Практическая работа №5

ИССЛЕДОВАНИЕ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ПАРОЛЬНЫХ СРЕДСТВ АУТЕНТИФИКАЦИИ ОКОНЕЧНЫХ СЕТЕВЫХ УСТРОЙСТВ

Цель работы. Изучить принципы парольной аутентификации субъектов оконечных устройств телекоммуникационных систем и оценить их эффективность.

Краткие сведения из теории

Реализация процедур опознания, которые включают в себя идентификацию и аутентификацию, является общей проблемой для любых управляющих систем, в которых требуется обеспечивать разграничение доступа к обрабатываемой информации. Особенно актуален этот вопрос для систем, управляющих стратегическими процессами в транспортных отраслях народного хозяйства.

Функционирование всех механизмов разграничения доступа, использующих аппаратные или программные средства, основано на предположении, что любой субъект системы представляет собой конкретное лицо. Следовательно, существует некоторый механизм, обеспечивающий установление подлинности субъекта, обращающегося к системе. **Идентификация** – это процесс распознавания субъекта с помощью заранее присвоенного идентификатора. **Аутентификация** – это процесс, заключающийся в проверке подлинности субъекта.

Таким образом, **средство аутентификации** – это программный модуль или аппаратно-программное устройство, которое обеспечивает проверку подлинности субъекта, т. е. устанавливает, является ли он тем, за кого себя выдает.

В общем случае существуют три класса опознания, на основании которых строятся все средства аутентификации. Эти классы *базируются*:

а) на условных, заранее присваиваемых признаках (сведениях), известных субъекту (что знает субъект);

б) физических средствах, действующих аналогично физическому ключу (что имеет субъект);

в) индивидуальных характеристиках субъекта, его физических данных, позволяющих выделить его среди других лиц (что присуще субъекту).

Рассмотрим данные классы подробнее.

1.1 Методы опознания на основе различных принципов

Что знает субъект. Парольные методы проверки подлинности субъектов при входе в систему могут применятся на основе простых и динамически изменяющихся паролей.

При использовании метода простого пароля его значение не изменяется в течение установленного администратором службы безопасности времени действия.

Метод простых паролей заключается в том, что субъект на клавиатуре пульта ввода данных, или на специально имеющемся наборном поле набирает только ему известную комбинацию букв и цифр, являющуюся, собственно, паролем. Данный пароль сравнивается с эталонным, хранящимся в системе, и при положительном результате проверки субъект получает доступ к системе. Данная схема опознания является простой с точки зрения реализации, так как не требует никакой специальной аппаратуры и реализуется посредством небольшого объема программного обеспечения.

Схема с простым паролем имеет два недостатка:

– сложность запоминания для большинства субъектов произвольного набора символов, используемого в качестве пароля;

– уязвимость пароля при наборе, так как его значение можно «подсмотреть».

Модернизацией схемы простого пароля является *схема паролей однократного использования*. В этой схеме субъекту выдается список из N паролей. Такие же N паролей хранятся в системе. Здесь при каждом обращении к системе синхронно используется пароль с текущим номером, а все пароли с предыдущими номерами вычеркиваются. В случае если старый пароль из предыдущего сеанса стал известен другому субъекту, система его не воспринимает, так как действующим будет следующий по списку пароль. Данная схема обеспечивает большую степень безопасности, но она является и более сложной.

Схема паролей однократного использования имеет следующие недостатки:

– субъект должен помнить или иметь при себе весь список паролей и следить за текущим паролем;

– в случае, если встречается ошибка в процессе передачи, трудно определить, следует ли передавать тот же самый пароль или послать следующий;

– необходимо иметь разные таблицы паролей для каждого субъекта, так как может произойти рассинхронизация работы.

Последний недостаток можно устранить, используя так называемый генератор паролей. Его применение избавляет от необходимости хранить таблицы паролей для каждого субъекта, однако первые два недостатка данной схемы сохраняются.

При использовании динамически изменяющегося пароля его значение для каждого нового сеанса работы изменяется по определённым правилам.

Методы проверки подлинности на основе динамически изменяющегося пароля обеспечивают большую безопасность, так как частота смены паролей в них максимальна – пароль для каждого субъекта меняется ежедневно или через несколько дней. При этом каждый следующий пароль по отношению к предыдущему изменяется по правилам, зависящим от используемого метода проверки подлинности.

Существуют следующие методы парольной защиты, основанные на использовании динамически изменяющегося пароля:

– модификации схемы простых паролей;

– «запрос-ответ»;

– функциональные.

К *методам модификации схемы простых паролей* относят случайную выборку символов пароля и одноразовое использование паролей. При применении данного метода каждому субъекту выделяется достаточно длинный пароль, причем каждый раз для опознавания используется не весь пароль, а только его некоторая часть. В процессе проверки подлинности система запрашивает у субъекта группу символов по заданным порядковым номерам. Количество символов и их порядковые номера для запроса определяются с помощью датчика псевдослучайных чисел.

При одноразовом использовании паролей каждому субъекту выделяется список паролей. В процессе запроса номер пароля, который необходимо ввести, выбирается последовательно по списку или по схеме случайной выборки.

Недостатком методов модификации схемы простых паролей является необходимость запоминания субъектами длинных паролей или их списков. Запись же паролей на бумагу или в записные книжки приводит к появлению риска потери или хищения носителей информации с записанными на них паролями.

При использовании *метода «запрос-ответ»* заблаговременно создается и особо защищается массив вопросов, включающий в себя как вопросы общего характера, так и персональные вопросы, относящиеся к конкретному субъекту, например, вопросы, касающиеся известных только субъекту сведений из его жизни. В методе «запрос-ответ» набор ответов на m стандартных и n ориентированных на субъекта вопросов хранится в ЭВМ и управляет программой опознания. Когда субъект делает попытку включиться в работу, программа опознания случайным образом выбирает и задает ему некоторые (или все) из этих вопросов. Субъект должен дать правильный ответ на все вопросы, чтобы получить разрешение на доступ к системе. Вопросы могут быть выбраны таким образом, чтобы субъект запомнил ответы и не записывал их.

Основным требованием к вопросам в данном методе аутентификации является уникальность, подразумевающая, что правильные ответы на вопросы знают только субъекты, для которых эти вопросы предназначены.

Модификация этого метода предполагает изменение каждый раз одного или более вопросов, на которые субъект давал ответ до того.

Существует два варианта использования метода «запрос-ответ», вытекающие из условий $m = 0$ или $n = 0$. Вариант с $m = 0$ предполагает, что вопросы составлены на основе различных фактов биографии индивидуального субъекта, представляют собой имена его друзей, дальних родственников, старые адреса и т. д. На опознавательный вопрос субъект, который его сам предложил, всегда даст правильный ответ, что не сможет сделать злоумышленник.

Иногда предпочтительнее вариант с $n = 0$, т. е. субъектам задается большее количество стандартных вопросов, и от них требуются ответы на те, которые они сами выберут. Достоинство рассмотренной схемы в том, что субъект может выбирать вопросы, а это дает весьма хорошую степень безопасности в процессе включения в работу. В то же время нет необходимости хранить в системе тексты вопросов для каждого субъекта, достаточно хранить указатели на вопросы, выбранные данным субъектом, вместе с информацией, устанавливающей его подлинность. Текст каждого стандартного вопроса необходимо ввести для хранения только один раз, поэтому в системе с большим числом субъектов это может дать экономию памяти.

Метод «запрос-ответ» наряду с достоинствами все же имеет недостатки, ограничивающие возможность его использования. Во-первых, он требует проявления изобретательности со стороны самих субъектов, что для них является дополнительной нагрузкой. Во-вторых, для большинства людей опознавательные вопросы и ответы, как правило, приобретают стереотипность, и весьма вероятно, что настойчивый нарушитель может, собрав статистику, подготовиться по многим вопросам. В-третьих, метод требует обмена множеством опознавательных запросов и соответствующих им ответов, что для субъектов является сложным и утомительным. Кроме того, в силу его некоторой громоздкости метод «запрос-ответ» может удачно использоваться только для небольших организованных групп субъектов и неприменим для массового использования.

Среди *функциональных методов* наиболее распространенными являются метод функционального преобразования пароля, а также метод «рукопожатия».

В процессе «рукопожатия» субъект должен обменяться с алгоритмом последовательностью паролей (команд), которые должны быть названы правильно и в правильной последовательности, хотя сам субъект не знает алгоритма. Правильное завершение алгоритма подтверждает подлинность субъекта.

Метод функционального преобразования основан на использовании некоторой функции F, которая должна удовлетворять следующим требованиям:

– для заданного числа или слова X легко вычислить $Y = FA(X)$;

– зная X и Y, сложно или невозможно определить функцию $Y = FA(X)$.

Необходимым условием выполнения данных требований является наличие в функции $FA(X)$ динамически изменяющихся параметров, например, текущих даты, времени, номера дня недели или возраста субъекта.

Метод «рукопожатия» заключается в следующем. Для установления подлинности система выдает субъекту число, выбранное случайным образом, а затем запрашивает от него ответ. Для подготовки ответа субъект A применяет собственное, заранее подготовленное преобразование F_A. Информацией, на основе которой принимается решение, здесь является не пароль, а преобразование F_A. ЭВМ посылает значение X, а субъект отвечает значением $F_A(X)$. Любое постороннее лицо для проникновения в систему даже в случае знания значений X и $F_A(X)$ должно тем не менее отгадать функцию преобразования на основе нескольких вводов и выводов, так как сама функция преобразования никогда не передается по линиям связи, по которым посылается только X и $F_A(X)$. Функция преобразования может быть различной для каждого субъекта, что позволяет однозначно идентифицировать каждое лицо, обращающееся к системе.

С целью достижения высокого уровня безопасности функция преобразования пароля, задаваемая для каждого субъекта, должна периодически меняться. Для высокой безопасности функцию «рукопожатия» целесообразно циклически менять через определенные интервалы времени.

Достоинством метода «рукопожатия» является то, что никакой конфиденциальной информации между субъектом и системой не передается. По этой причине эффективность данного метода особенно велика при его применении в вычислительных сетях для подтверждения подлинности субъектов, пытающихся осуществить доступ к серверам или центральным ЭВМ.

В некоторых случаях может оказаться необходимым субъекту проверить подлинность той ЭВМ, к которой он хочет осуществить доступ. Необходимость во взаимной проверке может понадобиться и когда два субъекта хотят связаться друг с другом по линии связи. Методы простых паролей, а также методы модификации схем простых паролей в этом случае не подходят. Наиболее подходящим здесь является метод «рукопожатия». При его использовании ни один из участников сеанса связи не будет получать никакой секретной информации.

Способ «рукопожатия» более труден для раскрытия, чем пароль, но сложнее в реализации. В отличие от паролей преобразование никогда не появляется в линиях связи, однако в силу своей неизменности также может быть достаточно просто определено. Основным недостатком метода «рукопожатия» является временная задержка, выражающаяся в необходи-

мости, как в методе «запрос-ответ», организации обмена несколькими сообщениями между субъектом и системой в процессе опознания.

Что имеет субъект. К этому классу опознания относятся методы, основывающиеся на физических средствах, которые имеет при себе данный субъект, обращающийся к системе. К ним относятся идентификационные карты с перфорированным или магнитным кодом, а также ряд активных устройств, называемых электронными ключами, включающих в себя: смарт-карты с процессорами, USB-брелоки, устройства Touch Memory и прочие подобные технические средства.

В магнитных картах информация записывается на нескольких дорожках магнитного слоя и представляет собой данные, используемые для идентификации. К этим данным относятся: номер субъекта или его имя, пароль, количество допустимых использований карты и т. д. Наряду с очевидной простотой использования магнитные карты обладают низкой защищенностью от копирования содержимого. Для защиты от копирования магнитные карты снабжаются различными защитными средствами. Один из методов состоит в *нанесении магнитного слоя обычного типа поверх второго слоя* с более высокой коэрцитивной силой, т. е. для изменения состояния того слоя требуется более сильное магнитное поле. Тогда обычными методами невозможно считать или изменить запись нижнего слоя. Считывающее устройство, читая карту, содержащую идентификатор, вначале создает поле, стирающее любую запись, сделанную обычным способом, а затем уже считывает лежащую ниже «твердую» запись, в которой действительно находится информация.

Другой метод использует *постоянную магнитную разметку ленты*, которая наносится в процессе ее производства. Метод, известный под названием «влажной разметки», состоит в определенной ориентации осей ферромагнитных кристаллов, пока наполнитель еще не высох, причем селективная ориентация осей кристаллов в различных частях ленты создает магнитную запись, которую никак нельзя изменить. Чтобы прочесть эту запись, кристаллы необходимо подвергнуть воздействию постоянного магнитного поля с определенной ориентацией. Изменение положения кристаллов вдоль ленты будет наводить внешнее поле, которое можно прочитать с помощью обычных удобно расположенных головок. Изготовленные таким образом идентификационные карточки могут обеспечить «уникальную» идентичность, которую трудно подделать, поскольку для этого требуется овладеть технологией производства магнитных покрытий и влажной разметки.

Ясно, что для осуществления защиты от подделки или копирования карточки требуют сложной технологии их изготовления и, соответственно, сложной аппаратуры для считывания записанной на них информации. Следует отметить, что при любых способах достичь абсолютной защиты от ко-

пирования магнитных карт практически невозможно, так как носитель всегда открыт для доступа посторонних лиц.

Электронный ключ в самом общем смысле представляет собой физический носитель идентификатора субъекта, его пароля. В отличие от парольных систем при использовании электронного ключа субъект имеет ряд преимуществ:

– ему не надо запоминать значение пароля, так как пароль записан в ключе;

– он освобожден от функции защиты пароля от компрометации при его вводе, так как пароль считывается из ключа;

– все функции по защите от подделки пароля или его несанкционированного использования (метод разовых паролей, метод «рукопожатия») возлагаются на электронный ключ;

– идентификатор можно сделать сколь угодно большим, так как субъект с ним не работает.

В силу того что, как и идентификационная магнитная карта, электронный ключ является физическим средством хранения идентификатора субъекта, его можно скопировать и подделать. В основном все многообразие электронных ключей и классифицируется по основному признаку, определяющему их защищенность от копирования и подделки, так как быстродействие, объем хранимого идентификатора, габариты и другие характеристики являются, по существу, производными от него.

Ключ, который невозможно подделать, является активным устройством, содержащим в памяти идентификатор, не доступный для чтения. Например, электронный ключ может содержать криптосхему, в которую при изготовлении загружается случайное значение ключа. Вне криптосхемы это значение нигде не записывается. Устройство можно сконструировать таким образом, что попытка прочесть ключ приводит к его уничтожению. Устройство такого типа обладает «индивидуальностью», которую можно выявить только посредством задания устройству различных цифровых значений и записи его ответов.

Электронный ключ может использоваться локально, подобно ключу от дверного замка, или на расстоянии, например, для идентификации удаленных субъектов, обращающихся к ЭВМ. Для своего восприятия электронный ключ должен иметь «замок» (ответную часть), запрашивающий ключ и проверяющий его идентичность. В начале идентичность необходимо определить каким-либо независимым способом, чтобы ввести в действие замок, отвечающий данному ключу. Затем замок посылает набор запросов к ключу и запоминает его ответы. Впоследствии, когда ключ действительно используется для аутентификации субъекта, некоторые из этих наборов повторяются в качестве опознавательных вопросов к ключу, а ответы сравниваются с

уже хранящимися в памяти. Если аутентификация осуществляется многократно, то замок может послать новые цифровые комбинации, которые добавляются к списку опознавательных вопросов и ответов. Например, для своего восприятия смарт-карта должна иметь ридер, в процессе обмена информацией с которым происходит опознание *смарт-карты*. Аутентификация субъекта происходит после подтверждения им того, что именно он является владельцем смарт-карты в результате ввода с клавиатуры PIN-кода. Аналогом ридера для *USB-ключей* выступает стандартный USB-порт, а для электронного ключа *Touch Memory* – считывающее устройство.

Один и тот же ключ может подходить к нескольким замкам, и один и тот же замок может отвечать нескольким ключам, не нарушая при этом секретности ни замка, ни ключа. Никакие исследования такого физического замка не позволят определить хранящийся ключ, если он защищен эффективной криптосхемой. Однако если имеется возможность перехвата всех опознавательных вопросов и ответов для данного замка, то ключ можно подделать. Такой поддельный ключ может приниматься за подлинный во всех последующих сеансах аутентификации до тех пор, пока он не будет выявлен новыми опознавательными вопросами. Используя большое число ответов и создавая каждый раз новые, можно повысить уровень защиты, однако более надежным способом является применение методов шифрования для защиты передаваемых идентификаторов от удаленных абонентов в ЭВМ.

Что присуще субъекту. К данному классу опознания относятся методы, базирующиеся на определении индивидуальных характеристик, присущих каждому субъекту и позволяющих выделить его среди других. Указанные методы также называют **биометрическими.** Биометрические методы аутентификации можно разделить на две большие категории – физиологические и психологические. К первой относятся методы, основанные на физиологической (статической) характеристике субъекта, т. е. неотъемлемой, уникальной характеристике, данной ему от рождения. Здесь анализируются такие признаки, как отпечатки пальцев, черты лица, структура глаза (сетчатки или радужной оболочки), параметры пальцев, ладонь, форма руки.

К группе психологических относят методы, которые основываются на поведенческой (динамической) характеристике субъекта. Они используют особенности, характерные для подсознательных движений в процессе воспроизведения какого-либо действия. К таким характеристикам относятся голос субъекта, особенности его подписи, динамические параметры письма, особенности ввода текста с клавиатуры.

В основе метода опознания *по отпечатку пальца* лежит уникальность рисунка капиллярных узоров на пальцах у каждого субъекта. Существуют два основополагающих алгоритма распознавания отпечатков пальцев:

– по отдельным деталям (характерным точкам);

– по рельефу всей поверхности пальца.

В первом случае устройство регистрирует только некоторые участки, уникальные для конкретного отпечатка, и определяет их взаимное расположение. Во втором случае обрабатывается изображение всего отпечатка.

Метод опознания субъекта *по лицу* основан на уникальности черт лица. Метод заключается в преобразовании черт конкретного лица в алгоритмическую модель, которая сравнивается или с фотографией на пропуске, или с содержимым базы фотографических данных.

Метод опознания субъекта *по радужной оболочке глаза* основан на уникальности рисунка радужной оболочки каждого субъекта. Радужная оболочка субъекта сканируется, разворачивается и преобразуется в цифровую последовательность. Подтверждение подлинности субъекта происходит на основании сравнения полученной цифровой последовательности с эталонной.

Метод опознания *по образцу голоса* основан на том, что у каждого субъекта неповторимый голосовой рисунок, который зависит от пола, физических особенностей, типа строения голосовых связок, полости носа, формы рта, таких характеристик, как частота и амплитуда. Этот метод построен на выделении различных сочетаний частотных и статистических характеристик голоса.

1.2 Показатели эффективности средств аутентификации

Любая техническая система (средство) создается для выполнения вполне определенного набора задач (функций). **Операцией** называется выполнение технической системой (средством) заданного набора задач (функций).

Эффективность операции есть степень соответствия реального (фактического или ожидаемого) результата операции требуемому или, иными словами, как степень достижения цели операции.

Эффективность *технического средства* можно определить как степень выполнения заданного набора функций.

Как и всякое свойство, эффективность обладает определенной интенсивностью своего проявления. Мера интенсивности проявления эффективности называется *показателем* эффективности.

Следовательно, показатель эффективности любой технической системы (средства) есть мера степени соответствия реального достигаемого результата R выполнения операции требуемому результату $R_{тр}$. Основным требованием при выборе показателя эффективности является его соответствие цели операции, которая отображается требуемым результатом.

Основной задачей средства аутентификации является надежное опознание личности конкретного человека. В соответствии с этим *показатель эффективности средства аутентификации* можно определить как меру при-

ближения вероятности правильного опознания субъекта данным средством в реальных условиях функционирования $P_{по}$ требуемой $P_{тр}$.

При условии равенства $P_{по}$ и $P_{тр}$ эффективность средства аутентификации должна быть равна единице, а если $P_{по}$ стремится к нулю, то и эффективность также должна стремиться к нулю.

Вероятность правильного опознания субъекта средством аутентификации в реальных условиях функционирования можно определить как

$$P_{по} = 1 - P_{пч}, \quad (1)$$

где $P_{пч}$ – вероятность пропуска «чужого» субъекта средством аутентификации.

Средство аутентификации может пропустить «чужого» субъекта в том случае, когда произойдет хотя бы одно из следующих событий:

– подбор аутентификатора нарушителем;

– выдача разрешающего выходного сообщения в результате отказа (сбоя) оборудования;

– выдача разрешающего выходного сообщения в результате действий нарушителя.

В таком случае **вероятность пропуска «чужого» субъекта средством аутентификации** будет определяться следующим выражением:

$$P_{пч} = P_{па} + P_{от} + P_{дн} - P_{от}P_{дн} - P_{па}P_{от} - P_{па}P_{дн} + P_{па}P_{от}P_{дн}, \quad (2)$$

где $P_{па}$ – вероятность подбора аутентификатора;

$P_{от}$ – вероятность пропуска «чужого» в результате отказов (сбоев) оборудования;

$P_{дн}$ – вероятность пропуска «чужого» в результате действий нарушителя.

Вероятность правильного опознания субъекта средством аутентификации, согласно выражению (1), будет иметь вид

$$P_{по} = (1 - P_{па})(1 - P_{от})(1 - P_{дн}). \quad (3)$$

Рассмотрим способы определения указанных в выражении (3) вероятностей.

Вероятность $P_{па}$ зависит от объёма алфавита, длины аутентификатора и является функцией числа попыток подбора:

$$P_{па} = 1 - \prod_{b=1}^{k} (1 - P_{паb}), \quad (4)$$

где k – число попыток подбора.

$$P_{\text{пав}} = \frac{1}{A^m - b + 1}, \tag{5}$$

где A – объём алфавита;

m – длина аутентификатора.

Вероятность $P_{\text{от}}$ определяется надёжностью элементов средства аутентификации и является функцией интенсивности их отказов:

$$P_{\text{от}}(\lambda) = 1 - e^{-\sum_{j=1}^{n} \lambda_{sj} t}, \tag{6}$$

где λ_{sj} – интенсивность отказов элементов, выполняющих s-ю функцию;

n – количество элементов, реализующих s-ю функцию.

Вероятность пропуска «чужого» в результате действия нарушителя вычисляется как произведение вероятности того, что действие нарушителя было реализовано, и того, что оно привело к пропуску «чужого»:

$$P_{\text{дн}} = P_{\text{рдн}} P_{\text{пдн}}, \tag{7}$$

где $P_{\text{рдн}}$ – вероятность того, что действие нарушителя было реализовано;

$P_{\text{пдн}}$ – вероятность того, что реализованное действие нарушителя привело к пропуску «чужого».

Эффективность средства аутентификации зависит как от характеристик самого средства аутентификации, так и от условий его функционирования.

В качестве требуемой вероятности правильного опознания выберем вероятность, дополняющую до единицы вероятность пропуска средством аутентификации «чужого» субъекта в результате подбора им аутентификатора с первой попытки:

$$P_{\text{тр}} = 1 - P_{\text{па1}}. \tag{8}$$

Вероятность $P_{\text{па1}}$, а следовательно, и вероятность $P_{\text{тр}}$ определяется только конструктивными особенностями средства аутентификации, не зависит от внешних и внутренних негативных факторов и поэтому может служить верхней границей вероятности $P_{\text{по}}$.

1.3 Принципы, повышающие стойкость парольных методов опознания

Эффективность средств аутентификации определяется вероятностью подбора аутентификатора с первой попытки. Для повышения эффективности этих средств при их проектировании необходимо использовать следующие **принципы**:

– максимального правдоподобия;

– ограничения попыток;

– цикличности.

Принцип максимального правдоподобия заключается в следующем. Пусть $A = \{a_i\}$, $i = 1, n$ – эталонные значения параметров, используемых для аутентификации, а $X = \{x_i\}$, $i = 1, n$ – значения параметров, предъявляемых для опознания.

Пусть независимые попытки опознания имеют частные вероятности $\rho(X, A)$, тогда принцип максимального правдоподобия состоит в выборе в качестве истинного такого параметра X, при котором максимизируется функция правдоподобия:

$$L(\theta) = \rho(x_1, a_1), \rho(x_2, a_2), \ \ldots, \ \rho(x_n, a_n) . \qquad (9)$$

Для средств опознания, основанных на том, «что знает субъект» и «что имеет субъект», принцип максимального правдоподобия заключается в том, что опознание считается успешным при абсолютном совпадении всех сравниваемых признаков входного воздействия, предоставленного субъектом, и эталонного, хранящегося в памяти средства опознания. Это обусловлено тем, что результат преобразования признаков, предоставляемых одним и тем же субъектом, в понятный средству опознания вид всегда имеет одинаковые значения.

В этом случае *вероятность подбора пароля с первой попытки*

$$P_{\text{па1}} = \frac{1}{N} , \qquad (10)$$

где N – объем алфавита.

Для паролей *объем алфавита*

$$N = A^n , \qquad (11)$$

где A – используемый алфавит пароля (общее число знаков);

n – длина пароля.

Тогда

$$P_{\text{па1}} = \frac{1}{A^n} . \qquad (12)$$

В средствах опознания с использованием смарт-карт субъект предоставляет PIN-код, состоящий из цифр. Поэтому алфавит PIN-кода равен десяти. Для этих средств опознания *формула определения вероятности подбора PIN-кода с первой попытки* имеет следующий вид

$$P_{\text{па1}} = \frac{1}{10^n}. \quad (13)$$

В средствах опознания с использованием электронных ключей или брелоков используются битовые ключи, поэтому алфавит ключей равен двум. *Формула определения вероятности подбора битового ключа с первой попытки* имеет вид

$$P_{\text{па1}} = \frac{1}{2^n}. \quad (14)$$

Вероятность подбора пароля с первой попытки при неповторяющихся символах в пароле

$$P_{\text{па1неповт}} = \prod_{i=0}^{n-1} \frac{1}{N-i}. \quad (15)$$

В данном случае количество символов не может быть больше алфавита.

Увеличение вероятности правильного опознания субъекта для данных средств аутентификации достигается за счет расширения алфавита или длины аутентификатора.

Для биометрических средств аутентификации абсолютное совпадение всех сравниваемых признаков входного воздействия и эталонного недостижимо. Это обусловлено тем, что процесс преобразования признаков, предоставленных субъектом, в понятный средству аутентификации вид носит вероятностный характер. В этом случае принцип максимизации правдоподобия заключается в том, что аутентификация считается установленной, если величина несовпадения всех сравниваемых признаков входного воздействия, предоставленного субъектом, и эталонного, хранящегося в памяти средства аутентификации, не превышает некоторого значения меры близости сравниваемых признаков.

Увеличение вероятности правильного опознания субъекта для биометрических средств аутентификации достигается за счет минимизации значения меры близости сравниваемых признаков, что, с другой стороны, может привести к увеличению вероятности блокировки «своих» субъектов. Другим путем увеличения вероятности правильного опознания является максимизация алфавита биометрических признаков за счет изменения точности их получения и сравнения с эталонными. Например, для средства аутентификации по отпечатку пальца максимизацию алфавита биометрических признаков проводят за счет увеличения разрешения картинки отпечатка пальца, а для средства аутентификации по голосу – за счёт увеличения размера секторов, в которых происходит определение типа минуций.

Принцип ограничения попыток заключается в том, что при опознании субъекта ограничивается число попыток неправильного входа в систему. При *отсутствии ограничения* на число попыток неправильного входа значение вероятности подбора пароля определяется по формуле

$$P_{\text{па}} = P_{\text{па}1} + (1-P_{\text{па}1})P_{\text{па}2} + (1-P_{\text{па}1})(1-P_{\text{па}2})P_{\text{па}3} + \\ + \cdots + (1-P_{\text{па}1}) \times \cdots \times (1-P_{\text{па}n\text{-}1})P_{\text{па}n}, \tag{16}$$

где $P_{\text{па}i}$ – вероятность подбора пароля при наборе i-й комбинации с учетом того, что $i-1$ комбинаций уже опробовано и нет смысла набирать их заново;

$$P_{\text{па}i} = \frac{1}{n-i+1}, i = 1, 2, ..., n.$$

Подставив в формулу (16) выражения для $P_{\text{па}i}$, получим

$$P_{\text{па}} = \frac{1}{n} + \left(1-\frac{1}{n}\right)\frac{1}{n-1} + \left(1-\frac{1}{n}\right)\left(1-\frac{1}{n-1}\right)\frac{1}{n-2} + \cdots \\ + \left(1-\frac{1}{n}\right) \times \cdots \times \left(1-\frac{1}{n-n+2}\right)\frac{1}{n-n+1} = \frac{1}{n} + \frac{n-1}{n}\frac{1}{n-1} + \\ + \frac{n-1}{n}\frac{n-2}{n-1}\frac{1}{n-2} + \cdots + \frac{n-1}{n} \times \cdots \times \frac{n-n+1}{n-n+2}\frac{1}{n-n+1} = \\ = \frac{1}{n} + \frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n} = n\frac{1}{n} = 1.$$

При использовании принципа ограничения попыток *вероятность подбора пароля за k попыток*

$$P_{\text{па}} = \frac{1}{n} + \left(1-\frac{1}{n}\right)\frac{1}{n-1} + \cdots + \left(1-\frac{1}{n}\right) \times \cdots \times \left(1-\frac{1}{n-k+2}\right)\frac{1}{n-k+1} = \frac{k}{n}, \tag{17}$$

где k – допустимое количество попыток неправильного входа в систему.

Вероятность подбора пароля за k попыток означает, что пароль будет подобран с первой или со второй, или … с k-й попытки. Поэтому в формулах (16) и (17) каждое слагаемое является вероятностью подбора пароля с определенной попытки.

Таким образом, *вероятность подбора пароля с i-й попытки*

$$P_{\text{сп}} = (1-P_{\text{па}1})(1-P_{\text{па}2}) \times \cdots \times (1-P_{\text{па}i\text{-}1})P_{\text{па}i}. \tag{18}$$

Подставив в формулу (17) выражения для $P_{\text{па}i}$, получим

$$P_{\text{сп}} = \left(1 - \frac{1}{n}\right)\left(1 - \frac{1}{n-1}\right) \times \cdots \times \left(1 - \frac{1}{n-i+2}\right)\frac{1}{n-i+1} = \frac{1}{n}. \qquad (19)$$

Реализация данного принципа заключается в блокировке средства аутентификации при превышении допустимого количества попыток неправильного входа в систему.

Принцип ц и к л и ч н о с т и заключается в том, что средство опознания функционирует по заранее установленному жесткому циклу, и ни при каких входных воздействиях цикл его работы не нарушается.

При использовании данного принципа в качестве параметра, учет которого позволяет повысить эффективность средства опознания, выступает безопасное время действия пароля, связанное с вероятностью его подбора простым соотношением

$$T_{\text{без}} = \frac{P_{\text{т}}}{P_1} T_{\text{ц}} = NP_{\text{т}} T_{\text{ц}}, \qquad (20)$$

где $T_{\text{без}}$ – безопасное время действия пароля;

$P_{\text{т}}$ – вероятность подбора пароля за время $T_{\text{без}}$;

$T_{\text{ц}}$ – время выполнения средством опознания одного цикла работы.

В силу того, что цикл работы жестко фиксирован, путем ввода некоторой временно́й задержки в конце цикла можно существенно повысить безопасное время действия пароля при постоянной вероятности подбора пароля. В данном случае *безопасное время действия пароля*

$$T_{\text{без}} = \frac{P_{\text{т}}}{P_1}(T_{\text{ц}} + t_{\text{з}}) = NP_{\text{т}}(T_{\text{ц}} + t_{\text{з}}), \qquad (21)$$

где $t_{\text{з}}$ – временная задержка.

Отсюда

$$P_{\text{т}} = \frac{T_{\text{без}}}{N(T_{\text{ц}} + t_{\text{з}})}. \qquad (22)$$

Так как безопасное время действия пароля принято измерять, как минимум, в часах, а время выполнения средством опознания одного цикла работы и временной задержки – в секундах, то в формулу (22) следует ввести коэффициент, переводящий безопасное время действия пароля в часы:

$$P_{\text{т}} = \frac{3600T_{\text{без}}}{N(T_{\text{ц}} + t_{\text{з}})}. \qquad (23)$$

В этом случае *вероятность подбора пароля за безопасное время его действия*

$$P_{\text{т}} = \frac{3600T_{\text{без}}}{A^n(T_{\text{ц}} + t_{\text{з}})}. \quad (24)$$

При использовании PIN-кода формула (16) имеет следующий вид:

$$P_{\text{т}} = \frac{3600T_{\text{без}}}{10^n(T_{\text{ц}} + t_{\text{з}})}, \quad (25)$$

а при использовании двоичного ключа –

$$P_{\text{т}} = \frac{3600T_{\text{без}}}{2^n(T_{\text{ц}} + t_{\text{з}})}. \quad (26)$$

Во многих средствах опознания предусматривается возможность субъектам самим назначать себе пароли независимо друг от друга. В этом случае существует вероятность того, что у двух разных пользователей могут оказаться одинаковые пароли. Это приводит к тому, что средство опознания при обращении к ней одного субъекта может принять его за другого. Поэтому такие системы опознания должны проверяться по критерию «парадокс дней рождения».

Математически парадокс дней рождений формируется следующим образом. Если $an^{-0,5}$ предметов выбирается с возвращением из некоторой совокупности размером n, то вероятность того, что два из них окажутся одинаковыми, составляет величину

$$P_{\text{д}} = 1 - e^{\left(-\frac{a^2}{2}\right)}. \quad (27)$$

Практически это означает, что в случайно подобранной группе из 24 человек вероятность наличия двух лиц с одним и тем же днём рождения составляет величину порядка 0,5.

Если количество пользователей системы принять за d, то тогда

$$a = \frac{d}{A^{n/2}}. \quad (28)$$

Подставив выражение (28) в выражение (27), получим

$$P_{\text{д}} = 1 - e^{\left(-\frac{d^2}{2A^n}\right)}. \quad (29)$$

Порядок выполнения работы

1 Изучить краткие сведения из теории.

2 Для решения задач из пп. 5–10 по первой цифре шифра необходимо выбрать один из алфавитов пароля (A), представленных в таблице 1.

Таблица 1

Первая цифра шифра	A	Первая цифра шифра	A
0	10	5	59
1	26	6	69
2	33	7	76
3	36	8	128
4	43	9	256

3 Для решения задач из пп. 6–9 по предпоследней цифре шифра необходимо выбрать длину пароля (k), представленную в таблице 2.

Таблица 2

Предпоследняя цифра шифра	k	Предпоследняя цифра шифра	k
0	9	5	10
1	6	6	4
2	11	7	7
3	13	8	12
4	8	9	5

4 Для решения задач из пунктов 5 и 10 по последней цифре шифра необходимо выбрать вероятность подбора пароля (P), которые представлены в таблице 3.

Таблица 3

Последняя цифра шифра	P	Последняя цифра шифра	P
0	10^{-10}	5	10^{-9}
1	10^{-15}	6	10^{-13}
2	10^{-8}	7	10^{-11}
3	10^{-12}	8	10^{-16}
4	10^{-14}	9	10^{-7}

5 Изучить методику выбора оптимальных параметров парольной системы. Определить минимально необходимую длину пароля, удовлетворяющую следующим условиям:

а) алфавит пароля A, вероятность подбора пароля с первой попытки ($P_{па1}$) не более P;

б) алфавит пароля A, вероятность подбора пароля за время $T_{без} = 10$ ч ($P_т$) не более P; время одной попытки подбора пароля $t = 60$ с;

в) вероятность появления двух одинаковых паролей ($P_д$) при общем количестве субъектов $n = 10000$ не более P.

6 Изучить вероятности подбора пароля с n-й и за n попыток. Определить вероятности подбора пароля с первой попытки, с десятой попытки и за десять попыток при алфавите пароля A и длине пароля k.

7 Определить вероятности подбора пароля с первой попытки при алфа-

вите пароля A и длине пароля k для следующих случаев:

а) символы в пароле могут повторяться;

б) символы в пароле не повторяются.

8 Определить вероятности подбора комбинированного пароля с первой попытки и за время T = 2 ч, если первая часть пароля является 16-байтной произвольной строкой из некоторого файла, а вторая часть пароля задается для алфавита пароля A и длине ключа k. Время ввода одного варианта каждой части комбинированного пароля t = 10 с.

9 Изучить методику оценки времени, необходимого для подбора пароля. Определить время подбора пароля, если алфавит пароля A, длина пароля k, время ввода одного символа пароля t' = 0,5 с, клавиатура блокируется:

а) после каждого набора пароля – на $t_б$ = 0 с;

б) после каждого набора пароля – на $t_б$ = 3 с;

в) после каждого десятого набора пароля – на $t_б$ = 5 с;

г) после первого набора пароля – на $t_б$ = 1 с, после второго – на $t_б$ = 2 с, после i-го – на $t_б = i$ с.

10 Произвести оценку необходимой длины пароля для удовлетворения требований, предъявляемых к системе опознания. Определить минимальную достаточную длину пароля, удовлетворяющую следующим параметрам: алфавит пароля A, время ввода одного символа пароля t' = 0,5 с, вероятность подбора пароля за время, отводимое на подбор пароля, $T_{без}$ = 92 дня, ($P_т$) не более P.

Примеры решения задач

Задача 1. Определить, каким должно быть минимальное число символов в пароле для удовлетворения следующим условиям: вероятность определения пароля с первого раза $P_{па1} = 10^{-10}$; алфавит A = 10.

Решение. Вероятность подбора пароля с первой попытки

$$P_{па1} = \frac{1}{A^k}.$$

Выразим k:

$$A^k = \frac{1}{P_1}; k = \log_A \frac{1}{P_1}.$$

Подставив исходные данные, получим

$$k = \log_{10} 10^{10} = 10.$$

Ответ: k = 10.

Задача 2. Определить вероятность подбора пароля за 8 ч (T) при длине ключа k = 4, алфавите A = 30 и времени ввода одного символа t = 1 с.

Решение. Вероятность подбора пароля за безопасное время его действия

$$P_{\text{т}} = \frac{3600T_{\text{без}}}{A^n(T_{\text{ц}} + t_{\text{з}})}.$$

Подставив исходные данные, получим

$$P_{\text{т}} = \frac{3600T}{A^k kt} = \frac{3600 \cdot 8}{30^4 \cdot 4 \cdot 1} = \frac{7200}{81} \cdot 10^{-4} = 8{,}89 \cdot 10^{-3}.$$

Ответ: $P_{\text{т}} = 8{,}89 \cdot 10^{-3}$.

Задача 3. Определить вероятность подбора пароля за три попытки при длине ключа $k = 4$ и алфавите $A = 20$.

Решение. Вероятность подбора пароля за три попытки

$$P_{\text{пп}} = \frac{3}{N}.$$

Объем алфавита для паролей

$$N = A^k.$$

Тогда

$$P_{\text{пп}} = \frac{3}{20^4} = 3 \cdot 20^{-4} = 1{,}875 \cdot 10^{-5}.$$

Ответ: $P_{\text{пп}} = 1{,}875 \cdot 10^{-5}$.

Задача 4. Определить вероятность подбора комбинированного пароля за 8 ч (T), состоящего из двух частей: длиной $k_1 = 8$ из алфавита $A_1 = 10$ и длиной $k_2 = 4$ из алфавита $A_2 = 20$ при времени ввода первой части ключа $t_1 = 2$ с, а второй – $t_2 = 1$ с.

Решение. Вероятность подбора комбинированного пароля

$$P_{\text{т}} = P_{\text{т}1} P_{\text{т}2}.$$

Вероятность подбора пароля за безопасное время его действия

$$P_{\text{т}} = \frac{3600T_{\text{без}}}{A^n(T_{\text{ц}} + t_{\text{з}})}.$$

Тогда

$$P_{\text{т}} = \frac{3600 \cdot 8}{10^8 \cdot 2} \cdot \frac{3600 \cdot 8}{20^4 \cdot 1} = 14400 \cdot 10^{-8} \cdot 1800 \cdot 10^{-4} = 2{,}592 \cdot 10^{-5}.$$

Ответ: $P_{\text{т}} = 2{,}592 \cdot 10^{-5}$.

Задача 5. Определить минимальную длину ключа, необходимую для удовлетворения парольной системой следующих условий: вероятность подбора пароля за время $T = 4000$ ч $P_т = 10^{-10}$; алфавит $A = 10$; время набора одного символа $t = 2$ с.

Решение. Вероятность подбора пароля за безопасное время его действия

$$P_т = \frac{3600T_{без}}{A^n(T_ц + t_з)}.$$

Время выполнения средством опознания одного цикла работы в таком случае будет

$$T_ц = kt.$$

Тогда

$$P_т = \frac{3600T_{без}}{A^n(kt + t_з)}.$$

Отсюда при условии $t_з = 0$

$$kA^k \geq \frac{3600T}{P_т t}.$$

Подставив исходные данные, получим

$$k \cdot 10^k \geq \frac{3600 \cdot 4000}{10^{-10} \cdot 2}; k \cdot 10^k \geq 7{,}2 \cdot 10^{16}; k = 16.$$

Ответ: $k = 16$.

Задача 6. Определить время подбора пароля, состоящего из шести символов (k) из алфавита $A = 20$ при времени ввода одного символа $t = 3$ с.

Решение. Вероятность подбора пароля за безопасное время его действия

$$P_т = \frac{3600T_{без}}{A^n(T_ц + t_з)}.$$

Отсюда, при условии, что $P_т = 1$, $T_ц = kt$ и $t_з = 0$,

$$T = \frac{A^k tk}{3600}.$$

Подставив исходные данные, получим

$$T = \frac{20^6 \cdot 3 \cdot 6}{3600} = 36{,}5 \text{ года.}$$

Ответ: T = 36,5 года.

Содержание отчета

1 Цель работы.
2 Исходные данные.
3 Результаты расчетов.
4 Вывод по работе.

Контрольные вопросы

1 Что такое идентификация субъекта?
2 Что такое аутентификация субъекта?
3 Классы средств аутентификации.
4 Как оценивается эффективность парольного средства аутентификации?.
5 Как оценить время жизни пароля?
6 Что такое комбинированные пароли?
7 Что такое «парадокс дня рождения»?