УДК 004.056.5

Подсистема защиты авторского права в сфере программного обеспечения

А.В. Чернышова, Д.В. Кубашевский
Донецкий национальный технический университет
chernyshova.alla@rambler.ru, dehax12@gmail.com

Чернышова А.В., Кубашевский Д.В. Подсистема защиты авторского права в сфере программного обеспечения.

В данной работе раскрыта проблема нелегального использования ПО, описаны недостатки существующих механизмов защиты авторского права на программное обеспечение и представлена реализация новой программной подсистемы защиты ПО с использованием криптографических алгоритмов шифрования.

Введение

В настоящее время широко распространена проблема нелегального копирования и распространения программного обеспечения. Ежедневно огромное количество пиратских копий программных продуктов скачиваются бесплатно в сети Интернет, что наносит огромный ущерб разработчикам этих продуктов.

В последнее время разработчики коммерческого ПО внедряют в свои программные продукты подсистемы защиты от нелегального копирования. Зачастую, подобные подсистемы защиты ненадёжны, так как её разработке уделяется недостаточно сил. Через некоторое время хакеры исследуют и взламывают подсистему защиты, и программный продукт попадает на рынок пиратского ПО [1].В связи с этим возникает необходимость реализации подсистемы защиты таким образом, чтобы программный продукт не мог функционировать без подтверждения лицензии на использование ПО, а процесс взлома такой защиты был максимально затруднён.

Постановка задачи

Необходимо разработать программную подсистему защиты авторского права в программном обеспечении, которая представляла бы компромиссный вариант между усилиями, затраченными на её реализацию, и эффективностью её функционирования. Для реализации этой задачи необходимо пересмотреть принципы и методы защиты от анализа и взлома ПО.

Обычно проверка лицензии на использование ПО пользователем основана на активации программного продукта через сервер лицензий. После проверки правильности данных лицензии, предоставленных пользователем, сервер должен дать подтверждение действительности лицензии, и в этом случае подсистема защиты открывает доступ пользователю к функциональным возможностям ПО. Данная идея защиты содержит существенный недостаток — можно реализовать поддельный сервер лицензий, который всегда будет подтверждать действительность лицензии, или модифицировать подсистему защиты таким образом, чтобы проверка активации программного продукта не осуществлялась.

Поэтому была разработана подсистема защиты, которая основана не на предоставлении права на функционирование ПО, а на предоставлении некоторых функциональных возможностей ПО, то есть некоторой части программного кода, без которой продукт не может работать и выполнять важные для пользователя функции. Модификация подсистемы защиты или реализация пиратского сервера лицензий не позволяет получить доступ к необходимым функциям программы.

Структура программной системы

Разработанная программная система имеет клиент-серверную архитектуру. Диаграмма развёртывания представлена на рисунке 1.

Клиентскую часть представляет простейшее тестовое приложение «DLSTestSoft», которое содержит и взаимодействует с модулем подсистемы защиты «DLS». Подсистема защиты выполняет запросы к серверу лицензий «DLSServer». Запросы от клиентской части к серверу будут выполняются посредством TCP-соединения [2].

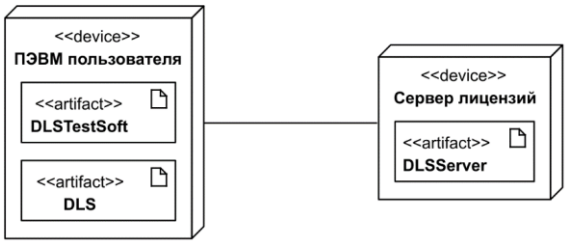

Рисунок 1 — Диаграмма развёртывания

Диаграмма вариантов использования (диаграмма прецедентов) для сервера приведена на рисунке 2.

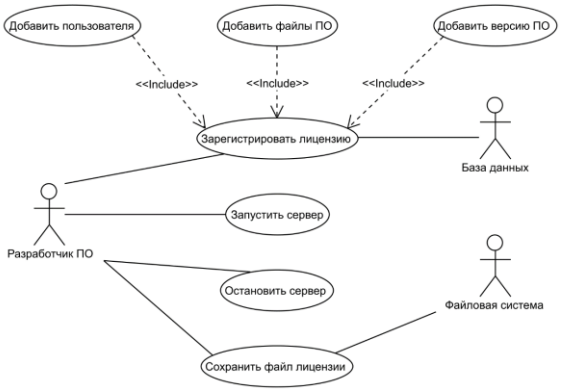

Рисунок 2 — Диаграмма вариантов использования сервера

Сервер хранит выданные пользователям лицензии на использование ПО в локальной базе данных. Разработчик может выполнять регистрацию новых лицензий. При необходимости в базу данных добавляются записи о новых пользователях и версиях ПО, для каждой версии заполняется список файлов программы, которые будут проверяться на наличие изменений в них.

Среди функций, доступных пользователю сервера — разработчику ПО, обязательными являются запуск и остановка сервера, а также возможность сохранить запись о лицензии в файл для передачи его пользователю защищаемого ПО.

Диаграмма вариантов использования программной системы в целом представлена на рисунке 3.

На диаграмме отображено взаимодействие подсистемы защиты с сервером. При запуске защищаемого программного обеспечения подсистема защиты выполняет попытку проверки и активации лицензии. После успешной активации подсистема защиты включает полнофункциональный режим работы программы.

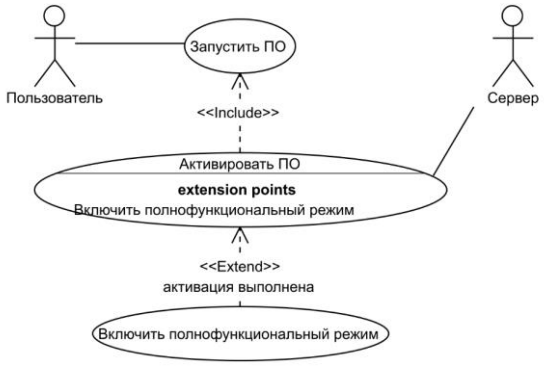

Рисунок 3 — Диаграмма вариантов использования программной системы

Модуль подсистемы защиты отправляет серверу данные лицензии, сервер проверяет правильность данных и наличие в своей базе данных записи о выданной лицензии. После успешной проверки сервер отправляет клиенту зашифрованный файл, который предоставляет дополнительный функционал защищаемому ПО. Клиент получает данный файл, и подсистема защиты переводит программу в полнофункциональный режим, которая сможет использовать дополнительный функционал, предоставленный сервером после успешной активации лицензии.

Проектирование структур системы

Сервер подсистемы защиты взаимодействует с базой данных, которая имеет определённую структуру. В базе данных хранится информация о каждой выданной лицензии, затем разработчик ПО имеет возможность сохранить информацию о лицензии в файл и передать его пользователю ПО для активации лицензии при работе с программным продуктом.

Схема базы данных сервера лицензий представлена на рисунке 4.

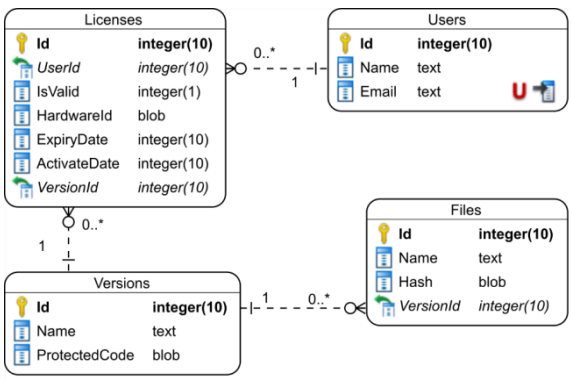

Рисунок 4 — Схема базы данных

База данных содержит 4 таблицы. Таблица «Users» содержит записи о пользователях защищаемого программного обеспечения.

Таблица «Versions» содержит записи о версиях защищаемого программного обеспечения. Наличие записей о версии программы позволит контролировать процесс активации лицензии. Лицензия, выданная для одной версии, не действительна для работы активации другой версии.

Таблица «Files» содержит записи о файлах ПО, которые будут проверяться на наличие изменений при активации лицензии.

Таблица «Licenses» содержит записи о выданных пользователям лицензиях на использование ПО.

Файл лицензии на использование ПО имеет формат XML [3]. Пример содержимого файла лицензии приведён на рисунке 5.

```
<DLS>
  <Id>1</Id>
  <Name>Денис Кубашевский</Name>
  <Email>dehax12@gmail.com</Email>
  <HardwareId>BK3vkmrkghPcg6T6PD2Hfg==</HardwareId>
  <Version>1.0.0.0</Version>
  <Files>
    <File Name="log4net.dll" Hash="9ktzPq5EyMZiFzhtWg8r8A==" />
  </Files>
  <ActivateDate>2012-01-01</ActivateDate>
  <ExpiryDate>2020-01-01</ExpiryDate>
  <Signature>805ucg4CQgTrkVLUz+ICQtBUb8qUrgk0GZd618Df1DcONzq3R9HUSQ==</Signature>
  <PublicKey>
BgIAAAAiAABEU1MxAAQAAEt7nUo6GaPF71YsmksTjrRExEicYM+Aj3pWGAYhyjn+AvZcCehs5QbjEi
UxeLmYxCkQWgyI7P4drphmqiZuybwFORokQBbMrK2+VZUzoWkpnGAmP/JPkpOoIs5WwtbbT2vtIg/b
Odhz8xbBUqHnd8/itXcCWm/0oopexdSyrbHP8/dtE9tPgPKqv0EJi6dBm+r84f5hdQpPpYPGHYA5o3
czAhE6eumMSic97AB62TPMbL1hSpBY2EXbSjkk640Znv+r7iJrwidTObJg5aw6/VwXbMhMsdcesNl2
Rv6oTFo0o0jUDd9fy4w2j9v8oaOp29ublBxmSaRCFnGlph5pxNF59QFOHdFPKqR/UXT/sO7OP5K6Is
RURpxvQAW9SSptv0ZSh8JG45L4zsqyJp1hYr7FuUzxtMNcjZc410nARZ48aTXkFYBLRKWS3U2bQBqi
4Lso+7vWXuoHWmbT2jksJyU7GUbIB2xcEwSyc1v6IA+3w4qCKnUup6cm9ELK0P2U2wjK6juKfqrDXd
gshTc/NlicR2mzKwEAAOoE56E7T9OVMdcpnNyZLF3ntwEH</PublicKey>
</DLS>
```

Рисунок 5 — Пример содержимого файла лицензии

Корневой тег «DLS» включает в себя другие XML-теги, которые содержат данные лицензии.

Программная реализация

Для реализации программной системы была выбрана программная платформа «.NET Framework» [4] версии 4.6.1 и высокоуровневый объектно-ориентированный язык программирования C# [5] версии 7.0. В качестве интегрированной среды разработки (IDE) использовалась «Microsoft Visual Studio» версии 2017.

Для реализации базы данных выбрана компактная встраиваемая реляционная БД «SQLite» [6].

Основной задачей реализации программной системы является обеспечение функционирования алгоритма подсистемы защиты авторского права. Полный алгоритм активации лицензии представлен на рисунке 6.

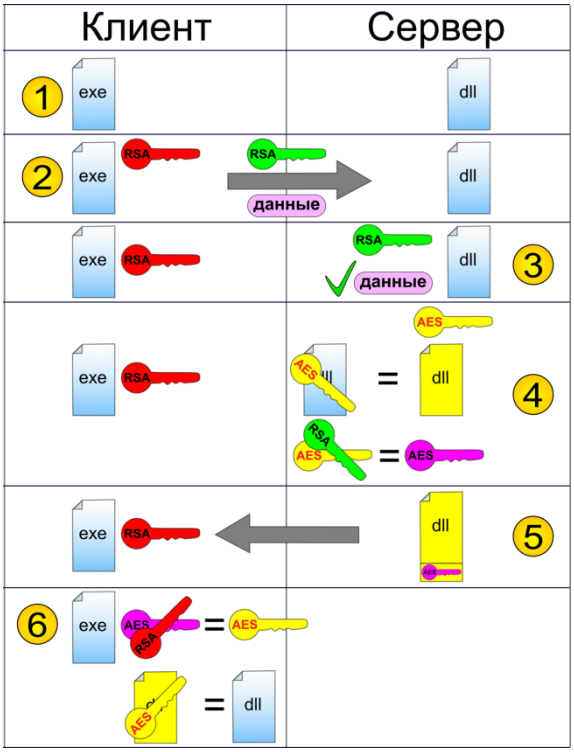

Рисунок 6 — Алгоритм активации лицензии [7]

После успешной проверки файла лицензии начинается отправка данных лицензии на сервер для прохождения проверки и получения данных «защищённого кода». На втором шаге алгоритма модуль подсистемы защиты генерирует пару ключей RSA [8] и отправляет на сервер открытый ключ вместе с данными лицензии.

На третьем шаге сервер подтверждает подлинность и действительность данных, после чего на четвёртом шаге генерирует ключ AES [9] и с помощью его зашифровывает файл «защищённого кода». Ключ AES зашифровывается с помощью полученного от клиента открытого ключа RSA.

На пятом шаге сервер передаёт обратно клиенту зашифрованный «защищённый код» и зашифрованный ключ, который клиент на шестом шаге расшифровывает с помощью своего оставшегося закрытого ключа RSA. После этого расшифрованным ключом AES расшифровывается файл «защищённого кода» и модуль подсистемы защиты сохраняет в памяти данные «защищённого кода», что позволяет перевести ПО в полнофункциональный режим.

Алгоритм проверки и активации лицензии модуля подсистемы защиты представлен на рисунке 7. При запуске тестового приложения происходит обращение к модулю подсистемы защиты с целью проверки лицензии и выполнения активации лицензии.

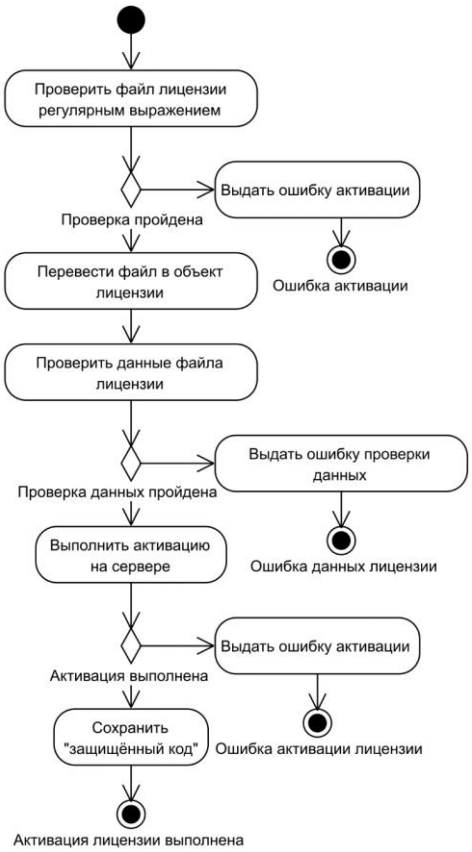

Рисунок 7 — Диаграмма деятельности алгоритма проверки лицензии

Диаграмма деятельности алгоритма запуска тестового приложения представлена на рисунке 8.

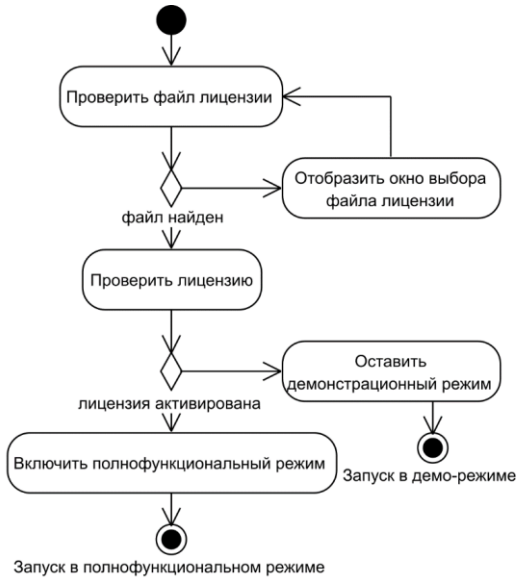

Рисунок 8 — Диаграмма деятельности алгоритма запуска тестового приложения

Пример использования системы

После запуска приложения сервера появится основное окно, которое изображено на рисунке 9.

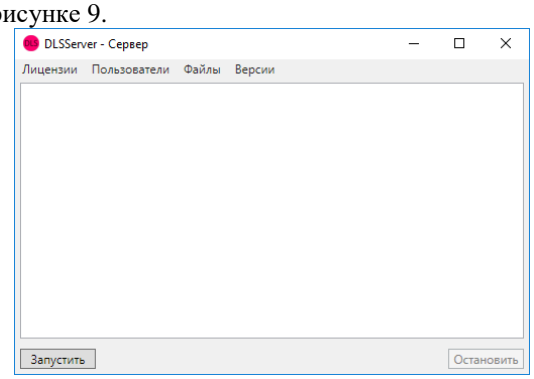

Рисунок 9 — Основное окно приложения сервера

Для запуска сервера, который будет ждать запросов от клиентов, необходимо нажать кнопку «Запустить». После запуска сервера кнопка «Запустить» будет заблокирована и доступной окажется кнопка «Остановить» для остановки функционирования сервера.

Главное меню окна позволяет перейти к окнам просмотра записей таблиц базы данных.

После первого запуска тестового приложения пользователю будет предложено выбрать файл лицензии, который был предоставлен разработчиком ПО при покупке программного продукта. При последующих запусках указывать файл лицензии пользователю не потребуется, в процессе первой активации файл лицензии будет сохранён в каталог приложения в личной папке пользователя. В среде операционной системы Windows путь к данному каталогу — «%LOCALAPPDATA%\DehaxSoft\DLSTestSoft».

После приобретения пользователем программного продукта разработчик должен выдать лицензию на использование ПО. Для этого необходимо в основном окне приложения сервера выбрать пункт меню «Лицензии», чтобы перейти к окну просмотра записей таблицы лицензий БД. Данное окно представлено на рисунке 10.

Для выдачи новой лицензии необходимо нажать кнопку «Добавить», после чего появится окно добавления новой записи о лицензии в БД. Для добавления новой записи о лицензии потребуется, чтобы предварительно были добавлены:

– запись о пользователе, которому выдаётся лицензия;

– запись о версии ПО, для которой будет выдана лицензия;

– записи о файлах ПО, которые подлежат проверке при активации ПО.

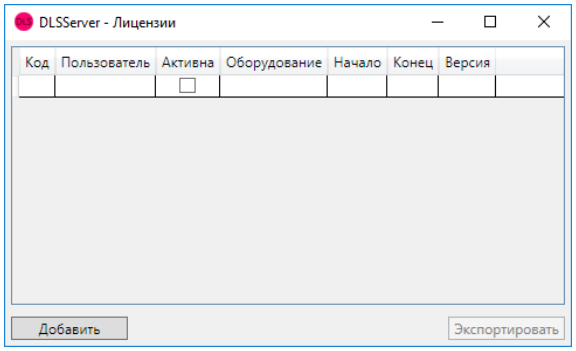

Рисунок 10 — Список выданных лицензий

Добавление этих записей осуществляется подобным образом. Доступ к таблицам предоставляется из главного меню основного окна приложения сервера. В каждом из окон для просмотра записей таблиц пользователей, версий ПО и файлов ПО также присутствует кнопка «Добавить» для создания новых записей БД.

Окно добавления новой записи о лицензии на использование ПО изображено на рисунке 11.

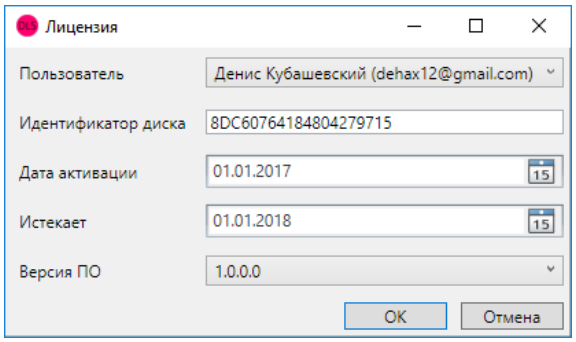

Рисунок 11 — Выдача новой лицензии

В поле «Пользователь» разработчик может выбрать пользователя из списка, которому будет выдана лицензия. В поле «Идентификатор диска» указывается серийный номер первого жёсткого диска ПЭВМ пользователя. Поля «Дата активации» и «Истекает» позволяют контролировать срок действия лицензии. В поле «Версия ПО» из списка также можно выбрать версию программного продукта, для которого предназначена лицензия.

После нажатия кнопки «ОК» запись о лицензии будет сохранена в базе данных. Теперь необходимо сгенерировать для пользователя файл лицензии, с помощью которого он сможет выполнить активацию. Для этого в окне списка лицензий необходимо выбрать соответствующую запись о лицензии и нажать кнопку «Экспортировать». Файл лицензии с именем адреса электронной почты пользователя и расширением «dls» будет помещён в папку «Документы» операционной системы. Далее разработчик передаёт файл пользователю, после чего у пользователя появляется лицензия на использование ПО.

При первом запуске тестового приложения отобразится сообщение о том, что файл лицензии не найден и появится окно, которое изображено на рисунке 12, позволяющее пользователю указать файл лицензии для проведения активации.

Рисунок 2 — Окно выбора файла лицензии

После нажатия кнопки «ОК» будет произведена проверка файла лицензии, затем модулем подсистемы защиты будет выполнен запрос на сервер с передачей данных лицензии. При успешном выполнении активации отобразится основное окно тестового приложения, которое изображено на рисунке 13.

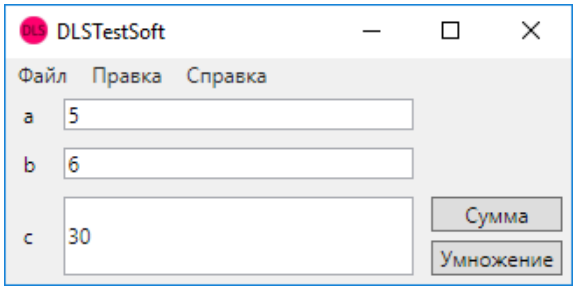

Рисунок 13— Полнофункциональный режим работы тестового приложения

На рисунке 13 представлен полно-функциональный режим работы тестового приложения, в который подсистема защиты перешла после успешного прохождения процедуры активации лицензии.

Если Интернет-соединение на этапе активации отсутствует, пользователю отображается соответствующее сообщение с предложением повтора попытки активации, которое представлено на рисунке 14.

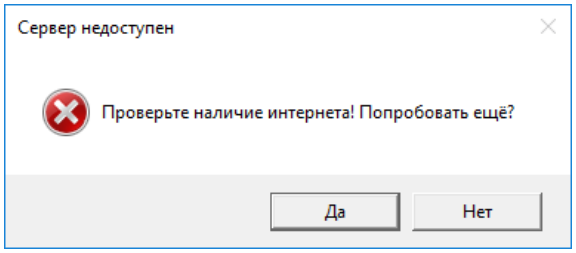

Рисунок 14 — Сообщение об отсутствии соединения с сервером

После нажатия кнопки «Нет» тестовое приложение продолжит работу в демонстрационном режиме, который остаётся активным также в случае возникновения ошибок при активации лицензии. Основное окно тестового приложения в демонстрационном режиме работы представлено на рисунке 15.

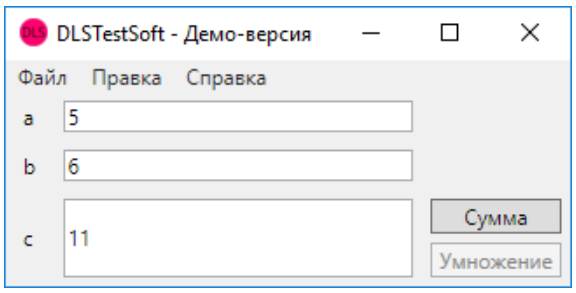

Рисунок 15 — Демонстрационный режим работы приложения

В демонстрационном режиме работы тестового приложения доступна только кнопка «Сумма», которая позволяет выполнить операцию сложения значений полей «a» и «b», получив результат в поле «c».

В полнофункциональном режиме работы доступна также операция умножения и отсутствует надпись «демо-версия» в заголовке окна, что подтверждает успешную активацию лицензии и право на использование ПО.

Выводы

В ходе выполнения данной работы была раскрыта проблема нелегального использования ПО, описаны недостатки существующих механизмов защиты авторского права на программное обеспечение и представлена реализация новой программной подсистемы защиты ПО с использованием криптографических алгоритмов шифрования.

Защита, обеспечиваемая компонентами данной программной системы, позволяет противостоять действиям хакеров среднего уровня, поскольку исследование алгоритма защиты не позволит взломать защиту. Использование длинных ключей криптографических алгоритмов позволит исключить метод перебора для выполнения расшифровки защищаемых данных.

В дальнейшем планируется расширение реализованной подсистемы защиты до системы защиты ПО, которая будет работать с несколькими программными продуктами и поддерживать распределённые базы данных [10] для оптимизации взаимодействия модуля системы защиты с серверами лицензий и уменьшения на них нагрузки при большом количестве пользователей защищаемого ПО.

Литература

1. Пиратское ПО // SecurityLab.ru. [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/news/tags/%EF%E8%F0%E0%F2%F1%EA%EE%E5+%CF%CE/

2. Протокол TCP // OpenNET. [Электронный ресурс]. – Режим доступа: https://www.opennet.ru/docs/RUS/inet_book/4/44/tcp_443.html

3. Extensible Markup Language (XML) // W3C. [Электронный ресурс]. – Режим доступа: https://www.w3.org/XML/

4. .NET // Microsoft. [Электронный ресурс]. – Режим доступа: https://www.microsoft.com/net

5. .NET Programming Languages // Microsoft. [Электронный ресурс]. – Режим доступа: https://www.microsoft.com/net/Learn/Languages

6. SQLite // SQLite. [Электронный ресурс]. – Режим доступа: https://www.sqlite.org/

7. Чернышова, А.В. Подсистема защиты авторского права в программном обеспечении / А.В. Чернышова, Д.В. Кубашевский // Информатика и кибернетика. – 2016. – № 2(4). – С. 68-72.

8. Алгоритм RSA // НОУ ИНТУИТ. [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/studies/courses/691/547/lecture/12391

9. Как устроен AES // Хабрахабр. [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/112733/

10. Распределённые и параллельные системы баз данных // CIT Forum. [Электронный ресурс]. – Режим доступа: http://citforum.ru/database/classics/distr_and_paral_sdb/

A.V. Chernyshova, D.V. Kubashevskiy.The Copyright Protection Subsystem in Software.*The article deals with the problem of illegal software using. It describes the disadvantages of existing mechanisms for the copyright protection of software and introduces the realization of the new software protection subsystem which uses cryptographic encryption algorithms.*

Keywords*:Software license, additional module, software protection, symmetric encryption algorithms, asymmetric encryption algorithms*

А.В. Чернышова, Д.В. Кубашевский. Подсистема защиты авторского права в сфере программного обеспечения. *В данной работе раскрыта проблема нелегального использования ПО, описаны недостатки существующих механизмов защиты авторского права на программное обеспечение и представлена реализация новой программной подсистемы защиты ПО с использованием криптографических алгоритмов шифрования.*

Ключевые слова*:Лицензия на программное обеспечение, вспомогательный модуль, защита ПО, симметричные алгоритмы шифрования, ассиметричные алгоритмы шифрования*

Статья поступила в редакцию 17.10.2017
Рекомендована к публикации доктором технических наук В.Н. Павлышом