УДК 004.056.53

# МЕТОДИКА ОБНАРУЖЕНИЯ НЕАВТОРИЗОВАННОГО ДОСТУПА В ИНФОРМАЦИОННУЮ СИСТЕМУ И ЗАЩИТЫ ЭЛЕКТРОННОЙ ПОЧТЫ ПРЕДПРИЯТИЯ

***Авилова Н. В., Газизов А. Р.***
Донской государственный технический университет, Ростов-на-Дону, Российская Федерация
av170556@rambler.ru
gazandre@yandex.ru

Рассматривается методика выявления фактов неавторизованного доступа в информационную систему предприятия, несанкционированного управления системой и защиты электронной почты предприятия.

**Ключевые слова:** информационная система предприятия, программно-аппаратное средство, система антивирусной защиты, система защиты электронной почты, система обнаружения вторжений, средства информационных и коммуникационных технологий.

UDC 004.056.53

# METHOD FOR UNAUTHORIZED ACCESS DETECTION TO INFORMATION SYSTEM AND ENTERPRISE E-MAIL PROTECTION

***Avilova N. V., Gazizov A. R.***
Don State Technical University, Rostov-on-Don, Russian Federation
av170556@rambler.ru
gazandre@yandex.ru

The article considers the method for unauthorized access detection to enterprise information system or the unauthorized use of the system, as well as company email protection.

**Keywords:** enterprise information system, software and hardware, virus protection system, e-mail protection system, intrusion detection system, means of information and communication technologies.

**Введение.** Под информационной системой (ИС) предприятия, функционирующей на базе средств информационных и коммуникационных технологий (ИКТ), к которым относятся программные, программно-аппаратные и технические средства и устройства, функционирующие на базе микропроцессорной, вычислительной техники, а также современных средств и систем транслирования информации, информационного обмена, обеспечивающие операции по сбору, продуцированию, накоплению, хранению, обработке, передаче информации и возможность доступа к информационным ресурсам локальных и глобальной компьютерных сетей, понимается система передачи и приема информации, состоящая из источника информации, передатчика, канала связи, приемника информации и источника помех [1,2].

**Постановка задачи.** В статье рассматривается методика выявления фактов неавторизованного доступа в информационную систему предприятия либо несанкционированного управления системой, а также защиты электронной почты предприятия.

**Основная часть.** Для выявления фактов неавторизованного доступа в ИС предприятия либо несанкционированного управления системой применяется специальное программно-аппаратное средство — система обнаружения вторжений (СОВ) [3,4].

СОВ разработаны позже систем антивирусной защиты (АВЗ). В связи с этим, на большинстве предприятий используются другие модули защиты ИС. В современных условиях очевидна необходимость формирования СОВ при построении защищенной ИС предприятия.

В отличие от межсетевых экранов, работающих на основе изначально установленных политик, СОВ проверяют подозрительную активность в ИС предприятия, позволяя выявить неавторизованный доступ, вторжение и сетевую атаку на ИС; а также предпринимают действия для предотвращения атаки.

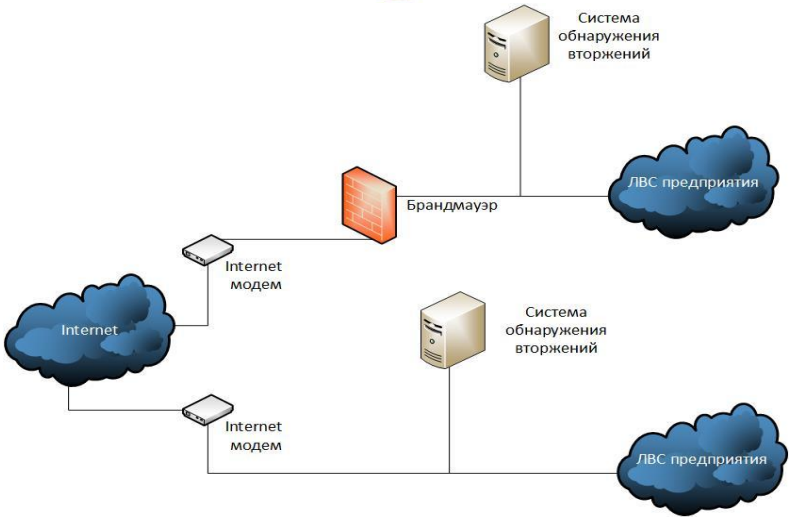


Рис. 1. Система обнаружения вторжений

СОВ является программно-аппаратным средством, которое позволяет делать прогнозы относительно будущих атак, а также определять уязвимость системы. Злоумышленник изначально сканирует ИС на наличие уязвимостей, соответственно СОВ не только выявляет попытку вторжения или сетевой атаки и позволяет документировать действия в ИС предприятия, а также блокировать источник атаки вне зависимости от ее характера [3,4].

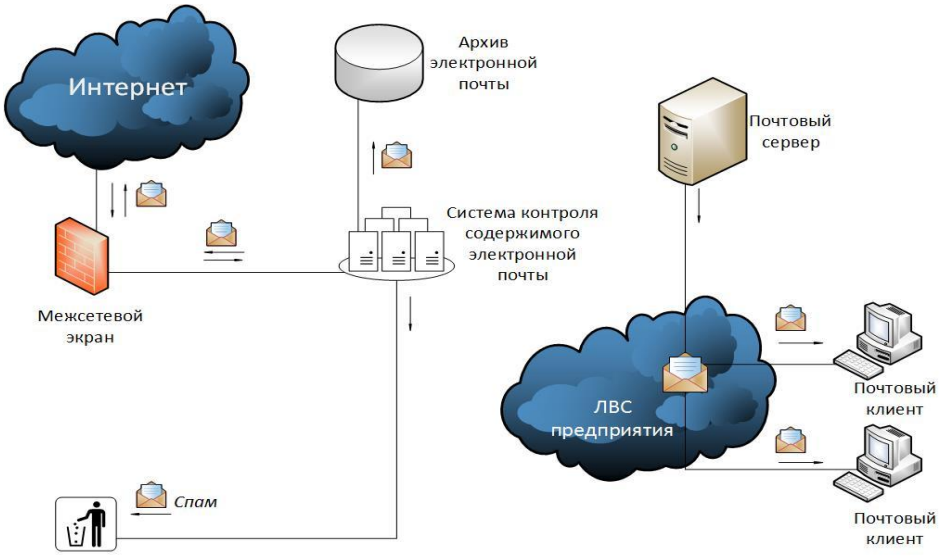


Рис. 2. Система защиты ЭП предприятия

На базе СОВ функционирует подсистема предотвращения вторжений (ПВ), являясь ее составной частью. Различие их состоит в том, СОВ является пассивной, так как она лишь осуществляет проверку сетевых пакетов, сличая сетевой трафик с установленными правилами и оповещая при выявлении атаки. Подсистема ПВ нейтрализует подозрительный сетевой пакет. При риске вторжения в ИС предприятия сетевое соединение отключается или блокирует доступ пользователя к информационным ресурсам предприятия.

Кроме этого, подсистема ПВ может перенастроить межсетевой экран или маршрутизатор для блокирования атаки на ИС предприятия. Применение СОВ и подсистемы ПВ не делает ИС предприятия совершенно безопасной. Структурная схема СОВ представлена на рисунке 1.

Подход к защите электронной почты (ЭП) на предприятии должен быть всесторонним и комплексным. Необходимо сочетать организационные меры с использованием соответствующих

технических средств.

Структурная схема системы защиты ЭП представлена на рисунке 2.

При построении системы защиты ЭП предприятия следует применять [3,4]:

1) Организационные методы защиты ЭП. К ним можно отнести внедрение на предприятии политики применения ЭП. Политика применения ЭП первична относительно программных средств ее защиты, так как является базисом для их формирования. Изначально формулируется политика, то есть регламент применения ЭП, а также выясняется реакция подсистемы защиты ЭП на определенные нарушения политики применения ЭП. После этого регламент применения ЭП переводится на язык программного средства, применяемого при контроле соблюдения требований политики применения ЭП.

Таким образом, политика применения ЭП — это регламент, определяющий порядок и правила применения ЭП всеми участниками информационного обмена на предприятии.

2) Программные методы защиты ЭП. К ним отнесем специализированное ПО, которое называется программной системой контроля содержимого ЭП. Функциями этого ПО являются:

– контроль трафика ЭП;
– формирование архива переписки по ЭП.

Система контроля содержимого ЭП должна отвечать следующим требованиям:

– функционал анализа текстов;
– функционал фильтрации передаваемых сообщений — относительно размера данных и их объема, количества вложений в сообщения, типа файлов, адреса ЭП;
– функционал мониторинга использования ресурсов ЭП, а также — разграничения доступа к этим ресурсам разных категорий пользователей ПЭВМ;
– функционал отложенной доставки сообщений ЭП согласно расписанию;
– функционал формирования архива ЭП.

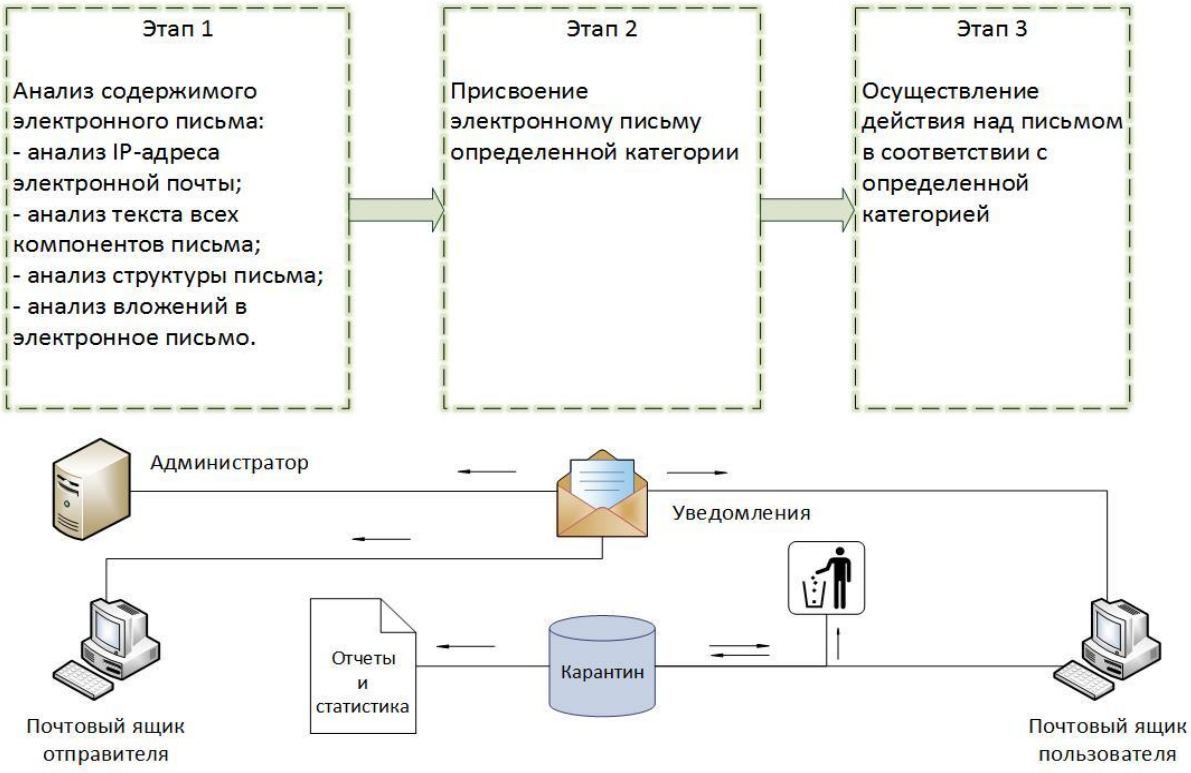


Рис. 3. Архитектура системы контроля содержимого ЭП

Функционирование системы защиты ЭП обеспечивается следующими программными механизмами [2,3]:

- механизм рекурсивной декомпозиции — специализированный алгоритм, используемый для разделения сообщений ЭП на сегменты и анализа содержания сегментов;
- механизм эвристического определения текстовых кодировок;
- механизм выяснения типа файлов согласно их сигнатуре;
- механизм полнотекстового поиска по архиву ЭП и пр.

Система защиты ЭП не решает задачи защиты информации на предприятии. Программная система контроля содержимого ЭП является инструментом реализации и соблюдения политики применения ЭП. Внедрение политики использования ЭП требует от руководства предприятия понимания, что наличие только документально оформленной политики не гарантирует ее выполнения.

Необходимо создание на предприятии соответствующих условий реализации данной политики. При этом важнейшим условием является наличие в сети программно-технических средств контроля выполнения положений и требований политики. К таким средствам относятся системы контроля содержимого ЭП.

Системы контроля содержимого ЭП — это ПО, способное анализировать содержание письма по различным компонентам и структуре в целях реализации политики использования ЭП. Архитектура системы контроля содержимого ЭП представлена на рисунке 3. Спектр возможностей всех категорий систем контроля содержимого ЭП достаточно широк и существенно меняется в зависимости от производителя. Однако ко всем системам предъявляются наиболее общие требования, которые позволяют решать задачи, связанные с контролем почтового трафика.

**Заключение.** Методика обнаружения неавторизованного доступа в информационную систему и защиты электронной почты предполагает возможность дальнейшего совершенствования систем ОВ и защиты ЭП предприятия, необходимо поэтапное формирование и внедрение обозначенных систем по модульному принципу, чтобы обеспечить техническую возможность их дальнейшей модернизации.

**Библиографический список**

1. Гафнер, В. В. Информационная безопасность: учеб. пособие / В. В. Гафнер. — Ростов на Дону : Феникс, 2010. — 324 с.

2. Роберт, И. В. Теория и методика информатизации образования / И. В. Роберт — Москва : ИИО РАО, 2010. — 356 с.

3. Роберт, И. В. Толковый словарь терминов понятийного аппарата информатизации образования / И. В. Роберт — Москва : ИИО РАО, 2009. — 96 с.

4. Челухин, В.А. Комплексное обеспечение информационной безопасности автоматизированных систем: учеб. пособие / В. А. Челухин — Комсомольск-на-Амуре : КНАГТУ, 2014. — 207 с.