симально снижал бы риски, мог быстро перестроиться с учетом изменений, то есть должен быть достаточно гибким. С целью разработки такого контракта и контроля за ходом его исполнения необходимо создать специальную команду. Внутри организации должна быть создана атмосфера понимания происходящих изменений.

Все это вызывает рост трансакционных издержек, связанных с внедрением аутсорсинговой схемы.

На сегодняшний день не существует единого стандартизированного подхода к определению того, какой из видов деятельности можно передать аутсорсерам и уже тем более для многих организаций будет довольно затратно проводить аудит на предмет определения с кем из ауторсеров сотрудничать.

Таким образом, эффективность применения аутсорсинга в плане сокращения трансакционныых затрат возможно только при сопоставлении прироста затрат на аутсорсинг с экономией на внутренних трансакциях.

Литература.

1. Козулина Т.И. Методы снижения трансакционных издержек в сфере предпринимательства // Научное сообщество студентов XXI столетия. Экономические науки: сб. ст. по мат. XLIV междунар. студ. науч.-практ. конф. № 7(44). URL:https://sibac.info/archive/economy/7(44).pdf (дата обращения: 17.03.2017)
2. Крюкова О.Н. Оптимизация структуры трансакционных издержек сельскохозяйственных организаций Вестник Алтайского государственного аграрного университета № 2 (136), 2016 С.165-170
3. Искосков М.О. Аутсорсинг как один из способов снижения трансакционных издержек // Вектор науки ТГУ. Серия: Экономика и управление. 2012. No4(11) С.71-73

СИСТЕМЫ АУТЕНТИФИКАЦИИ СООБЩЕНИЙ НА ОСНОВЕ ЦВЗ И ОБЛАСТИ ИХ ПРИМЕНЕНИЯ.

А.В. Шокарев, к.т.н.

Юргинский технологический институт (филиал) Томского политехнического университета

E-mail: Shokarev_AV@mail.ru

Аннотация: Компьютерная стеганография является молодым, развивающимся направлением, и в последние годы привлекает множество ученых для исследований в данной области. Основное предназначение стеганографии – это сокрытие самого факта наличия скрытой информации. Далее в статье будут рассмотрена возможность применения методов стеганографии в системах графических паролей, а так же другие области применения цифровых водяных знаков (ЦВЗ) в направлении защиты информации и аутентификации пользователей в информационных системах.

Системы графических паролей начинают набирать свою популярность в области компьютерной безопасности. Это обусловлено тем, что рекомендации по использованию символьных паролей сводятся к бессмысленному набору символов и частой сменой. Такие пароли очень трудно запоминать как обычным, так и продвинутым пользователям систем.

Среди существующих методов контроля подлинности сообщений, передаваемых по каналам связи, наиболее широко распространены методы аутентификации сообщений на основе имитовставки и методы аутентификации сообщений на основе цифровой подписи [1]. Данные криптографические методы могут быть рассмотрены на обобщенной модели, приведенной на рисунке 1.

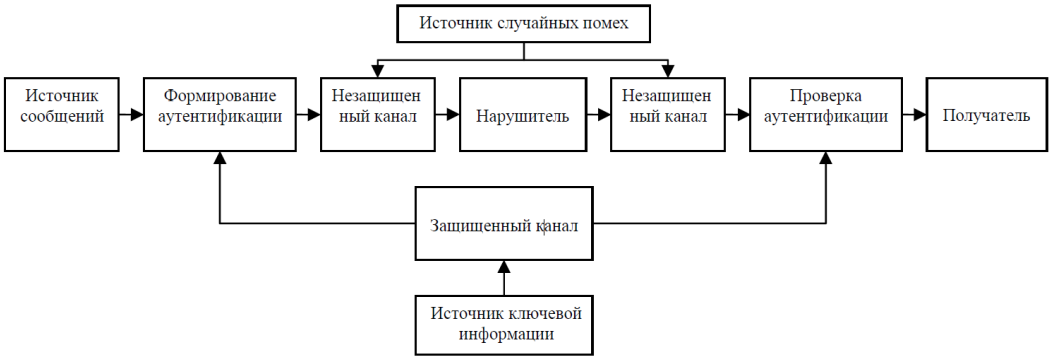

Рис. 1. Модель системы аутентификации сообщений на основе имитовставки или цифровой подписи

Источник сообщений генерирует сообщение, подлинность которого требуется заверить. Для этого отправителем из сообщения формируется кодограмма аутентификации, передаваемая по неза-

щищенному от активного противодействия нарушителем каналу. Нарушитель имеет возможность от имени законного отправителя передавать получателю ложные сообщения (атака маскарада), существует так же возможность перехвата истинного сообщения с заменой на ложное сообщение (атака замены) отправить получателю. А так же применить другие атаки на подлинность и целостность сообщения. На приеме устройство проверки должно определить, является ли принятое сообщение подлинным и только тогда передать его получателю. Если принятое сообщение ложное, то оно не передается адресату. Законные отправитель и получатель используют ключ формирования, а так же ключ проверки подлинности кодограмм аутентификации, которые доставляются им по защищенным от нарушителя каналам. В системы аутентификации сообщений на основе формирования и проверки имитовставок сообщений оба ключа, как правило, совпадают и являются конфиденциальными [3]. В системы аутентификации на основе формирования и проверки цифровой подписи сообщений используется конфиденциальный ключ формирования цифровой подписи, который должен быть известен только отправителю (автору) сообщения, и общеизвестный ключ проверки подлинности цифровой подписи [1,4].

Существующие методы аутентификации имеют определенные недостатки, связанные в основном с их низкой помехоустойчивостью. Множество каналов связи не обеспечивает высокую вероятность доставки сообщений, заверенных с использованием существующих методов имитозащиты, и как следствие при использовании нарушителем оптимизированных преднамеренных помех помехозащищенность методов на основе имитовставки и цифровой подписи ухудшается, равно как и при увеличении размера аутентифицируемых сообщений. Как следствие, помехоустойчивость передачи аутентифицированных сообщений падает при переходе от методов на основе имитовставок к методам на основе цифровой подписи и при увеличении длины кодограмм аутентификации. За удобство использования открытого ключа и повышение имитостойкости приходится использовать каналы передачи более высокого качества. Низкая помехоустойчивость передачи аутентифицированных сообщений объясняется тем, что при возникновении любой ошибки в самом сообщении или в его имитовставке (цифровой подписи) существующие методы аутентификации расценивают это как факт воздействия нарушителя и предписывают стирать такое сообщение, даже если основное смысловое содержание сообщения не искажено, следовательно:

- использование существующих методов имитозащиты для контроля подлинности избыточных сообщений требует каналов связи с вероятностью ошибки на передаваемый бит по крайней мере на 2–2,5 порядка лучше, чем при передаче тех же сообщений без защиты их подлинности;
- существующие системы аутентификации пользователей в информационных системах на основе имитовставки и цифровой подписи не эффективны при использовании в каналах связи для передачи сообщений, допускающих некоторую приемлемую для их получателя погрешность.

Актуальной теоретической и практической задачей представляется разработка методов аутентификации пользователей, которые устойчивы к комплексному навязыванию ложных сообщений нарушителем и воздействию случайных и преднамеренных ошибок в каналах связи. В ходе поиска решения данной задачи возможно использование методов контроля подлинности сообщений на основе ЦВЗ.

На рисунке 2 представлена обобщенная модель системы аутентификации сообщений на основе ЦВЗ для применения в системах графического пароля.

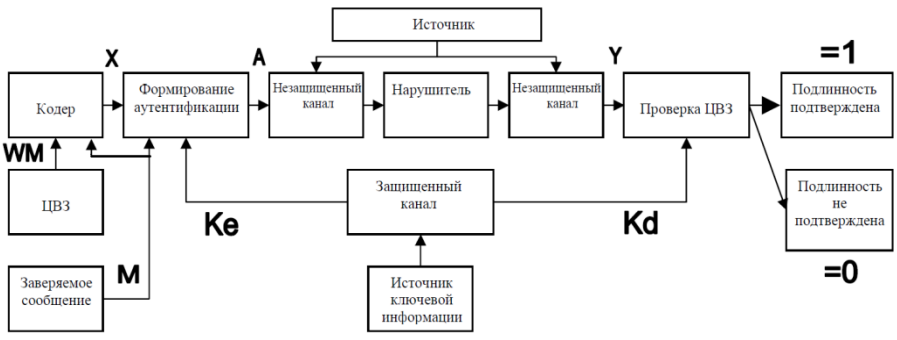

Рис. 2. Модель аутентификации сообщений на основе ЦВЗ

После генерирования отправителем сообщения M, подлинность заверяется цифровым водяным знаком WM, который индивидуален для каждого отправителя. Далее ЦВЗ в кодере приводится в

удобный для встраивания его в сообщение вид. При формировании водяного знака X алгоритм можно представить в виде:

$$X=F(M, WM) \quad (1)$$

После чего конструкция ЦВЗ встраивается в сообщение, используя конфиденциальный ключ Ke:

$$A=\Psi(X, M, Ke) \quad (2)$$

В канале связи на заверенное сообщение A воздействуют навязывание имитовставок нарушителя, а также преднамеренные и случайные помехи. При таком воздействии на проверку ЦВЗ поступает сообщение Y с возможными искажениями. Алгоритмом обнаружения цифрового водяного знака может формироваться оценка одним из следующих способов:

$$WM^{\wedge} = D(Y, Kd) \text{ или } WM^{\wedge} = D(Y, WM, Kd) \quad (3)$$

При проверке подлинности сообщения можно использовать одну из приведенных оценок. Возможны решения следующих видов:

- $WM^{\wedge} = 1$ (все сообщение подлинное)
- $WM^{\wedge} = 0$ (подлинность не подтверждена).

Но возможны и другие оценки ЦВЗ:

- $0{,}5 \le WM_j^{\wedge} \le 1$ – скорее всего j-й фрагмент сообщения подлинный
- $0 \le WM_j^{\wedge} < 0{,}5$ – скорее всего j-й фрагмент сообщения навязан или возможно искажен помехами передачи.

При формировании оценки ВЗ могут возникнуть следующие ошибки обнаружения получателем сообщения.

1. **Ошибки обнаружения первого рода:** ЦВЗ обнаружен, хотя и отсутствует в сообщении Y. Вероятность ошибки обнаружения первого рода (вероятность ложной тревоги) обозначим $O_{пр.}$
2. **Ошибки обнаружения второго рода:** ЦВЗ не обнаружен, хотя и присутствует в сообщении Y. Вероятность ошибки обнаружения второго рода (вероятность не обнаружения) обозначим $O_{вр.}$

В общем случае при увеличении $O_{пр}$ уменьшается $O_{вр.}$, и наоборот.

Если сравнивать систему аутентификации пользователей на основе ЦВЗ с системой криптографической аутентификации, то первая имеет следующие особенности:

- передаваемое сообщение со встроенным в него ЦВЗ взаимозависимы и при разрушении или искажении сообщения разрушается цифровой водяной знак, а если ЦВЗ сохранил свою целостность, то и сообщение целостность не потеряет;
- в случае приема фрагмента с искаженным сообщением получатель не обязательно должен отказываться от всего сообщения, а может отказаться лишь от искаженного фрагмента и запросить не достающий фрагмент повторно.

Общими недостатками для методов контроля подлинности на основе имитовставки и цифровой подписи являются:

- отсутствует устойчивость к удалению аутентификатора заверенного сообщения без разрушения всего сообщения;
- отсутствует механизм обнаружения несанкционированного копирования сообщений с ЦВЗ;
- согласование метода защиты только с сообщениями, порожденными бернуллиевским источником;
- отсутствие допущения ограниченной погрешности сообщения без потери его подлинности;
- существенный рост требований к пропускной способности канала связи при передаче аутентифицированных сообщений по сравнению с их передачей без контроля подлинности.
- Методы контроля подлинности на основе ЦВЗ при сравнении с методами контроля подлинности на основе имитовставки и цифровой подписи, обладают следующими достоинствами:
- высокая устойчивость к удалению аутентификатора заверенного сообщения, не разрушая сообщение;
- обнаружение копирования злоумышленником заверенных сообщений;
- согласованность со всеми источниками сообщений, такими как изображение, видео или звуковой сигнал.

Исходя из этого, выявляются возможные области применения ЦВЗ в информационно-телекоммуникационных системах различного назначения, представленные на рисунке 3[2,4].

Рис. 3. Области применения ЦВЗ в информационно-телекоммуникационных системах

Требования, предъявляемые к системам аутентификации сообщений на основе ЦВЗ:

- имитостойкость: невозможность нарушителем, не знающим ключ подписи, формировать любое сообщения с верным цифровым водяным знаком;
- практическая невозможность без обнаружения несанкционированного копирования заверенного сообщения;
- при подписании разными водяными знаками одного и того же сообщения должна прослеживаться очередность подписей и имеющиеся подписи не должны разрушать друг друга;
- невозможность отказа автора от подписанного сообщения (для систем с ассиметричными ключами);
- невозможность формирования получателем верного ЦВЗ отправителя сообщения (для систем с ассиметричными ключами);
- невозможность разрушения, а так же удаления ЦВЗ без разрушения сообщения;
- устойчивость ЦВЗ к воздействию преднамеренных или случайных помех, то есть содержащаяся информация в заверенном сообщении не должна разрушаться;
- при внедрении и последующей проверке ЦВЗ в сообщении не обязательно участие третьей доверенной стороны (арбитра);
- возможность работы полученной системы с современными методами криптографической защиты, передачи, хранения и повышение помехоустойчивости;
- возможность обрабатывать заверенные сообщения стандартными методами (архивация, масштабирование, фильтрация, сжатие, и другие) без разрушения водяных знаков.

Литература.

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А.Воронцов и др.: Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. – М.: Горячая линия – Телеком, 2009. – 552 с.: ил.
2. Hartung F., Kutter M. Multimedia waterwarking techniques //Proceeding of the IEEE, vol. 87, № 7, 1999, pp.1079–1107.
3. ГОСТ РФ 34.10-94. Информационная технология. Криптографическая защита информации. Электронная цифровая подпись.// М.: Госстандарт РФ.
4. Shokarev A. V. Current Graphical Password Systems. Implementation Algorithms by Digital Watermarking // Applied Mechanics and Materials. - 2013 - Vol. 379. pp. 229-234.
5. Оков И.Н., Ковалев Р.М. Электронные водяные знаки как средство аутентификации передаваемых сообщений. // Конфидент, №3, 2001.