=strchr(tmp,Key[i])-tmp;
// «сброс» уже найденного символа отсортированного ключа
tmp[Perm[i]]=’\1’;
//получение очередного символа шифротекста
```

```
res[i]=str[Perm[i]];
}
res[n]='\0';
}
/* функция расшифрования шифротекста str длиной n по ключу key с записью восстановленного открытого текста в res*/
void Encrypt(const char *str, const char *key,char *res, unsigned n)
{ char tmp[MAXLEN];
if (n<strlen(key)) strcpy(tmp,key,n);
else strcpy(tmp, key);
while(strlen(tmp)<n)
strncat(tmp," ",1);
char Key[MAXLEN];
strcpy(Key,tmp);
qsort(tmp,n,sizeof(char),It);
unsigned Perm[MAXLEN];
// цикл расшифрования
for (unsigned i=0;i<n;i++)
{ Perm[i]=strchr(tmp,Key[i])-tmp;
tmp[Perm[i]]='\1';
// восстановление очередного символа открытого текста
res[Perm[i]]=str[i];}
res[n]='\0';}
```

Достоинством шифрования перестановкой является высокая скорость получения шифротекста. При шифровании двоичных файлов (например, программных) можно дополнительно сократить временные затраты, если ограничиться перестановками только наиболее важных участков шифруемого файла.

К недостаткам шифрования перестановкой относятся:

• сохранение частотных характеристик открытого текста после его шифрования (символы открытого текста лишь меняют свои позиции в шифротексте);

• малое число возможных ключей шифрования.

При шифровании с помощью подстановки (замены) символы открытого текста заменяются символами того же (одноалфавитная подстановка) или другого (многоалфавитная подстановка) алфавита в соответствии с определяемым ключом шифрования правилом.

При использовании одноалфавитной подстановки каждый символ открытого текста заменяется в шифротексте символом, номер которого в используемом алфавите больше номера символа открытого текста на величину ключа шифрования (используется сложение в кольце вычетов по модулю, равному мощности применяемого алфавита):

$$\forall i, 1 \le i \le n, C_i = P_i + k \{\mathrm{mod}\, m\},$$

где $P = \{P_1, P_2, ...P_i, ...P_n\}$ – открытый текст;

n – длина открытого текста;

$A = \{A_1, A_2, ..., A_m\}$ – алфавит символов открытого текста;

$(\forall i, 1 \le i \le n, P_i \in A)$; $C = \{C_1, C_2, ..., C_i, ..., C_n\}$ – шифротекст;

k – ключ шифрования $(0 \le k < m)$; $\forall a_i \in A, 1 \le i \le m, a_i + k = a_{i+k}$.

При расшифровании символ шифротекста заменяется символом, номер которого в используемом алфавите больше номера символа шифротекста (применяется операция сложения в кольце вычетов по модулю m) на величину m – k (m – мощность используемого алфавита; k – ключ шифрования):

$$\forall i, 1 \le i \le n, C_i = P_i + m - k \{\mathrm{mod}\, m\}.$$

Пример. При шифровании открытого текста «наступайте» с помощью одноалфавитной подстановки по ключу 3 (так называемой подстановки Цезаря) получаем шифротекст «ргфхцгтмхз».

Приведем пример функций на языке С, выполняющих шифрование и расшифрование одноалфавитной подстановкой заданной строки символов.

```
/*функция шифрования открытого текста str длиной n по ключу key с записью полученного шифротекста в res*/
void Crypt(const char *str, char key, char *res, unsigned n)
{
for (unsigned i=0;i<n;i++)
res[i]=(str[i]+key)%256;
res[n]='\0';
}
/*функция расшифрования шифротекста str длиной n по ключу key с записью полученного шифротекста в res*/
void Encrypt(const char *str, char key, char *res, unsigned n)
{
```

```
for (unsigned i=0;i<n;i++)
res[i]=(str[i]+256-key)%256;
res[n]='\0';
}
```

Основные недостатки шифрования с помощью одноалфавит ной подстановки:

• не скрывается частота появления различных символов открытого текста в шифротексте (одинаковые символы открытого текста остаются одинаковыми и в шифротексте);

• малое число возможных ключей.

При использовании многоалфавитной подстановки каждый символ открытого текста заменяется в шифротексте символом, номер которого в применяемом алфавите больше номера символа открытого текста на величину, равную очередному элементу ключа шифрования (используется сложение в кольце вычетов по модулю, равному мощности алфавита):

$$\forall i, 1 \le i \le n, C_i = P_i + k \{\mathrm{mod}\, m\},$$

где $P = \{P_1, P_2, ...P_i, ...P_n\}$ – открытый текст;

n – длина открытого текста;

$A = \{A_1, A_2, ..., A_m\}$ – алфавит символов открытого текста;

$(\forall i, 1 \le i \le n, P_i \in A)$; $C = \{C_1, C_2, ..., C_i, ..., C_n\}$ – шифротекст;

$k = \{k_1, k_{2,}, ..., k_i, ...k_n\}$ – ключ шифрования $(\forall i, 1 \le i \le n, 0 \le k_i < m); \forall a_i \in A, 1 \le i \le m, a_i + k = a_{i+k}$

Расшифрование выполняется аналогично шифрованию, за исключением того, что увеличение номера в алфавите, соответствующего символу шифротекста, происходит на величину m – k; (m – мощность алфавита; k_i – очередной элемент ключа):

$$\forall i, 1 \le i \le n, C_i = P_i + m - k \{\mathrm{mod}\, m\}.$$

Если длина ключа меньше длины открытого текста, то необходимо разбить открытый текст на блоки, длина которых равна длине ключа, и последовательно применить ключ подстановки к каждому блоку открытого текста. Если длина открытого текста не кратна длине ключа, то последний блок следует дополнить необходимым числом одних и тех же символов.

Приведем пример функций на языке С, выполняющих шифрование и расшифрование многоалфавитной подстановкой заданной строки символов (в этом примере открытый текст не разбивается на блоки).

```
#include <string.h>
. . .
/*функция шифрования открытого текста str длиной n по ключу key с записью полученного шифротекста в res*/
void Crypt (const char *str, const char *key, char *res,unsigned n)
{
char tmp[MAXLEN];//ключ скорректированной длины
/* выравнивание длин открытого текста и ключа: усечение или дополнение пробелами ключа */
if(n<strlen(key)) strncpy(tmp, key, n);
else strcpy(tmp, key);
while (strlen(tmp)<n)
strncat(tmp,” ”, 1);
//цикл шифрования
for (unsigned i=0;i<n;i++)
res[i]=(str[i]+tmp[i])%256;
res[n]=’\0’;}
/*функция расшифрования шифротекста str длиной n по ключу key с записью полученного шифротекста в res*/
void Encrypt(const char *str, const char *key, char *res, unsigned n)
{char tmp [MAXLEN];
if (n<strlen(key)) strncpy(tmp, key, n);
else srtcpy(tmp, key);
while (strlen(tmp)<n)
strncat(tmp,” ”,1);
// цикл расшифрования
for (unsigned i=0;i<n;i++)
res[i]=(str[i]+256-tmp[i])%256;
res[n]=’\0’;}
```

Достоинством многоалфавитной подстановки является то, что в шифротексте маскируется частота появления различных символов открытого текста, поэтому криптоаналитик не может при вскрытии шифра использовать частотный словарь букв естественного языка.

Разновидностью шифрования с применением многоалфавитной подстановки является побайтное шифрование, при котором каждый следующий байт открытого текста складывается с предыдущим байтом, а нулевой байт открытого текста – с последним байтом.

На рисунках 1 и 2 приведены алгоритмы побайтного шифрования и расшифрования открытого текста $P = \{P_0, P_1, ...P_i, ...P_n\}$. При модификации алгоритма побайтного шифрования к очередному байту открытого текста добавляется значение байта с определяемым ключом шифрования смещением. Недостаточная криптостойкость данного алгоритма шифрования при его использовании в чистом виде определяется тем, что ключ шифрования содержится в шифротексте.

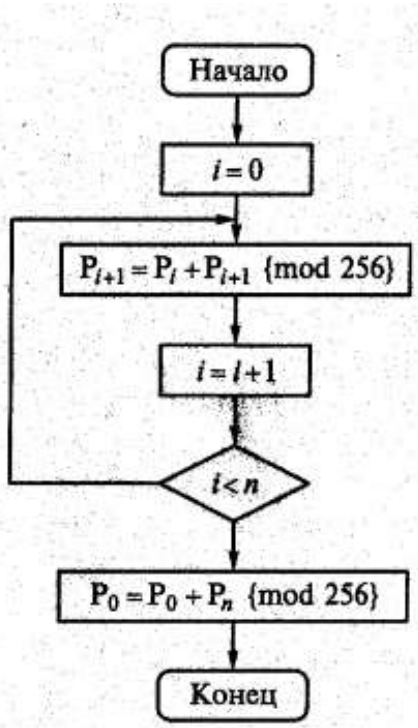


Рис. 1. Алгоритм побайтного шифрования

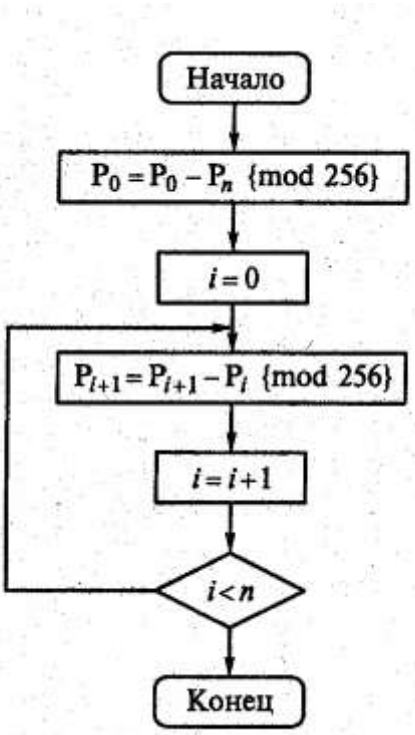


Рис. 2. Алгоритм побайтного расшифрования

При гаммировании шифротекст получается путем наложения на открытый текст гаммы шифра с помощью какой-либо обратимой операции (как правило, поразрядного сложения по модулю 2):

$$\forall i, 1 \le i \le n, C_i = P_i \oplus G_i ,$$

где $P = \{P_1, P_2, ...P_i, ...P_n\}$ – открытый текст;

n – длина открытого текста;

$C = \{C_1, C_2, ..., C_i, ..., C_n\}$ – шифротекст;

$G = \{G_1, G_2, ..., G_i, ..., G_n\}$ – гамма шифра;

$\oplus$ – операция поразрядного сложения по модулю 2.

Расшифрование в этом случае заключается в повторном наложении той же гаммы шифра на шифротекст:

$$\forall i, 1 \le i \le n, P_i = C \oplus G_i .$$

Гамма шифра вычисляется с помощью программного или аппаратного датчика (генератора) псевдослучайных чисел, параметры которого определяются ключом шифрования. Одним из наиболее простых датчиков псевдослучайных чисел является линейный конгруэнтный датчик:

$$\forall i, 1 \le i \le n, G_i = aG_{i-1} + c\{\mathrm{mod}\, m\},$$

где a, c и G_0 – определяемые ключом параметры датчика псевдослучайных чисел;

$m = 2^s$ (s – длина машинного слова в битах, обычно 32 или 64).

Доказано, что максимальный период генерируемой линейным конгруэнтным датчиком псевдослучайной последовательности достигается при нечетном значении параметра c и $a = \{\mathrm{mod}\, 4\}$.

Другим примером датчика псевдослучайных чисел являются линейные последовательные машины (М – последовательности). Определяемое ключом шифрования исходное двоичное значение $a_0, a_1, ..., a_{k-1}$ помещается в сдвиговый регистр. На каждом такте работы датчика происходит сдвиг k двоичных разрядов, вытесняемый бит a_0 добавляется к гамме шифра, а затем замещает бит $a_{к-1}$ по следующему правилу:

$$a_k = -\sum_{j=0}^{k-1} h_j a_j ,$$

где $h = \{h_0, h_1, ..., h_{k-1}\}$ – определяемые ключом шифрования коэффициенты передачи $(\forall j, 0 \le j \le k, h_j = 0 \vee h_j = 1)$;

$\sum$ – операция суммирования по модулю 2.

Если в качестве коэффициентов передачи выбираются коэффициенты неприводимого многочлена степени k (который нельзя разложить на сомножители-многочлены степени меньше k), то данный тип генератора псевдослучайных чисел обеспечивает выдачу последовательности двоичных чисел с периодом, равным $2^к - 1$.

Приведем пример функций на языке С, выполняющих шифрование и расшифрование гаммированием заданной строки символов (используется линейный конгруэнтный датчик псевдослучайных чисел):

```
/*функция шифрования открытого текста str длиной n по ключу a, c и g0 с записью полученного шифротекста в res*/
void Crypt(const char *str, char a, char c, char g0, char *res, unsigned n)
{
char Gamma=g0;// гамма шифра
//цикл шифрования
for (unsigned i=0;i<n;i++)
{Gamma = (a*Gamma+c)%256;
res[i]=str[i]^Gamma;
res[n]='\0';}
/*функция расшифрования шифротектса текста str длиной n по ключу a, c и g0 с записью восстановленного открытого текста в res*/
void Encrypt(const char *str, char a, char c, char g0, char *res, unsigned n)
{ char Gamma=g0;// гамма шифра
//цикл расшифрования
for (unsigned i=0;i<n;i++)
{Gamma = (a*Gamma+c)%256;
res[i]=str[i]^Gamma;
res[n]='\0';}
```

Гаммирование лежит в основе потоковых шифров, в которых открытый текст преобразуется в шифротекст последовательно по одному биту. Криптостойкость потоковых шифров полностью определяется структурой используемого генератора псевдослучайной последовательности (чем меньше период псевдослучайной последовательности, тем ниже криптостойкость потокового шифра).

Основным преимуществом потоковых шифров является их высокая производительность. Эти шифры наиболее пригодны для шифрования непрерывных потоков открытых данных (например, в сетях передачи данных или связи). К наиболее известным современным потоковым шифрам относятся:

• RC4 (Rivest Cipher 4), разработанный Р. Ривестом (R. Rivest); в шифре RC4 может использоваться ключ переменной длины;

• SEAL (Software Encryption ALgorithm) – приспособленный для программной реализации потоковый шифр, использующий ключ длиной 160 бит;

• WAKE (Word Auto Key Encryption).

Важнейшим показателем качества построенного шифра является отсутствие каких-либо закономерностей в шифротексте (частотная и позиционная равномерность кодов-символов в нем). Поэтому из-за недостаточной криптостойкости в настоящее время не используются шифры перестановок или подстановок в чистом виде.

Большинство современных симметричных криптосистем относятся к разряду блочных шифров. В этих криптосистемах открытый текст разбивается на блоки, как правило, фиксированной длины, к каждому блоку применяется функция шифрования, использующая перестановки битов блока и многократное повторение операций подстановки и гаммирования, после чего над зашифрованными блоками может выполняться дополнительная операция перед включением их в шифротекст.

К наиболее распространенным способам построения блочных шифров относится сеть Фейштеля, при использовании которой каждый блок открытого текста представляется сцеплением двух полублоков одинакового размера $L_0 \| R_0$. Затем для каждой итерации (раунда) i выполняются следующие действия:

$$1) L_i = R_{i-1};$$
$$2) R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

где f – функция шифрования;

k_i – ключ, используемый на i-м раунде шифрования (k_i определяется исходным ключом шифрования открытого текста и называется внутренним ключом).

К основным характеристикам современных блочных шифров относятся длина блока, длина ключа шифрования и число раундов. В таблице 1 приведены значения данных характеристик для наиболее известных блочных шифров.

Таблица 1

Значения характеристик наиболее известных блочных шифров

Шифр	**Длина блока в битах**	**Число раундов**	**Длина ключа в битах**
DES (DataEncryptionStandart)	64	16	64 (8 контрольных)
3 – DES (Triple – DES)	64	48	168
DESX (DES eXtended)	64	16	184
ГОСТ 28147 – 89	64	32	256

IDEA (International Data Encryption Algorithm)	64	8	128
AES (Advanced Encryption Standart)	128	14	128,192,256
RC2 (Rivest Cipher 2)	64	Переменное	Переменная
RC5 (Rivest Cipher 5)	32,64,128	Переменное	Переменная
RC6 (Rivest Cipher 6)	Переменная	Переменное	Переменная
CAST (C. Adams, S. Tavares)	64	16	128
Blowfish	64	16	Переменная
SAFER+	128	8,12,16	128,192,256
Skipjack	64	32	80

Может ли быть построен идеальный, абсолютно стойкий шифр? Ответ на этот вопрос был дан К. Шенноном. Для того чтобы шифр обладал абсолютной стойкостью к взлому, он должен обладать двумя свойствами:

1) ключ шифрования должен вырабатываться совершенно случайным образом (в частности, один и то же ключ должен применяться для шифрования только одного открытого текста);

2) длина шифруемого открытого текста не должна превышать длину ключа шифрования.

К сожалению, в большинстве случаев обеспечить выполнение этих условий практически невозможно, хотя короткие и наиболее важные сообщения следует шифровать именно так. Для открытых текстов большой длины главной проблемой симметричной криптографии является генерация, хранение и распространение ключа шифрования достаточной длины.

Очевидно, что за счет увеличения длины ключа шифрования можно уменьшить требования к сложности алгоритма блочного шифрования (например, уменьшить число раундов), и, наоборот, более короткий ключ требует увеличения сложности криптоалгоритма.

Генерация случайного ключа шифрования возможна с помощью программного или аппаратного датчика псевдослучайных чисел и случайных событий, создаваемых пользователем при нажатии клавиш на клавиатуре или движением мыши. Ключ шифрования будет в этом случае создан из порций, взятых из псевдослучайной последовательности в момент возникновения инициированных пользователем событий.

Для того чтобы на основе одного ключа шифрования сгенерировать несколько различных сеансовых ключей (session keys), которые будут использованы для шифрования отдельных сообщений (файлов), могут применяться добавляе-

мые к ключу случайные значения (salt values). Особенно полезны случайные значения при шифровании большого числа практически идентичных пакетов данных – будет обеспечено получение совершенно разных шифротекстов. В отличие от ключей шифрования случайные значения могут быть открытыми и передаваться (храниться) вместе с шифротекстом.

Если для хранения ключей шифрования используются открытые магнитные носители, то эти ключи должны храниться только в зашифрованном с помощью мастер-ключа виде. Мастер-ключ не зашифровывается, но хранится в защищенной части аппаратуры КС, причем его потеря в результате аппаратной ошибки не должна приводить к потере зашифрованных с его помощью данных.

Для распределения ключей шифрования между субъектами распределенной КС могут применяться центры распределения ключей (Key Distribution Center, KDC). В этом случае на каждом объекте КС должен храниться ключ шифрования для связи с KDC. Недостатком применения центра распределения ключей является то, что в KDC возможно чтение всех передаваемых в КС сообщений. Для организации анонимного распределения ключей симметричного шифрования могут использоваться протоколы, основанные на криптографии с открытым ключом.

Вернуться к содержанию

13.2 Криптографическая система DES и ее модификации

Стандарт шифрования данных DES (Data Encription Standart) опубликован в 1977 г. Национальным бюро стандартов США.

Стандарт DES предназначен для защиты от несанкционированного доступа к важной, но не секретной информации в государственных и коммерческих организациях США. Алгоритм, положенный в основу стандарта, распространялся достаточно быстро, и уже в 1980 году был одобрен Национальным институтом стандартов и технологий США (НИСТ). С этого момента DES превращается в стандарт не только по названию (Data Encription Standart), но и фактически. Появляется специальное программное обеспечение и специализированные микроЭВМ, предназначенные для шифрования и расшифрования информации в сетях передачи данных. Алгоритм DES до 2001 г. являлся федеральным стандартом США на защиту информации, не относящейся к государственной тайне.

Алгоритм шифрования данных DES является типичным представителем семейства блочных шифров, допускающим эффективную аппаратную и программную реализацию при достижении скоростей шифрования до нескольких ме-

габайт в секунду. Алгоритм предназначен для шифрования данных 64 – битовыми блоками. Обобщенная схема шифрования в алгоритме DES показана на рисунке 3.

Рис. 3. Обобщенная схема шифрования в алгоритме DES

DES представляет собой комбинацию двух основных методов шифрования подстановки и перестановки. Основным комбинационным блоком алгоритма является применение к тексту единичной комбинации этих двух методов. Такой блок называется раундом. DES включает 16 раундов, то есть одна и та же комбинация методов применяется к открытому тексту 16 раз.

При описании алгоритма DES (рис. 4.) применимы следующие обозначения:

L и R – последовательности битов (левая и правая);

LR – конкатенация последовательностей L и R, то есть такая последовательность битов, длина которой равна сумме длин L и R; в последовательности LR биты последовательности R следуют за битами последовательности L;

XOR – операция побитового сложения по модулю 2.

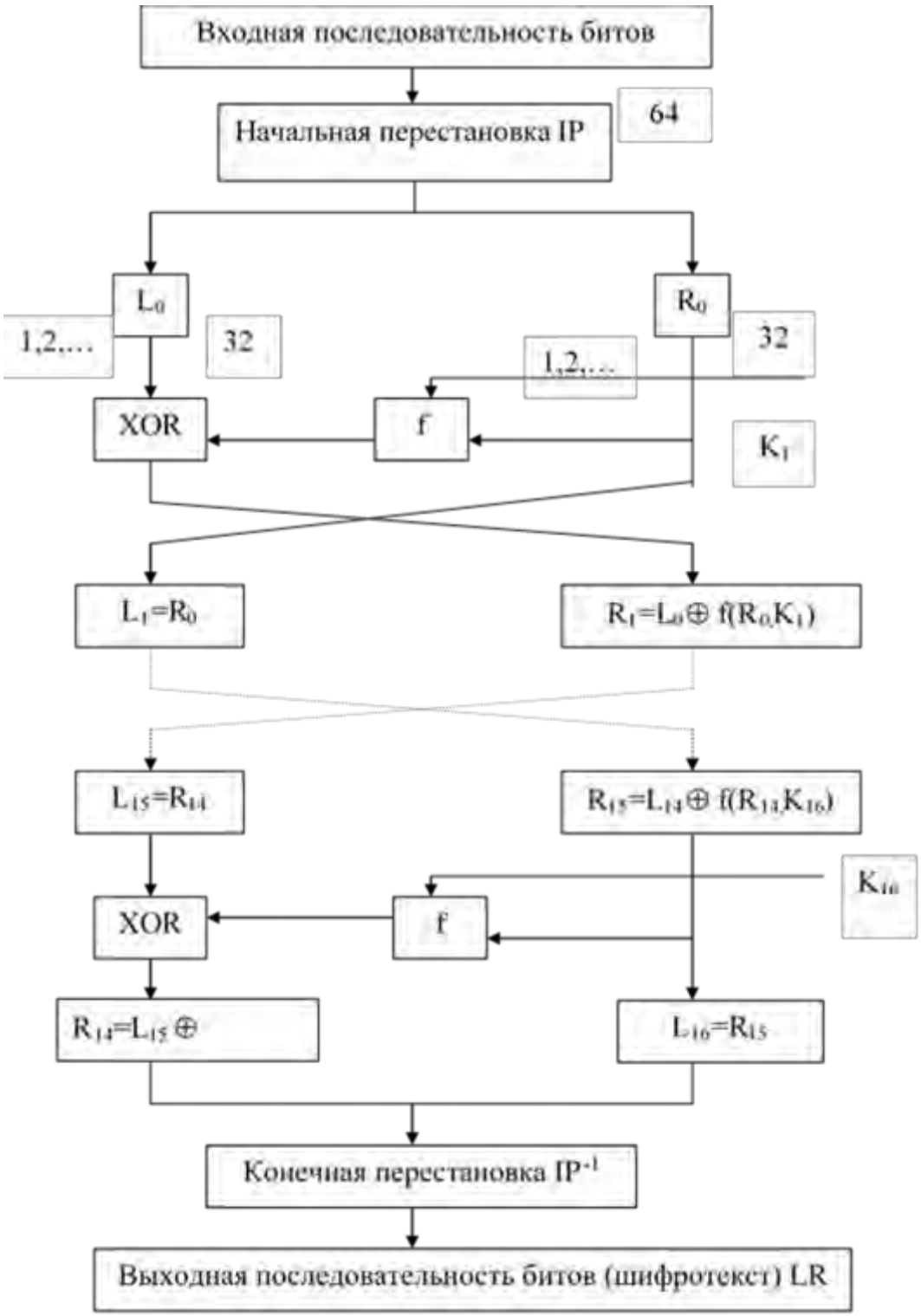


Рис. 4. Структурная схема шифрования в алгоритме DES

Битовый блок исходного текста преобразуется с помощью матрицы начальной перестановки IP, то есть биты входного блока переставляются в соответствии с матрицей IP.

Полученная последовательность битов разделяется на две последовательности: L_0 – левые или старшие биты, R_0 – правые или младшие биты, каждая из

которых содержит 32 бита. Далее выполняется итеративный процесс шифрования, состоящий из 16 циклов. Результат *i*-й итерации можно описать следующими соотношениями:

$$L_i = R_{i-1}; i = 1,2,...,: R_i = L_{i-1} \oplus f(R_{i-1}, K_i), i = 1,2,...,16$$

Функция f называется функцией шифрования. Её аргументами являются последовательность R_{i-1}, полученная на предыдущем шаге итерации, и 48-битовый ключ K_i, который является результатом преобразования 64-битового ключа К. Таким образом, из приведенной выше схемы следует, что после первоначальной перестановки 64-битовый блок разбивается на правую и левую половины длиной по 32 бита каждая. Затем выполняется 16 раундов одинаковых преобразований с помощью функции f, в которых данные объединяются с соответствующим подключом. После 16 раунда правая и левая половины объединяются и алгоритм завершается заключительной обратной перестановкой IP^{-1}. По отношению к процессу зашифрования, процесс расшифрования является инверсным, то есть все действия должны быть выполнены в обратном порядке. Это означает, что расшифрованные данные сначала переставляются в соответствии с матрицей IP^{-1}, а затем над последовательностью битов $R_{16}L_{16}$ выполняются те же действия, что и в процессе расшифрования, который может быть описан следующими соотношениями:

$$R_{i-1} = L_i, i = 1,2,...,16;$$
$$L_{i-1} = R_i \oplus f(L_i, K_i), i = 1,2,...,16.$$

Откуда следует, что для процесса расшифрования с переставленным входным блоком $R_{16}L_{16}$ на первой итерации используется ключ K_{16}, на второй итерации – K_{15} и т. д.

На последнем шаге итерации будут получены последовательности L_0 и R_0, которые конкатенируются в 64-битовую последовательность L_0R_0. Затем в этой последовательности 64 бита переставляются в соответствии с матрицей IP. Результатом такого преобразования является расшифрованное 64-битовое значение.

Таким образом, алгоритм DES позволяет использовать для зашифрования или расшифрования блока одну и ту же функцию.

Единственное отличие состоит в том, что ключи должны использоваться в обратном порядке. Иными словами, если в раундах зашифрования использовались ключи K_1, K_2, K_3,…, K_{16}, то ключами расшифрования будут K_{16}, K_{15}, K_{14},…, K_1.

Вернуться к содержанию

13.3. Режимы использования блочных шифров

Для применения DES в различных приложениях были определены четыре режима его работы:

- электронная кодовая книга ECB (Electronic Code Book);
- сцепление блоков шифра CBC (Ciper Block Chaining);
- обратная связь по шифротексту CFB (Ciper Feed Back);
- обратная связь по выходу OFB (Output Feed Back).

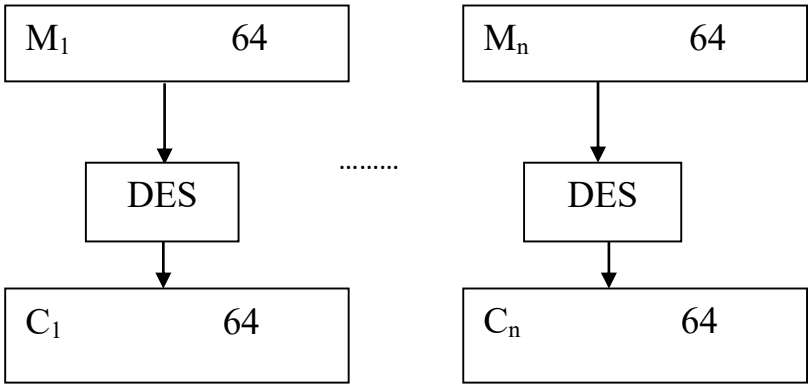
Считается, что этих четырех режимов вполне достаточно для того, чтобы использовать DES практически в любой области, для которой этот алгоритм подходит. Он позволяет непосредственно преобразовать 64-битовый входной открытый текст в 64-битовый выходной шифрованный текст.

13.3.1. Режим электронной кодовой книги (Electronic Code Book)

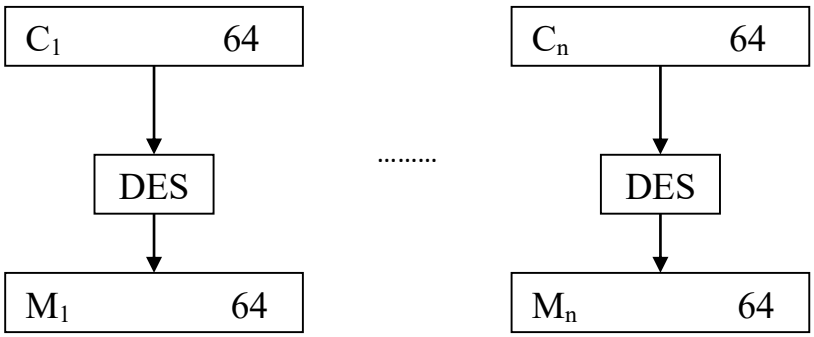
В режиме ECB открытый текст обрабатывается блоками по 64 бита и каждый блок шифруется одним и тем же ключом. При заданном ключе каждый 64-битовый блок открытого текста представляется уникальным блоком шифрованного текста, то есть для каждой последовательности открытого текста указана соответствующая последовательность шифрованного текста. При длине сообщения, превышающей 64 бита, отправитель делит это сообщение на 64-битовые блоки. На рисунке 5 открытый текст обозначен как $M_1, M_2, \ldots, M_n$, а соответствующий шифрованный текст – $C_1, C_{2,\ldots}, C_n$. Основным достоинством данного метода является простота реализации. Метод идеален для небольших объемов данных.

В режиме ECB одинаковые блоки открытого текста остаются одинаковыми и в шифротексте, что облегчает задачу криптоанализа шифротекста. Изменение одного блока в шифротексте приведет к изменению всего блока в расшифрованном открытом тексте. Кроме того, нарушитель может свободно удалять, повторять или переставлять блоки шифротекста для воздействия на расшифрованный открытый текст.

Вернуться к содержанию



Зашифрование



Расшифрование

Рис. 5. Схема работы алгоритма в режиме электронной кодовой книги

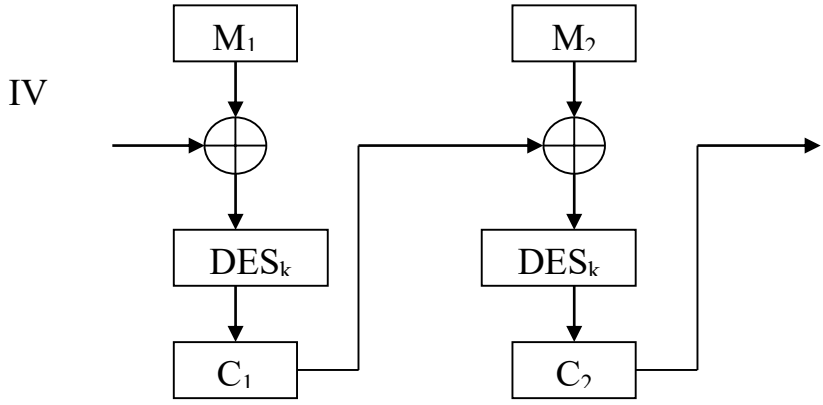
Вернуться к содержанию

13.3.2. Режим сцепления блоков шифра (Ciper Block Chaining)

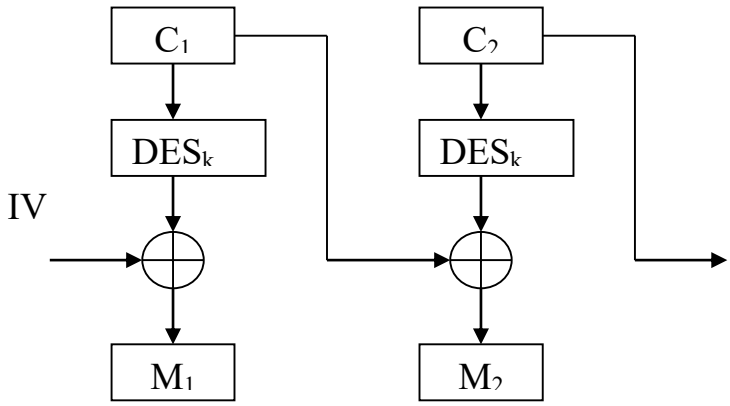
В режиме сцепления блоков шифра каждый блок открытого текста перед шифрованием складывается по модулю 2 с предыдущим блоком шифротекста, а первый блок – с вектором инициализации (синхропосылкой) IV (дополнительным параметром шифра, который должен сохраняться и передаваться вместе с ключом шифрования).

При использовании режима CBC одинаковые блоки открытого текста становятся различными в шифротексте (см. рис. 6).

При изменении одного бита в шифротексте будет полностью искажен соответствующий блок воостановленного открытого текста, а также аналогичный бит предыдущего блока.



Зашифрование



Расшифрование

Рис. 6. *Режим работы блочного алгоритма в режиме сцепления блоков шифра*

13.3.3. Режим обратной связи по шифротексту (Ciper Feed Back)

Данный режим использует регистр замены (сдвига), в который первоначально помещается вектор инициализации. После шифрования блока в регистре замены происходит его сдвиг влево на величину, равную длине порции данных (например, 1/4 длины регистра замены), и сложение по модулю 2 вытесняемой части регистра с очередной порцией открытого текста. Результат последней операции образует очередную порцию шифротекста и одновременно помещается в освободившуюся часть регистра сдвига.

В режиме CFB искажение одного бита шифротекста приведет к искажению последовательности расшифрованных блоков открытого текста.

13.3.4. Режим обратной связи по выходу (Output Feed Back)

В режиме OFB также используется регистр замены и вектор инициализации. После шифрования блока в регистре замены и сдвига вытесняется часть,

которая замещает свободную область регистра и одновременно складывается по модулю 2 с очередной порцией открытого текста.

Особенности режима OFB по сравнению с CFB заключается в том, что любые искажения внутри одного блока шифротекста не распространяются на следующие восстановленные блоки открытого текста. Режим OFB часто используется для генерации псевдослучайных чисел, а также применяется в спутниковых системах связи.

Для повышения криптостойкости алгоритма DES, вызванной недостаточным на сегодняшний день длиной ключа шифрования и числом раундов, используются различные модификации этой криптосистемы. Среди них наиболее известны 3 – DES и DESX.

В операционных системах Windows, как в открытых начиная с версии Windows 95 OSR2, так и в защищенных, доступ к шифрованию по алгоритму DES и другим возможен с помощью функций криптографического интерфейса CryptoAPI.

Вернуться к содержанию

13.4. Блочный шифр TEA

Блочный алгоритм TEA (Tiny Encryption Algorithm) приведен как пример одного из самых простых в реализации стойких криптоалгоритмов.

Параметры алгоритма:

Размер блока – 64 бита.

Длина ключа – 128 бит.

В алгоритме использована сеть Фейштеля с двумя ветвями в 32 бита каждая. Образующая функция F обратима.

Сеть Фейштеля несимметрична из-за использования в качестве операции наложения не исключающего "ИЛИ", а арифметического сложения.

Ниже приведен код криптоалгоритма на языке программирования PASCAL.

```
type TLong2=array[0.. 1] of longint;
TLong2x2=array[0.. 1] of TLong2;
const Delta=$9E3779B9;
var   key:TLong2x2;
procedure EnCryptRouting(var data);
var y,z,sum:longint; a:byte;
begin
```

```
y:=TLong2(data)[0];z:=TLong2(data)[1];sum:=0;
for a:=0 to 31 do
  begin
  inc(sum,Delta);
  inc(y,((z shl 4)+key[0,0]) xor (z+sum) xor ((z shr 5)+key[0,1]));
  inc(z,((y shl 4)+key[1,0]) xor (y+sum) xor ((y shr 5)+key[1,1]));
  end;
TLong2(data)[0]:=y;TLong2(data)[1]:=z
end;
```

Отличительной чертой криптоалгоритма TEA является его размер. Простота операций, отсутствие табличных подстановок и оптимизация под 32-разрядную архитектуру процессоров позволяет реализовать его на языке ASSEMBLER в предельно малом объеме кода. Недостатком алгоритма является некоторая медлительность, вызванная необходимостью повторять цикл Фейштеля 32 раза (это необходимо для тщательного «перемешивания данных» из-за отсутствия табличных подстановок).

Вернуться к содержанию

13.5. Алгоритм шифрования данных IDEA

Алгоритм IDEA (International Data Encryption Algorithm) является блочным шифром. Он оперирует 64битовыми блоками открытого текста. Несомненным достоинством алгоритма является то что его ключ имеет длину 128 бит. Один и тот же алгоритм используется для шифрования и для расшифрования.

Первая версия алгоритма IDEA была предложена в 1990 г., ее авторы – X. Лей и Дж. Мэсси. Первоначальное название алгоритма – PES (Proposed Encryption Standart). Улучшенный вариант этого алгоритма, разработанный в 1991 г., получил название IPES (Improved Proposed Encryption Standart). В 1992 г. IPES изменил свое название на IDEA. Как и большинство других блочных шифров, алгоритм IDEA использует в шифровании процессы смешивания и рассеивания, причем все процессы легко реализуются аппаратными и программными средствами.

В алгоритме IDEA используются следующие математические операции:

– поразрядное сложение по модулю 2 (операция «исключающее ИЛИ»);
– сложение беззнаковых целых по модулю 2^{16};

– умножение целых по модулю $2^{16} + 1$ (модуль 65537), рассматриваемых как беззнаковые целые, за исключением того, что блок из 16 нулей рассматривается как 2^{16}.

Комбинирование этих трех операций обеспечивает комплексное преобразование входа, существенно затрудняя криптоанализ IDEA по сравнению с DES, который базируется исключительно на операции «исключающее ИЛИ».

Вернуться к содержанию

13.6. Алгоритм шифрования AES

Алгоритм шифрования AES разработали два специалиста по криптографии – Дж. Деймен (J. Daemen) и В. Риджен (V. Rijmen) из Бельгии. Этот алгоритм является нетрадиционным блочным шифром, поскольку не использует сеть Фейштеля для криптопреобразований. Алгоритм представляет каждый блок кодируемых данных в виде двумерного массива байтов размером 4 * 4, 4 * 6 или 4 * 8 в зависимости от установленной длины блока. Далее на соответствующих этапах производятся преобразования либо над независимыми столбцами, либо над независимыми строками, либо вообще над отдельными байтами в таблице.

Алгоритм состоит из определенного количества раундов (от 10 до 14 – это зависит от размера блока и длины ключа), в которых последовательно выполняются преобразования Sub Bytes, Shift Rows, Mix Columns, Add Round Key. Они воздействуют на массив State, который адресуется с помощью указателя State. Преобразование Add Round Key использует дополнительный указатель для адресации ключа раунда Round Key.

Преобразование Sub Bytes – нелинейная байтовая подстановка (см. рис. 7), которая воздействует независимо на каждый байт массива State, используя таблицу подстановок S – box. Эта таблица является обратимой.

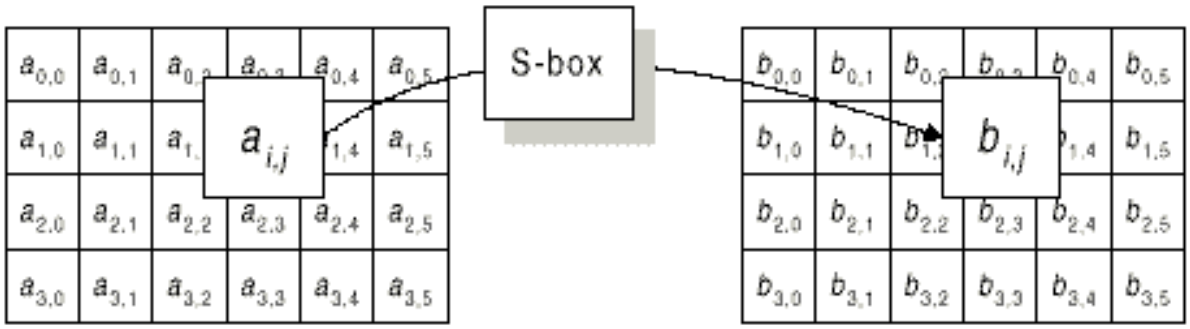


Рис. 8. *Преобразование Sub Bytes, использующее таблицу подстановок S-box для обработки каждого байта массива State*

При преобразовании Shift Rows байты в трех последних строках двумерного массива State циклически сдвигаются на различное число байтов. При этом первая строка не сдвигается (см. рис. 8).

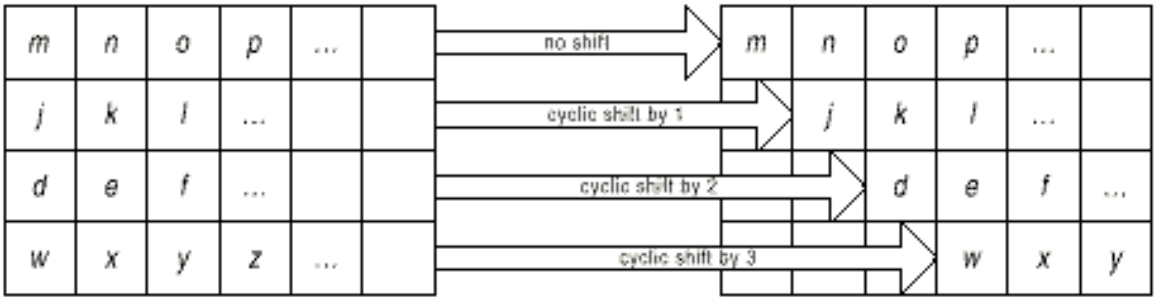


Рис. 7. Преобразование Shift Rows, использующее циклический сдвиг трёх последних строк в массиве State

Mix Columns – это математическое преобразование, перемешивающее данные внутри каждого столбца массива State (см. рис. 9). Преобразование Mix Columns воздействует поочередно на столбцы массива State.

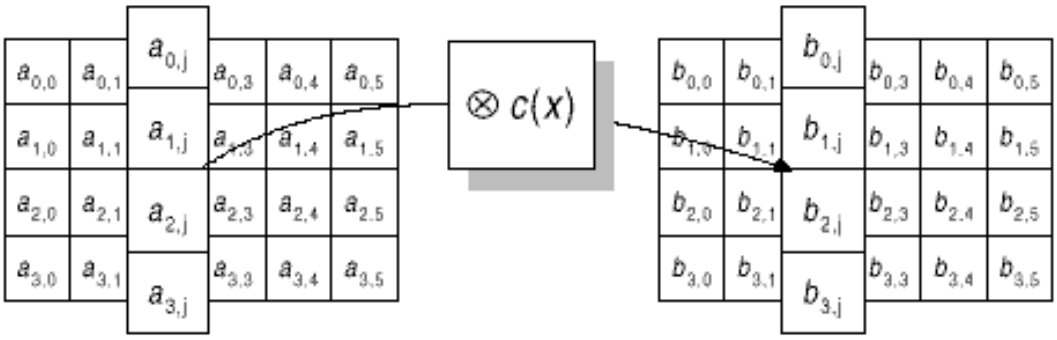


Рис. 9. Преобразование Mix Columns, поочередно обрабатывающее столбцы массива State

При преобразовании Add Round Key ключ раунда Round Key прибавляется к массиву State с помощью операции простого побитового сложения XOR (сложения по модулю 2) (рис. 10).

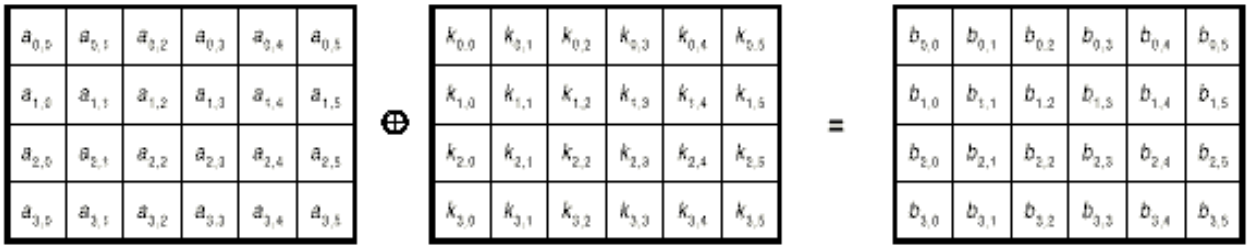


Рис. 10. Преобразование Add Round Key, производящее сложение XOR каждого массива State со словами из ключевого набора

Все преобразования в шифре AES имеют строгое математическое обоснование. Сама структура и последовательность операций позволяет выполнять данный алгоритм эффективно как на 8-битовых, так и на 32-битовых процессорах. В структуре алгоритма заложена возможность параллельного исполнения некоторых операций, что может повысить скорость шифрования на многопроцессорных рабочих станциях в четыре раза.

Рассмотрим особенности применения алгоритмов симметричного шифрования.

1. Алгоритмы симметричного шифрования используют ключи относительно небольшой длины и могут быстро шифровать большие объемы данных.

2. При симметричной методологии шифрования отправитель и получатель применяют для осуществления процессов зашифрования и расшифрования сообщения один и тот же секретный ключ

3. Алгоритмы симметричного шифрования применяются для абонентского шифрования данных, то есть для шифрования информации, предназначенной для отправки кому-либо например, через Internet.

Порядок использования систем с симметричными ключами таков:

1. Безопасно создается, распространяется и сохраняется симметричный секретный ключ.

2. Для получения зашифрованного текста отправитель применяет к исходному сообщению симметричный алгоритм шифрования вместе с секретным ключом.

3. Отправитель передает зашифрованное сообщение. Симметричный секретный ключ никогда не передается в открытой форме по незащищенным каналам связи.

4. Получатель применяет к зашифрованному тексту тот же самый симметричный алгоритм шифрования / расшифрования вместе с тем же самым симметричным ключом (который уже есть у получателя) для восстановления исходного текста. Его успешное восстановление идентифицирует того, кто знает секретный ключ.

Для симметричных криптосистем актуальна проблема безопасного распределения секретных ключей. Всем системам симметричного шифрования присущи следующие недостатки:

– принципиальным является требование защищенности и надежности канала передачи секретного ключа для каждой пары участников информационного обмена;

– предъявляются повышенные требования к службе генерации и распределения ключей.

Поэтому без эффективной организации защищенного распределения ключей широкое использование обычной системы симметричного шифрования в больших сетях, в частности глобальных, практически невозможно.

Вернуться к содержанию

13.7. Принципы построения асимметричных криптографических систем

В основе асимметричных криптографических систем лежит понятие однонаправленной функции f, обладающей свойствами:

– простое (не требующее больших ресурсов) вычисление значений функции $y = f(x)$;

– существование обратной функции f^{-1};

– сложное вычисление значения обратной функции $x = f^{-1}(y)$.

Фактически в асимметричной криптографии используется подкласс однонаправленных функций – однонаправленные функции с обходными путями, для которых обратная функция может быть вычислена так же просто, как и прямая, только если известна специальная информация об обходных путях. Эта специальная информация исполняет роль секретного ключа.

Пусть pk – открытый ключ функции шифрования E, а sk – секретный ключ функции расшифрования D. Тогда должны выполняться следующие условия, чтобы E и D образовывали асимметричную криптосистему.

1. $D_{sk}(E_{pk}(P)) = P$ (расшифрование должно восстанавливать открытый текст P).

2. Функции E_{pk} и D_{sk} должны быть просты в реализации.

3. При раскрытии преобразования, выполняемого с помощью $E_{pk,}$ не должно раскрываться преобразование, выполняемое с помощью D_{sk} (из открытого ключа нельзя получить секретный ключ)

4. $D_{pk}(E_{sk}(P)) = P$ (возможно использование секретного ключа для шифрования, а открытого – для расшифрования).

Четвертое условие является необязательным и не все асимметричные криптосистемы им обладают.

К основным применениям асимметричных криптосистем относятся:

– передача ключа симметричного шифрования по открытой сети (отправитель зашифровывает этот ключ с помощью открытого ключа получателя, который только и сможет расшифровать полученное сообщение с помощью своего секретного ключа);

– системы электронной цифровой подписи для защиты электронных документов (создатель документа удостоверяет его подлинность с помощью своего секретного ключа, после чего любой владелец соответствующего открытого ключа сможет проверить аутентичность данного документа).

В отличие от классической симметричной криптографии криптография с открытым ключом появилась сравнительно недавно – во второй половине XX века. К особенностям современных асимметричных криптосистем, которые не позволяют им полностью заменить симметричные криптосистемы, относятся:

– большая продолжительность процедур шифрования и расшифрования (примерно в 1000 раз больше);

– необходимость использования существенно более длинного ключа шифрования для обеспечения той же криптостойкости шифра.

К наиболее известным асимметричным криптосистемам относятся RSA (Rivest, Shamir, Adleman), Диффи – Хеллмана, Эль – Гамаля и криптосистема на основе эллиптических кривых.

Вернуться к содержанию

13.8. Алгоритм шифрования RSA

Алгоритм RSA является классикой асимметричной криптографии. В нем в качестве необратимого преобразования отправки используется возведение целых чисел в большие степени по модулю.

Алгоритм RSA стоит у истоков асимметричной криптографии. Он был предложен тремя исследователями-математиками Рональдом Ривестом (R. Rivest), Ади Шамиром (A. Shamir) и Леонардом Адльманом (L. Adleman) в 1977-78 годах.

Первым этапом любого асимметричного алгоритма является создание пары ключей: открытого и закрытого и распространение открытого ключа «по всему миру». Для алгоритма RSA этап создания ключей состоит из следующих операций :

1. Выбираются два простых числа p и q
2. Вычисляется их произведение $n(=p*q)$
3. Выбирается произвольное число e $(e<n)$, такое, что $НОД(e,(p-1)(q-1)) = 1$, то есть e должно быть взаимно простым с числом $(p-1)(q-1)$.
4. Методом Евклида решается в целых числах (!) уравнение $e*d + (p-1)(q-1)*y = 1$.

Здесь неизвестными являются переменные d и y – метод Евклида как раз и находит множество пар (d,y), каждая из которых является решением уравнения в целых числах.

5. Два числа (e, n) публикуются как открытый ключ.
6. Число d хранится в строжайшем секрете – это и есть закрытый ключ, который позволит читать все послания, зашифрованные с помощью пары чисел (e, n).

Как же производится собственно шифрование с помощью этих чисел :

1. Отправитель разбивает свое сообщение на блоки, равные $k = [log_2(n)]$ бит, где квадратные скобки обозначают взятие целой части от дробного числа.
2. Подобный блок может быть интерпретирован как число из диапазона $(0;2^k - 1)$. Для каждого такого числа (назовем его m_i) вычисляется выражение $c_i = ((m_i)^e) mod\ n$. Блоки c_i и есть зашифрованное сообщение. Их можно спокойно передавать по открытому каналу, поскольку операция возведения в степень по модулю простого числа является необратимой математической задачей. Обратная ей задача носит название «логарифмирование в конечном поле» и является на несколько порядков более сложной. То есть даже если злоумышленник знает числа e и n, то по c_i прочесть исходные сообщения m_i он не может никак, кроме как полным перебором m_i.

А вот на приемной стороне процесс расшифрования все же возможен, и поможет нам в этом хранимое в секрете число d. Достаточно давно была доказана теорема Эйлера, частный случай которой утверждает, что если число n представимо в виде двух простых чисел p и q, то для любого x имеет место равенство:

$$(x^{(p-1)(q-1)}) mod\ n = 1.$$

Для расшифрования RSA-сообщений воспользуемся этой формулой. Возведем обе ее части в степень (-y) :

$$(x^{(-y)(p-1)(q-1)})mod\ n = 1^{(-y)} = 1.$$

Теперь умножим обе ее части на x:

$$(x^{(-y)(p-1)(q-1)+1})mod\ n = 1*x = x.$$

А теперь вспомним, как мы создавали открытый и закрытый ключи. Мы подбирали с помощью алгоритма Евклида d такое, что $e*d + (p-1)(q-1)*y = 1$, то есть $e*d = (-y)(p-1)(q-1) + 1$. А следовательно, в последнем выражении предыдущего абзаца мы можем заменить показатель степени на число $(e*d)$. Получаем $(x^{e*d})mod\ n = x$. То есть для того, чтобы прочесть сообщение $c_i=((m_i)^e)mod\ n$, достаточно возвести его в степень d по модулю m:

$$((c_i)^d)mod\ n = ((m_i)^{e*d})mod\ n = m_i.$$

На самом деле операции возведения в степень больших чисел достаточно трудоемки для современных процессоров, даже если они производятся по оптимизированным по времени алгоритмам. Поэтому обычно весь текст сообщения кодируется обычным блочным шифром (намного более быстрым), но с использованием ключа сеанса, а вот сам ключ сеанса шифруется как раз асимметричным алгоритмом с помощью открытого ключа получателя и помещается в начало файла.

Вернуться к содержанию

13.9. Алгоритм шифрования Диффи – Хеллмана

Метод Диффи – Хеллмана использует алгоритм, подобный алгоритму RSA, для первоначального обмена ключами в симметричных криптосистемах по открытому каналу, но только такому, в котором невозможна фальсификация сообщений.

Он помогает обмениваться секретным ключом для симметричных криптосистем, но использует метод, очень похожий на асимметричный алгоритм RSA. Алгоритм назван по фамилиям его создателей Диффи (Diffie) и Хеллмана (Hellman).

Определим круг его возможностей. Предположим, что двум абонентам необходимо провести конфиденциальную переписку, а в их распоряжении нет первоначально оговоренного секретного ключа. Однако между ними существует

канал, защищенный от модификации, то есть данные, передаваемые по нему, могут быть прослушаны, но не изменены (такие условия имеют место довольно часто). В этом случае две стороны могут создать одинаковый секретный ключ, ни разу не передав его по сети, по следующему алгоритму.

Предположим, что обоим абонентам известны некоторые два числа v и n. Они, впрочем, известны и всем остальным заинтересованным лицам. Для того, чтобы создать неизвестный более никому секретный ключ, оба абонента генерируют случайные или псевдослучайные простые числа : первый абонент – число x, второй абонент – число y. Затем первый абонент вычисляет значение $(v^x) \bmod n$ и пересылает его второму, а второй вычисляет $(v^y) \bmod n$ и передает первому. Злоумышленник получает оба этих значения, но модифицировать их (вмешаться в процесс передачи) не может.

На втором этапе первый абонент на основе имеющегося у него x и полученного по сети $(v^y) \bmod n$ вычисляет значение

$(((v^y) \bmod n)^x) \bmod n$,

а второй абонент на основе имеющегося у него y и полученного по сети $(v^x) \bmod n$ вычисляет значение

$(((v^x) \bmod n)^y) \bmod n$.

На самом деле операция возведения в степень переносима через операцию взятия модуля по простому числу (коммутативна в конечном поле), то есть у обоих абонентов получилось одно и то же число: $((v^{x*y}) \bmod n$. Его они и могут использовать в качестве секретного ключа, поскольку здесь злоумышленник снова встретится с проблемой RSA при попытке выяснить по перехваченным $(v^x) \bmod n$ и $(v^y) \bmod n$ сами числа x и y – это очень и очень ресурсоемкая операция, если числа v,n,x,y выбраны достаточно большими.

Необходимо еще раз отметить, что алгоритм Диффи – Хеллмана работает только на линиях связи, надежно защищенных от модификации. Если бы он был применим на любых открытых каналах, то давно снял бы проблему распространения ключей и, возможно, заменил собой всю асимметричную криптографию. Однако в тех случаях, когда в канале возможна модификация данных, появляется очевидная возможность вклинивания в процесс генерации ключей «злоумышленника-посредника» по той же самой схеме, что и для асимметричной криптографии.

Вернуться к содержанию

14. ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ И ЕЕ ПРИМЕНЕНИЕ

Механизм электронной цифровой подписи должен обеспечить защиту от следующих угроз безопасности электронных документов, передаваемых по открытым компьютерным сетям или хранящихся на открытых носителях:

– подготовка документа от имени другого субъекта;
– отказ автора документа от факта его подготовки;
– изменение получателем документа его содержания;
– изменение содержания документа третьим лицом;
– повторная передача по компьютерной сети ранее переданного документа.

Электронная цифровая подпись (ЭЦП) представляет собой относительно небольшой по объему блок данных, передаваемый (хранящийся) вместе (реже – отдельно) с подписываемым с ее помощью документом. Механизм ЭЦП состоит из двух процедур: получение подписи с помощью секретного ключа автора документа и проверка ЭЦП при помощи открытого ключа автора документа.

Перед получением ЭЦП в подписываемый документ должны быть включены дополнительные сведения:

– дата и время постановки подписи;
– срок окончания действия секретного ключа данной подписи;
– реквизиты (фамилия, имя, отчество подписывающего лица, его должность и название представляемой организации);
– идентификатор секретного ключа (для возможности выбора лицом, проверяющим ЭЦП, нужного открытого ключа).

В системе ЭЦП подпись под электронным документом невозможно подделать без знания секретного ключа автора документа, поэтому компрометация секретного ключа недопустима.

Известны следующие системы ЭЦП:

– RSA (на основе асимметричной криптосистемы RSA);
– DSS (Digital Signature Standart, стандарт США на основе асимметричной системы Эль-Гамаля);
– ГОСТ Р 34.10 – 94 (российский стандарт ЭЦП на основе асимметричной криптосистемы Эль-Гамаля);
– ГОСТ Р 34.10 – 2001) – 2001 (российский стандарт ЭЦП, использующий асимметричную криптосистему на основе эллиптических кривых).

Алгоритмы получения и проверки ЭЦП в системе RSA не отличаются от алгоритма шифрования и расшифрования в аналогичной криптосистеме, за исключением того, что получение ЭЦП производится с применением секретного ключа y, а проверка ЭЦП – с применением открытого ключа x.

Алгоритмы получения и проверки ЭЦП в системе Эль-Гамаля отличаются от алгоритмов шифрования и расшифрования в аналогичной криптосистеме.

Защищенность системы ЭЦП от угрозы аутентичности и целостности подписанных документов зависит не только от стойкости алгоритмов используемой асимметричной криптосистемы, но и от стойкости функции хеширования. На функции хеширования, используемые в системах ЭЦП, налагаются очевидные дополнительные условия:

– чувствительность к любым изменениям в документе (вставкам, удалениям, перестановкам, заменам фрагментов и отдельных символов);

– минимальность вероятности того, что хеш-значение двух разных документов, независимо от длин, совпадут.

К наиболее известным функциям хеширования относятся:

– MD2, MD4, MD5 (Message Digest) – получают хеш-значение длиной 160 бит и используются в системе ЭЦП RSA;

– SHA (Secure Hash Algorithm) – получает хеш-значение длиной 160 бит и используется в системе ЭЦП DSS;

– ГОСТ Р 34.11 – 94 – получает хеш-значение длиной 256 бит и используется в российских стандартах ЭЦП;

– RIPEMD (Race Integrity Primitives Evaluation Message Digest) – получает хеш-значение длиной 128 или 160 бит (две модификации).

Контрольные суммы

Наиболее простой способ проверки целостности данных, передаваемых в цифровом представлении, – это метод контрольных сумм. Под контрольной суммой понимается некоторое значение, рассчитанное путем сложения всех чисел из входных данных. Если сумма всех чисел превышает максимально допустимое значение, заранее заданное для этой величины, то величина контрольной суммы равна коэффициенту полученной суммы чисел, то есть это остаток от деления итоговой суммы на максимально возможное значение контрольной суммы, увеличенное на единицу.

$$\textbf{Checkssum = Total \% (MaxVal + 1),}$$

где Total – итоговая сумма, рассчитанная по входным данным, и MaxVal – максимально допустимое значение контрольной суммы, заданное заранее.

Недостаток метода контрольных сумм заключается в том, что, хотя несовпадение значений этих сумм служит верным доказательством, что рассматриваемый документ подвергается изменению, равенство сравниваемых значений еще не дает гарантии, что информация осталась неизменной. Можно произвольным образом изменить порядок следования чисел в документе, а контрольная сумма при этом сохранит прежнее значение.

Примеры использования контрольных сумм

В примерах обычно вычисляется некоторая функция (контрольная сумма) от цифр номера. Если она равна 0, то номер признаётся правильным. (В некоторых случаях удобнее вычислять контрольное число и сверять его с имеющимся. Формально контрольной суммой можно считать разность между имеющимся и вычисленным контрольными числами). Цифры номера нумеруются справа налево: $\ldots n_3 n_2 n_1$, так же, как и соответствующие им коэффициенты $\ldots k_3 k_2 k_1$. Обычно содержательная информация (код страны, товара, банка и т. п.) находится в левой части номера, а контрольное число (цифра) является завершающей (самой правой) и имеет номер 1 (n_1), однако с математической точки зрения все цифры кода, как правило, равноправны, и любая из них может считаться контрольной для остальных.

Контрольные суммы вычисляются по сходному алгоритму. Кроме того, тот же алгоритм (таблица обрезается или продолжается влево по очевидному правилу) используется во многих других случаях, например для номеров товаров в магазинах.

	k_{13}	k_{12}	k_{11}	k_{10}	k_9	k_8	k_7	k_6	k_5	k_4	k_3	k_2	k_1
EAN-13	1	3	1	3	1	3	1	3	1	3	1	3	1
UPC-12													
EAN-8													

Контрольная сумма есть остаток от деления на 10 суммы из цифр номера, умноженных на соответствующие коэффициенты из таблицы. Если контрольная сумма есть 0, то номер признаётся правильным.

Если нужно подсчитать требуемое контрольное число для произвольного номера, нужно вначале поставить «0» на крайнюю правую позицию, посчитать

контрольную сумму, а затем, если она не равна нулю, заменить этот «0» на «10 – контрольная сумма».

1) Штрих-код товаров

4600051000057 (сигареты «Прима») – код EAN-13.

4 × 1 + 6 × 3 + 0 × 1 + 0 × 3 + 0 × 1 + 5 × 3 + 1 × 1 + 0 × 3 + 0 × 1 + 0 × 3 + 0 × 1 + 5 × 3 + 7 × 1 = 4 + 18 + 0 + 0 + 0 + 15 + 1 + 0 + 0 + 0 + 0 + 15 + 7 = 60.

Контрольная сумма = 0 – номер правильный.

46009333 (папиросы «Беломорканал») – код EAN-8.

4 × 3 + 6 × 1 + 0 × 3 + 0 × 1 + 9 × 3 + 3 × 1 + 3 × 3 + 3 × 1 = 12 + 6 + 0 + 0 + 27 + 3 + 9 + 3 = 60.

Контрольная сумма = 0 – номер правильный.

041689300494 (бензин для зажигалки «Zippo») – код UPC-12.

0 × 3 + 4 × 1 + 1 × 3 + 6 × 1 + 8 × 3 + 9 × 1 + 3 × 3 + 0 × 1 + 0 × 3 + 4 × 1 + 9 × 3 + 4 × 1 = 0 + 4 + 3 + 6 + 24 + 9 + 9 + 0 + 0 + 4 + 27 + 4 = 90.

Контрольная сумма = 0 – номер правильный.

Восстановление контрольного числа. Дан номер 460154602129?, EAN-13 с потерянной контрольной цифрой «?».

Для 4601546021290:

4 × 1 + 6 × 3 + 0 × 1 + 1 × 3 + 5 × 1 + 4 × 3 + 6 × 1 + 0 × 3 + 2 × 1 + 1 × 3 + 2 × 1 + 9 × 3 + 0 × 1 = 4 + 18 + 0 + 3 + 5 + 12 + 6 + 0 + 2 + 3 + 2 + 27 + 0 = 82.

Контрольная сумма = 2 – номер неправильный, но если вместо «?» подставить «10 – 2» = «8», то номер станет правильным. Таким образом, контрольное число (цифра) есть «8».

2) Номера банковских карт

Номера кредитных карт American Express всегда начинаются на цифру 3, VISA начинается на 4, MasterCard – на 5 и Maestro – на 6.

Контрольные суммы вычисляются по сходному алгоритму. Правило продолжения таблицы влево (для длинных номеров) и усечения её для коротких номеров очевидно.

В случае наличия в номере (коде) ISIN английских букв, каждая из них заменяется на 2 цифры, представляющие собой порядковый номер буквы в латинском алфавите, увеличенный на 9 (т. е. A ~ 10, B ~ 11, …, Z ~ 35).

	k_{16}	k_{15}	k_{14}	k_{13}	k_{12}	k_{11}	k_{10}	k_9	k_8	k_7	k_6	k_5	k_4	k_3	k_2	k_1	
	банковские карты, 16 цифр	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1
	ценные бумаги																
	банковские карты, 13 цифр																

Контрольная сумма. Цифры кода умножаются на коэффициенты из таблицы, если результат умножения превосходит 9, то вычитаем из него 9, получившиеся числа складываем. Берём остаток от деления суммы на 10.

Если контрольная сумма есть 0, то номер признаётся правильным.

Восстановление «контрольного числа» аналогично способу для штрих-кода.

4000-0000-0000-6 – 13-значная банковская карта **Visa.**

Произведения: 4 x 1, 0 x 2, 0 x 1, 0 x 2, 0 x 1, 0 x 2, 0 x 1, 0 x 2, 0 x 1, 0 x 2, 0 x 1, 0 x 2, 6 x 1;

После вычитания 9: 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6;

Их сумма: 10;

Контрольная сумма = 0 – номер правильный.

5610-0000-0000-0001 – 16-значная банковская карта **Australian Bankcard.**

Произведения: 5 x 1, 6 x 2, 1 x 1, 0 x 2, 0 x 1, 0 x 2, 0 x 1, 0 x 2, 0 x 1, 0 x 2, 0 x 1, 0 x 2, 1 x 1;

После вычитания 9: 5, 3, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1;

Их сумма: 10;

Контрольная сумма = 0 – номер правильный.

RU0007661625 – ISIN акции Газпрома номиналом 5 руб.

Буквы RU заменяем на 2730 и получаем 14-значный номер 27300007661625, который и будем проверять.

Произведения: 2 x 2, 7 x 1, 3 x 2, 0 x 1, 0 x 2, 0 x 1, 0 x 2, 7 x 1, 6 x 2, 6 x 1, 1 x 2, 6 x 1, 2 x 2, 5 x 1;

После вычитания 9: 4, 7, 6, 0, 0, 0, 0, 7, 3, 6, 2, 6, 4, 5;

Их сумма: 50;

Контрольная сумма = 0 – номер правильный.

DE0001136927 – пример ISIN с сайта Банка Эстонии.

Буквы DE заменяем на 1314 и получаем 14-значный номер 13140001136927.

Произведения: 1 х 2, 3 х 1, 1 х 2, 4 х 1, 0 х 2, 0 х 1, 0 х 2, 1 х1, 1 х 2, 3 х 1, 6 х 2, 9 х 1, 2 х 2, 7 х 1;

После вычитания 9: 2, 3, 2, 4, 0, 0, 0, 1, 2, 3, 3, 9(!), 4, 7;

Их сумма: 40;

Контрольная сумма = 0 – номер правильный.

3) Номер карточки медицинского страхования

Номер карточки медицинского страхования (он же СНИЛС) проверяется на валидность контрольным числом. СНИЛС имеет вид: «XXX-XXX-XXX YY», где XXX-XXX-XXX – собственно номер, а YY – контрольное число. Алгоритм формирования контрольного числа СНИЛС таков:

1) Проверка контрольного числа Страхового номера проводится только для номеров больше номера 001-001-998.

2) Контрольное число СНИЛС рассчитывается следующим образом:

2.1) Каждая цифра СНИЛС умножается на номер своей позиции (позиции отсчитываются с конца);

2.2) полученные произведения суммируются;

2.3) если сумма меньше 100, то контрольное число равно самой сумме;

2.4) если сумма равна 100 или 101, то контрольное число равно 00;

2.5) если сумма больше 101, то сумма делится нацело на 101 и контрольное число определяется остатком от деления аналогично пунктам 2.3 и 2.4

ПРИМЕР: Указан СНИЛС 112-233-445 95

Проверяем правильность контрольного числа:

цифры номера 1 1 2 2 3 3 4 4 5

номер позиции 9 8 7 6 5 4 3 2 1

Сумма = 1 х 9 + 1 х 8 + 2 х 7 + 2 х 6 + 3 х 5 + 3 х 4 + 4 х 3 + 4 х 2 + 5 х 1 = 95

Контрольное число 95 – указано верно

4) Номера ИНН

Бывают 10-значные (1 контрольная цифра в конце) и 12-значные (2 контрольные цифры в конце).

	k_{12}	k_{11}	k_{10}	k_9	k_8	k_7	k_6	k_5	k_4	k_3	k_2	k_1	
	вычисление контрольного числа n_2 для 12-значного ИНН	7	2	4	10	3	5	9	4	6	8		
	вычисление контрольного числа n_1 для 12-значного ИНН	3	7	2	4	10	3	5	9	4	6	8	
	вычисление контрольного числа n_1 для 10-значного ИНН												

Проверку ИНН удобнее проводить, вычисляя контрольные числа:

Шаг 1 (только для 12-значного ИНН). Контрольное число n_2 есть остаток от деления на 11 суммы из цифр номера, умноженных на соответствующие коэффициенты из таблицы (из строки «вычисление контрольного числа n_2»). Если остаток есть 10, то $n_2 = 0$.

Шаг 2. Контрольное число n_1 есть остаток от деления на 11 суммы из цифр номера, умноженных на соответствующие коэффициенты из таблицы (из строки «вычисление контрольного числа n_1»). Если остаток есть 10, то $n_1 = 0$.

ИНН 500100732259 – 12 цифр (первый попавшийся в Интернете ИНН).

Шаг 1: 5 * 7+ 0 * 2+ 0 * 4+ 1 * 10+ 0 * 3+ 0 * 5+ 7 * 9+ 3 * 4+ 2 * 6+ 2 * 8 = 148 148= 11*13 + 5 (остаток); совпадает

Шаг 2: 5 * 3+ 0 * 7+ 0 * 2+ 1 * 4+ 0 * 10+ 0 * 3+ 7 * 5+ 3 * 9+ 2 * 4+ 2 * 6 + 5 * 8 = 141 141= 11 * 12 + 9 (остаток); совпадает

Оба контрольных числа совпадают, номер правильный.

ИНН 7830002293 – 10 цифр (Санкт-Петербургская бумажная фабрика Гознака).

Шаг 2: 7 * 2+ 8 * 4+ 3 * 10+ 0 * 3+ 0 * 5+ 0 * 9+ 2 * 4+ 2 * 6 + 9 * 8 = 168 168 = 11 * 15 +3 (остаток). Контрольное число совпадает, номер правильный.

Контроль CRC

Более совершенный способ цифровой идентификации некоторой последовательности данных – это вычисление контрольного значения ее циклического избыточного кода (Cyclic Redundancy Check – CRC). Алгоритм контроля CRC уже в течение длительного времени широко используется в системах сетевых адаптеров, контроллеров жесткого диска и других устройств для проверки идентичности входной и выходной информации.

А также этот механизм применяется во многих из ныне существующих коммуникационных программах для выявления ошибок при пакетной передаче по телефонным линиям связи.

Механизм основан на полиномиальном распределении, где каждый разряд некоторой порции данных соответствует одному коэффициенту большого полиномиального выражения.

Вернуться к содержанию

ЗАКЛЮЧЕНИЕ

Проблема обеспечения информационной безопасности становится все более актуальной для российских компаний. Это связано и с обострением конкурентной борьбы на внутренних рынках, и с выходом компаний на международный уровень. Многие из них уже не могут обеспечить защиту коммерческой информации собственными силами и вынуждены пользоваться услугами профильных профессиональных IT-консультантов.

Обеспечение информационной безопасности является не только российской, но и мировой проблемой. Так, в первые годы внедрения корпоративных локальных сетей головной болью компаний был несанкционированный доступ к коммерческой информации путем внешнего взлома (хакерской атаки). Сейчас, с точки зрения информационной безопасности, многие компании напоминают крепости, окруженные несколькими периметрами мощных стен – программными и аппаратными платформами ИБ. Однако практика показывает, что информация все равно утекает. При этом основной предпосылкой к утечке информации является отсутствие единого системного подхода к обеспечению ИБ в компаниях.

В течение многих лет компании отчаянно боролись с вирусными эпидемиями, обносили периметр межсетевыми экранами и системами предотвращения вторжений, внедряли мощные инструменты против неавторизованного доступа. Однако компании упустили из вида главную опасность. Осутствие единой политики информационной безопастности, а также единой концепции построения профиля информационной защиты компании зачастую обесценивает многомиллионные затраты на программные и аппаратные комплексы ИБ. Еще пару лет назад IT-службы отвечали за защиту от внешних угроз, а с внутренними угрозами разбиралась служба безопасности. Сегодня она просто физически не может контролировать перемещение информации по электронным сетям и с помощью переносных носителей. Для этого нужны специально разработанные регламенты, ликбез сотрудников, специально подготовленные сотрудники безопасности и технические средства для выявления попыток несанкционированного доступа или перемещения информации. Все эти меры должны реализоваться специалистом ИБ в рамках единой концепции.

Бурное развитие IT-технологий и направления ИБ приводит к росту спроса на профессиональных специалистов в данной области. Это актуализирует получение образования в области ИБ и широкой востребованости полученных профильных знаний на рынке труда.

Данное учебное пособие поможет будущим профессионалам в сфере IT получить тот общий набор знаний и умений в области ИБ, чтобы оказаться востребованными и высокооплачиваемыми сотрудниками престижных компаний.

Вернуться к содержанию

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Галатенко, В. А. Основы информационной безопасности / В. А. Галатенко. – М. : Интернет-университет информационных технологий – www.INTUIT.ru, 2014. – 208 с.

2. Галатенко, В. А. Стандарты информационной безопасности / В. А. Галатенко. – М. : Интернет-университет информационных технологий – www.INTUIT.ru, 2010. – 264 с.

3. Lonely, R. Алгоритм шифрования данных с открытым ключом RSA [Эл. ресурс] / R. Lonely.– URL: www.rusdoc.ru/material/raznoe/rsa.shtml

4. Антивирусная защита компьютерных систем : курс лекций для Интернет-университета информационных технологий от лаборатории Касперского – М. : Интернет-университет информационных технологий – www.INTUIT.ru, 2011. – URL : www.intuit.ru/department/security/antiviruskasp/

5. Вирусы и средства борьбы с ними : курс лекций для Интернет-университета информационных технологий от лаборатории Касперского – М. : Интернет-университет информационных технологий – www.INTUIT.ru, 2011. – URL : www.intuit.ru/department/security/viruskasper/

6. Мэйволд, Э. Безопасность сетей : курс лекций для Интернет-университета информационных технологий / Э. Мэйволд. – М. : Интернет-университет информационных технологий – www.INTUIT.ru, 2012. – URL : www.intuit.ru/department/security/netsec/

7. Кобб, М. Безопасность IIS : курс лекций для Интернет-университета информационных технологий / М. Кобб, М. Джост. – М. : Интернет-университет информационных технологий – www.INTUIT.ru, 2013. – URL: www.intuit.ru/department/internet/iissecurity/

8. Малюк, А. А. Информационная безопасность : концептуальные и методологические основы защиты информации : уч. пособие для вузов / А. А. Малюк. – М. : Горячая линия – Телеком, 2014. – 280 с.