ПРОБЛЕМА ОБРАБОТКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА В ПОДРАЗДЕЛЕНИЯХ МЧС РОССИИ

А.Ю. Иванов, доктор технических наук, профессор;
А.П. Тамошенко;
М.В. Сильников, доктор технических наук, профессор,
заслуженный деятель науки РФ.
Санкт-Петербургский университет ГПС МЧС России

Проведен анализ угроз безопасности информации, рассмотрены требования к построению автоматизированной системы мониторинга безопасности информации.

Ключевые слова: безопасность информации, мониторинг безопасности информации, нарушение безопасности информации

PROBLEM OF PROCESSING OF THE INFORMATION OF THE LIMITED ACCESS IN DIVISIONS OF EMERCOM OF RUSSIA

A.Y. Ivanov; A.P.Tamoshenko; M.V. Silnikov.
Saint-Petersburg university of State fire service of EMERCOM of Russia

The analysis of threats of safety of the information is carried out, requirements to construction of the automated system of monitoring of safety of the information are considered.

Key words: safety of the information, monitoring of safety of the information, infringement of safety of the information

Информационные технологии уверенно внедряются в различные сферы человеческой деятельности. МЧС России также разрабатывает и использует в своей деятельности информационные системы, предназначенные для различных направлений. Все это приводит к концентрации больших объемов информации в одной компьютерной сети.

Авторами рассмотрены проблемные вопросы при обработке на средствах вычислительной техники информации, которая в соответствии с требованием законодательства подлежит защите.

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию и информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа) [1].

Информацию ограниченного доступа составляют: сведения, составляющие государственную тайну; сведения конфиденциального характера [2].

Сведения конфиденциального характера, обрабатываемые в подразделениях МЧС России:

– персональные данные (сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность);

– служебные сведения, доступ к которым ограничен органами государственной власти (служебная тайна или информация для служебного пользования);

– сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами

(врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

– сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Из перечисленных сведений конфиденциального характера наиболее часто в подразделениях МЧС России обрабатываются персональные данные и информация для служебного пользования.

Предпосылки нарушения безопасности информации

В силу проявления человеческого фактора могут наблюдаться следующие ситуации:

– в период отсутствия на рабочем месте пользователь не блокирует компьютер, в результате чего доступ к информации имеют посторонние лица;

– при включении компьютера в сеть пользователь не знает, какая информация доступна другим пользователям;

– со своих рабочих компьютеров пользователи выходят в незащищенные сети общего пользования (Интернет), создавая возможность утечки информации;

– пользователи несанкционированно устанавливают на свои компьютеры постороннее программное обеспечение, которое снижает производительность и увеличивает риск выхода из строя системы.

Названные факторы возможны ввиду низкой квалификации или халатности пользователей, недостаточного контроля со стороны администратора безопасности или отсутствия мотивации со стороны руководителя, когда виновные в нарушениях остаются ненаказанными.

Для своевременного реагирования на нарушения необходимо проводить мониторинг безопасности информации, который предполагает постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установления его соответствия требованиям безопасности информации [3].

До настоящего времени в МЧС России отсутствует автоматизированная система мониторинга безопасности информации. В подразделениях, где не все компьютеры включены в одну сеть, этот процесс администратор безопасности реализует периодически, проводя анализ информации, находящейся на рабочих местах пользователей. Эта процедура занимает много времени и приводит к позднему реагированию на нештатные ситуации. Автоматизированная система мониторинга безопасности информации может быть создана только на базе информационной системы, где все компьютеры соединены в сеть, и администратор безопасности имеет доступ ко всем ресурсам этой сети.

Эффективность мониторинга безопасности информации увеличится, если администратор безопасности будет иметь возможность контролировать компьютерные сети подчиненных организаций в режиме удаленного доступа.

На рис. 1 изображена схема типовой компьютерной сети регионального центра МЧС России.

Требования к автоматизированной системе мониторинга безопасности информации

Автоматизированная система мониторинга безопасности информации должна осуществлять поиск информации, подлежащей защите, по типам файлов, по ключевым словам с любых носителей информации пользователя. Кроме того, появится возможность представления оператору информации о пользователях, которые с большой вероятностью нарушают безопасность информации, в том числе осуществляющие несанкционированный выход в незащищенные сети (Интернет) при помощи мобильных устройств, или несанкционировано устанавливают какое-либо программное обеспечение.

Для этого необходимо создание базы данных с типовыми документами должностных лиц для сравнения контента исходящего трафика с материалами из базы данных. В случае полного или частичного совпадения администратор безопасности ставится в известность для проведения углубленного анализа прецедента.

Схема принятия решения изображена на рис. 2.

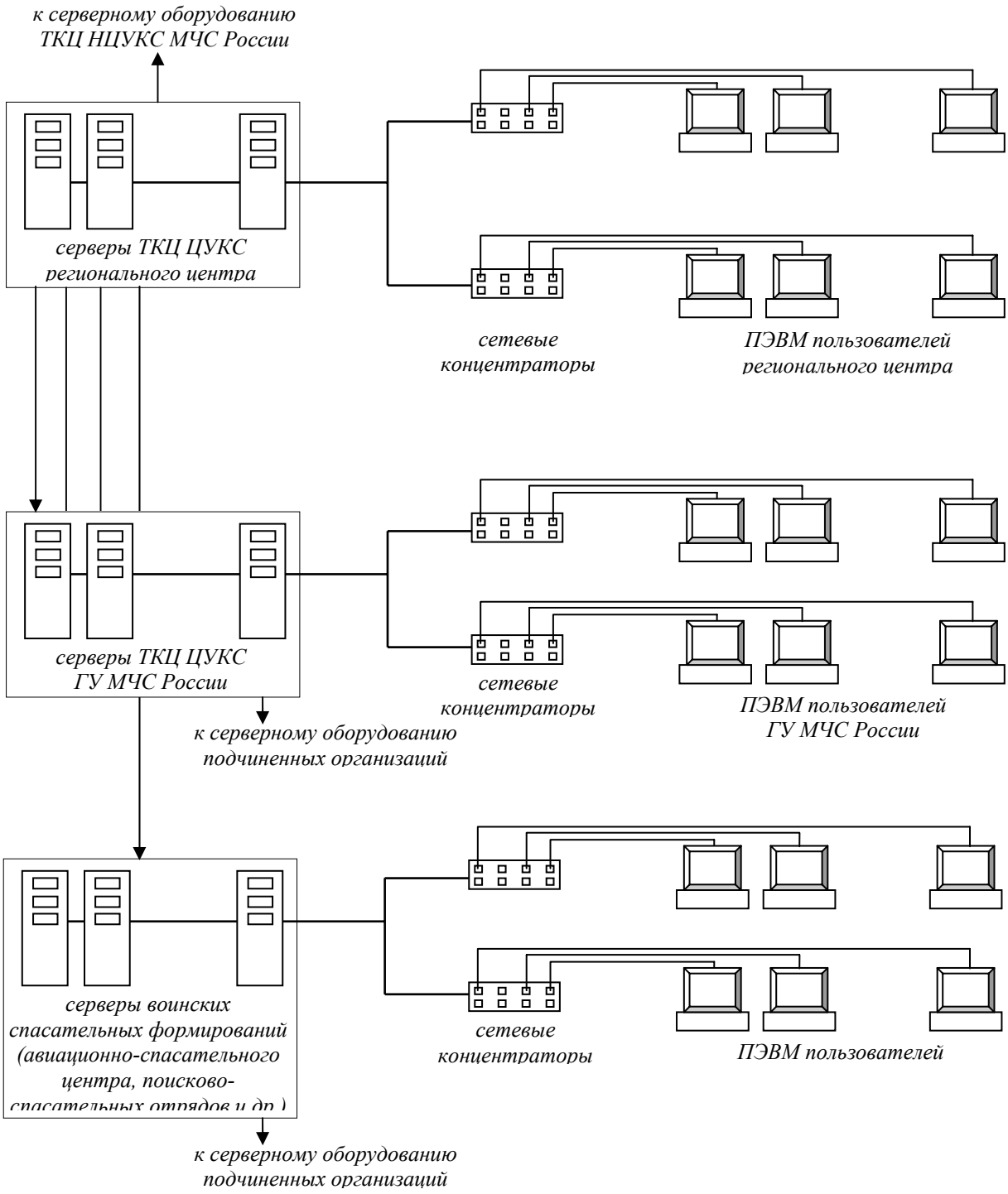

Рис. 1. **Схема типовой компьютерной сети регионального центра МЧС России**

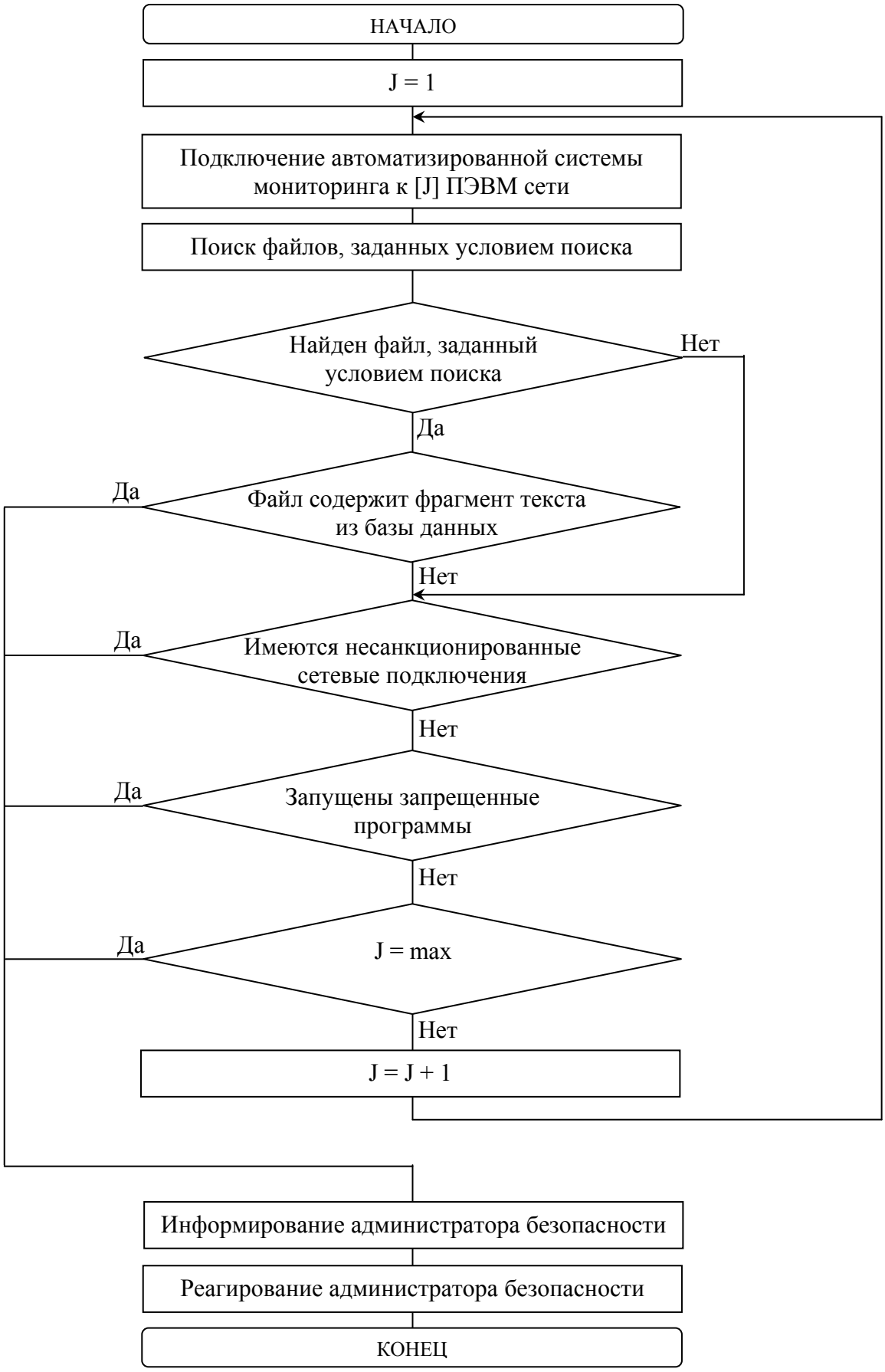

Рис. 2. **Схема принятия решения**

Можно выделить следующие основные проблемы создания автоматизированной системы мониторинга информационной безопасности:

– нет утвержденной типовой структуры компьютерной сети подразделения МЧС России;

– ранее построенные компьютерные сети создавались без учета требований законодательства в области безопасности информации, поэтому для таких сетей необходимо разрабатывать индивидуальные решения;

– финансирование работ по безопасности информации осуществляется не регулярно и не всегда в достаточном объеме;

– установка автоматизированной системы мониторинга информационной безопасности приведет к снижению производительности компьютерной сети;

– предусмотренная законодательством ответственность за нарушение информационной безопасности не всегда адекватна проступкам пользователей.

Эффективность защиты информации в организации МЧС России будет выше при выполнении следующих мероприятий:

– ознакомлении пользователей с требованиями в области безопасности информации и ответственности за их нарушения;

– периодической проверки знаний пользователей в области безопасности информации, в том числе с принятием зачетов;

– проведения мониторинга безопасности информации администратором безопасности с подготовкой проекта приказа о наказании виновных лиц;

– периодического контроля качества работы администратора безопасности.

Система мониторинга информационной безопасности также позволит осуществлять:

– анализ нагрузки ПЭВМ в режиме реального времени;

– определение объема работы за период;

– просмотр выполняемых программ в режиме удаленного доступа;

– оценку уровня подготовки пользователей при работе с электронными документами.

Литература

1. Об информации, информационных технологиях и о защите информации: Федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ. [Электронный ресурс]. URL:http//www.consultant.ru. (дата обращения: 27.01.2012).

2. О персональных данных: Федер. закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ. [Электронный ресурс]. URL: http//www.consultant.ru. (дата обращения:20.02.2012).

3. ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения. [Электронный ресурс]. URL:http//www.consultant.ru. (дата обращения: 15.02.2012).