Принятые меры должны предупредить возникновение опасности, ликвидировать ее или минимизировать до допустимого уровня [5].

На основании анализа проведенных исследований разработаны блок-схемы приемки, подготовки сырья и технологического процесса производства печенья обогащенного пищевыми волокнами. По итогам анализа технологического процесса в соответствии с нормативным документом [1] составлен перечень потенциально опасных факторов на технологических этапах производства печенья обогащенного пищевыми волокнами.

Программа формируется исходя из положений инструкций и программ, направленных на обеспечение безопасности продукции, и включают в себя комплекс обязательных мероприятий, который необходимо осуществлять как перед началом производства и на всем его протяжении, так и после окончания данного процесса.

Список литературы

1. Технический регламент Таможенного союза ТР ТС 021/2011 "О безопасности пищевой продукции".

2. Полякова С.П. Анализ организации контроля мучных кондитерских изделий и безопасности готовой продукции на производстве/С.П. Полякова // Кондитерское и хлебопекарное производство. - 2017. - №3.- С. 17-19.

3. Система контроля производства кондитерских изделий [Электронный ресурс] - Режим доступа: http://www.iksystems.ru/a329/.

4. Смирнова Н.А. Современные системы управления качеством и безопасностью пищевых продуктов / Н.А.Смирнова, А.А. Смирнов // Пищевая промышленность. - 2015.- № 3.- С.12-14.

5. Тарасова Е.Ю. Системы управления качеством в пищевой промышленности. / Е.Ю.Тарасова, Е.И. Петрова // Современное общество, образование и наука. Тамбов, 2015.- С. 160-162.

6. Тарасов Р.В. Анализ риска от воздействия потенциальных опасных факторов и разработка предупреждающих действий при производстве минеральной воды // Р.В. Тарасов, Л.В. Макарова, С. Ж. Умырова, Е. В. Медведкова // Современные научные исследования и инновации. №2 - 2014.

УДК 004.021

Е.В. Каширин
Управление специальной связи и информации
ФСО России в ДФО
г. Хабаровск, Россия

ПРИМЕНЕНИЯ МЕТОДОВ ЦИФРОВОЙ СТЕГАНОГРАФИИ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Специалисты в области инфокоммуникационных технологий уделяют большое внимание проблемам защиты информации, что связано со значительным охватом данными технологиями всех сфер жизнедеятельности. Ценность конфиденциальной информации постоянно возрастает и представляет огромный интерес злоумышленников, что приводит к возникновению угроз безопасности информации и ее утечке. Несмотря на то, что системы защиты информации постоянно совершенствуются, проблема продолжает существовать.

На сегодняшний день для информации, обрабатываемой на ПЭВМ и хранящейся на внешних носителях, наиболее актуальной угрозой является несанкционированное копирование (НСК), которое можно условно разделить на два направления [1, с. 68]:

1) НСК защищаемой информации;

2) НСК программного обеспечения.

НСК защищаемой информации может быть осуществлено путем записи содержащихся во внутренней памяти ПЭВМ файлов на внешние носители информации, их распечаткой, а также путем ее фотографирования с экрана монитора или перехвата побочных электромагнитных излучений ПЭВМ.

НСК программного обеспечения (компьютерное пиратство), может принимать различные формы, однако одной из самых часто встречающихся является простое копирование информации или конкретного программного продукта частными пользователями и организациями, не обладающими правами на выполнение таких действий [2, с. 132].

С учетом известных методов защиты информации (правовых, организационных, физических, технических и криптографических) предлагается реализовать способ защиты информации от НСК на основе применения методов цифровой стеганографии для обеспечения защиты информации, хранящейся на внешних (съемных) носителях информации [4, с. 96].

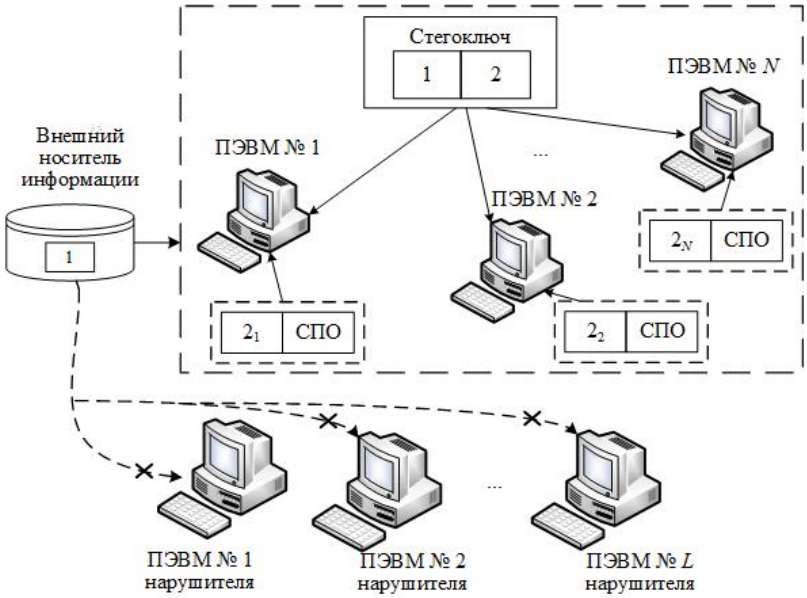

Рис. 1. **Структурно-функциональная схема способа защиты информации от несанкционированного копирования**

Согласно предлагаемому способу защита информации на внешних носителях осуществляется с помощью специального программного обеспечения (СПО), устанавливаемого на каждой ПЭВМ, реализующего функции шифрования таблицы разделов носителей информации на стегоключе, состоящем из двух частей, формирование которых производится администратором ПЭВМ в процессе настройки системы защиты (рис. 1).

Первая часть стегоключа K_1 формируется псевдослучайным образом с помощью соответствующих алгоритмов и помещается на внешний носитель информации. Вторая часть стегоключа K_2 формируется аналогичным образом и помещается на внутренний носитель информации ПЭВМ (НЖМД, *SSD*). Кроме того, вместо генератора псевдослучайных последовательностей (ГПСП) предварительные значения ключей K_1 и K_2 могут вводиться администратором ПЭВМ вручную с помощью клавиатуры. Однако в этом случае для обеспечения необходимых криптографических свойств ключей, а также формирования требуемой их длины должны производиться дополнительные преобразования таких подключей соответствующей криптографической хэш-функцией. Общий стегоключ K_o формируется сложением по модулю 2 первой и второй частей K_1 и K_2 (рис. 2).

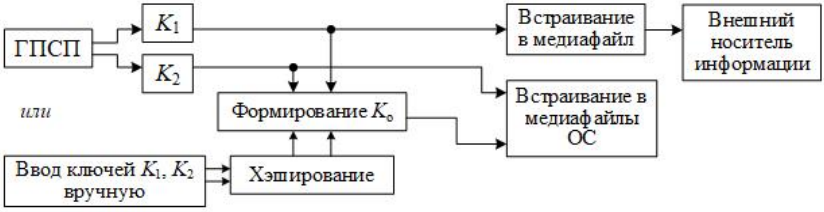

Рис. 2. **Формирование ключевых данных для способа защиты информации от несанкционированного копирования**

Обе части стегоключа, а также сам общий ключ, скрываются в медиафайлах (графических изображениях, музыкальных композициях, видеороликах) методами цифровой стеганографии [5, с. 3].

Перед использованием внешнего накопителя с защищаемой от НСК информацией необходимо произвести его специальное форматирование для формирования отдельного защищенного раздела файловой таблицы, а также обозначения размера открытого раздела с общедоступными файлами для любых операционных систем и пользователей (например, использование таблиц *GUID* стандарта *GPT*) [3, с. 421].

При этом для реализации предлагаемого способа защиты информации от НСК необходима модификация процесса взаимодействия подсистемы ввода-вывода информации с дополнением его функциями СПО, реализующего методы цифровой стеганографии и выполняющего преобразования пакетов *IRP* перед драйвером файловой системы (рис. 3).

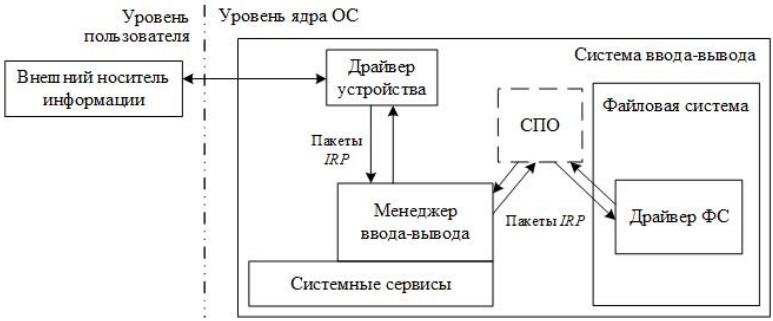

Рис. 3. **Схема модифицированного процесса взаимодействия подсистемы ввода-вывода информации**