

# Модель динамической системы обеспечения комплексной защиты информации при передаче голосовых сообщений

К. А. Коновалов, email: kkonov@gmail.com  
Н. Е. Балакирев, email: balakirev1949@yandex.ru

Московский авиационный институт  
(национальный исследовательский университет)

***Аннотация.** В данной работе представлена модель динамической системы обеспечивающая комплексную защиту информации. Предлагаемая динамическая система реализуется на примере программной системы "Голосовая почта", в которой апробируются все предлагаемые в статье механизмы.*

***Ключевые слова:** Защита информации, голосовая связь, передача информации, системы учета и контроля, индивидуальный код.*

## Введение

Статья посвящена вопросам организации защиты информации, включая процессы её передачи, на примере «Голосовой почты» [1].

Поскольку любая система защиты информации подвержена вскрытию, вопрос лишь только во временных интервалах, затрачиваемых злоумышленником. В связи с этим можно предложить средства регулярной смены защиты, соотносимые с временем для вскрытия информации. Понимая, что время вскрытия зависит от сложности предлагаемых механизмов защиты, требуется максимальное усложнение предлагаемых алгоритмов в рамках политик. Всё это необходимо было вложить в механизм, точнее модель, реализующую динамический подход, обеспечивающий глубоко эшелонированную систему защиты. Дело в том, что злоумышленник, желая получить конфиденциальную информацию, будет применять различные способы вскрытия, например анализ передаваемых потоков информации, либо анализ кода программного продукта, обеспечивающего средства защиты и порождающего защищенные потоки информации. Злоумышленник может применять инструментарий дизассемблирования, а далее анализ программы, либо утилиты по перехвату передаваемых данных для анализа. После чего, поняв алгоритм, лежащий в основе программного решения и алгоритм обеспечения защиты при передаче, злоумышленник выяснит, что за информация передавалась и как обеспечивается связь участников общения. В связи с вышесказанным, задача состоит в том, чтобы максимально усложнить эту процедуру комплексом мероприятий. Для обеспечения эффективных способов борьбы с потенциальными

возможностями злоумышленника, предлагается механизм, реализующий динамическую систему обеспечения комплексной защиты, который максимально обесценивает деятельность по дизассемблированию кода программного продукта и вскрытию передаваемых потоков информации.

### **Модель динамической системы**

Предлагаемая модель динамической системы подразумевает механизм взаимодействия участников обмена информации используя комплекс защитных мер при передаче информации. В рамках проводимых работ в качестве предмета исследования была рассмотрена передача звуковой информации, относительно которой рассматривались защитные механизмы.

Целью защиты информации является сохранение таких свойств информации, как целостность, доступность и конфиденциальность.

Для обеспечения данных свойств информации предложен комплекс мер, реализующих вариабельность кода программного продукта через индивидуализацию кода и индивидуализацию структур пакета передачи без изменения функциональности, а также возможность их периодического изменения. Данная мера призвана обеспечить бесполезность использования результатов вскрытия алгоритмов программного продукта, так как к завершению вскрытия код программного продукта уже может быть изменен. Периодичность изменения индивидуальных экземпляров программного продукта предлагается отработать на данной модели, имитируя действия злоумышленника, и осуществлять сменяемость продукта в рамках правил выбранной политики. Отсюда возникает необходимость в реализации службы, которая за каждым пользователем закрепляет свой индивидуальный экземпляр (индивидуализация) программного продукта и которая по мере необходимости регулярно перерегистрирует и обновляет программный продукт в соответствии с установленной политикой.

В итоге имеем систему, индивидуально обслуживающую каждого пользователя и реализующую динамичность передаваемой информации.

Возможность документированного установления источника утечки и обеспечение доказательной базы нарушения прав пользования программным продуктом является, пожалуй, наиболее важным дополнительным свойством указанной системы защиты и системы учета программных продуктов. Наряду с индивидуализацией добавляется набор возможностей, облегчающий выявление злоумышленника через маркировку передаваемой информации изменяемыми элементами «водяных знаков». Для этого предлагается закреплять за пользователями

— участниками общения определенные метаданные, реализуемые «водяными знаками», по которым однозначно можно идентифицировать как экземпляр конкретного владельца программного продукта, так и сеанс передачи привязанный к дате и времени передачи информации.

Для обеспечения учета и контроля за правомочностью и корректностью использования экземпляров программных продуктов было решено реализовать централизованную систему учета и контроля использования выдаваемых пользователю индивидуальных экземпляров программ.

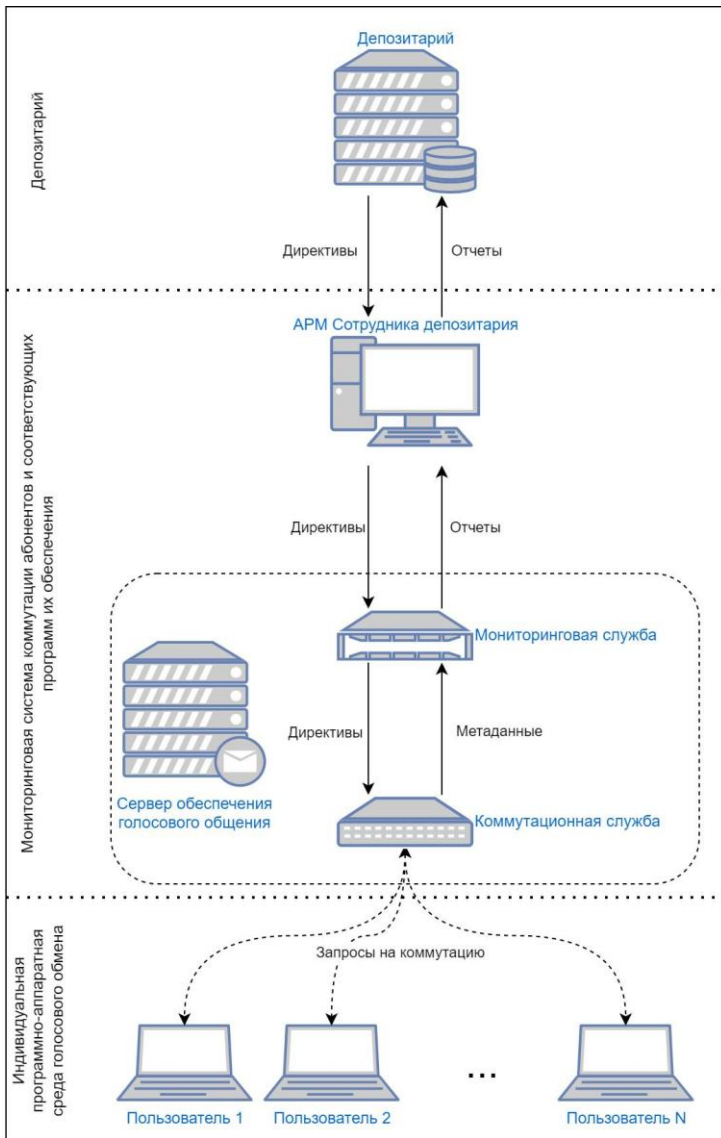
Таким образом, в рамках модельной системы «Голосовая почта», для реализации модели динамической системы обеспечения комплексной защиты информации необходимо, чтобы были реализованы механизмы охватывающие, интересующие с точки зрения обеспечения защиты, свойства информации целостности, доступности и конфиденциальности. Реализуемые механизмы следующие:

- Механизм *Идентификации*: передаваемая информация однозначно идентифицирует источник передачи — экземпляр программного продукта. Реализация: пользовательская информация дополняется «водяными знаками», для целей маркировки и дальнейшего контроля за перемещением информации.
- Механизм *Защиты*: передаваемая пользователем информация защищена от просмотра при перехвате, что реализуется структуризацией передаваемого потока амплитуд на базе качественного подхода к анализу данных.
- Механизм *Уникальности*: экземпляр программного обеспечения побайтно уникален для каждого пользователя, т.е. для каждого пользователя создается персональный экземпляр программного продукта посредством индивидуализации программного кода.
- Механизм *Функциональности*: экземпляр программного обеспечения функционально уникален для каждого пользователя, т.е. каждый экземпляр программного продукта, включая компоненты, реализующие структуры данных и протоколы передачи данных, соотносится только с одним пользователем (решено дать название — индивидуализация программного продукта).
- Механизм *Учета и контроля*: уникальные экземпляры программного продукта выдаются пользователям, на основе индивидуализации обеспечивается система учета и контроля предоставления программного продукта.

- Механизм *Мониторинга*: на основе интегральной информации об индивидуальном продукте производится регулярный мониторинг использования программного кода и контроль процесса приема-передачи.

Большинство указанных механизмов обеспечения защиты информации прошли предварительную апробацию, показав свою эффективность, и были включены в комплексную модель [2; 3; 4; 5; 6].

Реализация модельной системы «Голосовая почта» предлагается осуществить согласно концептуальной модели, показанной на рисунке, на которой изображена общая концептуальная модель системы учета и контроля с взаимодействием участников и компонентов моделирующего комплекса.



*Рисунок.* Концептуальная схема работы моделирующего комплекса «Голосовая почта»

В комплексе выделено три компонента:

1. *депозитарий* (по аналогии с банковскими депозитариями [5; 6]),
2. *мониторинговая система коммутации* абонентов и соответствующих программ их обеспечения [3; 4; 5; 6],
3. *индивидуальная программно-аппаратная среда голосового обмена* [3; 4].

Первым на рисунке идет компонент *депозитарий*, на который возлагаются задачи по агрегированию и последующему хранению сведений участников общения с проверкой согласно протоколу взаимодействия этих участников общения со стороны второго компонента (обеспечивая механизмы *Функциональности* и *Учета и контроля*).

Вторым компонентом идет *мониторинговая система коммутации*, призванная реализовать механизм взаимодействия участников общения и не допустить подключение злоумышленника под видом легитимного пользователя (обеспечивая механизмы *Идентификации*, *Защиты* и *Мониторинга*).

Третий компонент рисунка *индивидуальная программно-аппаратная среда голосового обмена* показана в общем виде (реализация механизма *Уникальности*), т. к. уже ранее [4; 6] упоминалось, что предлагается реализация нескольких стратегий общения: симплексное, дуплексное, а также один к одному или один ко многим с их комбинациями (в рамках указанного выше механизма *Функциональности*). Если рассматривать эту часть схемы в конкретных примерах, то будут такие варианты, как отправитель к только слушающему получателю (получателям) или равноправные (с точки зрения возможности отправки и получения) участники.

### **Заключение**

Предложенная модель динамической системы комплексной защиты информации должна обеспечить высокую степень надежности, а индивидуализация экземпляров программного обеспечения дает документальную основу для выявления злоумышленников.

### **Литература**

1. Коновалов К. А., Балакирев Н. Е.. Создание системы обеспечения учета и контроля защиты информации при передаче голосовой информации. 20-я Международная конференция «Авиация и космонавтика». 22-26 ноября 2021 года. Москва. Тезисы. Сс. 231-232. ISBN 978-5-00189-750-7.
2. Думанский А. И., Семенова Т. Б., Бабуджи С. Ю., Балакирев Н. Е.. Обеспечение конфиденциальной передачи информации через

интернет. Гагаринские чтения — 2019. Сборник тезисов докладов. 2019. С. 337.

3. Думанский А. И., Федюк Ю. О., Балакирев Н. Е.. Защита программного продукта через его индивидуализацию на примере модели голосовой почты. Гагаринские чтения - 2020. Сборник тезисов докладов. 2020. С. 294-295.

4. Федюк Ю. О., Балакирев Н. Е.. Разработка различных стратегий использования голосовой почты с целью обеспечения дополнительных видов конфиденциальности. Гагаринские чтения - 2020. Сборник тезисов докладов. 2020. С. 523-524.

5. Селиванов Д. А., Думанский А. И., Балакирев Н. Е.. Индивидуализация кода программ, учитываемых в депозитарии. XLVII Гагаринские чтения 2021. Сборник тезисов работ. 2021. С. 451-452.

6. Думанский А. И., Балакирев Н. Е., Зеленова М. В., Лазунин К. А., Фадеев М. М.. Распределенная система защитных механизмов программного комплекса «Голосовая почта» на базе структуризации звукового потока волн. Информатика: проблемы, методы, технологии. Материалы XXI Международной научно-методической конференции. Воронеж, 2021. С. 709-716.