Содержание:

ВВЕДЕНИЕ

Информационная безопасность предприятия – это защищенность информации, которой располагает предприятие (производит, передает или получает) от несанкционированного доступа, разрушения, модификации, раскрытия и задержек при поступлении. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода. Целью комплексной информационной безопасности является сохранение информационной системы предприятия в целости и сохранности, защита и гарантирование полноты и точности выдаваемой ею информации, минимизация разрушений и модификация информации, если таковые случаются.

Компьютеризация, развитие телекоммуникаций предоставляют сегодня широкие возможности для автоматизированного доступа к различным конфиденциальным, персональным и другим важным, критическим данным в обществе (его граждан, организаций и т.д.).

Проблема создания и поддержания защищенной среды информационного обмена, реализующая определенные правила и политику безопасности современной организации, является весьма актуальной. Информация давно уже перестала играть эфемерную, чисто вспомогательную роль, превратившись в весьма важный и весомый, чуть ли не материальный, фактор со своими стоимостными характеристиками, определяемыми той реальной прибылью, которую можно получить от ее (информации) использования. В то же время, вполне возможен сегодня и вариант ущерба, наносимого владельцу информации (предприятию) путем несанкционированного проникновения в информационную структуру и воздействия на ее компоненты.

Объектом исследования являются: информационная безопасность.

Предмет исследования: защита информации.

Таким образом, цель данной работы изучение информационной безопасности.

Для достижения поставленной цели необходимо выполнить следующие задачи: рассмотреть оценку безопасности информационных систем, виды, методы и средства защиты информации; проанализировать структуру системы защиты информации.

Глава 1. Общие вопросы защиты информации

Коммерческая деятельность тесно взаимосвязана с получением, накоплением, хранением, обработкой и использованием разнообразных информационных потоков. Возникает вопрос: вся ли эта информация подлежит защите или только отдельные ее группы? Если же для защиты выделяется только определенная группа информации, то по каким критериям (свойствам)?

Отвечая на поставленные вопросы, следует подчеркнуть, защите подлежит не вся информация, а только та, которая представляет ценность для предпринимателя. При определении ценности коммерческой информации необходимо руководствоваться такими критериями (свойствами), как:

- полезность;
- своевременность;
- достоверность поступивших сведений.

Полезность информации состоит в том, что она создает субъекту выгодные условия для принятия оперативного решения и получения эффективного результата.

В свою очередь, полезность информации зависит от своевременного ее доведения (получения) до субъекта предпринимательства. Например, из-за несвоевременного поступления полезных по своему содержанию сведений упускается возможность заключить выгодную торговую или иную сделку. Результат — время упущено, информация теряет свою полезность.

Критерии полезности и своевременности тесно взаимосвязаны и взаимозависимы с критерием достоверности оцениваемой информации. Недостоверные сведения сводят к нулевому эффекту своевременность и кажущуюся их полезность для субъекта предпринимательства. При этом сам факт (например, желание конкретного лица заключить договор купли-продажи) может существовать реально, тогда, как сведения о нем содержат искаженное представление. Причины возникновения недостоверных сведений различны: неправильное восприятие (в

силу заблуждения, недостаточного опыта или профессиональных знаний) источником факта или умышленное, с определенной целью, искажение о нем сведений. Как правило, сведения, представляющие интерес для предпринимателя, а также источник их поступления должны подвергаться перепроверке.

Можно сослаться еще и на такой критерий, как полнота информации. Однако вести речь о том, насколько полна информация о конкретном объекте (факте) и где ее границы, довольно затруднительно и, к тому же, малоэффективно. В коммерческой деятельности этот критерий особой роли не играет.

В итоге, субъект оценки коммерческой информации, ее владелец (собственник), на основании совокупности перечисленных критериев, определяется ценность поступивших сведений для своей хозяйственной деятельности и принимает по ним оперативное решение.

Определение стоимости тех или иных сведений требует дифференцированного подхода. В одних случаях, дешевле обойдется метод собственных проб и ошибок, в других же, целесообразнее получить (купить) информацию о том, как избежать подобных ошибок, а в-третьих, как сохранить ценную информацию от доступа посторонних лиц, чтобы не потерять ее стоимость, а следовательно, ожидаемую от нее результативность. Факт утечки информации напрямую связан с падением ее ценности для лица, из владения которого она вышла.

Важное значение в условиях развития многообразных форм собственности имеет вопрос определения принадлежности информации на правах интеллектуальной собственности конкретному субъекту предпринимательства, а в итоге наличия у него правомочий на ее защиту.

Закон РФ регламентирующий предпринимательскую деятельность, предусматривает, что владельцами (собственниками) коммерческой информации, как интеллектуальной собственности, могут быть граждане России, граждане иностранных государств, лица без гражданства, а также объединения граждан — коллективных предпринимателей.

Обширны и направления коммерческой деятельности. Это внутренние и внешние экономические сферы производственной, посреднической, коммерческой, научно-технической, инвестиционной, сервисной деятельности.

Если подвести итог краткому анализу, то можно убедиться, что субъекты предпринимательства, формы и направления их деятельности далеко не

равнозначны, а следовательно, и информационные потоки, циркулирующие в этих сферах, не равноценны.

Так, государственные предприятия, занимающиеся коммерческой деятельностью, могут обладать сведениями, определяемыми как государственные или служебные секреты.

Информация государственных режимных предприятий (учреждений), в зависимости от степени важности (ценности), подразделяется на сведения, составляющие:

- государственную тайну;
- военную тайну;
- служебную тайну;
- иные сведения, не составляющие тайны, но представляющие интерес для иностранных спецслужб.

Наряду с режимными мерами, безопасность государственных секретов обеспечивается также нормами уголовного закона. Уголовная ответственность за передачу, а равно сбор и хранение сведений, составляющих государственную тайну, с целью передачи ее иностранному государству предусмотрена ст. 276 Уголовного кодекса РФ

Защита государственной секретной информации возложена на сотрудников режимных служб и правоохранительных органов (ст. 126 УПК РФ).

Обеспечение безопасности государственной интеллектуальной собственности под грифом “совершенно секретно”, “секретно” не имеет прямого отношения к защите частной коммерческой информации. Однако следует указать на некоторые исключения. В случае, если спецслужба иностранного государства проявит интерес к получению определенной коммерческой информации, то наряду с другими мерами оказывать ей противодействие будет и контрразведка. Под защиту специальных органов государства может быть взята коммерческая информация, оцененная как особо важная не только для ее частного собственника, но государства, когда не исключено, что к ней может проявить интерес иностранная спецслужба. Вопрос о подобной защите должен решаться на договорной основе между предпринимателем и органом федеральной безопасности с обозначением пределов и функций профессиональной деятельности последних.

Что касается основной массы коммерческой информации, то она подобной уголовно-правовой, оперативно-следовательской и режимной защитой не обладает и не пользуется.

В гражданском законодательстве, тем не менее, предпринята попытка узаконить коммерческую информацию в качестве защищаемой.

Воспроизведем статью 139 части первой Гражданского кодекса Российской Федерации, называющейся: “Служебная и коммерческая тайна”:

Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.

Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору”.

По существу в пункте 1 вышеизложенной статьи законодатель дал определение понятию “коммерческая тайна”.

Подводя итоги изложенному, можно сделать следующие выводы:

- субъектом оценки предпринимательской (коммерческой) информации является ее владелец (собственник);
- поступившие сведения и их источник подлежат обязательной перепроверке;
- ценность информации определяется с помощью таких критериев (свойств), как полезность, своевременность и достоверность;
- коммерческая информация в зависимости от ценности имеет свою стоимость;
- информация подлежит защите при условии, что ценность информации зависит от сохранности в тайне от третьих лиц, доступ к информации закрыт на законном основании, обладатель информации принимает надлежащие меры

по ее охране;
- использование правовой системы позволяет предпринимателю правильно отделять частную информацию от сведений, составляющих государственные секреты, и не допустить конфликта с действующим уголовным правом.

1.1. Специальные вопросы защиты коммерческой информации

Коммерческая информация, циркулирующая в рыночно-конкурентной сфере деятельности, подразделяется на техническую, организационную, коммерческую, финансовую, рекламную, о спросе-предложении, конкурентах, криминальной обстановке и др. Прежде чем принимать меры к защите определенной информации, необходимо уточнить следующие вопросы:

- какие сведения нельзя скрывать, защищать от доступа к ним (от кого?);
- какие сведения невыгодно скрывать (почему?);
- какие сведения подлежат охране (кем и от кого?).

Ответ на первый вопрос дало российское правительство в своем постановлении “О перечне сведений, которые не могут составлять коммерческую тайну”. К ним относятся:

- организационные сведения (устав и учредительные документы предприятия, регистрационные удостоверения, лицензии, патенты);
- финансовые сведения (документы об исчислении и уплате налогов, других платежей, предусмотренных законом, документы о состоянии платежеспособности);
- сведения о штате и условиях деятельности (число и состав работающих, их заработная плата, наличие свободных мест, влияние производства на природную среду, реализация продукции, причиняющей вред здоровью населения, участие должностных лиц в предпринимательской деятельности, нарушение антимонопольного законодательства);
- сведения о собственности (размерах имущества, денежных средствах, вложениях платежей в ценные бумаги, облигации, займы, в уставные фонды совместных предприятий).

Не вполне определенным остается вопрос о том, кому предприниматель обязан предъявлять по требованию перечисленные сведения? Вместе с тем, исходя из

характеристики информации, можно предполагать, что претендовать на ознакомление с этими сведениями могут в пределах своей компетенции:

- прокурор в порядке надзора и в других случаях, предоставленных ему законом;
- правоохранительные органы по возбужденному уголовному делу;
- налоговые службы (управления);
- аудиторские фирмы (по просьбе самого владельца);
- профсоюзы;
- государственные предприятия (учреждения);
- санэпидемстанции;
- экологические организации;
- предпринимательские предприятия и частные лица, вступающие с ним в сделку.

Данный перечень не является исчерпывающим.

Указанные сведения не являются предметом защиты от ознакомления с ними третьих лиц, но это не исключает их охраны от общеуголовных преступлений.

Вторая группа сведений характеризуется тем, что ее невыгодно скрывать от окружения самому предпринимателю. Это касается, прежде всего, рекламной информации. Без рекламы в хозяйственной деятельности трудно добиться эффективного результата, особенно в условиях жесткой конкуренции. Однако пропаганда и широкое распространение рекламы имеют не только положительную, но и отрицательную сторону для предпринимателя. Суть в том, что рекламная информация становится достоянием не только законопослушных граждан (на которых она и рассчитана), но и преступных элементов. Коммерческая информация, рекламируемая в газетах, в журналах, по телевидению, радио помогает преступникам выйти на объект будущего посягательства, изучить его слабые (уязвимые, например, для закона отдельные виды деятельности, различного рода махинации) стороны, а затем принять решение, каким способом получить для себя от него выгоду.

Предприниматель, рекламирующий свою деятельность, должен быть готов к возможному посягательству и своему ответному действию. Некоторые из них, в подобных ситуациях, пытаются найти защиту от преступников у таких же преступников, но из другой группировки. В итоге, запутавшись с преступным миром, попадают под их полное влияние, а иногда лишаются своих предприятий

(фирм).

Итак, предприниматель, рекламирующий свою деятельность, должен знать, с какими препятствиями он может столкнуться, и как он сможет их преодолеть в своей конкретной ситуации. Не выход из данного положения и конспирация предпринимательской деятельности, как пытаются это делать некоторые фирмы. Без клиентуры, в зависимости от видов хозяйствования, они не будут иметь необходимой прибыли. Выход один — обеспечить свою безопасность с помощью государственных и частных форм защиты.

К третьей группе сведений относятся те, которые представляют хозяйственную ценность для предпринимателя, и на них не распространяется законный доступ третьих лиц. С понятием ценной информации мы уже определились. Проблема состоит в том, кто и как должен обеспечить сохранность информации.

Если обратиться к законодательным актам, то ни один из них не ставит прямо под свою защиту данный вид собственности. Если допустить, что такая норма имелась бы, например, в уголовном кодексе, то это еще не говорило бы о том, что коммерческая информация надежно защищена.

1.2. Коммерческая тайна

К коммерческой тайне могут быть отнесены самые разнообразные сведения, связанные с производством, технологией, управлением, финансами и другими вопросами деятельности предприятия. На практике наряду с термином “коммерческая тайна” широко используются такие термины, как “конфиденциальная информация”, “ноу-хау”, “секреты производства”. Все они, в сущности, обозначают одно и те же понятие, которое в Гражданском кодексе РФ именуется “коммерческой тайной”.

В соответствии со ст.139 Гражданского кодекса РФ коммерческая тайна — это информация, имеющая действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

Из данного определения вытекают следующие обязательные признаки коммерческой тайны.

Первый признак — информация должна иметь действительную или потенциальную коммерческую ценность. Поэтому из числа сведений, составляющих коммерческую тайну, исключаются те из них, которые не представляют никакого интереса для окружающих. При отнесении предприятием информации к кругу сведений, составляющих коммерческую тайну, действительная или потенциальная коммерческая ценность таких сведений предполагается и не нуждается в доказывании. Однако в случае возникновения судебного спора (например, по иску к контрагенту о возмещении убытков, причиненных разглашением коммерческой тайны) перед предприятием встанет необходимость доказывать суду наличие у информации коммерческой ценности.

Второй признак — к информации, составляющей коммерческую тайну, не должно быть свободного доступа на законном основании. Если информация может быть получена законным образом любым заинтересованным лицом (путем изучения печатных изданий, просмотра открытых баз данных и т.п.), то такая информация коммерческой тайной не является. Даже если информация стала известной не ограниченному круги лиц в результате чьих-либо неправомерных действий, то и в этом случае информация автоматически утрачивает статус коммерческой тайны, поскольку лишается одного из необходимых критериев — отсутствие к информации свободного доступа.

Третий признак — для того, чтобы информация считалась коммерческой тайной, требуется, чтобы обладатель такой информации принимал меры к охране ее конфиденциальности. Меры по охране коммерческой тайны могут быть организационными (например, утверждение внутренних документов, регулирующих порядок доступа персонала к коммерческой тайне), техническими (использование сигнализации, защита телефонных переговоров и т.п.) и юридическими (например, включение в трудовые контракты с персоналом и договоры с контрагентами положений о неразглашении конфиденциальной информации). При этом простое определение круга информации, составляющей коммерческую тайну, не может рассматриваться в качестве охранной меры.

Коммерческая тайна, как разновидность информации, может являться объектом интеллектуальной собственности. При соблюдении необходимых условий (информация приносит доход и может быть использована в течение периода, превышающего 12 месяцев) права на указанную информацию могут отражаться в бухгалтерском учете в виде нематериальных активов. В то же время законодательство не рассматривает факт отражения в бухгалтерском учете прав на информацию в качестве одного из признаков коммерческой тайны. Поэтому

отсутствие в учете указанных прав не может свидетельствовать об отсутствие самой коммерческой тайны.

Коммерческая тайна не требует для признания ее таковой какой-либо государственной регистрации или выполнения каких-либо иных формальностей. В то же время следует отметить, что не любая информация, соответствующая всем перечисленным выше критериям, может быть отнесена к коммерческой тайне. Государство вправе осуществлять контроль (в том числе налоговый) за деятельностью предприятий. Для этих целей законодательство определяет круг сведений, которые не могут составлять коммерческую тайну.

Так, например, Постановлением Правительства РФ от 05.12.91г. № 35 установлен перечень таких сведений, к которым, в частности, относятся:

- учредительные документы (решение о создании предприятия или договор учредителей) и устав;
- документы, дающие право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии, патенты);
- сведения, необходимые для проверки правильности исчисления и уплаты налогов;
- документы о платежеспособности;
- сведения о численности работающих и их заработной плате; документы об уплате налогов;
- сведения об участии должностных лиц предприятия в других организациях.

В соответствии с п.89 Положения по ведению бухгалтерского учета (утверждено Приказом Минфина РФ от 29.07.98г. № 34), годовая бухгалтерская отчетность организации является открытой для заинтересованных пользователей: банков, инвесторов, кредиторов, покупателей, поставщиков и др., которые могут знакомиться с указанной отчетностью.

Под коммерческой тайной предприятия (фирмы) следует понимать сведения, не являющиеся государственными секретами, но связанные с производством, технологией, управлением, финансами и другой деятельностью предприятия, разглашение которых может нанести ущерб его интересам. Защищаемые сведения дают определенные преимущества в конкурентной борьбе. Коммерческой тайной предприятия не может быть информация, сокрытие которой способно нанести ущерб обществу.

В соответствии с Законом РФ «О предприятиях и предпринимательской деятельности» перечень сведений, составляющих коммерческую тайну, определяется руководителем предприятия. Предприятие имеет право не предоставлять информацию, содержащую коммерческую тайну.Законом предусматривается, что порядок, организация защиты коммерческой тайны с учетом действующего законодательства устанавливается руководителем предприятия (фирмы).

Сведения, отнесенные к коммерческой тайне, должны иметь следующие признаки:

- не являться государственным секретом;
- относиться к производственной деятельности предприятия;
- не наносить ущерб интересам общества; иметь действительную или потенциальную коммерческую ценность и создавать преимущества в конкурентной борьбе;
- иметь ограничения в доступе, устанавливаемые руководителем предприятия на законном основании (предприятием (фирмы) должны приниматься меры по их охране).
- методика отнесения тех или иных сведений к коммерческой тайне в нашей стране еще окончательно не разработана, поэтому ограничимся лишь некоторыми.
- к коммерческой тайне могут быть отнесены:
- технология производства; технологические приемы и оборудование;
- модификации ранее известных технологий и процессов;
- перспективные методы управления;
- ценовая и сбытовая политика;
- сравнительные характеристики собственного ассортимента и товаров конкурентов с точки зрения качества, внешнего вида, упаковки и т.д.;
- производственные, коммерческие и финансово-кредитные отношения с партнерами;
- планы предприятия по расширению (свертыванию) производств;
- факты проведения переговоров по вопросам купли-продажи;
- данные, которые могут быть использованы для нанесения ущерба репутации предприятия (фирмы);
- информация о кадрах (текучесть кадров, ведущие специалисты и места их работы по совместительству);
- сил и условий для защиты коммерческой тайны, а также другие сведения.

- в повседневной жизни коммерческая тайна всегда выступает в форме коммерческих секретов. Поскольку всякая тайна есть секрет, но не всякий секрет есть тайна.
- коммерческие секреты – форма проявления коммерческой тайны. Представляют собой сведения в виде документов, схем, изделий, относящиеся к коммерческой тайне фирмы и подлежащие защите со стороны службы безопасности от возможных посягательств путем похищения, выведывания, утечки информации.
- они различаются по следующим признакам:
- по природе коммерческой тайны (технологические, производственные, организационные, маркетинговые, интеллектуальные, рекламные)
- по принадлежности собственности (собственность предприятия, группы предприятий, отдельного лица, группы лиц);
- по назначению коммерческих секретов.

Носитель коммерческого секрета – лицо, осведомленное о коммерческих секретах предприятия или фирмы (руководители и допущенные к коммерческим секретам исполнители).

Носители коммерческих секретов следует отличать от источников закрытой коммерческой информации («ноу-хау», схемы, документы, технологии, изделия, образцы).

Секретность в условиях рыночного хозяйствования защищает производителя от недобросовестной конкуренции, к которой относятся различные противоправные действия в виде скрытого использования торговой марки, подделки продукции конкурента, обманной рекламы, подкупа, шантажа и т.п. Не последнее место в этом ряду занимает промышленный шпионаж.

Лицо, пожелавшее заняться предпринимательством, как правило, уже имеет определенные познания в избранной области, а в случае недостаточности может их получить из обширного ассортимента отечественной и зарубежной литературы. Предпринимательство тесно взаимосвязано с конкуренцией. Осуществление последней может принимать самые различные формы, в том числе и такие, как хищение или сбор чужой информации, которая носит общеизвестное название шпионаж. Об этой области деятельности у подавляющего большинства людей сложилось довольно стереотипное представление, основанное на художественной литературе, кино- и телефильмах. И не возникало необходимости в более глубоком изучении этого явления. Тем не менее подходы к такому общественному явлению,

как шпионаж, в условиях рыночной конкурентной деятельности резко меняются, ибо лицам, занимающимся предпринимательством, уже приходится, ибо лицам, занимающимся предпринимательством, уже приходится сталкиваться с этой проблемой. С одной стороны, они вынуждены защищать свои секреты (ценную информацию), а с другой — пытаться завладеть секретами конкурента, чтобы выжить в рыночном противоборстве. Цель данного раздела, хотя бы в очень краткой форме, изложить отдельные вопросы, характеризующие понятие шпионажа, его виды и способы осуществления и тем самым оказать практическое содействие лицам, прямо или косвенно причастным к предпринимательской деятельности.

ГЛАВА 2. Методы и средства построения систем информационной безопасности

В современном обществе информация является очень ценным ресурсом в любой деятельности человека. Поэтому каждое предприятие заинтересованно в своей информационной безопасности. Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Целью информационной безопасности является защита ценности системы, сохранить и гарантировать точность и целостность информации, а также минимизировать разрушения, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, в ходе которых информация создается, модифицируется, распространяется или, когда к ней обеспечивается доступ. Обеспечения информационной безопасности организации осуществляются на практике использованием различных механизмов защиты, для создания которых применяют следующие средства:

- - физические
- - аппаратные
- - программные
- - аппаратно-программные (технические)
- - криптографические
- - административные (организационные)
- - законодательные (правовые)
- - морально-этические

Физические средства защиты - это разного рода механические, электронно-механические устройства, специально предназначенные для образования физических препятствий на возможных путях проникновения и доступа возможных нарушителей к компонентам автоматической системы и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации. Физическая безопасность связана с введением мер защиты, которые защищают от стихийных бедствий, например, таких как пожар, наводнение, ураган, землетрясение.

Аппаратные средства защиты — это различные электронные, электромеханические устройства, прямо встроенные в блоки автоматизированной информационной системы или оформленные в виде автономных устройств и сопрягающиеся с этими блоками. Их задача внутренняя защита структурных элементов средств и систем вычислительной техники, например, процессоров, терминалов, периферийного оборудования. Реализуются это с помощью метода управления доступом (идентификация, аутентификация и проверка полномочий субъектов системы, регистрация, реагирование).

Программные средства защиты используются для выполнения логических и интеллектуальных функций защиты. Включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля. Программные средства защиты являются наиболее распространенным видом защиты, так как они универсальны, просты в использовании, имеется возможностью изменения и развития. Данное обстоятельство делает их и самыми уязвимыми элементами защиты информационной системы организации. В настоящее время создано большое количество операционных систем, систем управления базами данных, сетевых пакетов и пакетов прикладных программ, включающих разнообразные средства защиты информации.

Аппаратно-программные средства защиты представляют собой различные электронные устройства и специальные программы, входящие в состав автоматической системы предприятия и исполняющие самостоятельно или в комплексе с другими средствами, функции защиты верификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации).

Криптографический метод защиты информации, основанный на принципе ее шифрования. Криптографический метод может быть осуществлен как

программными, так и аппаратными средствами. Средство криптографической защиты информации осуществляет криптографическое перестройку информации для обеспечения ее безопасности. Криптографическая защита или криптографическое преобразование информации, шифрование является одним из важных способов защиты информации.

Административный метод защиты является методом организационного характера, регламентирующие процессы функционирования системы обработки данных, применением ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой так, чтобы в максимальной степени затруднить или исключить возможность реализации угроз безопасности или минимизировать размер потерь в случае их осуществления. Главная цель административных мер сформировать политику в области обеспечения безопасности информации и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые средства защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

К морально-этическим средствам относятся нормы поведения и правила обращения с информацией. Которые традиционно сложились или складываются по мере распространения электронно-вычислительных машин в обществе, стране. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты. Однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные, например, общепризнанные нормы честности, так и писаные, то есть оформленные в некоторый устав правил или предписаний. Морально-этические средства защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

Нужно сказать, что, на данном этапе общемирового развития, роль информационной среды очень велика. Информация является системообразующим фактором во всех этапах жизни общества, она все более активно влияет на состояние политической, экономической, оборонной, личной, имущественной и других составляющих безопасности. Поэтому, несмотря на то, что построение эффективной системы информационной безопасности является сложным и непрерывным процессом, этому нужно уделять значительное внимания. А именно оперировать данными методами, которые обеспечат информационную безопасность.

2.1. Методы и средства обеспечения безопасности информации

Методы и средства обеспечения безопасности информации в автоматизированных информационных технологиях представлены на рис.1. Приложение 1. К ним относятся: препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение. Методы защиты информации представляют собой основу механизмов защиты.

Препятствие — метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. д.).

Управление доступом — метод защиты информации с помощью использования всех ресурсов информационной технологии. Управление доступом включает следующие функции зашиты:

- идентификация специалистов, персонала и ресурсов информационной технологии (присвоение каждому объекту персонального идентификатора);
- опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;
- проверка полномочий (соответствие дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- разрешение и создание условий работы в пределах установленного регламента;
- регистрация (протоколирование) обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытке несанкционированных действий.

Маскировка — метод защиты информации путем ее криптографического закрытия. Этот метод сейчас широко применяется как при обработке, так и при хранении информации, в том числе на дискетах. При передаче информации по каналам связи большой протяженности данный метод является единственно надежным.

Регламентация — метод защиты информации, создающий по регламенту в информационных технологиях такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

Принуждение — метод защиты, когда специалисты и персонал информационной технологии вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение — метод защиты, побуждающий специалистов и персонал автоматизированной информационной технологии не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Рассмотренные методы обеспечения безопасности в информационных технологиях реализуются на практике за счет применения различных средств защиты.

Все средства защиты информации делятся на следующие виды:

Формальные средства защиты – это средства, выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека

Неформальные средства защиты – это средства защиты, которые определяются целенаправленной деятельностью человека, либо регламентируют эту деятельность.

К основным формальным средствам защиты, которые используются в информационных технологиях для создания механизмов защиты, относятся следующие:

Технические средства реализуются в виде электрических, электромеханических и электронных устройств. Все технические средства делятся на следующие виды:

Аппаратные, представляющие собой устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с подобной

аппаратурой по стандартному интерфейсу.

Физические, представляющие собой автономные устройства и системы, создающие физические препятствия для злоумышленников (замки, решетки, охранная сигнализация и т.д.)

Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций зашиты информации.

К основным неформальным средствам защиты относятся:

Организационные средства. Представляют собой организационно технические и организационно правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты информации в информационных технологиях. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла (строительство и оборудование помещений экономического объекта, проектирование информационной технологии, монтаж и наладка оборудования, испытания, эксплуатация и т. д.).

Морально-этические средства. Реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи. Эти нормы большей частью не являются обязательными как законодательные меры, однако несоблюдение их ведет к утечке информации и нарушению секретности.

Законодательные средства определяются законодательными актами страны, в которых регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушения этих правил.

2.2. Криптографические методы защиты информации

Готовое к передаче информационное сообщение, первоначально открытое и незащищенное, зашифровывается и тем самым преобразуется в шифрограмму, т. е. в закрытые текст или графическое изображение документа. В таком виде сообщение передается по каналу связи, даже и не защищенному.

Санкционированный пользователь после получения сообщения дешифрует его (т. е. раскрывает) посредством обратного преобразования криптограммы, вследствие чего получается исходный, открытый вид сообщения, доступный для восприятия санкционированным пользователям.

Методу преобразования в криптографической системе соответствует использование специального алгоритма. Действие такого алгоритма запускается уникальным числом (последовательностью бит), обычно называемым шифрующим ключом.

Для большинства систем схема генератора ключа может представлять собой набор инструкций и команд либо узел аппаратуры, либо компьютерную программу, либо все это вместе, но в любом случае процесс шифрования (дешифрования) реализуется только этим специальным ключом. Чтобы обмен зашифрованными данными проходил успешно, как отправителю, так и получателю, необходимо знать правильную ключевую установку и хранить ее в тайне.

Стойкость любой системы закрытой связи определяется степенью секретности используемого в ней ключа. Тем не менее, этот ключ должен быть известен другим пользователям сети, чтобы они могли свободно обмениваться зашифрованными сообщениями. В этом смысле криптографические системы также помогают решить проблему аутентификации (установления подлинности) принятой информации. Взломщик в случае перехвата сообщения будет иметь дело только с зашифрованным текстом, а истинный получатель, принимая сообщения, закрытые известным ему и отправителю ключом, будет надежно защищен от возможной дезинформации.

Современная криптография знает два типа криптографических алгоритмов: классические алгоритмы, основанные на использовании закрытых, секретных ключей, и новые алгоритмы с открытым ключом, в которых используются один открытый и один закрытый ключ (эти алгоритмы называются также асимметричными). Кроме того, существует возможность шифрования информации и более простым способом — с использованием генератора псевдослучайных чисел.

Использование генератора псевдослучайных чисел заключается в генерации гаммы шифра с помощью генератора псевдослучайных чисел при определенном ключе и наложении полученной гаммы на открытые данные обратимым способом.

Надежность шифрования с помощью генератора псевдослучайных чисел зависит как от характеристик генератора, так и, причем в большей степени, от алгоритма

получения гаммы.

Этот метод криптографической защиты реализуется достаточно легко и обеспечивает довольно высокую скорость шифрования, однако недостаточно стоек к дешифрованию и поэтому неприменим для таких серьезных информационных систем, каковыми являются, например, банковские системы.

Для классической криптографии характерно использование одной секретной единицы — ключа, который позволяет отправителю зашифровать сообщение, а получателю расшифровать его. В случае шифрования данных, хранимых на магнитных или иных носителях информации, ключ позволяет зашифровать информацию при записи на носитель и расшифровать при чтении с него.

Наиболее перспективными системами криптографической защиты данных сегодня считаются асимметричные криптосистемы, называемые также системами с открытым ключом. Их суть состоит в том, что ключ, используемый для зашифровывания, отличен от ключа расшифровывания. При этом ключ зашифровывания не секретен и может быть известен всем пользователям системы. Однако расшифровывание с помощью известного ключа зашифровывания невозможно. Для расшифровывания используется специальный, секретный ключ. Знание открытого ключа не позволяет определить ключ секретный. Таким образом, расшифровать сообщение может только его получатель, владеющий этим секретным ключом.

Известно несколько криптосистем с открытым ключом. Наиболее разработана на сегодня система RSA. Приложение 2.

RSA— это система коллективного пользования, в которой каждый из пользователей имеет свои ключи зашифровывания и расшифровывания данных, причем секретен только ключ расшифровывания.

Специалисты считают, что системы с открытым ключом больше подходят для шифрования передаваемых данных, чем для защиты данных, хранимых на носителях информации. Существует еще одна область применения этого алгоритма — цифровые подписи, подтверждающие подлинность передаваемых документов и сообщений.

Из изложенного следует, что надежная криптографическая система должна удовлетворять ряду определенных требований:

- процедуры зашифровывания и расшифровывания должны быть «прозрачны» для пользователя;
- дешифрование закрытой информации должно быть максимально затруднено;
- содержание передаваемой информации не должно сказываться на эффективности криптографического алгоритма.

Процессы защиты информации, шифрования и дешифрования связаны с кодируемыми объектами и процессами, их свойствами, особенностями перемещения. Такими объектами и процессами могут быть материальные объекты, ресурсы, товары, сообщения, блоки информации, транзакции (минимальные взаимодействия с базой данных по сети). Кодирование кроме целей защиты, повышая скорость доступа к данным, позволяет быстро определять и выходить на любой вид товара и продукции, страну-производителя и т.д. В единую логическую цепочку связываются операции, относящиеся к одной сделке, но географически разбросанные по сети.

Например, штриховое кодирование используется как разновидность автоматической идентификации элементов материальных потоков, например товаров, и применяется для контроля за их движением в реальном времени. Достигается оперативность управления потоками материалов и продукции, повышается эффективность управления предприятием. Штриховое кодирование позволяет не только защитить информацию, но и обеспечивает высокую скорость чтения и записи кодов. Наряду со штриховыми кодами в целях защиты информации используют голографические методы.

Методы защиты информации с использованием голографии являются актуальным и развивающимся направлением. Голография представляет собой раздел науки и техники, занимающийся изучением и созданием способов, устройств для записи и обработки волн различной природы. Оптическая голография основана на явлении интерференции волн. Интерференция волн наблюдается при распределении в пространстве волн и медленном пространственном распределении результирующей волны. Возникающая при интерференции волн картина содержит информацию об объекте. Если эту картину фиксировать на светочувствительной поверхности, то образуется голограмма. При облучении голограммы или ее участка опорной волной можно увидеть объемное трехмерное изображение объекта. Голография применима к волнам любой природы и в настоящее время находит все большее практическое применение для идентификации продукции различного назначения.

Технология применения кодов в современных условиях преследует цели защиты информации, сокращения трудозатрат и обеспечение быстроты ее обработки, экономии компьютерной памяти, формализованного описания данных на основе их систематизации и классификации.

В совокупности кодирование, шифрование и защита данных предотвращают искажения информационного отображения реальных производственно-хозяйственных процессов, движения материальных, финансовых и других потоков, а тем самым способствуют обоснованности формирования и принятия управленческих решений.

ЗАКЛЮЧЕНИЕ

Подводя итоги проведенного исследования, следует сделать следующие выводы.

Информатизация общества порождает проблемы информационной безопасности, главные из которых – проблема информационных войн и информационного терроризма. Они носят глобальный характер, но для России приобретают особую остроту, что обусловлено ее геополитическим и экономическим положением.

- Информационная безопасность государства - защита конституционного строя, суверенитета, территориальной целостности с использованием информационных средств. Жизненно важные интересы государства в информационной сфере:
- создание условий для реализации интересов личности и общества в информационной сфере;
- формирование институтов общественного контроля за органами государственной власти;
- безусловное обеспечение законности и правопорядка;
- создание условий для развития собственной информационной инфраструктуры;
- формирование системы подготовки и реализации решений органов государственной власти, обеспечивающих национальные интересы страны;
- защита государственной информационной системы и информационных ресурсов (в том числе защита государственной тайны);
- защита единого информационного пространства страны;
- развитие равноправного и взаимного международного сотрудничества.

Национальная безопасность РФ существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Под информационной безопасностью РФ понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. На основе национальных интересов РФ в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Угрозы информационной безопасности государства:

- размывание единого правового пространства страны из-за принятия субъектами РФ не соответствовавших Конституции РФ правовых актов;
- разрушение единого информационного пространства России;
- вытеснение российских информационных агентств и средств массовой информации с внутреннего информационного рынка;
- монополизация информационного рынка;
- блокирование деятельности государственных средств массовой информации по информированию российской, зарубежной аудитории;
- ослабление роли русского языка как государственного языка РФ;
- несанкционированное целенаправленное вмешательство и проникновение в деятельность и развитие информационных систем;

низкая эффективность информационного обеспечения государственной политики (дефицит кадров, отставание информационных систем от международных стандартов).

Угрозы информационной безопасности России подразделяются по общей направленности (угрозы конституционным правам и свободам граждан, духовной жизни общества, информационной структуре, информационным ресурсам) и по способам воздействия (собственно информационные, программно-математические, физические и организационные).

В современном обществе информационная безопасность является важнейшим компонентом национальной безопасности. От нее в значительной степени зависит уровень экономической, оборонной, социальной, политической и других видов безопасности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1.Белов Е.Б., Лось В.П., Мещеряков Р.В. Основы информационной безопасности: Учебное пособие. М.: Изд-во Горячая линия – Телеком, 2006. 544

2.Информационные системы в экономике: Учебник. / Под ред. Титоренко Г.А. 2-е изд. перераб. и доп. М.: Изд-во ЮНИТИ-ДАНА, 2008. 463 с.

3.Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие. М.: Изд-во Горячая линия – Телеком, 2004. 280 с.

4.Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. М.: Изд-во ДМК Пресс, 2004. 384 с.

5.Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие. М.: Изд-во Горячая линия – Телеком, 2005. 229 с.

6.Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учебное пособие. 2-е изд. М.: Издательско-торговая корпорация Дашков и К°, 2005. 336 с.

7.Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учебное пособие. М.: Изд-во ИНФРА-М, 2001. 304 с.

8.Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. Украина: Изд-во Юниор, 2003. 504 с.

9.Садердинов А. А., Трайнев В. А., Федулов А. А. Информационная безопасность предприятия: Учебное пособие. 2-е изд. М.: Издательско-торговая корпорация Дашков и К°, 2005.

10.Информационные системы в экономике: Учебник. / Под ред. Титоренко Г.А. 2-е изд., доп. и перераб. М.: Изд-во ЮНИТИ-ДАНА, 2008. 463 с.

11.Информационные системы в экономике: Учебник. / Под ред. Титоренко Г.А. 2-е изд. перераб. и доп. М.: Изд-во ЮНИТИ-ДАНА, 2008. с.218.

12.Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие. М.: Изд-во

Горячая линия – Телеком, 2004. с. 202.

13.Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учебное пособие. М.: Изд-во ИНФРА-М, 2001. с.23-24

14.Информационные системы в экономике: Учебник. / Под ред. Титоренко Г.А. 2-е изд.М.: Изд-во ЮНИТИ-ДАНА, 2008. с.219.

15.Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учебное пособие. М.: Изд-во ИНФРА-М, 2001. 304 с.

16.Белов Е. Б., Лось В. П., Мещеряков Р. В. Основы информационной безопасности: Учебное пособие. М.: Изд-во Горячая линия – Телеком, 2006. с.248

17.Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. Украина: Изд-во Юниор, 2003. с. 338.

18.Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие. М.: Изд-во Горячая линия – Телеком, 2005. с. 52.

19.Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. М.: Изд-во ДМК Пресс, 2004. с.7.

ПРИЛОЖЕНИЕ

Приложение 1

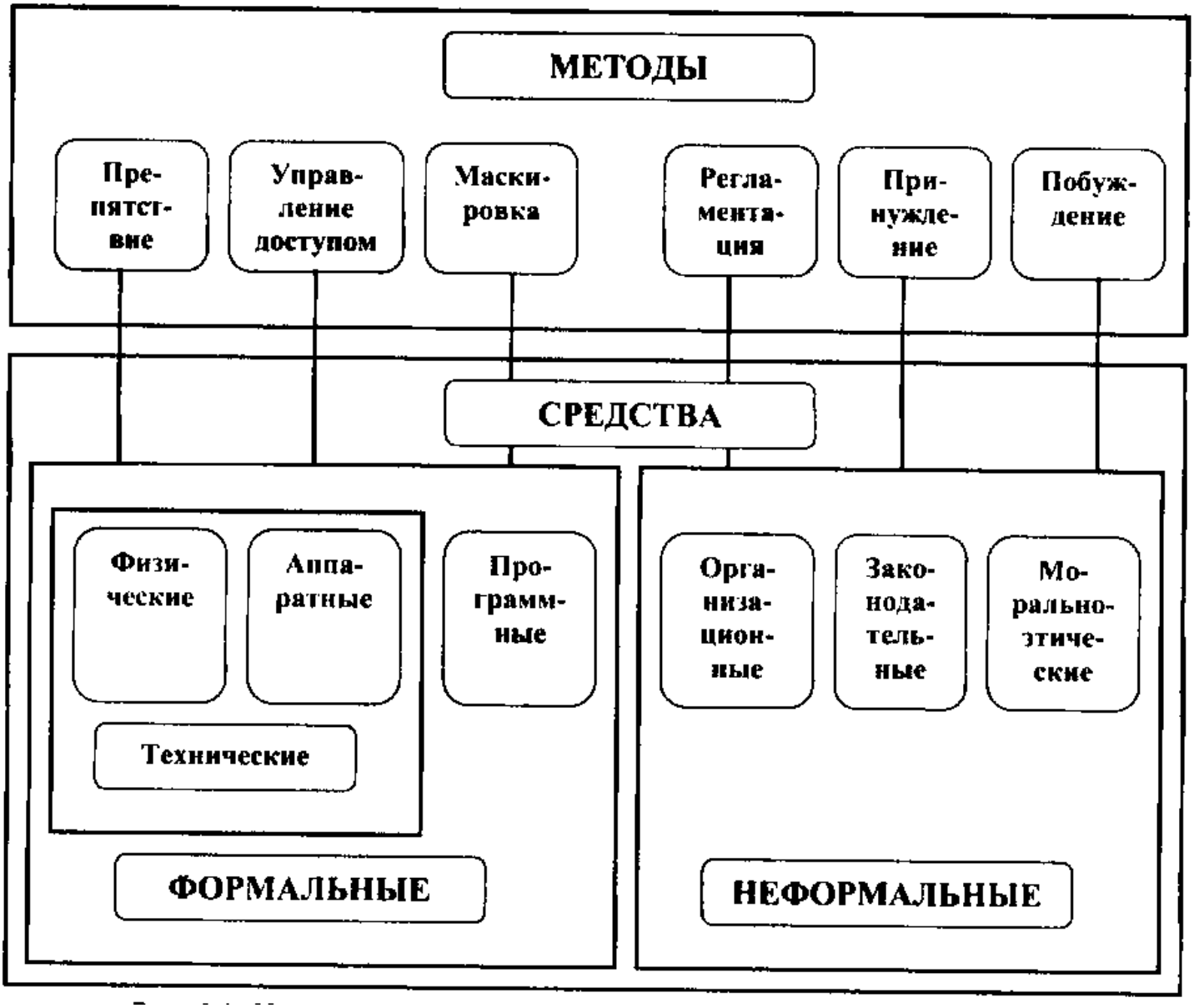

Рис.1 Методы и средства обеспечения безопасности информации

Приложение 2

Шаг первый. Подготовка ключей

Я должен проделать предварительные действия: сгенерировать публичный и приватный ключ.

Выбираю два простых числа. Пусть это будет p=3 и q=7.

Вычисляем модуль — произведение наших p и q: $n=p\times q=3\times 7=21$.

Вычисляем функцию Эйлера: $\varphi=(p-1)\times(q-1)=2\times 6=12$.

Выбираем число e, отвечающее следующим критериям: (i) оно должно быть простое, (ii) оно должно быть меньше φ — остаются варианты: 3, 5, 7, 11, (iii) оно должно быть взаимно простое с φ; остаются варианты 5, 7, 11. Выберем e=5. Это, так называемая, открытая экспонента. Теперь пара чисел {e, n} — это мой открытый ключ. Я отправляю его вам, чтобы вы зашифровали своё сообщение. Но для меня это ещё не всё. Я должен получить закрытый ключ.

Мне нужно вычислить число d, обратное e по модулю φ. То есть остаток от деления по модулю φ произведения d×e должен быть равен 1. Запишем это в обозначениях, принятых во многих языках программирования: (d×e)%φ=1. Или (d×5)%12=1. d может быть равно 5 ((5×5)%12=25%12=1), но чтобы оно не путалось с e в дальнейшем повествовании, давайте возьмём его равным 17. Можете проверить сами, что (17×5)%12 действительно равно 1 (17×5-12×7=1). Итак d=17. Пара {d, n} — это секретный ключ, его я оставляю у себя. Его нельзя сообщать никому. Только обладатель секретного ключа может расшифровать то, что было зашифровано открытым ключом.

Шаг второй. Шифрование

Теперь пришла ваша очередь шифровать ваше сообщение. Допустим, ваше сообщение это число 19. Обозначим его P=19. Кроме него у вас уже есть мой открытый ключ: {e, n} = {5, 21}. Шифрование выполняется по следующему алгоритму:

Возводите ваше сообщение в степень e по модулю n. То есть, вычисляете 19 в степени 5 (2476099) и берёте остаток от деления на 21. Получается 10 — это ваши закодированные данные.

Строго говоря, вам вовсе незачем вычислять огромное число «19 в степени 5». При каждом умножении достаточно вычислять не полное произведение, а только остаток от деления на 21. Но это уже детали реализации вычислений, давайте не будем в них углубляться.

Полученные данные E=10, вы отправляете мне.

Здесь надо заметить, что сообщение P=19 не должно быть больше n=21. иначе ничего не получится.

Шаг третий. Расшифровка

Я получил ваши данные (E=10), и у меня имеется закрытый ключ {d, n} = {17, 21}.

Обратите внимание на то, что открытый ключ не может расшифровать сообщение. А закрытый ключ я никому не говорил. В этом вся прелесть асимметричного шифрования.

Начинаем раскодировать:

Я делаю операцию, очень похожую на вашу, но вместо e использую d. Возвожу E в степень d: получаю 10 в степень 17 (позвольте, я не буду писать единичку с семнадцатью нулями). Вычисляю остаток от деления на 21 и получаю 19 — ваше сообщение.

Заметьте, никто, кроме меня (даже вы!) не может расшифровать ваше сообщение (E=10), так как ни у кого нет закрытого ключа.