СОДЕРЖАНИЕ

Введение

Обоснование темы диссертационной работы и ее актуальность.

Развитие информационно-коммуникационных технологий (ИКТ) является одним из основных факторов благосостояния и экономического роста страны. Сегодня ИКТ становится одним из основных приоритетов государственной политики Узбекистана [1].

В Постановлении Президента Республики Узбекистан "О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий. (Собрание законодательства Республики Узбекистан, 2012 г., № 13, ст. 139) одной из основных задачи дальнейшего внедрения и развития информационно-коммуникационных технологий, в частности, является программа мер по коренному и качественному улучшению функционирования национальной информационно-поисковой системы, увеличению количества ее пользователей [2].

Для того чтобы осуществить дестабилизирующее воздействие на конфиденциальную информацию, людям, не имеющим разрешенного доступа к ней, необходимо его получить. Такой доступ называется несанкционированным. Как правило, несанкционированный доступ бывает преднамеренным и имеет целью оказать сознательное дестабилизирующее воздействие на конфиденциальную информацию. Несанкционированный доступ, даже преднамеренный, не всегда является противоправным. Чаще всего он, конечно, бывает незаконным, но нередко не носит криминального характера. Несанкционированный доступ осуществляется через существующий или специально создаваемый канал доступа, который определяется как путь, используя который, можно получить неразрешенный доступ к конфиденциальной информации. Масштабы и сферы применения этой техники стали таковы, что наряду с проблемами надежности и устойчивости ее функционирования возникает проблема обеспечения безопасности циркулирующей в ней информации. При этом считается, что причиной этих событий могут быть случайные воздействия либо воздействия

в результате преднамеренного несанкционированного доступа человека-нарушителя (злоумышленника).

Началом работы по построению системы защиты информации от несанкционированного доступа в любой организации начинается с разработки концепции. Ключевыми моментами в разработке концепции являются четкость и ясность постановки задачи. В первую очередь это касается определений объекта и предмета защиты, а также потенциальных угроз.

Исходя из всего вышесказанного, можно сделать вывод об актуальности выбранной темы диссертационной работы.

Объектом исследования являются компьютерные системы и сети, системы защиты информации.

Предметом исследования являются информационные ресурсы. Это понятие имеет множественный характер и представляет собой множество предметов защиты. Границы этого множества никем и ничем не определены и устанавливаются разработчиком информационной системы по своему усмотрению с учетом рекомендаций специалистов.

Методы исследования. Для решения поставленных исследовательских задач в работе использовались подходы к созданию системы защиты информации от несанкционированного доступа, теории чисел, математического моделирования, дискретной математики и вероятности.

Публикация. По теме диссертации опубликована 2 работа.

Цель диссертационной работы является исследование системы защиты информации от несанкционированного доступа в информационно-коммуникационных системах.

Для достижения поставленной цели **необходимо решить** следующие задачи:

1. Анализировать средств обеспечения защиты информации от несанкционированного доступа.

2. Разработать подход к созданию системы защиты информации от несанкционированного доступа к информационно-коммуникационных системах.

3. Построить методики системы защиты информации от несанкционированного доступа.

4. Построить моделей системы защиты информации от несанкционированного доступа.

5. Разработать методического обеспечения защиты автоматизированных систем от несанкционированного доступа.

6. Разработать программное средство защиты информации от несанкционированного доступа в информационно-коммуникационных системах.

Краткий анализ литературы по теме диссертации.

Основные вопросы в области системы защиты информации от несанкционированного доступа освещаются в работах ученых А.Ю. Щеглова, А.В. Василькова, И.А. Василькова и Форристала и др., а также зарубежных K. Thomson, P. Stephenson. В результате предлагаются канали и методы несанкционированного доступа к информации, способов и средств защиты информации от несанкционированного доступа в ИКС, а также приведено разложение числа на простые множители, которая в математике известна как “проблема дискретного логарифма”.

Научная новизна. В результате выполнения диссертационной работы получены следующие новые научные результаты:

1. Предложен подход к созданию системы защиты информации от несанкционированного доступа в информационно-коммуникационных системах.

2. Разработаны методического обеспечения защиты автоматизированных систем от несанкционированного доступа.

Практическая значимость исследования заключается в том, что его результаты могут быть использованы в системе сертификации программных

систем защиты информации для повышения оперативности внедрения новых версии сертифицированных программных системах защиты информации от несанкционированного доступа в информационно-коммуникационных системах.

Структура диссертационной работы

Диссертационная работа состоит из введения, трех глав, заключения, списка использованной литературы и приложений.

Во введении обосновываются особенность и важность данной задачи, ставится цель, указываются объекты исследования.

В первом главе были анализированы потенциальные угрозы безопасности информации и концепции защиты от несанкционированного доступа к информации. Рассмотрены каналы и методы несанкционированного доступа к конфиденциальной информации, позволяющей предусматривать перекрытие всех потенциально существующих для конкретного предприятия каналов. Исследованы средств защиты информации от несанкционированного доступа в ИКС.

Во второй главе предложена методика системы защиты информации от несанкционированного доступа, позволяющая решить ряд задач перспективного стратегического развития организации. Построены моделей системы защиты информации от несанкционированного доступа, перекрывающих определенное количество возможных каналов несанкционированного доступа в соответствии с ожидаемым классом потенциальных нарушителей. Разработано методическое обеспечение защиты автоматизированных систем от несанкционированного доступа, которое идентифицируется с учетом определенных критериев и признаков соответствующих программных средств защиты информации. Была проанализирована оценка уровня безопасности информации от преднамеренней несанкционированного доступа.

Третья глава посвящена вопросам разработки программное средство защиты информации от несанкционированного доступа на базе алгоритма

шифрования методом открытого ключа, позволяющее обеспечить защищенности информации от несанкционированного доступа в информационно-коммуникационных системах.

В заключении приведены основные выводы глав диссертационной работы.

В приложениях приведен материал, дополняющий и поясняющий основной текст диссертационной работы.

Глава I. Анализ угроз и методов обеспечения безопасности информации в информационно-коммуникационные системы

1. Потенциальные угрозы безопасности информационных систем

Исследование и анализ многочисленных случаев воздействий на информацию и несанкционированного доступа к ней показывают, что их можно разделить на *случайные* и *преднамеренные.* Преднамеренные угрозы часто путем их систематического применения могут быть приведены в исполнение через случайные путем долговременной массированной атаки несанкционированными запросами или вирусами.

Последствия, к которым приводит реализация угроз:

- ***разрушение*** (утрата) информации;
- ***модификация*** (изменение информации на ложную, которая корректна по форме и содержанию, но имеет другой смысл);
- ***ознакомление*** с ней посторонних лиц.

Цена указанных событий может быть самой различной: от невинных недоразумений до сотен тысяч долларов и более.

Предупреждение приведенных последствий в информационной системе и есть основная цель создания системы безопасности информации.

Для создания средств защиты информации необходимо определить природу угроз, формы и пути их возможного проявления и осуществления в информационной системе. Для решения поставленной задачи все многообразие угроз и путей их воздействия приведем к простейшим видам и формам, которые были бы адекватны их множеству в информационной системе.

Случайные угрозы

Информация в процессе ввода, хранения, обработки, вывода и передачи подвергается различным случайным воздействиям[3]. В результате таких воздействий на аппаратном уровне происходят физические изменения уровней сигналов в цифровых кодах, несущих информацию.

При этом наблюдаются в одном или двух, трех и т. д. разрядах изменения 1 на 0 или 0 на 1, или то и другое вместе, но в разных разрядах, следствием этого в итоге является изменение значения кода на другое. Далее, если применяемые для этой цели средства функционального контроля способны обнаружить эти изменения (например, контроль по модулю 2 легко обнаруживает однократную ошибку), производится браковка данного кода, а устройство, блок, модуль или микросхема, участвующие в обработке, объявляются неисправными. Если функциональный контроль отсутствует или не способен обнаружить неисправность на данном этапе обработки, процесс обработки продолжается по ложному пути, т. е. происходит модификация информации. В процессе дальнейшей обработки в зависимости от содержания и назначения ложной команды возможна либо пересылка информации по ложному адресу, либо передача ложной информации адресату, либо стирание или запись другой информации в оперативном запоминающем устройстве или дистанционном запоминающем устройстве (внешнем), т. е. возникают нежелательные события: разрушение (утрата), модификация и утечка информации.

На программном уровне в результате случайных воздействий может произойти изменение алгоритма обработки информации на непредусмотренный, характер которого тоже может быть различным: в лучшем случае — остановка информационного или вычислительного процесса, а в худшем — его модификация. Если средства функционального контроля ее не обнаруживают, последствия модификации алгоритма или данных могут пройти незамеченными или привести также к разрушению информации, а при перепутывании адреса устройства — к утечке информации.

При программных ошибках могут подключаться программы ввода-вывода и передачи их на запрещенные устройства.

Причинами случайных воздействий при эксплуатации автоматизированной системы могут быть:

- отказы и сбои аппаратуры;
- помехи на линиях связи от воздействий внешней среды;
- ошибки человека как звена системы;
- схемные и системотехнические ошибки разработчиков;
- структурные, алгоритмические и программные ошибки;
- аварийные ситуации и другие воздействия.

Частота отказов и сбоев аппаратуры увеличивается при выборе и проектировании системы, слабой в отношении надежности функционирования аппаратуры. Помехи на линиях связи зависят от правильности выбора места размещения технических средств информационной системы относительно друг друга и по отношению к аппаратуре и агрегатам соседних систем.

При разработке сложных автоматизированных систем увеличивается число схемных, системотехнических, структурных, алгоритмических и программных ошибок. На их количество в процессе проектирования оказывает большое влияние много других факторов: квалификация разработчиков, условия их работы, наличие опыта и др.

На этапах изготовления и испытаний на качество входящей в информационную систему аппаратуры влияют полнота и качество документации, по которой ее изготавливают, технологическая дисциплина и другие факторы.

К ошибкам человека как звена системы следует относить ошибки человека как источника информации, человека-оператора, неправильные действия обслуживающего персонала и ошибки человека как звена, принимающего решения.

Ошибки человека могут подразделяться на ***логические*** (неправильно принятые решения), ***сенсорные*** (неправильное восприятие оператором информации) и ***оперативные,*** или ***моторные*** (неправильная реализация решения). Интенсивность ошибок человека может колебаться в широких

пределах: от 1—2 % до 15—40 % и выше общего числа операций, выполняемых при решении задачи.

Для расчета достоверности выходной информации важны статистические данные по уровню ошибок человека как звена системы. Интенсивность ошибок человека-оператора составляет $2 \cdot 10^{-2}$—$4 \cdot 10^{-3}$. Количество ошибок при работе человека-оператора, точнее, вероятность ошибок зависит от общего количества кнопок, количества кнопок в ряду, числа кнопок, которые необходимо нажимать одновременно, и расстояния между краями кнопок.

Немаловажное значение имеют также ошибки человека как звена системы, принимающего решение[4]. Особенно важное значение проблема борьбы с ошибками такого рода приобретает в автоматизированных информационных системах управления административного типа. Ошибки человека как звена системы, принимающего решение, определяются неполной адекватностью представления человеком реальной ситуации и свойством человека с заранее определенной установкой действовать по ранее намеченной программе. Например, руководитель, будучи заранее уверен, что мастер завысил требуемое количество дефицитного материала, уменьшает соответствующую заявку и тем самым вводит в систему ошибочные данные.

Другой важной особенностью человека является стремление к построению упрощенной модели рассматриваемой ситуации. Неверное упрощение конкретной ситуации, исключение из нее важных моментов и принятое при этом решение могут оказаться ошибочными.

К угрозам случайного характера следует также отнести аварийные ситуации, которые могут возникнуть на объекте размещения автоматизированной информационной системы. К аварийным ситуациям относятся:

- отказ функционирования информационной системы в целом, например выход из строя электропитания и освещения;

- стихийные бедствия: пожар, наводнение, землетрясение, ураганы, удары молнии, обвалы и т. д.;
- отказ системы жизнеобеспечения на объекте эксплуатации информационной системы.

Преднамеренные угрозы

Преднамеренные угрозы связаны с различными действиями человека, причинами которых может быть достаточно большой спектр его состояний: определенное недовольство своей жизненной ситуацией, сугубо материальный интерес или простое развлечение с самоутверждением своих способностей и т. д. Для постановки более конкретной задачи проанализируем объект защиты информации на предмет ввода-вывода, хранения и обработки информации и возможностей нарушителя по доступу к информации при отсутствии средств защиты в данной автоматизированной системе.

В качестве объекта защиты согласно классификации выбираем компьютерную систему, которая может быть элементом компьютерной сети или большой автоматизированной системы управления. Для компьютерных систем в этом случае характерны следующие штатные (законные) каналы доступа к информации:

- терминалы (рабочие станции, персональные компьютеры) пользователей;
- терминал (сервер или специализированная рабочая станция) администратора системы;
- терминал (рабочая станция) оператора функционального контроля;
- средства отображения информации;
- средства документирования информации;
- средства загрузки программного обеспечения в компьютерный комплекс;

- носители информации (оперативное запоминающее устройство, дистанционное запоминающее устройство, устройство резервирования и архивирования, бумажные носители);
- внешние каналы связи.

Имея в виду, что при отсутствии защиты нарушитель может воспользоваться как штатными, так и другими физическими каналами доступа, назовем возможные каналы несанкционированного доступа (ВКНСД) в компьютерной системе, через которые возможно получить доступ к аппаратуре, программному обеспечению и осуществить хищение, разрушение, модификацию информации и ознакомление с нею:

- все перечисленные выше штатные средства при их использовании законными пользователями не по назначению и за пределами своих полномочий;
- все перечисленные выше штатные средства при их использовании посторонними лицами;
- технологические пульты управления;
- внутренний монтаж аппаратуры;
- линии связи между аппаратными средствами данной компьютерной системы;
- побочное электромагнитное излучение информации с аппаратуры системы;
- побочные наводки информации по сети электропитания и заземления аппаратуры;
- побочные наводки информации на вспомогательных и посторонних коммуникациях;
- отходы обработки информации в виде бумажных, магнитных и лазерных носителей, брошенные в мусорную корзину.

Для наглядности на рис.1 представлены типового объекта автоматизированной обработки информации с централизованной обработкой

данных и потенциальные каналы несанкционированного доступа к информации. Обозначения на рис.1.:

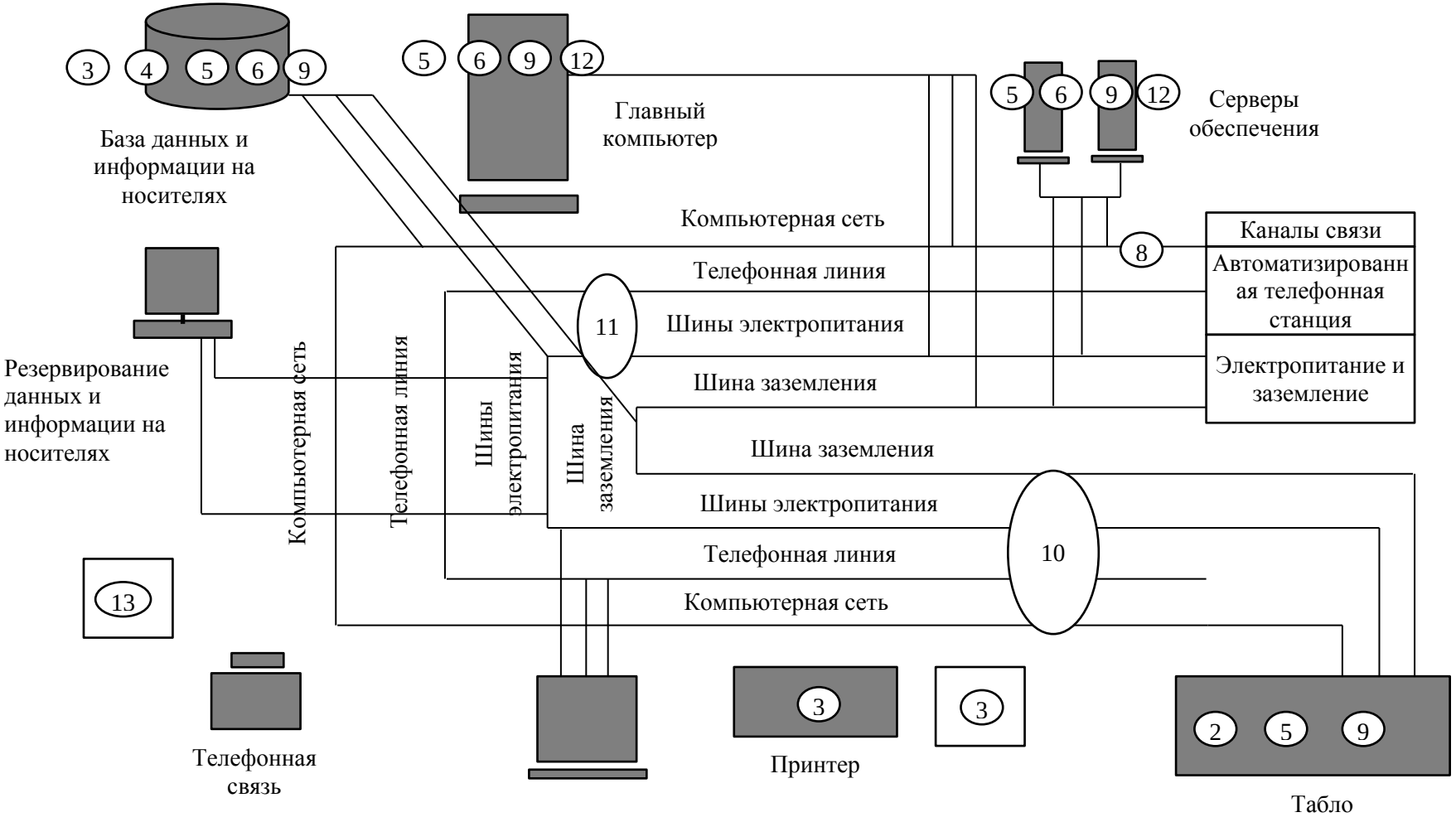


Рис.1 Состав типовой аппаратуры автоматизированной системы обработки информации и данных и возможные каналы несанкционированного доступа к информации

1. — несанкционированный доступ к терминалам и персональным компьютерам;
2. — несанкционированный доступ к средствам отображения информации;
3. — несанкционированный доступ к носителям информации;
4. — несанкционированный доступ к средствам загрузки программного обеспечения;
5. — несанкционированный доступ к информации при ремонте и профилактике аппаратуры;
6. — несанкционированный доступ к внутреннему монтажу аппаратуры;
7. — несанкционированный доступ к линиям связи;
8. — несанкционированный доступ к каналам связи;
9. — несанкционированный доступ к информации за счет побочного электромагнитного излучения информации;
10. — несанкционированный доступ к информации за счет наводок на цепях электропитания и заземления;
11. — несанкционированный доступ к информации за счет наводок на цепях вспомогательной и посторонней аппаратуры;
12. — несанкционированный доступ к технологическим пультам;
13. — доступ к отходам носителей информации.

Очевидно, что при отсутствии законного пользователя, контроля и разграничения доступа к терминалу квалифицированный нарушитель легко воспользуется его функциональными возможностями для несанкционированного доступа к информации путем ввода соответствующих запросов или команд. При наличии свободного доступа в помещения можно визуально наблюдать информацию на средствах отображения и документирования, а на последних похитить бумажный носитель, снять лишнюю копию, а также похитить другие носители с информацией: листинги, магнитные ленты, диски, флэш-носители и т. д. Особую опасность представляет собой бесконтрольная загрузка программного обеспечения в компьютер, в котором могут быть изменены данные, алгоритмы или введена

программа «троянский конь» — программа, выполняющая дополнительные незаконные функции: запись информации на посторонний носитель, передачу в каналы связи другого абонента компьютерной сети, внесение в систему компьютерного вируса и т. д. При отсутствии разграничения и контроля доступа к технологической и оперативной информации возможен доступ к оперативной информации со стороны терминала функционального контроля. Опасной является ситуация, когда нарушителем является пользователь компьютерной системы, который по своим функциональным обязанностям имеет законный доступ к одной части информации, а обращается к другой за пределами своих полномочий.

Со стороны законного пользователя существует много способов нарушать работу информационной системы, злоупотреблять ею, извлекать, модифицировать или уничтожать информацию. Для этой цели могут быть использованы привилегированные команды ввода-вывода, отсутствие контроля законности запроса и обращений к адресам памяти запоминающих устройств и т. д. При неоднозначной идентификации ресурсов нарушитель может подавить системную библиотеку своей библиотекой, а модуль, загружаемый из его библиотеки, может быть введен в супервизор- ном режиме. Свободный доступ позволит ему обращаться к чужим файлам и банкам данных и изменить их случайно или преднамеренно.

При техническом обслуживании (профилактике и ремонте) аппаратуры могут быть обнаружены остатки информации на магнитной ленте или дисках, поверхностях дисков и других носителях информации. Стирание информации обычными методами при этом не всегда эффективно. Ее остатки могут быть легко прочитаны. При транспортировании носителя по неохраняемой территории существует опасность его перехвата и последующего ознакомления посторонних лиц с секретной информацией.

Не имеет смысла создание системы контроля и разграничения доступа к информации на программном уровне, если не контролируется доступ к

пульту управления компьютера, внутреннему монтажу аппаратуры, кабельным соединениям.

Нарушитель может стать незаконным пользователем системы в режиме разделения времени, определив порядок работы законного пользователя либо работая вслед за ним по одним и тем же линиям связи. Он может также использовать метод проб и ошибок и реализовать «дыры» в операционной системе, прочитать пароли. Без знания паролей он может осуществить «селективное» включение в линию связи между терминалом и головным компьютером (сервером); без прерывания работы законного пользователя может продлить ее от его имени, аннулировав сигналы отключения законного пользователя.

Процессы обработки, передачи и хранения информации аппаратными средствами автоматизированной системы обеспечиваются срабатыванием логических элементов, построенных на базе полупроводниковых приборов, выполненных чаще всего в виде интегральных схем.

Срабатывание логических элементов обусловлено высокочастотным изменением уровней напряжений и токов, что приводит к возникновению в эфире, цепях питания и заземления, а также в параллельно расположенных цепях и индуктивностях посторонней аппаратуры электромагнитных полей и наводок, несущих в амплитуде, фазе и частоте своих колебаний признаки обрабатываемой информации. Использование нарушителем различных приемников может привести к их приему и утечке информации. С уменьшением расстояния между приемником нарушителя и аппаратными средствами вероятность приема сигналов такого рода увеличивается.

Непосредственное подключение нарушителем приемной аппаратуры и специальных датчиков к цепям электропитания и заземления, к каналам связи также позволяет совершить несанкционированное ознакомление с информацией, а несанкционированное подключение к каналам связи передающей аппаратуры может привести и к модификации информации.

Особо следует остановиться на угрозах, которым могут подвергаться каналы и линии связи компьютерной сети.

Предположено, что нарушитель может располагаться в некоторой точке сети, через которую должна проходить вся интересующая его информация. Например, в межсетевых условиях нарушитель может принять вид шлюза в некоторой промежуточной сети, которая обеспечивает единственный путь соединения между двумя процессами, являющимися концами интересующего нарушителя соединения, как показано на рис. 2. В этом случае, несмотря на то, что сеть-источник (А) и сеть-адресат (Г) защищены, нарушитель может воздействовать на соединение, так как оно проходит через шлюз, соединяющий сети Б и В. В общем случае предполагается, что нарушитель может занимать позицию, позволяющую осуществлять пассивный и активный перехват.

В случае ***пассивного перехвата*** нарушитель только следит за сообщениями, передаваемыми по соединению, без вмешательства в их поток. Наблюдение нарушителя за данными (прикладного уровня) в сообщении позволяет раскрыть ***содержание сообщений.*** Нарушитель может также следить за заголовками сообщений, даже если данные не понятны ему, с целью определения места размещения и идентификаторов процессов, участвующих в передаче данных. Нарушитель может определить длины сообщений и частоту их передачи для определения характера передаваемых данных, т. е. провести ***анализ потока сообщений.***

Нарушитель может также заниматься ***активным перехватом,*** выполняя множество действий над сообщениями, передаваемыми по соединению. Эти сообщения могут быть выборочно изменены, уничтожены, задержаны, переупорядочены, сдублированы и введены в соединение в более поздний момент времени. Нарушитель может создавать поддельные сообщения и вводить их в соединение.

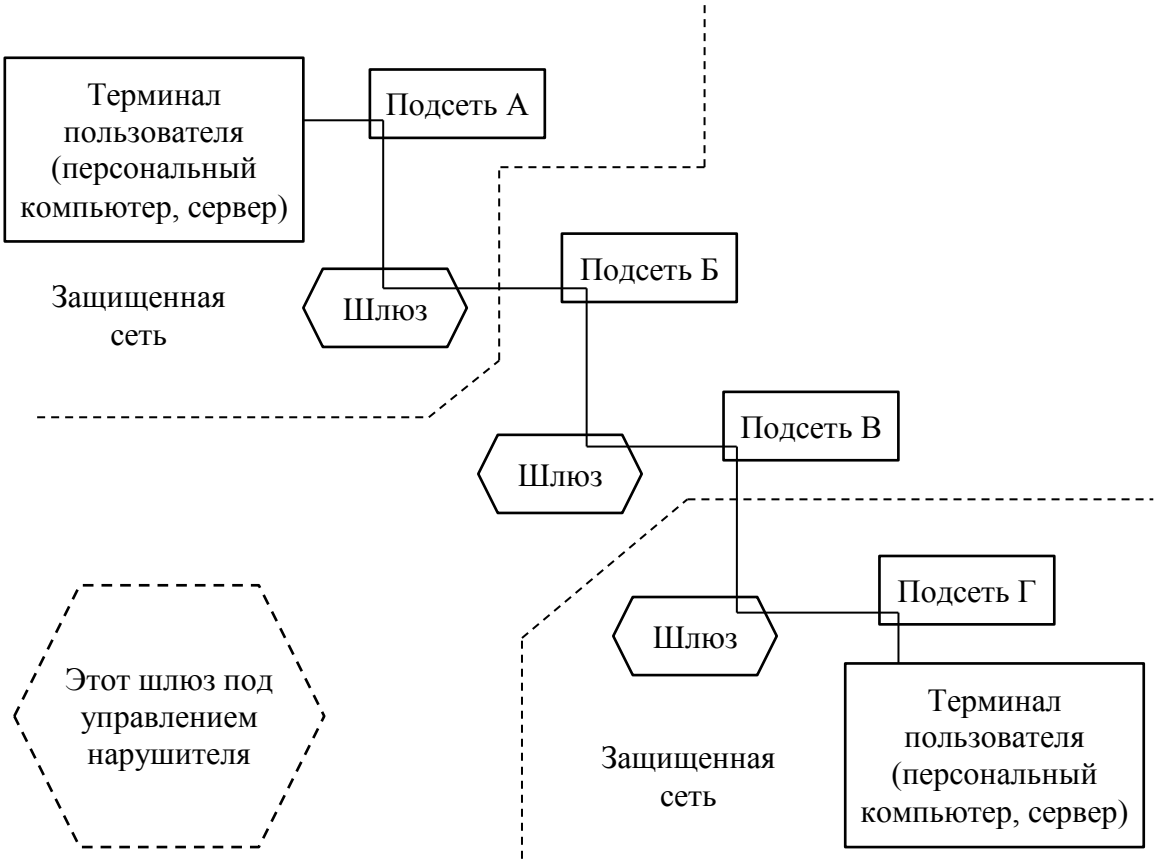


Рис.2 Схема возможного подключения нарушителя к компьютерной сети

соединение

Подобные действия можно определить как ***изменение потока и содержания сообщений.***

Кроме того, нарушитель может сбрасывать все сообщения или задерживать их. Подобные действия можно классифицировать как ***прерывание передачи сообщений.***

Попытки использования записи предыдущих последовательностей сообщений по инициированию соединений классифицируются как ***инициирование ложного соединения.***

Сформулируем пять основных категорий угроз безопасности информации и данных в компьютерных сетях:

1) раскрытие содержания передаваемых сообщений;

2) анализ трафика, позволяющий определить принадлежность отправителя и получателя данных к одной из групп пользователей сети, связанных общей задачей;

3) изменение потока сообщений, что может привести к нарушению режима работы какого-либо объекта, управляемого с удаленного компьютера;

4) неправомерный отказ в предоставлении услуг;

5) несанкционированное установление соединения.

Данная классификация не противоречит определению термина «безопасность информации» и делению потенциальных угроз на утечку, модификацию и утрату информации.

Угрозы 1 и 2 можно отнести к утечке информации, угрозы 3 и 5 — к ее модификации, а угрозу 4 — к нарушению процесса обмена информацией, т. е. к ее потере для получателя.

В компьютерных сетях нарушитель может применять следующие стратегии:

1) получить несанкционированный доступ к секретной информации;

2) выдать себя за другого пользователя, чтобы снять с себя ответственность или же использовать его полномочия с целью формирования ложной информации, изменения законной информации, применения ложного удостоверения личности, санкционирования ложных обменов информацией или же их подтверждения;

3) отказаться от факта формирования переданной информации;

4) утверждать о том, что информация получена от некоторого пользователя, хотя на самом деле она сформирована самим же нарушителем;

5) утверждать то, что получателю в определенный момент времени была послана информация, которая на самом деле не посылалась (или посылалась в другой момент времени);

6) отказаться от факта получения информации, которая на самом деле была получена, или утверждать о другом времени ее получения;

7) незаконно расширить свои полномочия по доступу к информации и ее обработке;

8) незаконно изменить полномочия других пользователей (расширить или ограничить, вывести или ввести других лиц);

9) скрыть факт наличия некоторой информации в другой информации (скрытая передача одной в содержании другой информации);

10) подключиться к линии связи между другими пользователями в качестве активного ретранслятора;

11) изучить, кто, когда и к какой информации получает доступ (даже если сама информация остается недоступной);

12) заявить о сомнительности протокола обеспечения информацией из-за раскрытия некоторой информации, которая согласно условиям протокола должна оставаться секретной;

13) модифицировать программное обеспечение путем исключения или добавления новых функций;

14) преднамеренно изменить протокол обмена информацией с целью его нарушения или подрыва доверия к нему;

15) помешать обмену сообщениями между другими пользователями путем введения помех с целью нарушения аутентификации сообщений[5].

Анализ последних возможных стратегий нарушителя в компьютерных сетях говорит о том, насколько важно знать, кого считать нарушителем. При этом в качестве нарушителя рассматривается не только постороннее лицо, но и законный пользователь. По-видимому, эти задачи следует рассматривать отдельно. С этих позиций приведенные выше пять видов угроз характерны для поведения постороннего нарушителя. Тогда из числа последних угроз можно отнести к пяти упомянутым выше видам следующие угрозы: 1, 10, 11, 15.

Анализ остальных угроз свидетельствует о том, что задачу защиты от них можно условно разделить на задачи двух уровней: пользователей и элементов сети, с которыми работают пользователи сети. К уровню элемента сети можно отнести угрозы под номерами 2, 7, 8, 13 и 14. Уровень взаимоотношений пользователей называется уровнем доверия одного

пользователя другому. Для обеспечения гарантий этого доверия, очевидно, потребуются специальные средства и критерии оценки их эффективности.

2. Концепция защиты от несанкционированного доступа к информации

Идейной основой набора руководящих документов является "Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации". Концепция излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от несанкционированного доступа (НСД), являющейся частью общей проблемы безопасности информации.

В концепции различаются понятия средств вычислительной техники (СВТ) и автоматизированной системы (АС), аналогично тому, как в Европейских Критериях проводится деление на продукты и системы.

Концепция предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в проблеме защиты информации от несанкционированного доступа. Это – направление, связанное со средствами вычислительной техники, и направление, связанное с автоматизированными системами.

Отличие двух направлений порождено тем, что средства вычислительной техники разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные автоматизированные системы, и поэтому, не решая прикладных задач, средства вычислительной техники не содержат пользовательской информации.

Пользовательской информации при создании автоматизированных систем появляются такие отсутствующие при разработке средств вычислительной техники характеристики автоматизированных систем, как полномочия пользователей, модель нарушителя, технология обработки

информации.

Существуют различные способы покушения на информационную безопасность – радиотехнические, акустические, программные и т.п. Среди них несанкционированный доступ выделяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средств вычислительной техники или автоматизированных систем. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

В концепции формулируются следующие основные принципы защиты от несанкционированного доступа к информации:

1. Защита средств вычислительной техники обеспечивается комплексом программно-технических средств.
2. Защита автоматизированных систем обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.
3. Защита автоматизированных систем должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики автоматизированных систем (надежность, быстродействие, возможность изменения конфигурации автоматизированных систем).

Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

Защита автоматизированных систем должна предусматривать контроль

эффективности средств защиты от несанкционированного доступа. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем автоматизированных систем или контролирующими органами.

Концепция ориентируется на физически защищенную среду, проникновение в которую посторонних лиц считается невозможным, поэтому нарушитель определяется как субъект, имеющий доступ к работе со штатными средствами автоматизированных систем и средствами вычислительной техники как части автоматизированных систем[6].

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами автоматизированных систем и средствами вычислительной техники. Выделяется четыре уровня этих возможностей.

Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

1. Первый уровень определяет самый низкий уровень возможностей ведения диалога в автоматизированных системах – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

2. Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

3. Третий уровень определяется возможностью управления функционированием автоматизированных систем, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию её оборудования.

4. Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств автоматизированных систем, вплоть до включения в состав средств вычислительной техники, собственных технических средств с новыми функциями по обработке информации.

В своем уровне нарушитель является специалистом высшей квалификации, знает все об автоматизированных системах и, в частности, о системе и средствах ее защиты[7].

В качестве главного средства защиты от несанкционированного доступа к информации в Концепции рассматривается система разграничения доступа (СРД) субъектов к объектам доступа. Основными функциями системы разграничения доступа являются:

- реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;
- реализация правил разграничения доступа субъектов и их процессов к устройствам создания твердых копий;
- изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;
- управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;
- реализация правил обмена данными между субъектами для автоматизированных систем и средств вычислительной техники, построенных по сетевым принципам.

Кроме того, концепция предусматривает наличие обеспечивающих средства для системы разграничения доступа, которые выполняют следующие функции:

- идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
- регистрацию действий субъекта и его процесса;
- предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
- реакцию на попытки несанкционированного доступа, например, сигнализацию, блокировку, восстановление после несанкционированного доступа;

- тестирование;
- очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;
- учет выходных печатных и графических форм и твердых копий в автоматизированной системе;
- контроль целостности программной и информационной части как системы разграничения доступа, так и обеспечивающих ее средств.

Технические средства защиты от несанкционированного доступа, согласно Концепции, должны оцениваться по следующим основным параметрам:

- степень полноты охвата правил разграничения доступа реализованной системы разграничения доступа и ее качество;
- состав и качество обеспечивающих средств для системы разграничения доступа;
- гарантии правильности функционирования системы разграничения доступа и обеспечивающих ее средств.

3. Каналы и методы несанкционированного доступа к конфиденциальной информации

Состав реальных каналов несанкционированного доступа к конкретной конфиденциальной информации и степень их опасности зависят от вида деятельности предприятия, состава носителей, способов обработки конфиденциальной информации, системы защиты информации, а также от состава, устремлений и возможностей соперников. Однако даже если соперники известны, определить их намерения и возможности практически невыполнимо, поэтому защита должна предусматривать перекрытие всех потенциально существующих для конкретного предприятия каналов.

1. Самым распространенным, многообразным по методам несанкционированного доступа, а потому и самым опасным каналом

является *установление контакта с лицами, имеющими или имевшими доступ к конфиденциальной информации***.** В первую группу входят лица, работающие на данном предприятии, а также не работающие на нем, но имеющие доступ к конфиденциальной информации предприятия в силу служебного положения (из органов власти, вышестоящих, смежных предприятий и др.). Вторая группа включает уволенных или отстраненных от данной конфиденциальной информации лиц, в том числе продолжающих работать на предприятии, а также эмигрантов и перебежчиков. Контакт с этими лицами может быть непосредственным или опосредованным и устанавливаться различными путями. Второй метод действительный прием на работу («переманивание»), одной из целей которого является получение от лица, принятого на работу, конфиденциальной информации, относящейся к прежнему месту его работы. Третий метод - разовая покупка конфиденциальной информации.

Использовались главным образом писцы, которые за взятки снабжали заинтересованных лиц секретной информацией либо устно, либо путем снятия копий с документов, правда, копии иногда были фальсифицированными. Характерно, что писцы не только охотно соглашались на подобные предложения, но нередко сами проявляли в этом инициативу. Четвертый метод - принуждение к выдаче конфиденциальной информации шантажом, различного рода угрозами, применением физического насилия как к лицу, владеющему информацией, так и к его родственникам и близким. Пятый метод - склонение к выдаче конфиденциальной информации убеждением, лестью, посулами, обманом, в том числе с использованием национальных, политических, религиозных факторов.

2. Вербовка и (или) внедрение агентов является вторым по степени опасности каналом. Отличие агентов от лиц, осуществляющих разовые продажи конфиденциальной информации, состоит в том, что агенты работают на постоянной основе, занимаются систематическим сбором

конфиденциальной информации и могут оказывать на нее другое дестабилизирующее воздействие. Большая часть агентов вербуется, при этом применяются различные приемы вербовки: подкуп, обещания, угрозы шантажа и насилия, психологическая обработка недовольных с использованием тщеславия, корысти, эгоизма вербуемых. Вербовку можно рассматривать и как составную часть (продолжение) первого канала, но учитывая, что завербованные агенты применяют собственные методы несанкционированного доступа к конфиденциальной информации, их правильнее будет относить к отдельному каналу. Нередко завербованными агентами становятся «добровольцы», предлагающие свои услуги за соответствующую плату[8]. Внедренные агенты являются специально подготовленными лицами государственных и частных разведывательных служб, которые устраиваются на работу к сопернику с тайным заданием добывать определенную конфиденциальную информацию. С помощью агентов разведывательные службы обычно стремятся получить доступ к такой конфиденциальной информации, которую нельзя добыть через другой, менее опасной канал. И хотя агентурная разведка, именуемая в уголовном праве шпионажем, сурово карается, она практикуется в широких масштабах, поскольку агенты могут получать не только конфиденциальную информацию, относящуюся к их служебной деятельности, но и иную, используя различные методы несанкционированного доступа к ней, а также оказывать другое дестабилизирующее воздействие на информацию. Методами несанкционированного получения иной информации могут быть в значительной мере методы, применяемые при использовании первого канала, а также:

- ознакомление с документами, находящимися на рабочих местах других сотрудников, в том числе с выведенными на экран дисплея, в отсутствие сотрудников (можно использовать и фотографирование) и при их присутствии;

- осмотр доступной продукции, наблюдение за технологическим процессом считывание информации в массивах других пользователей, в том числе с использованием паролей и терминалов этих пользователей;
- подслушивание разговоров, в том числе телефонных, напрямую и с использованием радиозакладок;
- прослушивание публичных выступлений, проводимых на предприятии;
- участие в различного рода комиссиях, общественных объединениях, использующих конфиденциальную информацию;
- кража носителей информации, в том числе и с помощью изготовления дубликатов ключей от сейфов (шкафов).

Другое дестабилизирующее воздействие на информацию может осуществляться с использованием видов и способов воздействия, рассмотренных в работе.

3. Третий канал - организация физического проникновения к носителям конфиденциальной информации сотрудников разведывательных служб (разведчиков) - используется сравнительно редко, поскольку он связан с большим риском и требует знаний о месте хранения носителей и системе защиты информации, хотя уровень защиты информации в некоторых государственных и многих частных структурах дает возможность получать через этот канал необходимую информацию.

Физическое проникновение лиц, не работающих на объекте, включает два этапа: проникновение на территорию (в здания) охраняемого объекта и проникновение к носителям конфиденциальной информации. При проникновении на территорию объекта возможно применение следующих методов:

- использование подложного, украденного или купленного (в том числе и на время) пропуска;

- маскировка под другое лицо, если пропуск не выдается на руки;

- проход под видом внешнего обслуживающего персонала;

- проезд спрятанным в автотранспорте;

-отвлечение внимания охраны для прохода незамеченным (путем создания

чрезвычайных ситуаций, с помощью коллеги и т.д.);

- изоляция или уничтожение охраны (в редких, чрезвычайных обстоятельствах);

- преодоление заграждающих барьеров (заборов) минуя охрану, в том числе и за счет вывода из строя технических средств охраны.

4. Анализ средств обеспечения защиты информации от несанкционированного доступа

Стремительный рост неоднородности и масштабности современных корпоративных сетей приводит к чрезмерному повышению уязвимости не только внешних, но и внутренних сетевых сервисов.

Чем больше масштабность сети, тем труднее администратору обеспечить надежную сетевую защиту, предусматривающую адекватную реакцию на всевозможные попытки взлома компьютерной системы. При этом следует учитывать, что угрозы информационно-компьютерной безопасности могут быть связаны не только с несанкционированным доступом (НСД) к рабочим станциям, серверам или линиям связи. Нападениям могут подвергаться и специализированные устройства, выполняющие функции внутри сетевой маршрутизации потока сообщений. Злоумышленник может перенаправить поток сообщений с целью выполнения над ним дальнейших несанкционированных действий.

Современные корпоративные сети объединяют разнотипные компьютеры с различным ПО. В рамках одной сети могут поддерживаться совершенно разные протоколы информационного взаимодействия. В неоднородной программно-аппаратной среде гораздо сложнее проверить согласованность конфигурации различных компонентов и осуществлять централизованное управление. Повышение неоднородности программно-аппаратных средств приводит к существенному повышению сложности

системы информационно-компьютерной безопасности. Для усложненной системы защиты практически невозможно формально или неформально доказать ее корректность, а также полностью проверить правильность ее функционирования.

В этих условиях усиливаются угрозы НСД к общим ресурсам корпоративной сети и со стороны внутренних нарушителей. Бороться с такими угрозами одними лишь средствами универсальных операционных систем (ОС) и программных серверов (СУБД, Web, электронной почты и др.) уже не представляется возможным. Универсальная ОС, как и любой программный сервер это слишком большой и сложный комплекс программ, который, с одной стороны, может содержать внутренние ошибки и недоработки, а с другой не всегда обеспечивает защиту от ошибок администраторов и пользователей. Современная технология программирования не позволяет сделать столь большие программы безопасными. Здесь характерны как явные ошибки разработки, так и существенные недостатки, связанные с недоработкой концептуальных и ряда детальных требований к системе безопасности. Кроме того, администратор, имеющий дело со сложной системой, далеко не всегда в состоянии эффективно ее настроить и сконфигурировать. Наконец, в универсальной многопользовательской системе бреши в безопасности постоянно создаются самими пользователями, например, тривиальные и редко изменяемые пароли.

Единственный выход из сложившейся ситуации усилить защиту общих ресурсов корпоративной сети уровнем разграничения внутри сетевого доступа, построенном на основе внутренних межсетевых экранов. Средства межсетевого экранирования, называемые также системами Firewall или брандмауэрами, обеспечивают целостную защиту общих сетевых сервисов от враждебной среды.

Особенности межсетевого экранирования

Для противодействия НСД брандмауэр должен располагаться в местах возможного разграничения внутри сетевых информационных потоков.

Любое взаимодействие между сегментами корпоративной сети, а также клиентами и наиболее важными сетевыми сервисами должно осуществляться только через межсетевой экран. Соответственно, стороны информационного взаимодействия (группы рабочих станций, серверов) должны быть выделены в отдельные сегменты сети, соединенные межсетевыми экранами (рис.4). Межсетевой экран не является симметричным. Для него отдельно задаются правила, ограничивающие доступ из одного сетевого сегмента в другой и наоборот.

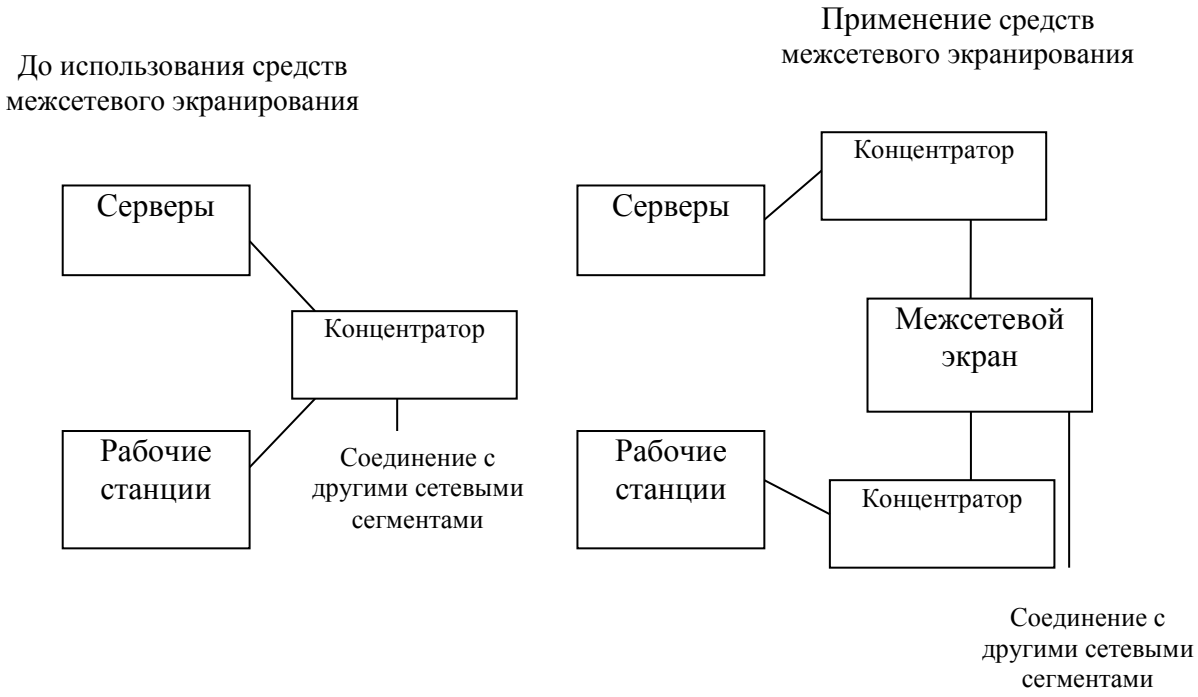


Рис.4 Схема фрагмента корпоративной сети до и после подключения межсетевого экрана

В общем случае работа межсетевого экрана основана на динамическом выполнении 2-х групп функций:

- фильтрации проходящих через него информационных потоков;
- посредничества при реализации межсетевых взаимодействий.

В качестве критериев анализа информационного потока могут использоваться следующие параметры:

- служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;

- непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов;
- внешние характеристики потока информации, например, временные, частотные характеристики, объем данных и т. д.

В процессе посредничества при реализации межсетевых взаимодействий экранирующие агенты, блокируя прозрачную передачу потока сообщений, могут выполнять следующие функции:

- идентификацию и аутентификацию пользователей;
- проверку подлинности передаваемых данных;
- разграничение доступа к ресурсам защищаемого сегмента сети;
- фильтрацию и преобразование потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации;
- трансляцию внутренних сетевых адресов для исходящих пакетов сообщений;
- регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерация отчетов;
- кэширование запрашиваемых данных.

В зависимости от типа экрана перечисленные функции фильтрации и посредничества могут выполняться с различной полнотой. Простые межсетевые экраны ориентированы на выполнение только отдельных групп функций. Комплексные экраны обеспечивают совместное выполнение большинства функций межсетевой защиты. Собственная защищенность брандмауэра достигается с помощью тех же средств, что и защищенность универсальных систем.

Чтобы эффективно обеспечивать безопасность сети, комплексный брандмауэр обязан управлять всем потоком, проходящим через него (рис.5), и отслеживать свое состояние.

Для принятия управляющих решений по используемым сервисам, межсетевой экран должен получать, запоминать, выбирать и обрабатывать информацию, полученную от всех коммуникационных уровней и от других

приложений. Недостаточно просто проверять пакеты по отдельности. Информация о состоянии соединения, полученная из инспекции соединений в прошлом и других приложений главный фактор в принятии управляющего решения при попытке установления нового соединения. Для принятия решения могут учитываться как состояние соединения (полученное из прошлого потока данных), так и состояние приложения (полученное из других приложений).

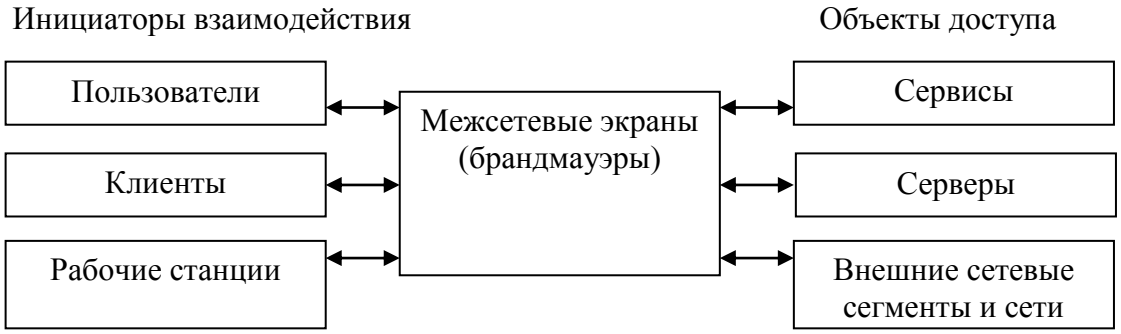


Рис.5 Схема контроля потока сообщений

Полнота и правильность управления требуют, чтобы комплексный брандмауэр имел возможность анализа и использования следующих элементов:

- информации о соединениях информации от всех семи уровней в пакете;
- истории соединений информации, полученной от предыдущих соединений. Например, исходящая команда PORT сессии FTP должна быть сохранена для того, чтобы в дальнейшем можно было проверить входящее соединение FTP data;
- состояния уровня приложения информации о состоянии, полученной из других приложений. Например, аутентифицированному до настоящего момента пользователю можно предоставить доступ через брандмауэр только для авторизованных видов сервиса;
- агрегирующих элементов вычислений разнообразных выражений, основанных на всех вышеперечисленных факторах.

Устройство, подобное межсетевому экрану, может использоваться и для защиты отдельного компьютера. В этом случае экран, уже не являющийся межсетевым, устанавливается на защищаемый компьютер. Такой экран, называемый персональным брандмауэром компьютера или системой сетевого экранирования, контролирует весь исходящий и входящий трафик, независимо от всех прочих системных защитных средств. При экранировании отдельного компьютера поддерживается доступность сетевых сервисов, но уменьшается или вообще ликвидируется нагрузка, индуцированная внешней активностью.

Разработка политики межсетевого взаимодействия

Политика межсетевого взаимодействия является той частью политики безопасности в организации, которая определяет требования к безопасности информационного обмена с внешним миром. Данные требования обязательно должны отражать 2 аспекта:

- политику доступа к сетевым сервисам;
- политику работы межсетевого экрана.

Политика работы межсетевого экрана задает базовый принцип управления межсетевым взаимодействием, положенный в основу функционирования брандмауэра. Может быть выбран один из двух таких принципов:

- запрещено все, что явно не разрешено;
- разрешено все, что явно не запрещено.

В первом случае межсетевой экран должен быть сконфигурирован таким образом, чтобы блокировать любые явно не разрешенные межсетевые взаимодействия. Учитывая, что такой подход позволяет адекватно реализовать принцип минимизации привилегий, он лучше, с точки зрения безопасности[9].

При выборе принципа разрешено все, что явно не запрещено межсетевой экран настраивается так, чтобы блокировать только явно запрещенные межсетевые взаимодействия.

Определение схемы подключения межсетевых экранов

Для подключения межсетевых экранов могут использоваться различные схемы, которые зависят от условий функционирования, а также количества сетевых интерфейсов брандмауэра. Для небольшой корпоративной сети может быть достаточным использование только 2-х межсетевых экранов (рис.6).

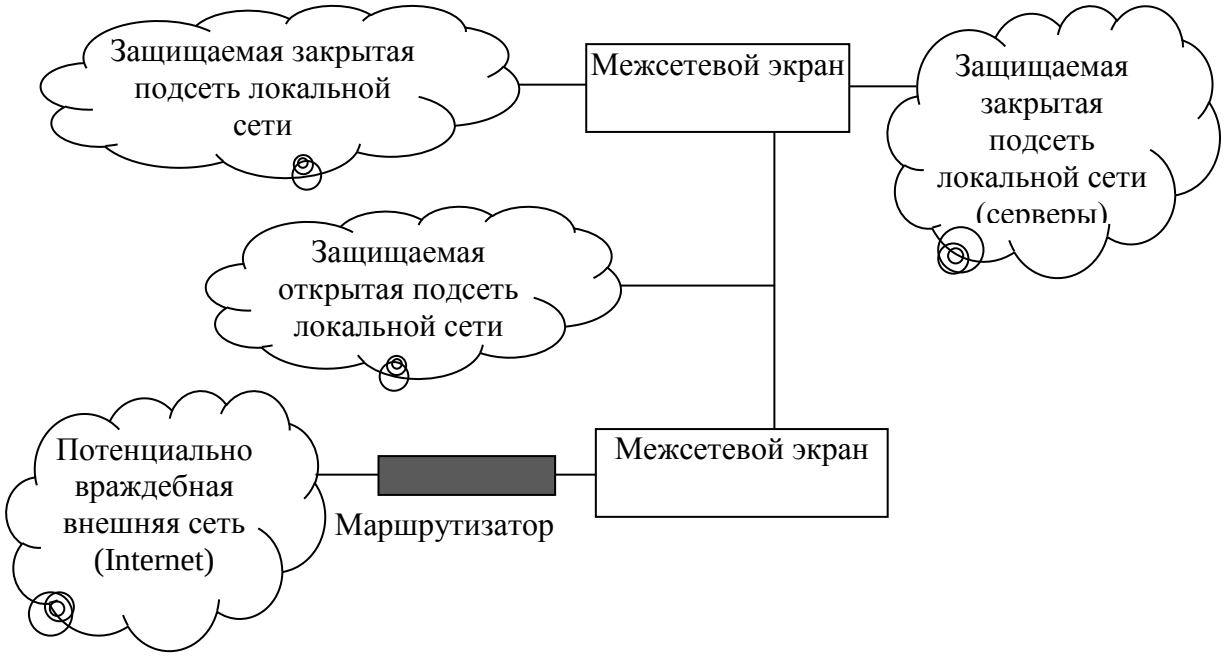


Рис.6 Пример схемы подключения межсетевых экранов

Защищаемая открытая подсеть здесь выступает в качестве экранирующей подсети. Обычно экранирующая подсеть конфигурируется таким образом, чтобы обеспечить доступ к компьютерам подсети как из потенциально враждебной внешней сети, так и из закрытых подсетей локальной сети. Однако прямой обмен информационными пакетами между внешней сетью и закрытыми подсетями невозможен. При атаке системы с экранирующей подсетью необходимо преодолеть, по крайней мере, две независимых линии защиты, что является весьма сложной задачей. Средства мониторинга состояния межсетевых экранов практически неизбежно обнаружат подобную попытку, и администратор системы своевременно предпримет необходимые действия по предотвращению НСД.

Выводы по первой главе

Проведенные анализов потенциальные угрозы информационной безопасности свидетельствует о том, что задачу защиты от них можно условно разделить на пользователей и элементов сети, с которыми работают пользователи сети. Концепции защиты информации предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в проблеме защиты информации от несанкционированного доступа. Рассмотренные каналы и методы несанкционированного доступа может иметь целью уничтожение или искажение информации с помощью лиц, имеющих к ней доступ, но, как правило, этот канал используется для получения конфиденциальной информации. Анализ средств защиты информации от несанкционированного доступа дают возможность контроля весь исходящий и входящий трафик, независимо от всех прочих системных защитных средств.

Глава II. Построение системы обеспечения безопасности информации от несанкционированного доступа в информационно-коммуникационных системах

1. Подход к созданию системы защиты информации от несанкционированного доступа к информационно-коммуникационным системам

В периоды необходимости выбора комплекса решений по обеспечению безопасности в качестве ограничений учитываются следующие требования к способам организации защиты информации:

- существование сертификатов по вопросам безопасности информации в соответствии с грифом обрабатываемой информации и порядком функционирования автоматизированных систем (АС);
- неизменность функционирования средств защиты;
- предоставление режима защиты охраняемых сведений, в том числе сохранения таких свойств защищенности информации, как конфиденциальность, доступность, целостность и подлинность;
- гарантированное сохранение целевых функций защищаемой автоматизированной системы - отсутствия ограничений, связанных с применением средств защиты, препятствующих реализации технологического цикла обработки информации.

В целях простого понимания и удобства описания разрабатываемых формализмов в рамках данного исследования введем следующее определение: транзактом называется любая попытка несанкционированного доступа (НСД), а также санкционированного доступа (СД) к ресурсам системы, в результате которого считывание или запись информации произошла с нарушением установленных правил.

Предположено, что успешная попытка СД с нарушением установленных правил (транзакт СД) приводит к искажению информации в базе данных.

В отличие от обычных заявок на обслуживание транзакт НСД имеет набор динамически изменяющихся особых свойств и параметров. Попытка несанкционированного доступа к информационным ресурсам (транзакт НСД) может привести к следующим результатам:

- копированию (считыванию) информации из базы данных;
- изменению (искажению) информации в базе данных;
- помехам в работоспособности (отказу в обслуживании) системы - полному прекращению или существенному замедлению исполнения функций по обслуживанию запросов.

Определение последствий транзактов НСД и их оценка осуществляется с учетом следующей системы допущений доступа к информационным ресурсам АС:

- необнаруженное поступление транзакта НСД в соответствующий элемент АС будем называть отказом определенного ресурса;
- данный отказ элемента АС влечет за собой ущерб, пропорциональный времени пребывания транзакта в системе;
- выявление транзакта НСД требует некоторого времени (зависящего от типа элемента АС, подвергшегося успешной атаке) для ликвидации последствий искажения информации (восстановление);
- прошедшему систему защиты транзакту НСД, становится доступным любой элемент (ресурс) АС;
- все потоки переходов предполагаются простейшими, то есть стационарными, ординарными и без последействия.

Возьмем за основу то, что в системе защиты информации используются следующие организационные и технические решения:

1) решения S_i, обеспечивающие аутентификацию и идентификацию персонала;
2) решения S_2 по управлению доступом пользователей к защищаемым ресурсам;
3) решения S_3, обеспечивающие регистрацию действий пользователей;

4) решения S_4 по дистанционной диагностике элементов защиты;

5) решения S_5, сориентированные на обеспечение целостности информационных ресурсов с использованием средств защиты информации;

6) решения S_6, устремленные на обеспечение в предельно возможной степени повышение достоверности и точности защищаемой информации;

7) решения S_7, способные обеспечить защиту от вредоносных программ;

8) решения S_8, позволяющие обеспечить противодействие нештатному созданию копий массивов информации;

9) решения S_9, ориентированные на предотвращение полной утраты накапливаемой информации;

10) решения S_{10}, устанавливающие регламенты обеспечения непрерывной работоспособности и восстановления системы.

Необходимо ввести следующие условные обозначения, которые будут применены при формализованном процессе несанкционированного доступа к информационным ресурсам АС:

λ- интенсивность поступления потока транзактов в АС. В силу выработанных предположений, поток транзактов будет пуассоновским, поэтому его можно охарактеризовать с помощью единственного параметра - интенсивности, при этом $\lambda \cdot \Delta t$ - вероятность поступления транзактов от момента времени *t* до момента времени $t + \Delta t$;

γ - интенсивность преодоления транзактом системы защиты; $\gamma \cdot \Delta t$ - вероятность преодоления системы защиты от момента времени *t* до момента времени $t + \Delta t$;

Л - интенсивность обнаружения транзактов в системе защиты; $\mu + \Delta t -$ вероятность обнаружения транзактов от момента времени *t* до момента времени $t + \Delta t$;

P_{ki} - вероятность поступления транзакта в определенный элемент АС;

ρ - интенсивность восстановления данного элемента АС;

$\frac{1}{\rho}$ – среднее время устранения последствий (восстановления), предполагается, что весь этот интервал времени системе наносится определенный ущерб;

x - математическое ожидание количества транзактов в системе;

z - математическое ожидание количества транзактов, прошедших систему защиты;

u - вероятность того, что данный элемент АС не подвергся успешной информационной атаке (транзакт не попал в данный элемент, либо последствия предыдущих успешных атак на данный элемент уже устранены);

v - вероятность события, содержащегося в том, что данный элемент АС подвергся успешному нападению и эти последствия либо не обнаружены, либо еще не устранены (отказ элемента).

На рис.1 изображен процесс поступления транзактов НСД в АС.

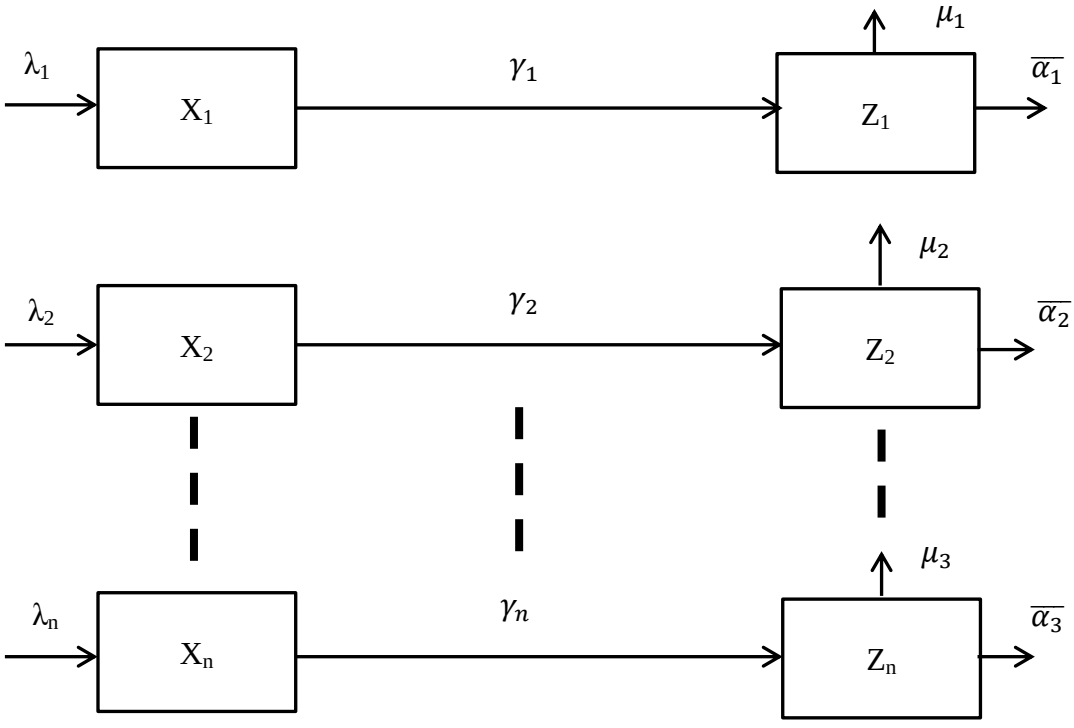


Рис.1 Графическое представление процесса поступления транзактов в АС

Первый уровень контроля транзакт проходит в первом состоянии (идентификацию и аутентификацию персонала S_1), а контроль доступа пользователей к защищаемым ресурсам осуществляется во втором состоянии

S_2. И только после этого проводится регистрация действий пользователей S_3 и т.д.

Окончательный выход из каждого состояния по результатам контроля происходит двумя путями:

- транзакт окончательно отрицается;
- транзакт допускается на вход АС для дальнейшей проверки.

С учетом принятой практики, транзакт, не прошедший контроля первой ступени, может поступать на вход системы неопределенное количество раз.

Интенсивность γ_k определяется по формуле:

$$\gamma = \frac{P_{nk}}{T_{nk}},$$

где P_{nk} - вероятность пропуска транзакта системой защиты; T_{nk} - среднее время «прорыва» транзакта через систему защиты.

В свою очередь:

$$\mu_k = \frac{P_{ok}}{T_{ok}}, \quad \overline{\alpha_k} = \frac{1-P_{ok}}{T_{ok}},$$

где P_{ok} - вероятность правильного анализа транзакта; T_{ok} - среднее время анализа транзакта в системе защиты

Прошедшие систему защиты все транзакты поступают в АС. В общем случае, каждый транзакт k-го типа может поступить на обработку в любой из m элементов системы с вероятностью P_{ki} (k - тип транзакта; i - тип элемента). Для всех P_{ki} должно соблюдаться условие нормировки (полная группа событий):

$$\sum_{k=1}^{m} P_{ki} = 1$$

Введено обобщенное понятие отказа элемента, заключающееся в том, что проведена успешная атака на АС, последствия которой либо не обнаружены, либо еще не устранены. При этом последствия атаки могут быть различными, однако все они приводят к нанесению определенного ущерба.

Отказы и сбои в работе вследствие поступления транзактов, не обнаруженных системой защиты, описываются графом, изображенным на рис.2.

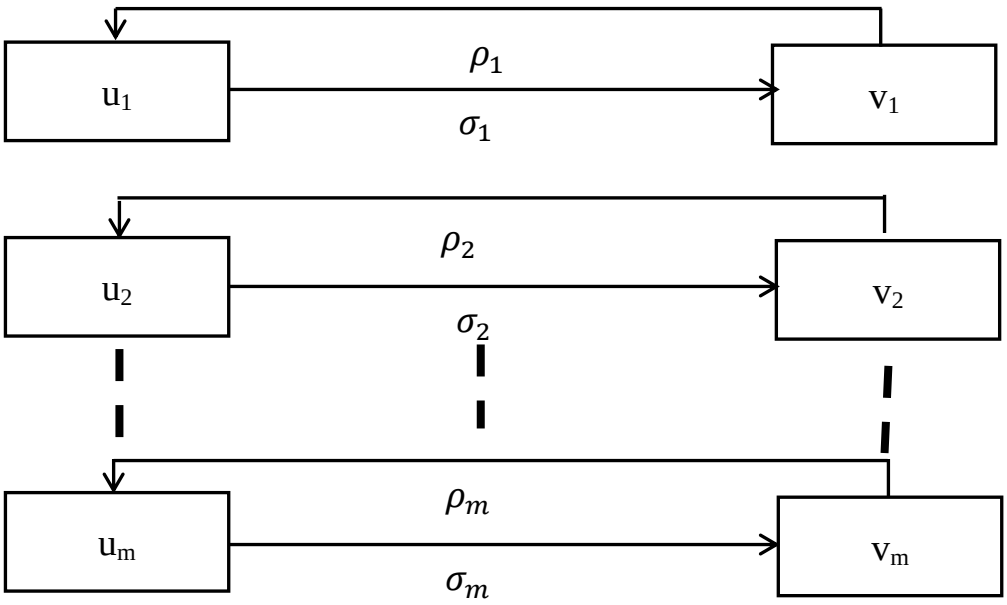


Рис.2 Графическое представление процесса отказов АС вследствие прохождения транзактов

В графическом описании процесса используются следующие условные обозначения:

ρ_j - интенсивность обнаружения и восстановления отказа *j-го* элемента АС;

σ_j- интенсивность отказов *j*-го элемента АС вследствие поступления необнаруженных транзактов.

Указанные выше интенсивности вычисляются по формулам:

$$p_j = \frac{P_{oj}}{P_{oj}T_{bj}+(1-P_{oj})T_{oj}},$$

где T_{oj} - среднее время обнаружения транзакта системой защиты в *j-м* элементе АС;

P_{oj} - вероятность обнаружения транзакта системой защиты в *j*-м элементе АС; t_{bj} – среднее время восстановления *j*-го элемента АС.

$$\sigma_j = \sum_{k=1}^{n} \overline{\alpha_k}\, P_{kj} z_k,$$

где P_{kj} - вероятность поступления транзакта k-го типа в элемент j-го типа.

Учитывая взаимосвязь обоих графов, а также простейший характер потоков перехода из состояния в состояние, можно получить следующую систему дифференциальных уравнений ($2n+m$):

$$\left.\begin{array}{c} x_k' = \lambda_k - \gamma_k x_k \\ z_k' = \gamma_k x_k - (\mu_k = \bar{\alpha}_k) z_k, \\ u_k' = \rho_j v_{kj} - \sigma_j u_{kj} \\ u_{kj} + v_j = 1, \\ k = \overline{1,n}, \\ j = \overline{1,m}. \end{array}\right\}$$

Решение этой системы уравнений необходимо проводить при следующих начальных условиях:

$$\left.\begin{array}{c} x_k(0) = 0, \\ z_k(0) = 0, \\ u_j(0) = 0, \\ v_j(0) = 0, \\ k = \overline{1,n}, \\ j = \overline{1,m}, \end{array}\right\}$$

Проинтегрировав данную систему уравнений на промежутке времени от 0 до T, можно получить математическое ожидание ущерба от проникновения в систему нарушителей различных типов по следующей формуле:

$$\left.\begin{array}{c} B(T_2 - T_1) \int\limits_{T_1}^{T_2} \sum\limits_{j=1}^{m} \beta_j v_j(t), \\ o \le T_1 \le T_2 \le T. \end{array}\right\}$$

где β_j - ущерб, наносимый системе при искажении соответствующего информационного ресурса в единицу времени.

Для того чтобы обеспечить работоспособность приведенной выше базовой модели, нужна разработка комплекса методов и методик вычисления параметров, являющихся входными для данной модели. Проведение

исследования и разработки должны проводиться в следующих основных направлениях:

- исследование потока транзактов НСД по типам и объемам;
- разработка методик для оценки эффективности систем защиты информации, прошедших определенные уровни защиты информации;
- разработка методов и методик восстановления работоспособности подсистем и элементов АС при их отказе, обусловленном поступлением в них транзактов НСД, прошедших основные виды контроля со стороны систем защиты;
- исследование и разработка методик оценки ущербов.

Нужно отметить, что в общем случае все эти исследования должны проводиться применительно к каждой конкретной АС как существующей, так и разрабатываемой[10].

Граф состояний для такой модели представлен на рис.3:

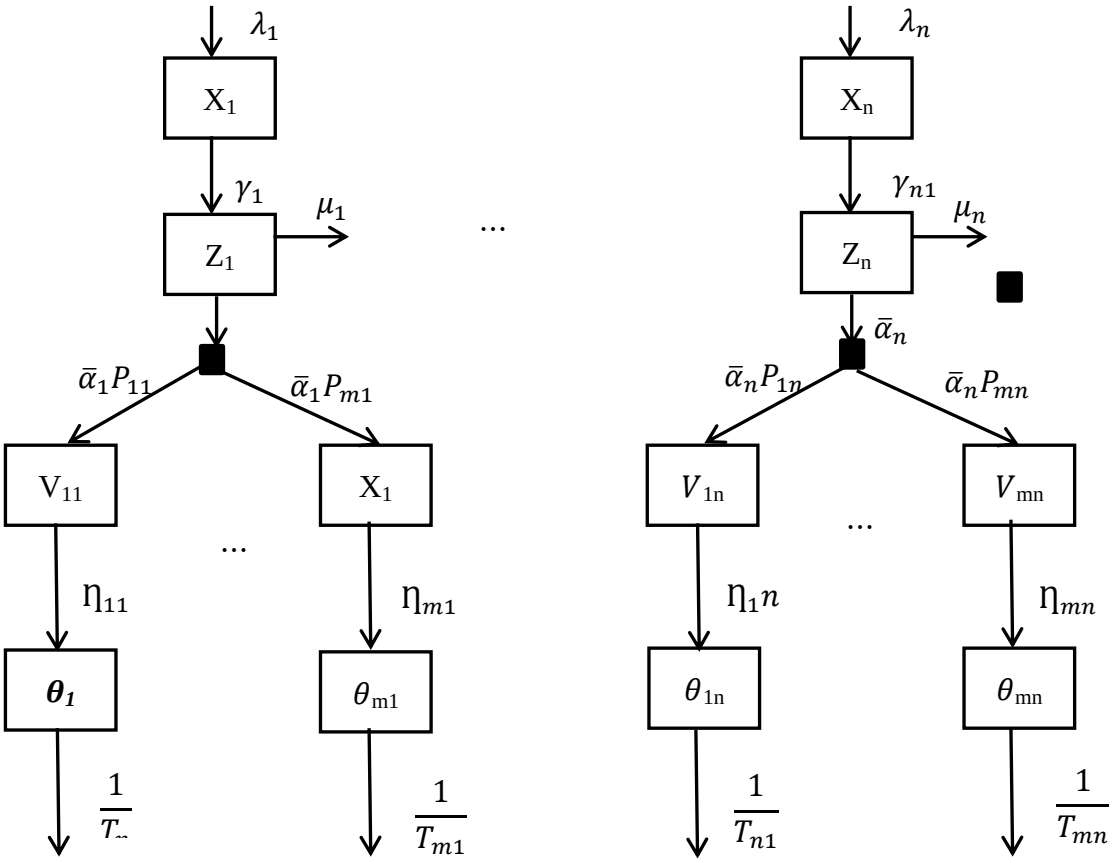


Рис.3 Графическое представление модели воздействия транзактов на различные элементы АС

Достижение этой цели реализовывается путем искажения информации о состоянии и деятельности подсистем и элементов данной социально-экономической системы за счет получения несанкционированного доступа к вычислительным ресурсам и базам данных обслуживающих ее АС.

Однако предположение о том, что «атакованный» элемент АС не подвергается новой информационной атаке до тех пор, пока не будут устранены последствия предыдущей атаки, является одним из предположений данной модели, существенно ограничивающим ее возможности. Введение этого предположения в случае, если среднее время между атаками превосходит суммарное среднее время обнаружения и восстановления последствий.

2. Методика построения системы защиты информации от несанкционированного доступа

Современные методики управления рисками, проектирования и сопровождения корпоративных систем защиты информации должны позволять решить ряд задач перспективного стратегического развития организации.

Во-первых, количественно оценить текущий уровень информационной безопасности компании, что потребует выявления рисков на правовом, организационно-управленческом, технологическом, а также техническом уровнях обеспечения защиты информации.

Во-вторых разработать и реализовать комплексный план совершенствования корпоративной системы защиты информации для достижения приемлемого уровня защищенности информационных активов компании. Для этого необходимо:

- обосновать и произвести расчет финансовых вложений в обеспечение безопасности на основе технологий анализа рисков, соотнести расходы на

обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения;

- выявить и провести первоочередное блокирование наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы;
- определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц по обеспечению информационной безопасности компании, создать необходимый пакет организационно-распорядительной документации;
- разработать и согласовать со службами организации, надзорными органами проект внедрения необходимых комплексов защиты, учитывающий современный уровень и тенденции развития информационных технологий;
- обеспечить поддержание внедренного комплекса защиты в соответствии с изменяющимися условиями работы организации, регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты. Решение названных задач открывает новые широкие возможности перед должностными лицами разного уровня.

На основе полученной оценки начальники отделов и служб смогут выработать и обосновать необходимые организационные меры (состав и структуру службы информационной безопасности, положение о коммерческой тайне, пакет должностных инструкций и инструкции действия в нештатных ситуациях). Менеджеры среднего звена смогут обоснованно выбрать средства защиты информации, а также адаптировать и использовать в своей работе количественные показатели оценки информационной безопасности, методики оценки и управления безопасностью с привязкой к экономической эффективности компании.

Практические рекомендации по нейтрализации и локализации выявленных уязвимостей системы, полученные в результате аналитических исследований, помогут в работе над проблемами информационной безопасности на разных уровнях и, что особенно важно, определить

основные зоны ответственности, в том числе материальной, за ненадлежащее использование информационных активов компании.

Разновидности аналитических работ по оценке защищенности

Аналитические работы в области информационной безопасности могут проводиться по следующим направлениям:

1) "Комплексный анализ информационных систем (ИС) компании и подсистемы информационной безопасности на правовом, методологическом, организационно-управленческом, технологическом и техническом уровнях. Анализ рисков";

2)"Разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому, общетехническому и программно-аппаратному обеспечению режима ИС организации";

3) "Организационно-технологический анализ ИС организации";

4) "Экспертиза решений и проектов";

5) "Работы по анализу документооборота и поставке типовых комплектов организационно-распорядительной документации";

6) "Работы, поддерживающие практическую реализацию плана защиты";

7) "Повышение квалификации и переподготовка специалистов".

К первой области также относятся работы, проводимые на основе анализа рисков, инструментальные исследования (исследование элементов инфраструктуры компьютерной сети и корпоративной информационной системы на наличие уязвимостей, исследование защищенности точек доступа в Internet). Данный комплекс работ также включает в себя и анализ документооборота, который, в свою очередь, можно выделить и как самостоятельное направление.

Рекомендации могут касаться общих основополагающих вопросов обеспечения безопасности информации (разработка концепции информационной безопасности, разработка корпоративной политики охраны информации на организационно-управленческом, правовом,

технологическом и техническом уровнях), применимых на многих компаниях. Также рекомендации могут быть вполне конкретными и относится к деятельности одной единственной компании (план защиты информации, дополнительные работы по анализу и созданию методологического, организационно-управленческого, технологического, инфраструктурного и технического обеспечения режима информационной безопасности компании).

Организационно-технологический анализ ИС компании в основном предполагает проведение оценки соответствия типовым требованиям руководящих документов к системе информационной безопасности компании в области организационно-технологических норм и анализ документооборота компании категории "конфиденциально" на соответствие требованиям концепции информационной безопасности, положению о коммерческой тайне, прочим внутренним требованиям компании по обеспечению конфиденциальности информации.

Правильная экспертиза решений и проектов играет важную роль в обеспечении функционирования всей системы информационной безопасности и должна соответствовать требованиям по обеспечению информационной безопасности экспертно-документальным методом. Экспертиза проектов подсистем - требованиям по безопасности экспертно-документальным методом[11].

Работы по анализу документооборота и поставке типовых комплектов организационно-распорядительной документации, как правило, включают два направления:

- анализ документооборота компании категории "конфиденциально" на соответствие требованиям концепции информационной безопасности, положению о коммерческой тайне, прочим внутренним требованиям компании по обеспечению конфиденциальности информации;

- поставку комплекта типовой организационно-распорядительной документации в соответствии с рекомендациями корпоративной политики ИБ организации на организационно-управленческом и правовом уровне.

Работы, поддерживающие практическую реализацию плана информационной безопасности, в частности, заключаются в следующем:

- разработка технического проекта модернизации средств защиты ИС, установленных на фирме по результатам проведенного комплексного аналитического исследования корпоративной сети;
- разработка расширенного перечня сведений ограниченного распространения как части политики безопасности;
- разработка пакета организационно-распорядительной документации в соответствии с рекомендациями корпоративной политики ИБ организации на организационно-управленческом и правовом уровне.

Уровень информационной безопасности компании во многом зависит от квалификации специалистов. В целях повышения квалификации и переподготовки кадров рекомендуется проводить тренинги по применению средств защиты информации, технологии защиты информации, обучать сотрудников основам экономической безопасности.

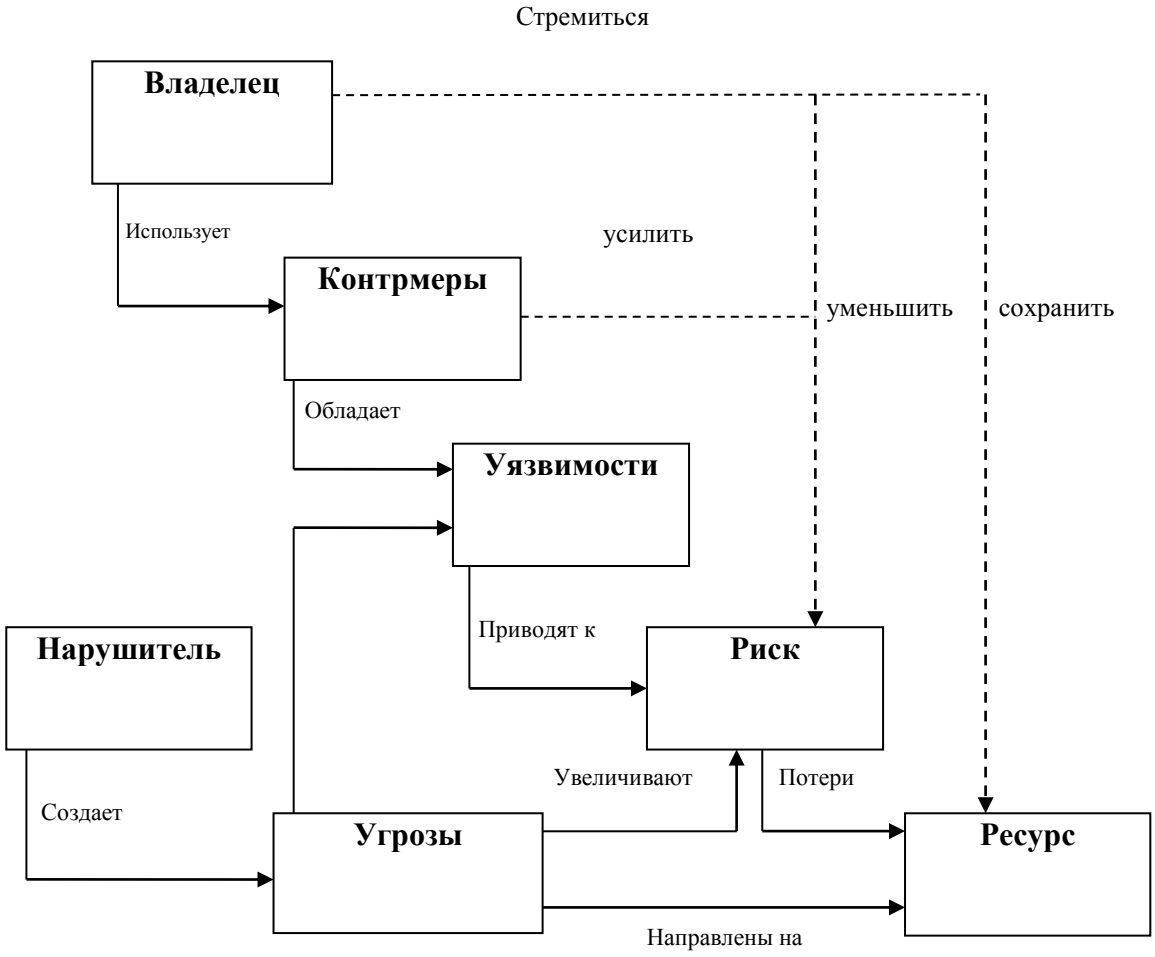
Методика построения системы защиты информации

Главная цель любой системы информационной безопасности заключается в обеспечении устойчивого функционирования объекта: предотвращении угроз его безопасности, защите законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, обеспечении нормальной производственной деятельности всех подразделений объекта. Другая задача сводится к повышению качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов.

Для этого необходимо:

- отнести информацию к категории ограниченного доступа (служебной тайне);
- создать условия для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, и тем самым ослабить возможное негативное влияние последствий нарушения информационной безопасности.

При выполнении работ можно использовать следующая архитектура построения системы защиты информации от несанкционированного доступа (рис.3).



Условные обозначения:

- естественное воздействие

- управляющее воздействие

Рис.3 Архитектура построения системы защиты информации от несанкционированного доступа

Представленная архитектура системы защиты информации - это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Рассматриваются следующие объективные факторы:

- угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;
- уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;
- риск - фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери - прямые или косвенные).

Для построения сбалансированной системы информационной безопасности предполагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для организации на основе заданного критерия. Систему информационной безопасности (контрмеры) предстоит построить таким образом, чтобы достичь заданного уровня риска.

Предлагаемая методика проведения аналитических работ позволяет полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности, избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, обеспечить проведение работ в сжатые сроки, представить обоснование для выбора мер противодействия, оценить эффективность контрмер, сравнить различные варианты контрмер.

Эта модель, в соответствии с предлагаемой методикой, строится следующим образом: для выделенных ресурсов определяется их ценность, как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т.д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут рекомендации по проведению регулярных проверок эффективности системы защиты.

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

3. Построение моделей системы защиты информации от несанкционированного доступа

Модель поведения потенциального нарушителя. Нарушением считается попытка несанкционированного доступа к любой части подлежащей защите информации, хранимой, обрабатываемой и передаваемой в информационной системе.

Поскольку время и место проявления преднамеренного несанкционированного доступа предсказать невозможно, целесообразно

воссоздать некоторую модель поведения потенциального нарушителя, предполагая наиболее опасную ситуацию:

а) нарушитель может появиться в любое время и в любом месте периметра информационной системы;

б) квалификация и осведомленность нарушителя может быть на уровне разработчика данной системы;

в) постоянно хранимая информация о принципах работы системы, включая секретную, нарушителю известна;

г) для достижения своей цели нарушитель выберет наиболее слабое звено в защите;

д) нарушителем может быть не только постороннее лицо, но и законный пользователь системы;

е) нарушитель действует один.

Данная модель позволяет определиться с исходными данными для построения защиты и наметить основные принципы ее построения.

Согласно п. «а» необходимо строить вокруг предмета защиты постоянно действующий замкнутый контур (или оболочку) защиты (периметр).

Согласно п. «б» свойства преграды, составляющие защиту, должны по возможности соответствовать ожидаемой квалификации и осведомленности нарушителя.

Согласно п. «в» для входа в систему законного пользователя необходима переменная секретная информация, известная только ему.

Согласно п. «г» итоговая прочность защитного контура определяется его слабейшим звеном.

Согласно п. «д» при наличии нескольких законных пользователей полезно обеспечить разграничение их доступа к информации в соответствии с полномочиями и выполняемыми функциями, реализуя таким образом принцип наименьшей осведомленности каждого пользователя с целью сокращения ущерба в случае, если имеет место безответственность одного из

них. Отсюда также следует, что расчет прочности защиты должен производиться для двух возможных исходных позиций нарушителя:

- за пределами контролируемой территории (периметра);
- внутри нее.

Согласно п. «е» в качестве исходной предпосылки также считаем, что нарушитель один, так как защита от группы нарушителей — задача следующего этапа исследований. Однако это не исключает возможности защиты предлагаемыми методами и средствами и от такого рода ситуаций, хотя подобная задача значительно сложнее. При этом под группой нарушителей понимается группа людей, выполняющих одну задачу под общим руководством.

На основании изложенного для выбора исходной модели поведения потенциального нарушителя целесообразен дифференцированный подход. Поскольку квалификация нарушителя — понятие весьма относительное и приближенное, возможно принять за основу четыре класса безопасности:

1-й класс рекомендуется для защиты жизненно важной информации, утечка, разрушение или модификация которой могут привести к большим потерям для пользователя. Прочность защиты должна быть рассчитана на нарушителя-профессионала;

2- й класс рекомендуется использовать для защиты важной информации при работе нескольких пользователей, имеющих доступ к разным массивам данных или формирующих свои файлы, недоступные другим пользователям. Прочность защиты должна быть рассчитана на нарушителя высокой квалификации, но не на взломщика-профессионала;

3- й класс рекомендуется для защиты относительно ценной информации, постоянный несанкционированный доступ к которой путем ее накопления может привести к утечке и более ценной информации. Прочность защиты при этом должна быть рассчитана на относительно квалифицированного нарушителя-непрофессионала;

4- й класс рекомендуется для защиты прочей информации, не представляющей интереса для серьезных нарушителей. Однако его необходимость диктуется соблюдением технологической дисциплины учета и обработки информации служебного пользования в целях защиты от случайных нарушений в результате безответственности пользователей и некоторой подстраховки от случаев преднамеренного несанкционированного доступа. Уровень безопасности защиты внутри класса обеспечивается количественной оценкой прочности отдельных средств защиты и оценкой прочности контура защиты от преднамеренного несанкционированного доступа по расчетным формулам, вывод которых приведен ниже.

Модель элементарной защиты. В общем случае простейшая модель элементарной защиты любого предмета может быть в виде, представленном на рис.4.

Предмет защиты помещен в замкнутую и однородную защитную оболочку, называемую ***преградой.*** Прочность защиты зависит от свойств преграды. Принципиальную роль играет способность преграды противостоять попыткам преодоления ее нарушителем. Свойство предмета защиты — способность привлекать его владельца и потенциального нарушителя. Привлекательность предмета защиты заключается в его цене. Это свойство предмета защиты широко используется при оценке защищенности информации в информационных системах.

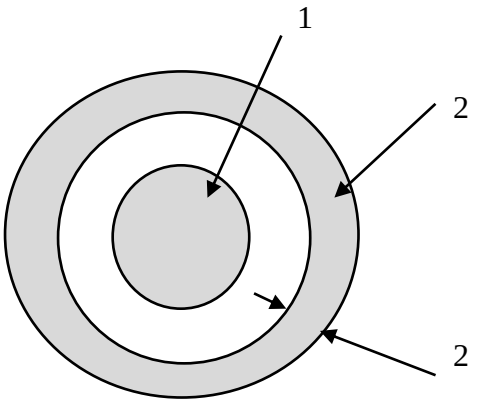


Рис.4 Модель элементарной защиты: 1-предмет защиты, 2-преграда, 3-прочность преграды

При этом считается, что прочность созданной преграды достаточна, если стоимость ожидаемых затрат на ее преодоление потенциальным нарушителем превышает стоимость защищаемой информации. Однако возможен и другой подход. Известно, что информация со временем теряет свою привлекательность и начинает устаревать, а в отдельных случаях ее цена может упасть до нуля. Тогда за условие достаточности защиты можно принять превышение затрат времени на преодоление преграды нарушителем над временем жизни информации[12]. Если обозначить вероятность не преодоления преграды нарушителем через $P_{СЗИ}$, время жизни информации через $t_ж$, ожидаемое время преодоления преграды нарушителем через $t_н$, вероятность обхода преграды нарушителем через $P_{обх}$, то для случая старения информации условие достаточности защиты получим в виде следующих отношений:

$P_{СЗИ} = I$, если $t_ж < t_н$ и $P_{обх} = 0$.

Вероятность $P_{обх}$, равная нулю, отражает необходимость замыкания преграды вокруг предмета защиты. Если$t_ж > t_н$, а $P_{обх} = 0$ то

$$P_{СЗИ} = (1 - P_{нр}) \quad (1)$$

где $P_{нр} -$ вероятность преодоления преграды нарушителем за время, меньшее $t_ж$.

Для реального случая, когда $t_ж > t_н$ и $P_{обх} > 0$, прочность защиты можно представить в виде

$$P_{СЗИ} = \left(1 - P_{нр}\right)(1 - P_{обх}),$$

где $P_{нр} = 0$, если $t_ж < t_н$; $P_{нр} > 0$, если $t_ж \geq t_н$.

Однако эта формула справедлива для случая, когда нарушителей двое, т. е. когда один преодолевает преграду, а второй ее обходит. Но в исходной модели поведения потенциального нарушителя мы условились, что нарушитель будет в единственном числе и ему известны прочность преграды и сложность пути ее обхода. Поскольку одновременно по двум путям он идти не сможет, он выберет один из них — наиболее простой, т. е. по формуле

«ИЛИ». Тогда формальное выражение прочности защиты в целом для данного случая будет соответствовать формуле

$$P_{\text{СЗИ}} = \left(1 - P_{\text{нр}}\right) \cup (1 - P_{\text{обх}}) \qquad (2)$$

где U — знак «ИЛИ».

Следовательно, прочность преграды после определения и сравнения величин $\left(1 - P_{\text{нр}}\right)$ и $(1 - P_{\text{обх}})$ будет равна наименьшему значению одной из них.

В качестве примера элементарной защиты, рассчитываемого по формуле (2), может быть названа криптографическая защита информации, где величина $P_{\text{нр}}$ может определяться путем оценки вероятности подбора кода ключа, с помощью которого можно дешифровать закрытую данным способом информацию.

Эту величину можно определить по формуле $P_{\text{нр}} = n/A^S$

где $n -$ количество попыток подбора кода; $A -$ число символов в выбранном алфавите кода ключа; S — длина кода ключа в количестве символов.

Величина $P_{\text{обх}}$ будет зависеть от выбранного метода шифрования, способа применения, полноты перекрытия текста информации, существующих методов криптоанализа, а также способа хранения действительного значения кода ключа и периодичности его замены на новое значение, если информация, закрытая данным способом, постоянно хранится у ее владельца. Возможны и другие обстоятельства, влияющие на вероятность обхода криптографической защиты.

Выбор и определение конкретной величины $P_{\text{обх}}$ сначала можно проводить экспертным путем на основе опыта специалистов. Величина $P_{\text{обх}}$ должна принимать значения от 0 до 1. При $P_{\text{обх}} = 1$ защита теряет всякий смысл. Возможно также, что у одной преграды может быть несколько путей обхода. Тогда формула (2) примет вид:

$$P_{\text{СЗИ}} = \left(1 - P_{\text{нр}}\right) \cup (1 - P_{\text{обх1}}) \cup (1 - P_{\text{обх2}}) \cup \ldots \cup (1 - P_{\text{обх}k}), \quad (4)$$

где k – число путей обхода преграды, т. е. прочность преграды равна наименьшему значению, полученному после определения и сравнения величин:

$$\left(1 - P_{\text{нр}}\right), (1 - P_{\text{обх1}}), (1 - P_{\text{обх2}}), \dots, (1 - P_{\text{обх}k}).$$

В том случае, когда информация, подлежащая защите, не устаревает или периодически обновляется, т. е. когда неравенство $t_{\text{ж}} > t_{\text{н}}$ постоянно или же когда обеспечить $t_{\text{н}} > t_{\text{ж}}$ по каким-либо причинам невозможно, обычно применяется постоянно действующая преграда, обладающая свойствами обнаружения и блокировки доступа нарушителя к предмету или объекту защиты. В качестве такой защиты могут быть применены человек или специальная автоматизированная система обнаружения под управлением человека.

Очевидно, что параметры этой преграды будут влиять на ее прочность. Способность преграды обнаруживать и блокировать несанкционированный доступ должна учитываться при оценке ее прочности путем введения в расчетную формулу (4) вместо $\left(1 - P_{\text{нр}}\right)$ величины $P_{\text{обл}}$ – вероятности обнаружения и блокировки несанкционированного доступа.

Принцип работы автоматизированной преграды основан на том, что в ней блоком управления производится периодический контроль датчиков обнаружения нарушителя. Результаты контроля наблюдаются человеком. Периодичность опроса датчиков автоматом может достигать тысячные доли секунды и менее. В этом случае ожидаемое время преодоления преграды нарушителем значительно превышает период опроса датчиков. Поэтому такой контроль часто считают постоянным. Но для обнаружения нарушителя человеком, управляющим автоматом контроля, только малого периода опроса датчиков недостаточно.

Необходимо еще и время на выработку сигнала тревожной сигнализации, т. е. время срабатывания автомата, так как оно часто значительно превышает период опроса датчиков и тем самым увеличивает

время обнаружения нарушителя. Но поскольку физический доступ к объекту защиты пока еще открыт, дальнейшие действия охраны сводятся к определению места и организации блокировки доступа нарушителя, на что также потребуется время.

Таким образом, условие прочности преграды с обнаружением и блокировкой несанкционированного доступа можно представить в виде соотношения

$$T_{\text{д}} + t_{\text{ср}} + t_{\text{ом}} + t_{\text{бл}}/t_{\text{н}} < 1, \qquad (5)$$

где $T_{\text{д}}$ – период опроса датчиков; $t_{\text{ср}}$ – время срабатывания тревожной сигнализации; $t_{\text{ом}}$ – время определения места доступа; $t_{\text{бл}}$ – время блокировки доступа.

Если обозначим сумму $\left(T_{\text{д}} + t_{\text{ср}} + t_{\text{ом}} + t_{\text{бл}}\right)$ через $T_{\text{обл}}$, получим соотношение

$$T_{\text{обл}}/t_{\text{н}} < 1, \qquad (6)$$

где $T_{\text{обл}}$ – время обнаружения и блокировки несанкционированного доступа.

Процесс контроля несанкционированного доступа и несанкционированных действий нарушителя во времени представлен на рис. 3.

Из диаграммы на рис.3 следует, что нарушитель может быть не обнаружен в двух случаях:

а) когда $t_{\text{н}} < T$;

б) когда $T < t_{\text{н}} < T_{\text{обл}}$.

В первом случае требуется дополнительное условие — попадание интервала времени $t_{\text{н}}$ в интервал T, т. е. необходима синхронизация действий нарушителя с частотой опроса датчиков обнаружения. Для решения этой задачи нарушителю придется скрытно подключить измерительную аппаратуру в момент выполнения несанкционированного доступа к информации, что является довольно сложной задачей для постороннего человека.

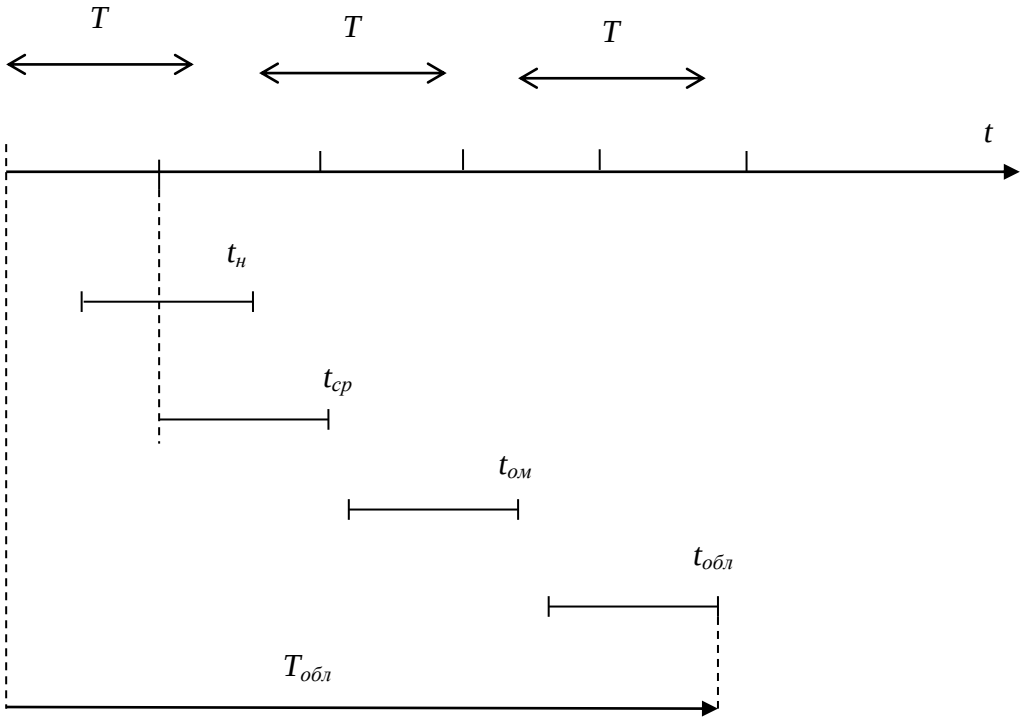


Рис.5 Временная диаграмма контроля несанкционированного доступа

Поэтому считается, что свои действия с частотой опроса датчиков он синхронизировать не сможет и может рассчитывать лишь на некоторую вероятность успеха, выражающуюся в вероятности попадания отрезка времени $\mathrm{t_н}$ в промежуток времени между импульсами опроса датчиков, равный T.

Согласно определению геометрической вероятности из курса теории вероятности получим выражение для определения вероятности успеха нарушителя в следующем виде:

$$P_{\text{нр}} = T - \frac{t_{\text{н}}}{T} = 1 - \frac{t_{\text{н}}}{T}. \qquad (7)$$

Тогда вероятность обнаружения несанкционированных действий нарушителя будет определяться выражением

$$P_{\text{об}} = 1 - P_{\text{нр}} \qquad (8)$$

или

$$P_{\text{об}} = \frac{t_{\text{н}}}{T}. \qquad (9)$$

При $t_н > T$ нарушитель будет обнаружен наверняка, т. е. $P_{об} = 1$. Во втором случае, когда $T < t_н < T_{обл}$, вероятность успеха нарушителя будет определяться по аналогии с предыдущим соотношением:

$$P_{нр} = 1 - \frac{t_н}{T_{обл}}. \qquad (10)$$

Вероятность обнаружения и блокировки несанкционированных действий нарушителя:

$$P_{обл} = (1 - P_{нр}); \qquad (11)$$

$$P_{обл} = \frac{t_н}{T_{обл}}. \qquad (12)$$

При $t_н > T_{обл}$ попытка несанкционированного доступа не имеет смысла, так как она будет обнаружена наверняка. В этом случае $T_{обл} = 1$.

Таким образом, расчет прочности преграды со свойствами обнаружения и блокировки можно производить по формуле

$$P_{СЗИ} = P_{обл} \cup (1 - P_{обх1}) \cup (1 - P_{обх2}) \cup \ldots \cup (1 - P_{обхj}) \qquad (13)$$

где j – число путей обхода этой преграды; U – знак «или».

Следует также отметить, что эта формула справедлива также и для организационной меры защиты в виде периодического контроля заданного объекта человеком. При этом полагаем, что обнаружение, определение места несанкционированного доступа и его блокировка происходят в одно время – в момент контроля объекта человеком, т. е. $T_{ср} = t_{ом} = t_{бл} = 0$, $T_{обл} = T$, где T период контроля человеком объекта защиты. Вероятность обнаружения и блокировки действий нарушителя будет определяться формулой 9.

Для более полного представления прочности преграды в виде автоматизированной системы обнаружения и блокировки несанкционированного доступа необходимо учитывать надежность ее функционирования и пути возможного обхода ее нарушителем.

Вероятность отказа системы определяется по известной формуле $P_{отк}(t) = e^{-\lambda t}$, (14)

где $\lambda -$ интенсивность отказов группы технических средств, составляющих систему обнаружения и блокировки несанкционированного доступа; $t -$ рассматриваемый интервал времени функционирования системы обнаружения и блокировки несанкционированного доступа.

С учетом возможного отказа системы контроля прочность преграды будет определяться по формуле

$$P_{\text{СЗИК}} = P_{\text{обл}}(1 - P_{\text{отк}}) \cup (1 - P_{\text{обх1}}) \cup (1 - P_{\text{обх2}}) \cup \ldots \cup \left(1 - P_{\text{обх}j}\right), \quad (15)$$

где $P_{\text{обл}}$ и $P_{\text{отк}}$ определяются соответственно по формулам (12) и (14); $P_{\text{обх}}$ и количество путей обхода j определяются экспертным путем на основе анализа принципов построения системы контроля и блокировки несанкционированного доступа.

Одним из возможных путей обхода системы обнаружения и блокировки может быть возможность скрытного отключения нарушителем системы обнаружения и блокировки (например, путем обрыва или замыкания контрольных цепей, подключения имитатора контрольного сигнала, изменения программы сбора сигналов и т. д). Вероятность такого рода событий определяется в пределах от 0 до 1 методом экспертных оценок на основе анализа принципов построения и работы системы. При отсутствии возможности несанкционированного отключения системы величина его вероятности равна нулю.

Таким образом, подводя итоги, сделаем вывод, что защитные преграды бывают двух видов:

- контролируемые человеком;
- неконтролируемые человеком.

Прочность ***неконтролируемой*** преграды рассчитывается по формуле (4), а ***контролируемой*** — по формуле (15). Анализ данных формул позволяет сформулировать первое правило защиты любого предмета:

Прочность защитной преграды является достаточной, если ожидаемое время преодоления ее нарушителем больше времени жизни предмета защиты

или больше времени обнаружения и блокировки его доступа при отсутствии путей скрытного обхода этой преграды.

Модель многозвенной защиты. В большинстве случаев защитный контур состоит из нескольких «соединенных» Примером такого вида защиты может служить помещение, в котором хранится аппаратура. В качестве преград с различной прочностью здесь могут служить стены, потолок, пол, окна и замок на двери между собой преград с различной прочностью. Модель такой защиты из нескольких звеньев представлена на рис.6.

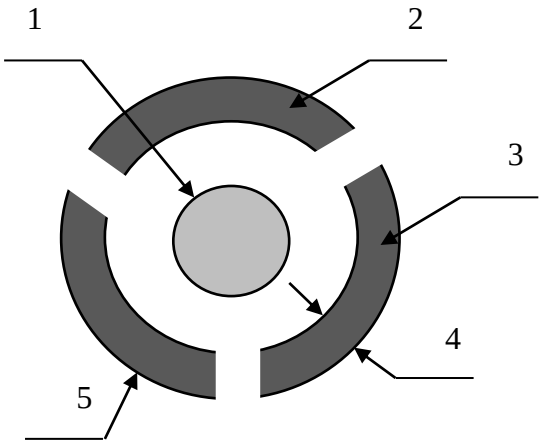


Рис.6 Модель многозвенной защиты: *1* — преграда 1; 2— преграда 2; *3* — предмет защиты; *4* — прочность преграды; 5 — преграда 3

Для информационной системы, модель которой представлена на рис.6, «соединение» преград (замыкание контура защиты) имеет тот же смысл, но иную реализацию[13]. Например, система контроля вскрытия аппаратуры и система опознания и разграничения доступа, контролирующие доступ к периметру информационной системы, на первый взгляд, образуют замкнутый защитный контур, но доступ к средствам отображения и документирования побочному электромагнитному излучению и наводкам (ПЭМИН), носителям информации и другим возможным каналам несанкционированного доступа к информации не перекрывают и, следовательно, таковыми не являются. Таким образом, в контур защиты в качестве его звеньев войдут еще система контроля доступа в помещения, средства защиты от ПЭМИН, шифрование и т. д. Все дело в точке отсчета, в данном случае в предмете защиты, т. е. контур защиты не будет замкнутым до тех пор, пока существует какая-либо

возможность несанкционированного доступа к одному и тому же предмету защиты.

Формальное описание для прочности многозвенной защиты практически совпадает с выражениями (2) и (15), так как наличие нескольких путей обхода одной преграды, не удовлетворяющих заданным требованиям, потребует их перекрытия соответствующими преградами. Тогда выражение для прочности многозвенной защиты при использовании неконтролируемых преград может быть представлено в виде:

$$P_{\text{СЗИ}} = P_{\text{СЗИ1}} \cup P_{\text{СЗИ2}} \cup P_{\text{СЗИ3}} \cup \ldots \cup P_{\text{СЗИ}i} \cup (1 - P_{\text{обх1}}) \cup (1 - P_{\text{обх2}}) \cup \ldots \cup (1 - P_{\text{обх}k}), \quad (16)$$

где $P_{\text{СЗИ}i}$ −прочность i −й преграды.

Выражение для прочности многозвенной защиты с контролируемыми преградами будет в следующем виде:

$$P_{\text{СЗИК}} = P_{\text{СЗИК1}} \cup P_{\text{СЗИК2}} \cup P_{\text{СЗИК3}} \cup \ldots \cup P_{\text{СЗИК}n} \cup (1 - P_{\text{обх1}}) \cup (1 - P_{\text{обх2}}) \cup \ldots \cup (1 - P_{\text{обх}j}), \quad (17)$$

где $P_{\text{СЗИК}n}$ − прочность n −й преграды.

Здесь следует подчеркнуть, что расчеты итоговых прочностей защиты для неконтролируемых и контролируемых преград должны быть раздельными, поскольку исходные данные для них различны, и, следовательно, это разные задачи, два разных контура защиты.

Если прочность слабейшего звена удовлетворяет предъявленным требованиям контура защиты в целом, возникает вопрос об избыточности прочности на остальных звеньях данного контура. Отсюда следует, что экономически целесообразно применять в многозвенном контуре защиты равнопрочные преграды.

При расчете прочности контура защиты со многими звеньями может случиться, что звено с наименьшей прочностью не удовлетворяет предъявленным требованиям. Тогда преграду в этом звене заменяют на более прочную или данная преграда дублируется еще одной преградой, а иногда двумя и более преградами. Но все дополнительные преграды должны

перекрывать то же количество или более возможных каналов несанкционированного доступа, что и первая. Тогда суммарная прочность дублированных преград будет определяться по формуле

$$P_{\Sigma} = 1 - \prod_{i=1}^{m}(1 - P_i), \qquad (18)$$

где $i = 1, m -$ порядковый номер преграды; $m -$ количество дублирующих преград; $P_i -$прочность $i -$ преграды.

4. Разработка методического обеспечения защиты автоматизированных систем от несанкционированного доступа

Осуществляется контроль не сетевых потоков, а структур более высокого уровня - информационных потоков. Каждый пакет должен быть отнесен к тому или иному информационному потоку. Таким образом контроль потоков влечет за собой контроль всего сетевого трафика.

Каждый поток идентифицируется с учетом определенных критериев/признаков соответствия:

- пользователь, инициирующий соединение;
- программа, инициирующая соединение или принимающая входящие соединения;
- узел отправитель пакета;
- узел получатель пакета;
- порт отправителя пакета;
- порт получателя пакета;
- используемый протокол прикладного уровня.

Каждый информационный поток может быть санкционированным и не санкционированным, далее, для простоты, будем называть не санкционированный информационный поток атакой.

Для разработки процедуры распознавания типа компьютерной атаки, требующей построения специальной системы распознавания, рассмотрим, что же представляет собой вероятность распознавания атаки.

Рассмотрено следующие случайные события:

- событие А- система обнаружения определяет атаку;
- событие $\overline{A}$ - система обнаружения не определяет атаку;
- событие В - атака;
- событие $\overline{B}$ - не атака.

Тогда:

– Р(АВ) - атака происходит и система обнаружения ее обнаруживает;

– $P(\overline{A}\,\overline{B})$ - атака не происходит и система обнаружения ее не обнаруживает;

– $P(\overline{A}B)$ - атаки нет, а система обнаружения говорит, что она есть;

– $P(A\overline{B})$ - атака есть, а система обнаружения говорит, что ее нет.

Полная группа событий:

$$P(AB) + P(\overline{A}\,\overline{B}) + P(\overline{A}B) + P(A\overline{B}) = 1.$$

Тогда вероятность правильного обнаружения атаки:

$$P_{ПРАВ.ОБНАРУЖЕНИЯ} = P(AB) + P(\overline{A}\,\overline{B}) = 1 - P(\overline{A}B) - P(A\overline{B}) =$$
$$= 1 - P(B)P_{В}(\overline{A}) - P(\overline{B})P_{\overline{В}}(A) = 1 - P(B)\alpha - P(\overline{B})\beta,$$

где б, в - ошибки 1-го и 2-го рода, составляющие 0,05.

Для минимизации защитных ресурсов необходимо уменьшать вероятности ложного срабатывания системы обнаружения атак, чтобы не терять производительность вычислительной системы на ликвидацию несуществующих каналов утечки[14].

Необходимо разработать методику идентификации типа компьютерной атаки, необходимую для количественной оценки вероятности идентификации компьютерной атаки и обоснования системы мер защиты.

Реализация процедуры распознавания типа компьютерной атаки требует построения специальной системы распознавания. Перед построением системы распознавания ее необходимо классифицировать, основываясь на следующих принципах. В зависимости от того, однородная или нет

информация используется для описания распознаваемых объектов, системы распознавания подразделяются на простые и сложные. В зависимости от количества априорной информации о распознаваемых объектах системы распознавания делятся на системы без обучения, обучающиеся и самообучающиеся. В зависимости от характера информации о признаках или свойств признаков распознаваемых объектов системы распознавания подразделяются на детерминированные, вероятностные, логические, структурные и комбинированные. В связи с очевидностью того, что процесс распознавания будет основан на анализе протоколов и значений конкретных их полей, имеющих известную структуру и бинарный характер, разрабатываемая система распознавания представляет собой простую систему распознавания без обучения, детерминированную. Алфавит классов представляет собой множество возможных решений системы управления, т. е. множество типов компьютерных атак, а признаки, на языке которых описываются классы - типы протоколов и значения их полей. Конкретные протоколы являются эталоном для системы распознавания.

Реализация может существенно отличаться от эталона, причиной чему могут быть как непреднамеренные искажения данных (например, помехи или сбои сетевого оборудования), так и преднамеренные искажения данных (т.е. конкретные атаки). Задача системы распознавания - отнести реализацию протокола (входной объект) к тому или иному классу. Наличие описаний классов на языке признаков позволяет определить оптимальные в смысле точности решения задачи распознавания границы между классами (решающие границы, решающие правила).

Протоколы, которые описываются n-мерными матрицами, в связи с тем, что служебные поля могут принимать различные значения, будут описываться применительно к нашей задаче вырожденными одномерными матрицами.

Введено расстояние рассматриваемые объекты можно охарактеризовать набором k-признаков, каждый из которых принимает

дискретное значение, то можно задать k-мерное векторное пространство, каждая координата которого представляет один признак. В этом случае объект задается некоторой точкой k-мерного пространства. Если ввести понятие расстояния, то объекты, в зависимости от расстояния друг от друга, можно считать сходными или различными.

Если различные объекты, занимают непересекающиеся характеристические объемы в k-мерном пространстве, то классификация объекта происходит в соответствии с положением области k-мерного пространства, в которой находится представляющая этот объект точка.

Исходной для методов автоматической классификации является таблица расстояний или различий.

Таблица логических данных содержит только нули и единицы, выражающие наличие или отсутствие соответствующей характеристики.

Существуют также удвоенные логические таблицы, где для каждого столбца $j \in J$ определяется новый столбец j, показывающий отсутствие характеристики j. Это "уравнивает" наличие и отсутствие свойства j. Помимо всего прочего, часто нет никаких причин приписывать единицу именно наличию свойства, а не его отсутствию[15]. Однако существуют ситуации, когда дублирование таблицы не является необходимым. В этих ситуациях система наблюдения не предусматривает симметрии, так что отсутствие каких-либо двух свойств вовсе не свидетельствует о сходстве. Выбор индекса Роджерса-Танимото для строк логической таблицы обосновывается тем, что он не меняется при ее удвоении.

В таблице 1. приведены несколько наиболее часто используемых расстояний, которые, конечно, не исчерпывают все возможные.

Таблица 1

Формула расчета расстояния	Автор
1-(N11/ (N11+ N01+ N10))	Жаккар
1-(2+ N11/(2+ N11+ N01+ N10))	Чекановски
1-((N11+ N00)/|J|	Сокэл и Миченер
1- N11/|J|	Рассел и Рао
(N10+ N01)/(N11+ N00)	Кульчински

1-(N11(1/ni-1/ni')/2)	Кульчински
1-(N11/(N11+2(N01+ N10)))	Сокэл и Снит
1- N11/(nini')1/2	Очаи
((N10+ N01)/|J|)1/2	Взвешенное евклидово

Для минимизации количества эталонов вводят "запрещающие" эталоны. "Запрещающий" эталон вводит в блок принятия решения опознающего устройства создаваемую им функцию принадлежности с отрицательным знаком. Такими эталонами будут являться описания конкретных видов атак.

В показателях сходства для логических таблиц используются следующие четыре величины:

- N11 - количество характеристик, общих для объектов i и i';
- N00 - количество характеристик, которыми не обладают ни i, ни i';
- N10 - количество характеристик, которыми обладает i, а i' не обладает;
- N01 - количество характеристик, которыми обладает i', а i не обладает.

Тогда индекс сходства Роджерса-Танимото будет выглядеть следующим образом:

$$S(i,i') = \frac{N_{11} + N_{00}}{N_{11} + N_{00} + 2(N_{10} + N_{01})}. \quad (1)$$

Приведено пример расчета индекса сходства на выбранной метрике.

Ограничим количество типов компьютерных атак до пяти, но учтем, что разрабатываемые программно-аппаратные комплексы необходимо оставлять открытыми для пополнения сигнатурами новых классов и признаков классов атак, т. к. нет никакой гарантии, что в ближайшее время компьютерные атаки не будут усложняться.

В таблице 2. приведены признаки каждого из выбранных в качестве примера видов атак.

Таблица 2

Алфавит классов	Признаки
Атака Land	Совпадение адресов отправителя и получателя пакета (в заголовке IP-пакета)
Использование ARP-запросов	"Нули" в поле "Аппаратный адрес получателя" в

	структуре сообщения ARP
Навязывание ложного маршрута с использованием протокола ICMP	Значение "1" поля "Код" в структуре заголовка сообщения ICMP "Redirect Message"
Передача широковещательного запроса ICMP Echo Request от имени "жертвы"	Значение "8" поля "Тип" сообщения ICMP ("Запрос эха") при условии наличия широковещательного адреса (FF-FF-FF-FF-FF-FF) на канальном уровне в заголовке IP-пакета
Нестандартные протоколы, инкапсулированные в IP	Нестандартное значение поля "Протокол верхнего уровня" в структуре заголовка IP-пакета

Множество классов будет состоять из шести классов, пять из которых представляют собой некоторые из рассмотренных выше типов компьютерных атак, а к шестому будут относиться объекты, выходящие за рамки данной классификации (неизвестные виды атак, неизвестные протоколы, пакеты, искаженные помехами и т. д.). Необходимо рассчитать коэффициент сходства эталона i’ с реализацией[16]. Решение об отнесении реализации i к тому или иному классу будет приниматься по значению коэффициента сходства (он должен быть максимальным).

При количестве атак, стремящемся к бесконечности, а также учитывая вероятностный характер реализаций коэффициент сходства будет иметь смысл вероятности сходства. Т. о. модель принятия решения будет иметь вид

$$P_{РАСПОЗНАВАНИЯ} = \max P_i. \quad (2)$$

Показателем идентификации типа КА выбирается вероятность распознавания Ррасп , а критерием Ррасп $\geq 0{,}9$.

В таблице 3. представлены реализации.

Таблица 3

Реализация
IP- пакет, в заголовке которого адреса отправителя и получателя пакета совпадают
Сообщение ARP с нулями в поле "Аппаратный адрес получателя"
Сообщение ICMP "Redirect Message" со значением "1" поля "Код" в структуре заголовка
Сообщение ICMP со значением "8" поля "Тип", в заголовке IP-пакета указан широковещательный адрес (FF-FF-FF-FF-FF-FF)
IP- пакет, в заголовке которого нестандартное значение поля "Протокол верхнего уровня"
Пакеты, выходящие за рамки данной классификации

В таблице 4. представлены характеристики реализаций 1 - 5 (словарь признаков системы распознавания).

Построено логическую таблицу. Множество I’ - это множество из пяти эталонов компьютерных атак (плюс один), а I - множество реализаций. Если атака i’∈ I’ содержит объект i∈ I, то $k_{I'I}(I', I) = 1$.

Рассчитано коэффициенты сходства между эталоном $i'_1 \in I'$ (атака Land) и реализациями i1-6∈ I. Коэффициенты сходства реализаций с другими эталонами рассчитываются аналогично.

Таблица 4

№ п/п	Признак	№ п/п	Признак
Заголовок IP-пакета		Сообщение ARP	
1	Номер версии	13	Тип сети
2	Длина заголовка	14	Длина аппаратного адреса
3	Тип сервиса	15	Тип протокола
4	Общая длина	16	Длина сетевого адреса
5	Идентификатор пакета	17	Тип операции
6	Флаги	18	Аппаратный адрес отправителя
7	Смещение фрагмента	19	IP-адрес отправителя
8	Время жизни	20	Аппаратный адрес получателя
9	Протокол верхнего уровня	21	IP-адрес получателя
10	Контрольная сумма	Сообщение ICMP	
11	IP-адрес источника	22	Заголовок IP-пакета (п/п 1-12)
		23	Тип сообщения ICMP
12	IP-адрес назначения	24	Код
		25	Контрольная сумма

$$P_{\text{расп}\ 1}(i_1, i_1^{'}) = \frac{N_{11} + N_{00}}{N_{11} + N_{00} + 2(N_{10} + N_{01})} = \frac{12 + 12}{12 + 12 + 2(0 + 0)} = 1;$$

$$P_{\text{расп}\ 2}(i_2, i_1^{'}) = \frac{N_{11} + N_{00}}{N_{11} + N_{00} + 2(N_{10} + N_{01})} = \frac{0 + 3}{0 + 3 + 2(9 + 12)} = 0,067\ ;$$

$$P_{\text{расп}\ 3}(i_3, i_1^{'}) = \frac{N_{11} + N_{00}}{N_{11} + N_{00} + 2(N_{10} + N_{01})} = \frac{12 + 9}{12 + 9 + 2(3 + 0)} = 0,777\ ;$$

$$P_{\text{расп}\ 4}(i_4, i_1^{'}) = \frac{N_{11} + N_{00}}{N_{11} + N_{00} + 2(N_{10} + N_{01})} = \frac{12 + 9}{12 + 9 + 2(3 + 0)} = 0,777\ ;$$

$$P_{\text{расп}\ 5}(i_5, i_1^{'}) = \frac{N_{11} + N_{00}}{N_{11} + N_{00} + 2(N_{10} + N_{01})} = \frac{10 + 12}{10 + 12 + 2(1 + 2)} = 0,786\ .$$

Система распознавания на основании модели принятия решения принимает решение об отнесении реализации i1 к первому классу атак.

5. Оценка уровня безопасности информации от преднамеренного несанкционированного доступа

Для оценки вероятности отражения угроз каждым из средств защиты использовался метод экспертной оценки.

Результат экспертной оценки вероятностей отражения угроз СЗИ приведен в таблице 1.

При использовании этого способа предположено, что $\forall\lambda_i = \alpha$, α = const, (1) что интенсивности угроз равные и равны константе. Таким образом, подставляя значения вероятностей p_i и сумму потерь C_i в формулу (1) получаем общий уровень защищенности системы равный:

D = 0.903932*100% = 90 %. (1)

Таблица вероятностей отражения угроз безопасности СЗИ, полученная экспертным методом оценки. Таблица 1

		Вероятность отражения угрозы с учетом средств защиты					Общая вероятность	Ci	Ci*(1-pi)
Вид уязвимости	Средство защиты	Межсетевой экран/NAT	VPN шлюз	Сервер обновлений	IDS	Антивирус		Ущерб, грн	
Троянские кони						0,95	0,95	30000	1500
Вирусы						0,90	0,9	10000	1000
DoS		0,80	0,99		0,99		0,99998	5000	0,1
DDoS		0,60	0,80		0,95		0,996	5000	20
Макро вирусы						0,60	0,6	30000	12000
Уязвимости ПО или ошибки				0,90			0,9	25000	2500
IP Spoofing		0,70	0,99		0,93		0,99979	20000	4,2
DNS Spoofing					0,90		0,9	25000	2500
WEB Spoofing					0,50		0,5	10000	5000
Захват сетевых подключений		0,50	0,99		0,90		0,9995	25000	12,5
Различные виды сканирования сети		0,60			0,90		0,96	5000	200
Недоступность данных					0,85		0,85	5000	750

Нарушение конфиденциальности данных		0,95	0,30			0,965	45000	1575
Некорректные параметры заголовков пакетов и запросов	0,7		0,5	0,8		0,97	9000	270
Автоматический подбор паролей (login)	0,75			0,9		0,975	35000	875
Атаки на протоколы			0,5	0,8		0,875	10000	1250
Неэффективный мониторинг событий безопасности в ИКС	0,3			0,7		0,79	25000	5250
Монополизация канала	0,6			0,9		0,96	4000	160
Неавторизованное использование прав(маскарадинг)	0,3			0,9		0,93	30000	2100
Манипуляция данных и ПО		0,5	0,6	0,3	0,6	0,944	25000	1400
Неконтролируемое использование ресурсов	0,5	0,6	0,3	0,8	0,6	0,9888	30000	336
Потеря конфиденциальности важных данных в UNIX системах	0,7	0,8			0,5	0,97	31000	930
Неавторизованное использование ИТ системы	0,6	0,7	0,3	0,8	0,66	0,99429	40000	228,48
Прослушивание сети		0,9				0,9	40000	4000
Злоупотребление правами пользователей и администраторов	0,1	0,1				0,19	10000	8100
Вредоносное ПО :spyware, adware				0,5	0,95	0,975	38000	950
Переполнение буфера			0,8			0,8	15000	3000
							582000	55911,28
Уровень защищенности								0,90393251

В данном случае была произведена оценка защищенности уже существующей реальной системы с необходимым набором средств защиты[17]. В практике чаще возникают ситуации когда необходимо выбрать из набора средств только те, которые в большей степени соответствуют нуждам компании, в данном случае обеспечивают наибольший уровень защиты, при этом система должна иметь минимальную стоимость и

оказывать минимальное воздействие на производительность всей системы в целом.

Применение методику для выбора оптимальной системы защиты для той же системы. При этом введено ограничения на стоимость такой системы защиты. Предположено, что система защиты должна составлять от 10 до 20 процентов от общей стоимости ИКС. Именно такой подход предлагают многие современные эксперты при оценке стоимости СЗИ. Допустим, что общая стоимость нашей ИКС согласно данных ее владельца составляет 150 000 грн. В этом случае целесообразно на систему защиты потратить 20000 грн. В общем случае ограничения на стоимость СЗИ ограничиваются сверху стоимостью информации.

Оценим уровень защищенности при использовании следующих средств защиты: МЭ, VPN-шлюз, сервер обновлений и сервер антивирусной защиты. Оценка приведена в таблице 2. В качестве альтернативного набора средств используется МЭ, VPN-шлюз, и систему IDS. Для такой системы уровень защиты будет равняться D = 0.697539*100% = 69 %. Стоимость второго решения будет составлять 35000-40000 грн.

Вероятностей отражения угроз СЗИ состоящей из 4 компонентов: МЭ, VPN-шлюз, сервер обновлений и сервер антивирусной защиты.

Вероятностей отражения угроз СЗИ Таблица 2

		Вероятность отражения угрозы с учетом средств защиты					Общая вероятность	Ci	Ci*(1-pi)
Вид уязвимости	Средство защиты	Межсетевой экран/NAT	VPN шлюз	Сервер обновлений	IDS	Антивирус		Ущерб, грн	
Троянские кони						0,95	0,95	30000	1500
Вирусы						0,90	0,9	10000	1000
DoS		0,80	0,99				0,998	5000	10
DDoS		0,60	0,80				0,92	5000	400
Макро вирусы						0,60	0,6	30000	12000
Уязвимости ПО или ошибки				0,90			0,9	25000	2500
IP Spoofing		0,70	0,99				0,997	20000	60
DNS Spoofing							0	25000	25000

WEB Spoofing						0	10000	10000
Захват сетевых подключений	0,50	0,99				0,995	25000	125
Различные виды сканирования сети	0,60					0,6	5000	2000
Недоступность данных						0	5000	5000
Нарушение конфиденциальности данных		0,95	0,30			0,965	45000	1575
Некорректные параметры заголовков пакетов и запросов	0,7		0,5			0,85	9000	1350
Автоматический подбор паролей (login)	0,75					0,75	35000	8750
Атаки на протоколы			0,5			0,5	10000	5000
Неэффективный мониторинг событий безопасности в ИКС	0,3					0,3	25000	17500
Монополизация канала	0,6					0,6	4000	1600
Неавторизованное использование прав(маскарадинг)	0,3					0,3	30000	21000
Манипуляция данных и ПО		0,5	0,6		0,6	0,92	25000	2000
Неконтролируемое использование ресурсов	0,5	0,6	0,3		0,6	0,944	30000	1680
Потеря конфиденциальности важных данных в UNIX системах	0,7	0,8			0,5	0,97	31000	930
Неавторизованное использование ИТ системы	0,6	0,7	0,3		0,66	0,97144	40000	1142,4
Прослушивание сети		0,9				0,9	40000	4000
Злоупотребление правами пользователей и администраторов	0,1	0,1				0,19	10000	8100
Вредоносное ПО: spyware, adware					0,95	0,95	38000	1900
Переполнение буфера			0,8			0,8	15000	3000
							582000	139122,4
Уровень защищенности								0,76095808

Стоит отметить что снижение производительности, оказываемое системой защиты на ИКС находится в пределах допустимых 10 процентов. В нашем случае уровень производительности системы задается каналом доступа в сеть интернет[18]. Для подключения к сети интернет вполне достаточной для нашей модели ИКС является скорость 10 мбит/с. Все средства, используемые для защиты работают со скоростью значительно превышающей 10 мбит/с и таким образом оказывают минимальное влияние на производительность системы.

Таблица вероятностей отражения угроз СЗИ состоящей из 3 компонентов: МЭ, VPN-люз, система IDS. Таблица 3

		Вероятность отражения угрозы с учетом средств защиты					Общая вероятность	Ci	Ci*(1-pi)
Вид уязвимости	Средство защиты	Межсетевой экран/NAT	VPN шлюз	Сервер обновлений	IDS	Антивирус		Ущерб, грн	
Троянские кони							0	30000	30000
Вирусы							0	10000	10000
DoS		0,80	0,99		0,99		0,99998	5000	0,1
DDoS		0,60	0,80		0,95		0,996	5000	20
Макро вирусы							0	30000	30000
Уязвимости ПО или ошибки							0	25000	25000
IP Spoofing		0,70	0,99		0,93		0,99979	20000	4,2
DNS Spoofing					0,90		0,9	25000	2500
WEB Spoofing					0,50		0,5	10000	5000
Захват сетевых подключений		0,50	0,99		0,90		0,9995	25000	12,5
Различные виды сканирования сети		0,60			0,90		0,96	5000	200
Недоступность данных					0,85		0,85	5000	750
Нарушение конфиденциальности данных			0,95				0,95	45000	2250
Некорректные параметры заголовков пакетов и запросов		0,7			0,8		0,94	9000	540
Автоматический подбор паролей (login)		0,75			0,9		0,975	35000	875
Атаки на протоколы					0,8		0,75	10000	2500
Неэффективный мониторинг событий безопасности в ИКС		0,3			0,7		0,79	25000	5250
Монополизация канала		0,6			0,9		0,96	4000	160

Неавторизованное использование прав(маскарадинг)	0,3			0,9		0,93	30000	2100
Манипуляция данных и ПО		0,5		0,3		0,65	25000	8750
Неконтролируемое использование ресурсов	0,5	0,6		0,8		0,96	30000	1200
Потеря конфиденциальности важных данных в UNIX системах	0,7	0,8				0,94	31000	1860
Неавторизованное использование ИТ системы	0,6	0,7		0,8		0,976	40000	960
Прослушивание сети		0,9				0,9	40000	4000
Злоупотребление правами пользователей и администраторов	0,1	0,1				0,19	10000	8100
Вредоносное ПО :spyware, adware				0,5		0,5	38000	19000
Переполнение буфера						0	15000	15000
							582000	176031,8
Уровень защищенности								0,697539863

Из проведенного анализа можно выделить как более эффективный первый набор СЗИ, так как он обеспечивает больший уровень защищенности и при этом требует меньших капиталовложений. С помощью методики мы определили, что для данного примера ИКС наиболее оптимальным решением по защите будет являться набор средств состоящий из: МЭ, VPN-шлюза, антивирусного сервера и сервера обновлений ПО. Если при анализе будет использоваться значительно большее количество вариантов СЗИ, для выбора наиболее эффективного может использоваться метод последовательных уступок, который был описан в предыдущем разделе.

Выводы по второй главе

Предложенный подход к созданию системы защиты информации является математической моделью функционирования автоматизированных систем общего вида в условиях постоянного внешнего влияния. Предлагаемая методика системы защиты информации от несанкционированного доступа позволяет полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности. Построенные моделей системы защиты информации от несанкционированного доступа, обеспечивают набором соответствующих средств защиты, перекрывающих определенное количество возможных каналов несанкционированного доступа в соответствии с ожидаемым классом потенциальных нарушителей. Разработанные методического обеспечения защиты автоматизированных систем от несанкционированного доступа идентифицирует с учетом определенных критериев и признаков соответствующих программных средств защиты информации. Проведенная оценка уровня безопасности информации от преднамеренней несанкционированного доступа, отражают угроз безопасности систем защиты информации, полученная экспертным методом оценки.

Глава III. Исследование программного средства защиты информации от несанкционированного доступа на базе алгоритма шифрования методом открытого ключа

1. Описание алгоритма программы на базе алгоритма шифрования методом открытого ключа

Требуется написать программу, осуществляющую:

– зашифрование содержания исходного текстового файла с расширением txt с получением текстового файла с расширением RSR, символы которого являются символами исходного файла, преобразованными по алгоритму шифрования методом открытого ключа (система RSA).

– расшифрование содержания текстового файла с расширением rsr по алгоритму шифрования методом открытого ключа с получением текстового файла, символы которого являются символами исходного текстового файла.

Описание алгоритма программы

Алгоритм программы заключается в следующем:

- при открытии файла код каждого символа запоминается в целочисленном массиве;
- в соответствии с введёнными пользователем значениями p и q (или значениями, используемыми по умолчанию) вычисляются и/или подбираются значения всех остальных чисел, участвующих в формировании ключа и формулах за- и расшифровывания;
- формируются открытый и закрытый ключи;
- массив исходных данных в соответствии с формулами за- и расшифровывания преобразуется в массив выходных данных;
- каждое значение массива выходных данных переводится в символ согласно таблице кодировок ANSI.

Как уже говорилось выше, надежность обуславливается практической неразрешимостью задачи разложения большого натурального числа на простые множители. Соответственно появляется и сложность в реализации

алгоритма работы с большими числами[19]. В данной программе данная проблема решается методом последовательного возведения в квадрат. После каждого возведения в квадрат результат сводится по модулю n. При этом никогда не возникает степеней больше n2.

Более подробно: рассмотрим двоичное представление r

$$r = \sum_{j=0}^{k} xj2j \ , \ xj = 0,1; \ k=[\log 2 \ r]+1$$

Предположено, что мы знаем все числа

(a2, mod n) , 0<=j<=k,

тогда (ar, mod n) может быть вычислено помощью не более k-1 произведений и сведением каждого произведения по модулю n. Таким образом, достаточно вычислить числа, которые требуют k модульных возведения в квадрат и дополнительно не более k –1 модульных произведений. Это означает, что вычисляется не более 2k – 1 произведений с обоими множителями, меньшими, чем n, и сведением произведений по модулю n. Если r является большим и известно m, то r может быть вначале взято по модулю

К примеру, вычисляя (783, mod 61),замечаем, что 760=1(mod61).Следовательно, мы можем вычислить (723, mod 61).С помощью возведения в квадрат мы получаем степени семёрки, где показатель в свою очередь является степенью двойки.

	j 0 1 2 3 4
72^j	7 49 22 54 16

Так как 23 = 10111, мы получаем желаемый результат следующим образом:

(723, mod 61) = (61*(22*(49*7)), mod 61) =17.

Описание алгоритма асимметричного метода шифрования с открытым ключом RSA

RSA очень медленный алгоритм. Для сравнения, на программном уровне DES по меньше мере в 100 раз быстрее RSA, на аппаратном в 1,000-10,000 раз, в зависимости от выполнения.

Алгоритм асимметричного метода шифрования с открытым ключом RSA:

1. Берутся два очень больших целых числа P и Q и находятся N=PQ и M=(P-1)(Q-1)

2. Выбирается случайное целое число D, взаимно простое с M и вычисляется E=(1MODM)/D

3. Потом публикуется D и N как открытый ключ, E сохраняется в тайне.

4. Если S - сообщение, длина которого, определяемая по значению выражаемого им целого числа, должна быть в интервале (1,N), то оно превращается в шифровку возведением в степень D по модулю N и отправляется получателю C=SD MOD N

5. Получатель сообщения расшифровывает его, возведя в степень E (число E ему уже известно) по модулю N, т.к. S=CE MOD N.

Структура программы

Данная программа написана на языке C# в соответствии с принципами структурного программирования и представляет собой набор процедур и функций, выполняющих определенные действия основной программы, осуществляющей синхронизацию процесса обработки данных и вызов соответствующих функций[20]. Такой подход к написанию программ позволяет с высокой степенью эффективности осуществлять их отладку, а также, изменять их функциональные возможности, так как в данном случае за каждую операцию, выполняемую программой, отвечает относительно автономная подпрограмма (процедура или функция).

Рассматриваемая программа предусматривает работу в диалоге с пользователем. Для этого разработана система меню и использована библиотека C#.

Основная программа представляет собой три этапа: подготовка к работе, сама работа и её завершение.

Алгоритм основной программы заключается в инициализации модулей программы и, в зависимости от выбора пользователя, управление передаётся одной из процедур или функций, находящейся в определённом модуле, либо осуществляется выход из программы. Все функции работают автономно и требуют для работы вызова основных модулей библиотеки C#.

Процедуры по обработке данных требуют предварительного введения исходных данных из файла.

Таким образом, с точки зрения пользователя программа представляет собой исполняемый EXE файл и два модуля небольшого размера. Для запуска программы используется EXE файл, действующий под управлением операционной системы Windows. Программный интерфейс программы представляет собой меню, из которого происходит доступ ко всем процедурам и функциям программы.

С точки зрения программиста программный продукт представляет собой структурированную программу на языке C#, хранящуюся в пяти исходных файлах, один из которых является главным и содержит код инициализации модулей, а четыре других являются модулями, содержащими основные процедуры и функции, выполняющие вычисления для преобразования символов. Таким образом, в текст программы, кроме основных подпрограмм управления процессом обработки информации и создающих интерфейс, входят следующие процедуры и функции:

- процедура вычисления n и m; в этой же процедуре находится d – взаимно обратное число с m и вычисляется e;
- функция для работы с большими числами, т.е. функция, осуществляющая алгоритм последовательного возведения в квадрат;

- функция возведения в степень (результат не должен превышать значение 9*1018);
- процедура зашифрования;
- процедура расшифрования.

Остальные процедуры и функции, использующиеся в программе, являются стандартными процедурами и функциями библиотеки языка C#.

2. Применение разработанной программы защиты информации от несанкционированного доступа

Описание интерфейса программы

Программа имеет удобный интерфейс, позволяющий работать с ней пользователям любого уровня. На рис.1. изображено начальное(стартовое) окно, предназначенное для ввода имени пользователя.

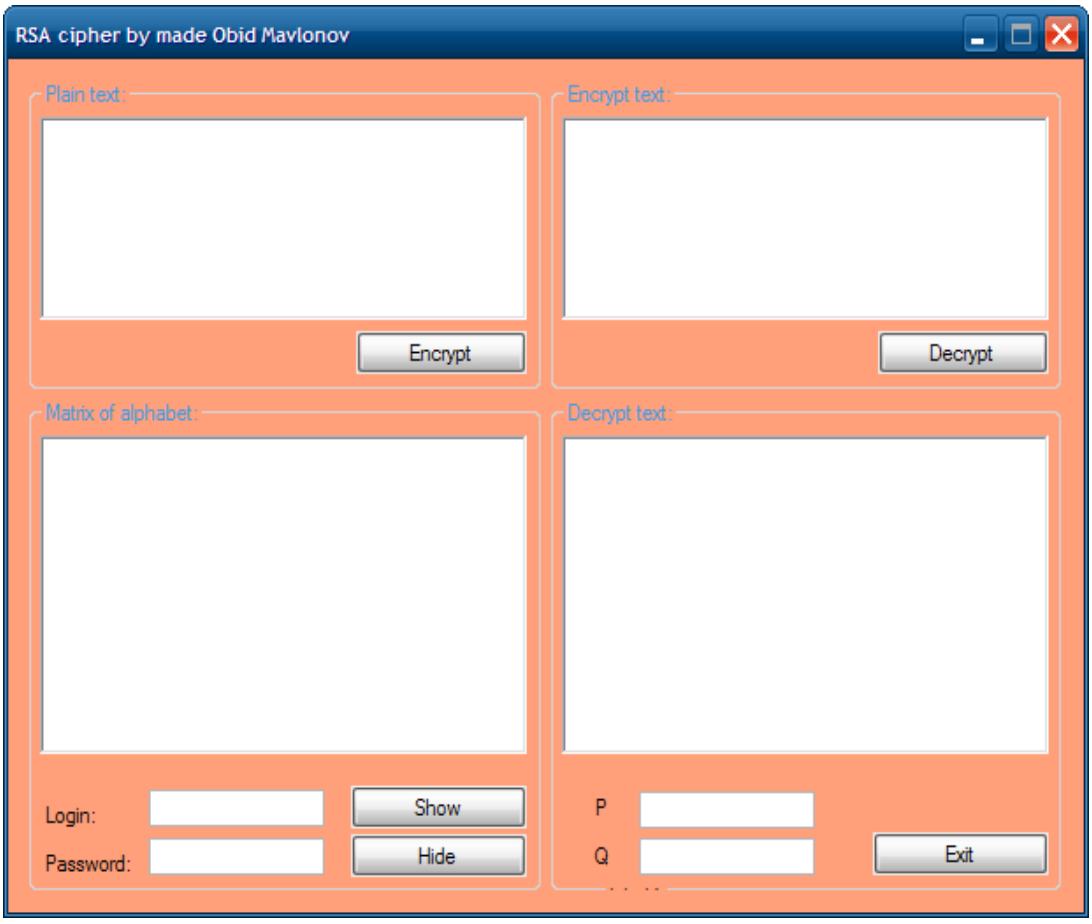


Рис.1 Начальное окно

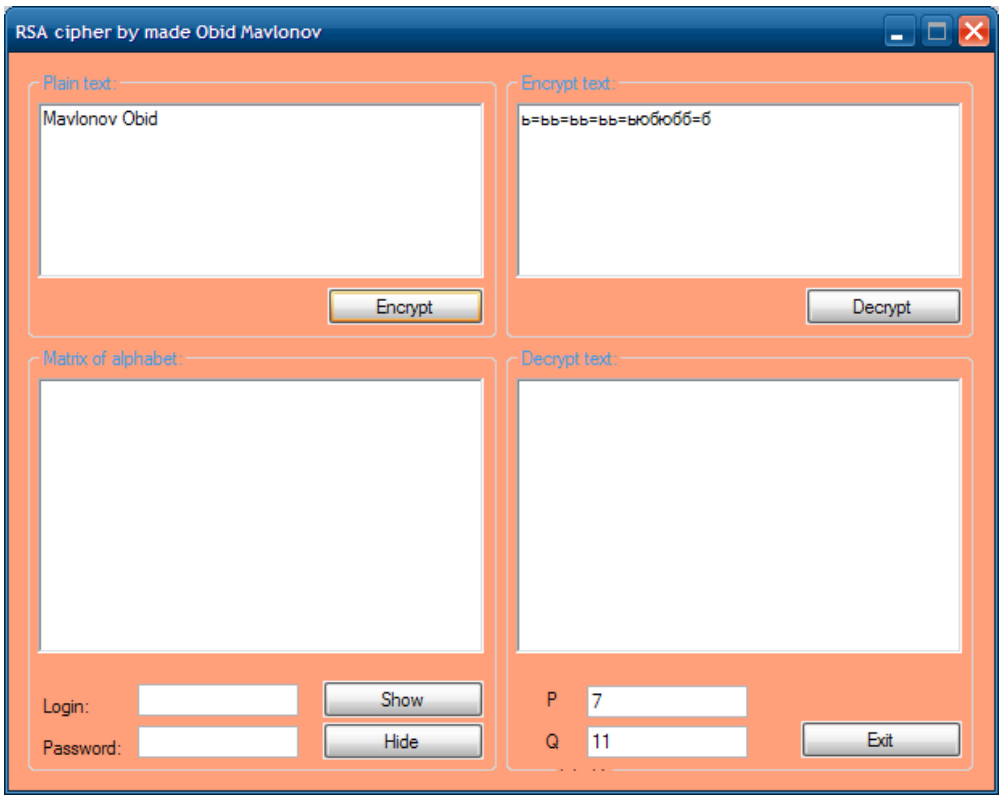


Рис.2 Окно программы шифрования информации

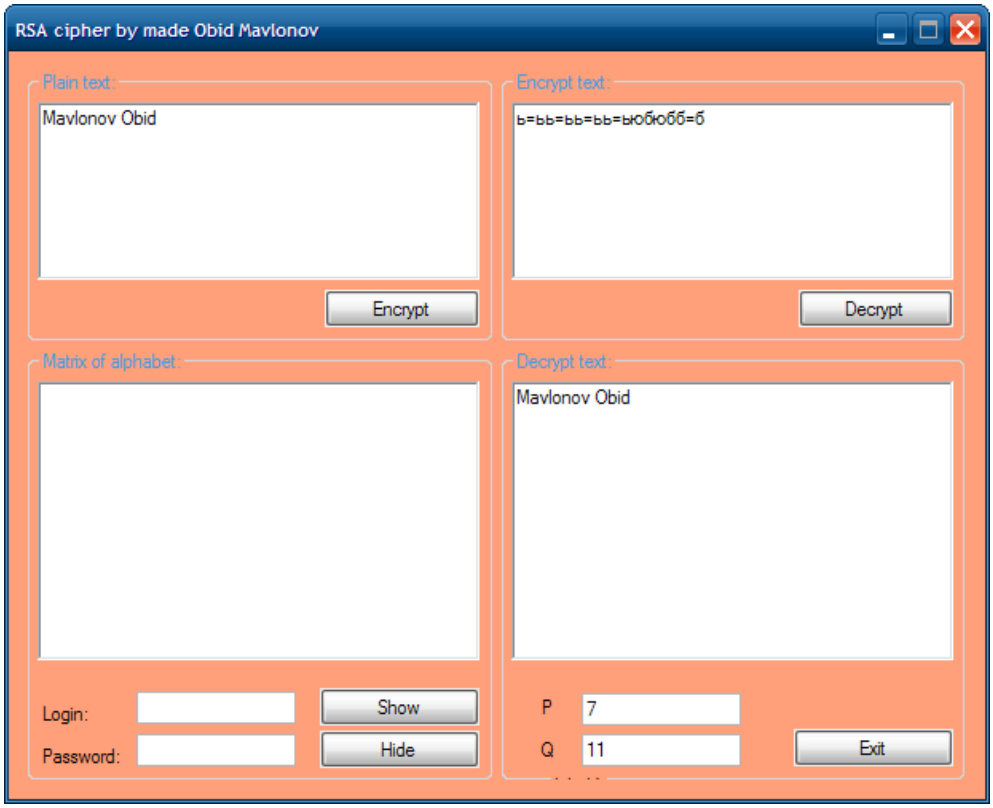


Рис.3 Окно программы дешифрования информации

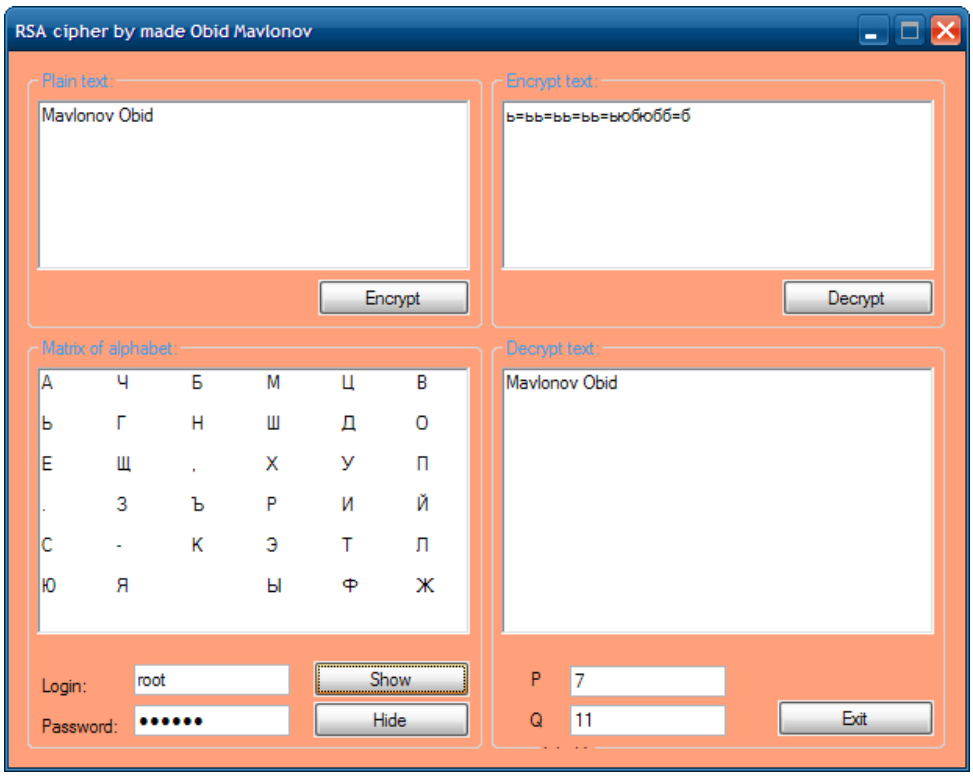


Рис.4 Окно матрица алфавита

Пользователь может использовать числа p и q, используемые для генерации открытого и закрытого ключей, как назначенные по умолчанию (это числа 127 и 331), так и собственные. Для записи собственных значений необходимо переключить режим Encryption Options в положение Personal. При обратном включении в положение Corporate текущие значения чисел p и q теряются и им присваиваются значения, назначенные по умолчанию.

Выводы по третьей главе

Данная программа разработана на базе алгоритма шифрования методом открытого ключа. Интерфейс программы удобен для использования. Выходные данные представлены в виде текстового файла. По своей структуре программа хорошо организована, что позволяет в случае необходимости легко ее модифицировать. Для проверки работоспособности программы и правильности обработки входных данных разработан тестовый пример. Тестирование программы подтвердило, что программа правильно выполняет обработку данных и выдаёт верные результаты.

Всё это свидетельствует о работоспособности программы и позволяет сделать вывод о пригодности программы к использованию её в целях шифрования данных.

Заключение

В заключении представлены основные результаты диссертационного исследования:

1. Исследованы потенциальные угрозы системы защиты информации от несанкционированного доступа.

2. Рассмотрены концепция защиты информации, излагающая систему взглядов и основных принципов, которые закладываются в основу проблемы защиты информации от несанкционированного доступа.

3. Приведены каналы и методы несанкционированного доступа к конфиденциальной информации.

4. Проведен анализ средств обеспечения защиты информации от несанкционированного доступа, позволяющий контролировать исходящий и входящий трафик, независимо от всех прочих системных защитных средств.

5. Предложен подход к созданию системы защиты информации от несанкционированного доступа в информационно-коммуникационных системах.

6. Предложена методика системы защиты информации от несанкционированного доступа, позволяющая проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности.

7. Построены моделей системы защиты информации от несанкционированного доступа в информационно-коммуникационных системах, перекрывающих определенное количество возможных каналов не-санкционированного доступа.

8. Разработаны методического обеспечения защиты автоматизированных систем от несанкционированного доступа, идентифицирующей определить критериев и признаков соответствующих программных средств защиты информации.

9. Была проанализирована оценка уровня безопасности информации от преднамеренней несанкционированного доступа.

10. Разработан программный модуль, позволяющий обеспечить защищенности информации от несанкционированного доступа в информационно-коммуникационных системах.

Список использованной литературы

1. Доклад Президента Республики Узбекистан Ислама Каримова на заседании кабинета министров, посвященном итогам социально-экономического развития страны в 2012 году и важнейшим приоритетным направлениям экономической программы на 2013 год.
2. Постановление Президента республики Узбекистан «О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий» (Собрание законодательства Республики Узбекистан, 2012 г., № 13, ст. 139).
3. А.Ю. Щеглов. Защита компьютерной информации от несанкционированного доступа. Наука и техника. Санкт-Петербург, 2004 г.
4. А.В. Васильков, И.А. Васильков. Безопасность и управление доступом в информационных системах. Форум, Москва, 2010 г.
5. Зима В.М., Молдавян А.А., Молдавян Н.А. Безопасность глобальных сетевых технологий. 2-е изд. СПб.: БХВ-Петербург, 2003. 368 с.
6. Германский стандарт «Руководство по защите информационных технологий для базового уровня защищенности».
7. Международный стандарт ISO 17799:2000 “Практические правила управления информационной безопасностью”.
8. Конеев И.Р., Беляев А.В.. Информационная безопасность предприятия. BHV-СПб. 2003.
9. Р. Финлейсон. Многоадресная IP-передача и брандмауэры (Ip multicast and firewalls). Рабочий документ RFC 2588, май 2005.
10. Мельников В. В. Безопасность информации в автоматизированных системах [Текст] : учебное пособие / В. В. Мельников. – М. : Финансы и статистика, 2009. – 368 с.: – ил. – 4000 экз. – ISBN: 5-279-02560-7.
11. Максимов, Ю. Н. Технические методы и средства защиты информации [Текст] : учебное пособие / Ю. Н. Максимов, В. Г. Сонников, В.

Г. Петров. – СПб : Полигон, 2000. – 314 с.: – ил. – 2000 экз. – ISBN: 5-89173-096-0.

12. Боридько, И.С., Забелинский, В.А., Тараскин, М.М. Методика исследования угроз, уязвимостей и рисков в организации. Монография. – М.:МИНИТ, 2013 г. – 124 с.

13. Галицкий А.. Защита информации в сети - анализ технологий и синтез решений. ДМК. 2004.

14. Системный анализ и принятие решений / В.И. Антюхов [и др.]; под ред. В.С. Артамонова. СПб.: С.-Петерб. ун-т ГПС МЧС России, 2009. 389 с.

15. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. — М.:Компания Айти ; ДМКПресс, 2004.

16. Л. Хмелев. Оценка эффективности мер безопасности, закладываемых при проектировании электронно-информационных систем. Труды научно-технической конференции "Безопасность информационных технологий", Пенза, июнь 2001.

17. Норткатт Стивен. Защита сетевого периметра. Dia Soft. 2004.

18. Стивен Норткат. Обнаружение нарушений безопасности в сетях. Изд.3. Диалектика-Вильямс. 2003.

19. Столлингс Вильям Криптография и защита сетей: принципы и практика, 2-е изд. – М. : Издательский дом «Вильямс», 2001.

20. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. — М.:ДМК, 2000.

21. Герберт Шилдт. Полный справочник по C#. Издательский дом "Вильяме", Москва, Санкт-Петербург. Киев 2004.

Приложение

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;

namespace Playfair_code
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }
        //матрица алфавита шифрования
       private string[,] encriptionMatrix =
                                           {
                                           {"А", "Ч", "Б", "М", "Ц", "В"},
//первая строка матрицы
                                           {"Ь", "Г", "Н", "Ш", "Д", "О"},
//вторая строка матрицы
                                           {"Е", "Щ", ",", "Х", "У", "П"},
//третья строка матрицы
                                           {".", "З", "Ъ", "Р", "И", "Й"},
//четвертая строка матрицы
                                           {"С", "-", "К", "Э", "Т", "Л"},
//пятая строка матрицы
                                           {"Ю", "Я", " ", "Ы", "Ф", "Ж"}
//шестая строка матрицы
                                           };

       private string text; //исходный текст для шифрования

       private int i_first = 0, j_first = 0;  //координаты первого символа
пары
       private int i_second = 0, j_second = 0;//координаты второго символа
пары
       private string  s1 = "", s2 = ""; //строки для хранения зашифрованного
символа
       private string encodetString; //зашифрованая строка
       private string decodetString; //расшифрованная строка
       private string login; //логин
       private string pass; //пароль

       #region Кодирование текста

       private void button1_Click(object sender, EventArgs e)
       {
            text = "";
            encodetString = "";

            text = Convert.ToString(richTextBox1.Text).ToUpper();
            int t = text.Length; //длина входного слова
            int i, j;
            ///проверяем, четное ли число символов в строке
            int temp = t % 2;
            if (temp != 0) //если нет
            {               //то добавляем в конец строки символ " "
```

```
                text = text.PadRight((t + 1), ' ');
            }

            int len = text.Length / 2; /*длина нового массива -
                                                    равная половине длины
входного слова
                                                     т.к. в новом масиве каждый
элемент будет
                                                       содержать 2 элемента из
старого массива*/

            string[] str = new string[len]; //новый массив

            int l = -1; //служебная переменная

            for (i = 0; i < t; i += 2) //в старом массиве шаг равен 2
            {
                l++; //индексы для нового массива
                if (l < len)
                {
                    //Элемент_нового_массива[i] =  Элемент_старого_массива[i]
+  Элемент_старого_массива[i+1]
                    str[l] = Convert.ToString(text[i]) +
Convert.ToString(text[i + 1]);
                }

            }

            ///координаты очередного найденного символа из каждой пары

            foreach (string both in str)
            {
                for (i = 0; i < 6; i++)
                {
                    for (j = 0; j < 6; j++)
                    {
                        //координаты первого символа пары в исходной матрице
                        if (both[0] == Convert.ToChar(encriptionMatrix[i,
j]))
                        {
                            i_first = i;
                            j_first = j;

                        }

                        //координаты второго символа пары в исходной матрице
                        if (both[1] == Convert.ToChar(encriptionMatrix[i,
j]))
                        {
                            i_second = i;
                            j_second = j;

                        }
                    }
                }

                ///если пара символов находится в одной строке
                if (i_first == i_second)
                {
                    if (j_first == 5) /*если символ последний в строке,
                                       кодируем его первым символом из
матрицы*/
                    {
```

```
                        s1 = Convert.ToString(encriptionMatrix[i_first, 0]);
                    }
                    //если символ не последний, кодируем его стоящим справа
от него
                    else
                    {
                        s1 = Convert.ToString(encriptionMatrix[i_first,
j_first + 1]);
                    }

                    if (j_second == 5) /*если символ последний в строке
                                        кодируем его первым символом из
матрицы*/
                    {
                        s2 = Convert.ToString(encriptionMatrix[i_second, 0]);
                    }
                    //если символ не последний, кодируем его стоящим справа
от него
                    else
                    {
                        s2 = Convert.ToString(encriptionMatrix[i_second,
j_second + 1]);
                    }

                }

                ///если пара символов находится в одном столбце
                if (j_first == j_second)
                {
                    if (i_first == 5)
                    {
                        s1 = Convert.ToString(encriptionMatrix[0, j_first]);
                    }
                    else
                    {
                        s1 = Convert.ToString(encriptionMatrix[i_first + 1,
j_first]);
                    }

                    if (i_second == 5)
                    {
                        s2 = Convert.ToString(encriptionMatrix[0, j_second]);
                    }

                    else
                    {
                        s2 = Convert.ToString(encriptionMatrix[i_second + 1,
j_second]);
                    }
                }

                ///если пара символов находиться в разных столбцах и строках
                if (i_first != i_second && j_first != j_second)
                {

                    s1 = Convert.ToString(encriptionMatrix[i_first,
j_second]);
                    s2 = Convert.ToString(encriptionMatrix[i_second,
j_first]);
                }

                if (s1 == s2)
                {
```

```
                encodetString = encodetString + s1 + "=" + s2;
            }
            else
            {

                //записыавем результат кодирования
                encodetString = encodetString + s1 + s2;
            }

            richTextBox2.Text = encodetString.ToLower();
        }
    }

    #endregion



    private void button3_Click(object sender, EventArgs e)
     {


        int count = 0;
        login = Convert.ToString(textBox1.Text);
        pass = Convert.ToString(textBox2.Text);

        if (login == "root" && pass == "qwerty")
        {
            foreach (string s in encriptionMatrix)
            {
                count++;
                if (count != 6)
                {
                    richTextBox3.Text += s + "\t";
                }
                if (count == 6)
                {
                richTextBox3.Text += s + "\t\n";
                count = 0;
                }
            }
        }
        else
        {
            MessageBox.Show("Notugri login va parol", "Xatolik sodir
buldi", MessageBoxButtons.OK, MessageBoxIcon.Warning);

        }
     }

     private void button4_Click(object sender, EventArgs e)
     {
        richTextBox3.Clear();
        textBox2.Clear();

     }


     #region Раскодирование текста
     private void button2_Click_1(object sender, EventArgs e)
     {
        decodetString = "";
```

```
            string tempString = ""; //переменная для хранения строки
подлежащей расшифровке
            int i, j;

            //удаляем символы "-" из зашифрованной строки
            for (i = 0; i < encodetString.Length; i++)
            {
                if (encodetString[i] != '=')
                {
                    tempString = tempString + encodetString[i].ToString();
                }
            }
            //MessageBox.Show(tempString);


            int len = tempString.Length / 2; /*длина нового массива -
                                                равная половине длины
входного слова
                                                 т.к. в новом масиве каждый
элемент будет
                                                   содержать 2 элемента из
старого массива*/

            string[] str2 = new string[len]; //новый массив

            int l = -1; //служебная переменная

            for (i = 0; i < tempString.Length; i += 2) //в старом массиве шаг
равен 2
            {
                l++; //индексы для нового массива
                if (l < len)
                {
                    //Элемент_нового_массива[i] =  Элемент_старого_массива[i]
+  Элемент_старого_массива[i+1]
                    str2[l] = Convert.ToString(tempString[i]) +
Convert.ToString(tempString[i + 1]);
                }

            }


            foreach (string both in str2)
            {
                for (i = 0; i < 6; i++)
                {
                    for (j = 0; j < 6; j++)
                    {
                        //координаты первого символа пары в исходной матрице
                        if (both[0] == Convert.ToChar(encriptionMatrix[i,
j]))
                        {
                            i_first = i;
                            j_first = j;
                        }

                        //координаты второго символа пары в исходной матрице
                        if (both[1] == Convert.ToChar(encriptionMatrix[i,
j]))
                        {
                            i_second = i;
                            j_second = j;
                        }
```

```
                    }
                }

                if (s1 == s2)
                {
                    if (i_first != 0 && i_second != 0)
                    {
                        s1 = Convert.ToString(encriptionMatrix[i_first - 1,
j_first]);
                        s2 = Convert.ToString(encriptionMatrix[i_second - 1,
j_second]);
                    }
                    else
                    {
                        s1 = Convert.ToString(encriptionMatrix[5, j_first]);
                        s2 = Convert.ToString(encriptionMatrix[5, j_second]);
                    }

                }
                if (s1 != s2)
                {
                    if (i_first == i_second)
                    {
                        if (j_first == 0) /*если символ первый в строке,
                                          кодируем его последним символом из
матрицы*/
                        {
                            s1 = Convert.ToString(encriptionMatrix[i_first,
5]);
                        }
                        //если символ не последний, кодируем его стоящим
справа от него
                        else
                        {
                            s1 = Convert.ToString(encriptionMatrix[i_first,
j_first - 1]);
                        }

                        if (j_second == 0) /*если символ последний в строке
                                          кодируем его первым символом из
матрицы*/
                        {
                            s2 = Convert.ToString(encriptionMatrix[i_second,
5]);
                        }
                        //если символ не последний, кодируем его стоящим
справа от него
                        else
                        {
                            s2 = Convert.ToString(encriptionMatrix[i_second,
j_second - 1]);
                        }

                    }
                    ///если пара символов находится в одном столбце
                    if (j_first == j_second)
                    {
                        if (i_first == 0)
                        {
                            s1 = Convert.ToString(encriptionMatrix[5,
j_first]);
                        }
                        else
```

```
                        {
                            s1 = Convert.ToString(encriptionMatrix[i_first -
1, j_first]);
                        }

                        if (i_second == 0)
                        {
                            s2 = Convert.ToString(encriptionMatrix[5,
j_second]);
                        }

                        else
                        {
                            s2 = Convert.ToString(encriptionMatrix[i_second -
1, j_second]);
                        }
                    }

                    ///если пара символов находиться в разных столбцах и
строках
                    if (i_first != i_second && j_first != j_second)
                    {

                        s1 = Convert.ToString(encriptionMatrix[i_first,
j_second]);
                        s2 = Convert.ToString(encriptionMatrix[i_second,
j_first]);

                    }
                }


                decodetString = decodetString + s1 + s2;
            }


            richTextBox4.Text = decodetString.ToLower();
        }
        #endregion


        private void button5_Click(object sender, EventArgs e)
        {
            Application.Exit();
        }



    }
}
```