ИНФОРМАТИКА

УДК 004.725.5

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В НАУЧНО-ОБРАЗОВАТЕЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ[1]

С.В. Исаев, А.В. Малышев*

В данной статье описываются наиболее часто встречаемые авторами на практике угрозы, приводящие к потере информации либо к отказам в функционировании сети. Все множество угроз информационной безопасности подразделяется на классы согласно международному стандарту OSI. Предлагаются комплексные решения и перспективы развития средств защиты.

В связи с бурным развитием Интернет-технологий и расширением круга пользователей, подключенных к сети Интернет, становятся все более актуальными задачи обеспечения информационной безопасности. Связанные с этим проблемы широко обсуждаются в литературе (например, [1],[2]), предлагается множество методов и решений для частных случаев. Несмотря на это, для комплексной защиты сети в каждом конкретном случае требуется вырабатывать адекватное техническое решение, учитывающее особенности организации сети, виды информации и прочие факторы.

Следует выделить особенности корпоративных сетей учебных и научных учреждений, которые существенны при построении системы безопасности:

- гетерогенность, т.е. функционирование в сети множества различных протоколов и сетевых операционных систем;
- распределенность – возможность осуществления входа пользователя в сеть и работы практически в любой ее точке;
- децентрализация – передача отдельных функций администрирования сети в периферийные подразделения;
- открытость информации – как правило, информация сети носит научно-образовательный характер и не является секретной;
- слабая защищенность рабочих мест – рабочие места в таких сетях обычно используются совместно несколькими сотрудниками или студентами, что затрудняет идентификацию конкретного пользователя.

Компьютерная сеть Красноярского научного центра СО РАН (КС КНЦ) в этом смысле – типичная научно-образовательная сеть, которая предназначена для предоставления доступа научных сотрудников, студентов и аспирантов к единому информационному пространству. От системы безопасности требуется обеспечение комфортной работы пользователей с минимизацией угроз, как внешних, так и внутренних. Следует отметить, что самая совершенная система безопасности, очень ограничивающая удобство работы конечного пользователя, будет либо игнорироваться, либо существенно снижать производительность работы.

Для удобства разделим все множество угроз информационной безопасности на несколько классов, согласующихся с уровнями широко известной модели организации взаимодействия открытых систем (OSI):

1. Угрозы физического уровня.
2. Угрозы канального уровня.
3. Угрозы сетевого уровня.
4. Угрозы прикладного уровня.

На **физическом** уровне сеть КНЦ представляет собой оптоволоконную кабельную систему с общей длиной линий связи более 4-х километров. Оптоволоконные линии как сами не излучают, так и не подвержены внешним электромагнитным излучениям, поэтому единственной угрозой является физическая поломка кабеля либо оконечного оборудования.

Для отслеживания этих неисправностей в сети КНЦ внедрена система автоматизированного мониторинга и оповещения. Она функционирует на нескольких серверах сети и при пропадании соединения выдает сообщения на электронную почту и мобильные телефоны администраторам сети. Дополнительно есть возможность получать информацию о текущем состоянии соединений и узлов сети через WAP-браузер мобильного телефона.

[1]Работа выполнена при финансовой поддержке гранта РФФИ № 05-07-90201-в.

*© С.В. Исаев, А.В. Малышев, Институт вычислительного моделирования СО РАН, 2006. E-mail: si@krasn.ru, amal@krasn.ru

Благодаря функционированию такой системы администратор своевременно оповещается о неисправностях и имеет возможность устранить их в минимально возможный срок. Кроме того, данная система может использоваться для накопления статистической информации по сбоям сети для дальнейшей обработки и анализа.

На **канальном** уровне наиболее часто встречающиеся проблемы связаны с неисправностями, неправильной настройкой либо умышленными воздействиями на уровне протокола передачи. Основным средством контроля и управления сетью являются управляемые коммутаторы, с помощью которых удается решать проблемы блокирования отдельных узлов сети по их физическому адресу, организации виртуальных сетей, фильтрации трафика и автоматической защиты от трафика ненормальной интенсивности.

На одном из Unix-серверов внутренней сети функционирует демон ArpWatch, собирающий информацию о физических адресах подключенных к сети узлов и уведомляющий администратора о новых подключениях. Новые узлы сети по заявкам администраторов институтов регистрируются в общей базе данных. Доступ во внешние сети возможен только после регистрации.

Благодаря имеющимся средствам администрации сети доступен список зарегистрированных пользователей, информация о новых подключениях в режиме реального времени, что позволяет оперативно локализовывать и разрешать возникающие проблемы.

На **сетевом** уровне сеть КНЦ обладает несколькими степенями защиты.

1. Статические сетевые фильтры на ключевых маршрутизаторах сети. Ограничивают сетевой трафик по отдельным адресам и группам адресов. Эффективны для разделения уровней доступа разных категорий пользователей. Настройка фильтров хорошо освещена в литературе [3] и не нуждается в дополнительных комментариях.
2. Физическое разделение внутренней и внешней сетей путем использования адресов интранет-диапазона и механизма трансляции адресов на граничном маршрутизаторе внутренней сети. Данный прием обеспечивает защиту внутренней сети от входящих внешних соединений. Каждое соединение может быть инициировано только из внутренней сети.
3. Поддерживается система учета Интернет-трафика, протоколирующая соединения компьютеров сети с внешней средой. Помимо предоставления информации о потребляемом трафике, данные этой системы позволяют производить анализ сетевой активности, принимать решения по управлению и планированию развития сети.
4. Система блокирования сканирующих хостов, основанная на динамически изменяемых параметрах сетевых фильтров.

Особый интерес представляет система блокирования сканирующих хостов. Ее необходимость обусловлена выявлением многочисленных атак на внешние узлы сети, связанных с подбором паролей и сканированием доступных портов. В настоящее время система ориентирована на предотвращение атак на популярный протокол SSH, по которому пользователям предоставляется возможность удаленного входа на компьютер по защищенному соединению.

Клиентская часть функционирует на граничных маршрутизаторах внутренней и внешней сетей, а управляющая программа – на отдельном Unix-сервере. Статистика соединений собирается на граничном маршрутизаторе Cisco по технологии NetFlow [4].

Система отслеживает попытки входа и авторизации и при обнаружении признаков попытки взлома блокирует входящий трафик с данного хоста на всех граничных маршрутизаторах. Периодически выполняется очистка списков блокированных хостов с тем, чтобы не повышать нагрузку на оборудование. Также списки очищаются при каждой перезагрузке хранящего их сервера/маршрутизатора. В среднем блокируется 5-7 сканирующих хостов в сутки.

В настоящее время на основе имеющихся систем предполагается создать централизованную интеллектуальную систему реагирования на несанкционированные действия (рис. 1). Рассмотрим основные функции этой системы:

1. Сбор данных реального времени о сетевом трафике (реализовано).
2. Регистрация пользователей и компьютеров сети (реализовано).
3. Составление сводных отчетов по трафику (реализовано).
4. Классификация пользователей и компьютеров сети по выполняемым задачам.
5. Наполнение базы знаний по признакам деструктивных воздействий.
6. Анализ трафика реального времени и реагирование согласно классификации и обнаруженным признакам (реализовано частично).

В настоящее время часть нереализованных функций системы (анализ трафика, блокирование хостов) выполняет администратор, но с наполнением базы знаний возможно большая часть действий будет выполнятся в автоматическом режиме, что позволит повысить оперативность реагирования.

На **прикладном** уровне наиболее уязвимыми сервисами сети являются электронная почта, DNS, встроенные сервисы операционных систем семейства Microsoft Windows. Следует сказать, что централизованно защитить узлы внутренней сети от пользователей внутренней же сети представляется невозможным. Поэтому в этом направлении наибольший эффект имеют превентивные действия, а именно:

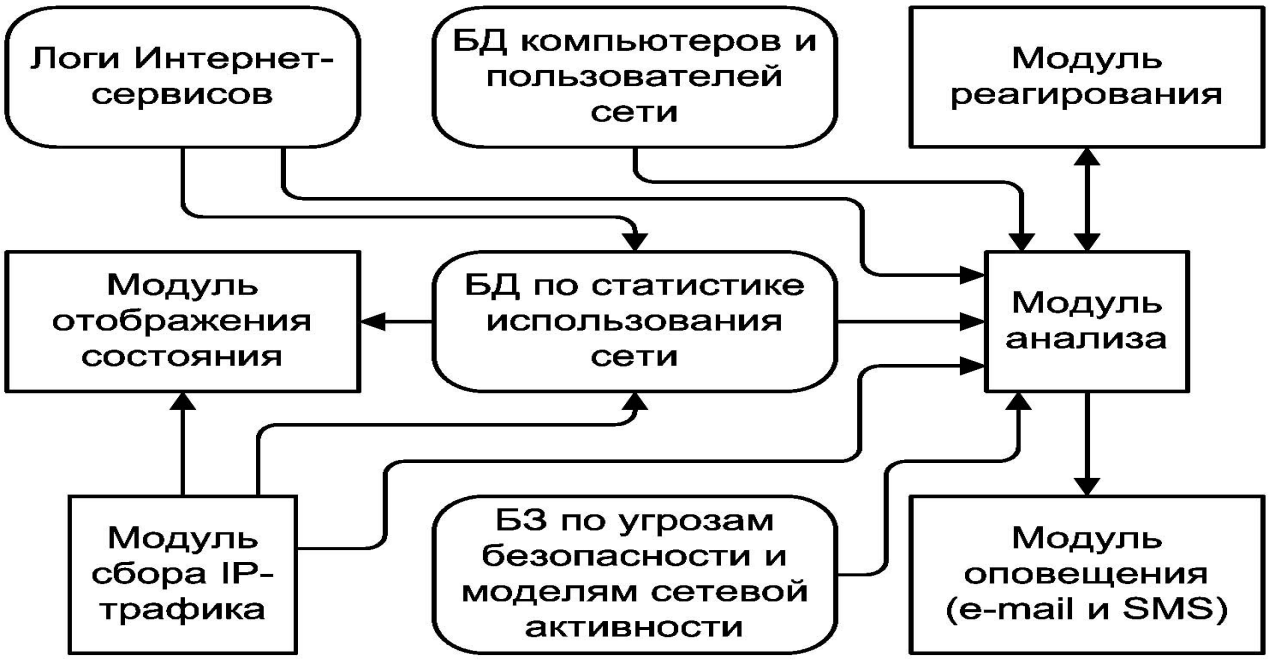

Рис. 1. Структурная схема системы комплексной защиты

- своевременная установка обновлений безопасности и информирование о новых угрозах;
- централизованное обновление антивирусных баз;
- отключение ненужных и потенциально проблемных служб ОС;
- мониторинг сетевой активности и своевременное отключение потенциально опасных узлов.

Наиболее актуальной проблемой для конечного пользователя остаются почтовые вирусы, черви и троянские программы, а также несанкционированные рассылки (спам). По статистике антивирусных компаний, более 95 % всех вредоносных программ, распространяющихся в глобальной сети, составляют сетевые черви, и 99 % из них являются почтовыми червями. По оценкам мировых аналитиков, спам приносит ежегодно около 100 млрд долларов, и в некоторые интервалы времени процент бесполезных писем занимает до 95 % от всей почтовой корреспонденции.

Несмотря на большое количество решений для индивидуальных пользователей, эффективно эту проблему можно решить только централизованно. Рассмотрим пример комплексной защиты сервиса электронной почты на корпоративном почтовом сервере КНЦ СО РАН.

Почтовый сервер ИВМ СО РАН поддерживает около 600 ящиков электронной почты пользователей Красноярского научного центра СО РАН. В настоящее время средняя доля спама среди входящих писем – около 47 %. Средняя доля вирусов среди входящих писем – около 5 %. Большинство писем с вирусами не содержат полезной информации и не принимаются сервером. Среднее ежедневное количество писем – 2400, из них около 1000 составляет спам и около 105 – письма с вирусами.

Система пометки спама и антивирусной проверки на сервере (рис. 2) включает в себя четыре уровня. При выполнении условия на любом уровне входящее письмо помечается как спам. Все проверки выполняются только для входящих соединений извне.

1. IP-уровень:
   - проверка IP-адреса отправителя на попадание в блэк-листы. Из множества таких листов отобраны для использования имеющие наиболее адекватную политику пополнения;
   - проверка обратного доменного имени хоста отправителя на соответствие характерным для источников спама шаблонам.
2. SMTP-уровень:
   - проверка приветствия HELO/EHLO, выдаваемое удаленным сервером. Если приветствие совпадает с одним из перечисленных в черном списке, либо совпадает с IP-адресом отправителя, либо не содержит точки (т.е. не является FQDN), то письмо признается спамом;
   - проверка на ожидание ответа после HELO/EHLO приветствия. Если отправитель не ожидает ответов от сервера согласно протоколу SMTP, письмо признается спамом;
   - проверка существования почтового домена из адреса отправителя.
3. HEADER-уровень. После приема письма и успешного прохождения проверок на вирусы письмо проверяется на совпадение заголовков письма с заданными регулярными выражениями образцами.

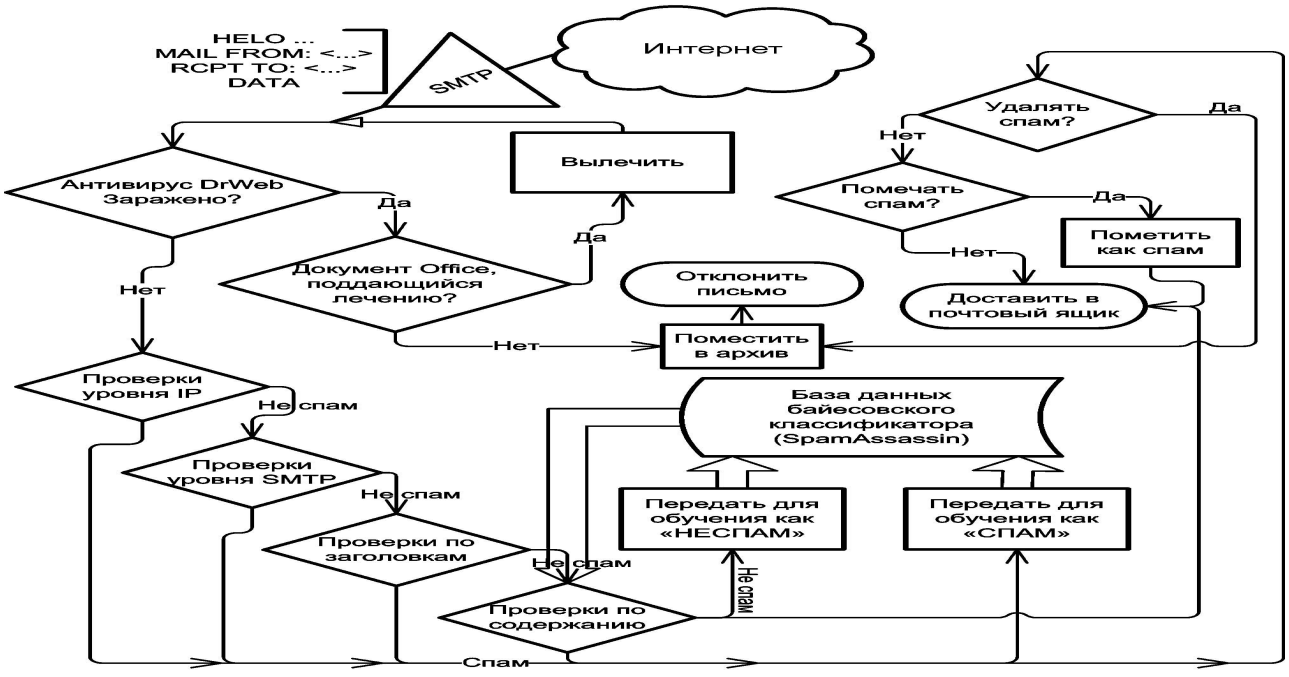

Рис. 2. Система пометки спама и антивирусной проверки

4. CONTENT-уровень. Последняя проверка выполняется средствами статистического классификатора SpamAssassin, точнее, его демоном spamd. Если рейтинг SpamAssassin превышает значение «5», письмо признается спамом.

Все принятые письма, признанные спамом по любому правилу, помечаются (для тех пользователей, которые заказали себе такую пометку). В заголовок добавляется тэг «X-SpamMarkReason:», содержащий причину пометки (правило в том или ином виде), а в поле «Subject:» перед прежним содержимым вставляется строка «***SPAM***». Это позволяет пользователю принимать решение относительно таких писем самостоятельно, пользуясь возможностями своего почтового клиента: откладывать в отдельную папку, удалять, читать и т.д.

Одно из важнейших свойств системы – это обучаемость её 4-го уровня. Письма, признанные спамом по любому критерию, подаются классификатору для обучения, что существенно повышает эффективность его работы. Во избежание «перекоса» в обучении входящая почта, для которой все проверки прошли успешно, также предъявляется для обучения классификатору.

Благодаря такой системе защиты пользователи корпоративного почтового сервера КНЦ СО РАН ограждены от получения вредоносных программ и траты времени на просмотр массовых рассылок. Следует отметить, что регулярно имеют место и ложные срабатывания обоих видов – помеченный неспам либо непомеченный спам, однако доля таких писем среди корректно помеченных невелика. По каждому случаю ложной пометки выполняются подстройки системы – переобучение классификатора и (если нужно) корректировка «белых списков» для соответствующих случаю правил пометки.

Описанные проблемы и средства их разрешения выявлены из опыта более чем пятилетней работы сотрудников отдела средств телекоммуникаций и вычислительной техники ИВМ СО РАН. Следует отметить, что прогресс в данной области ведет к постоянному возникновению и обнаружению новых угроз и вынуждает к совершенствованию средств защиты. Поэтому даже в перспективе едва ли можно говорить о завершенности вышеописанных работ, структур и систем, но поддержание значения вероятности реализации какой-либо из известных угроз информационной безопасности сети на приемлемо низком уровне вполне реально.

Список литературы

[1] Соколов А. *Защита информации в распределенных корпоративных сетях и системах*/ А. Соколов, В. Шаньгин. – М.: ДМК Пресс, 2002. – 656 с.

[2] Галицкий А. *Защита информации в сети - анализ технологий и синтез решений*/ А. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. – М.: ДМК Пресс, 2004. – 615 с.

[3] Польман Н. *Архитектура брандмауэров для сетей предприятия*/ Н. Польман, Т. Кразерс. – М.: Вильямс, 2003. – 432 с.

[4] Уэнстром М. *Организация защиты сетей Cisco*/ М. Уэнстром. – М.: Вильямс, 2003. – 768 с.

PROBLEMS OF ALL-ROUND PROTECTION IN COMPUTER NETWORKS OF SCIENCE AND HIGHER EDUCATION

S.V. Isaev, A.V. Malyshev

In this article authors describe frequently occurring security threats causing a data loss or network faults. The variety of security threats is divided into some classes according to the Open System Interconnection (OSI) model. End-to-end solutions and trends overview of security facilities development are proposed.