УДК 004.056.53

ОБ АЛГОРИТМЕ ПОСТРОЕНИЯ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ ВОДНОГО ТРАНСПОРТА

***А. Р. Газизов*[1], *Е. Р. Газизов*[2]**
[1]Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация
[2]Казанский (Приволжский) федеральный университет, г. Казань, Российская Федерация
gazandre@yandex.ru
gazizov.e @ bk.ru

Рассмотрен алгоритм построения системы антивирусной защиты локальной вычислительной сети предприятия водного транспорта — правовые, организационные и программно-технические мероприятия с целью обеспечения защиты сети от компьютерных вирусов; функции и составляющие системы антивирусной защиты, а также — этапы её построения.

Ключевые слова: компьютерные вирусы; локальная вычислительная сеть; правовые, организационные и программно-технические мероприятия; система антивирусной защиты; средства информационных и коммуникационных технологий; предприятие водного транспорта; этапы.

UDC 004.056.53

ON THE ALGORITHM OF CONSTRUCTING A SYSTEM OF ANTI-VIRUS PROTECTION OF A LOCAL AREA NETWORK OF WATER TRANSPORT COMPANIES

***A. R. Gazizov*[1], *E. R. Gazizov* [2]**
[1]Don State Technical University, Rostov-on-Don, Russian Federation
[2]Kazan (Volga region) Federal University, Kazan, Russian Federation

gazandre@yandex.ru
gazizov.e @ bk.ru

The article considers the algorithm of construction of the system of anti-virus protection of a local computer network of water transport companies – legal, organizational and program-technical measures to ensure protection of a network from computer viruses; the functions and components of anti-virus protection, as well as the stages of its construction.

Keywords: computer viruses; local area network; legal, organizational and program-technical measures; virus protection system; means of information and communication technologies; water transport companies; stages.

Введение. В условиях информатизации общества, применение средств информационных и коммуникационных технологий (ИКТ), к которым следует отнести [1,2] 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; становится все более актуальным в процессах автоматизации информационной деятельности и организационного управления процессами документооборота на предприятиях водного транспорта.

Теоретическая часть. Под водным транспортом необходимо понимать вид транспортных средств, перевозящих грузы и пассажиров по водным путям сообщения, как естественным — океанам, морям, рекам и озерам, так и искусственным — каналам, водохранилищам и водоёмам. Основным транспортным средством является судно.

По типу используемых акваторий водный транспорт подразделяется на речной и морской. Морские суда должны обладать мореходностью, т. е. способностью не разрушаться и не тонуть

при волнении; при этом — морские суда крупнее речных. Перевозки по озёрам обычно относят к речному транспорту; за исключением самых крупных озёр (например — Каспийское море).

Для погрузки и выгрузки грузов служат особые предприятия — морские и речные порты; для пассажиров сооружают морские и речные вокзалы.

Основная часть. Средства ИКТ, применяемые на предприятии водного транспорта, включают: локальные вычислительные сети (ЛВС) предприятия; современные средства связи, обеспечивающие информационное взаимодействие пользователей как на локальном уровне (например, в рамках одного или нескольких предприятий), так и глобальном (в рамках всемирной информационной сети Интернет). При этом — средства ИКТ обеспечивают коммуникаций на основе использования локальных и глобальных ЛВС; обрабатывают информацию при ведении делопроизводства; обеспечивают автоматизацию принятия управленческих решений посредством средств искусственного интеллекта [3].

Применение средств ИКТ позволяет автоматизировать процессы информационно-методического обеспечения производственного процесса и организационного управления предприятием водного транспорта. Вместе с тем, присутствует один существенный недостаток: наличие ЛВС и телекоммуникационных сетей, обеспечивающих информационное взаимодействие пользователей, предопределяет наличие потенциальной возможности заражения компьютерными вирусами (КВ).

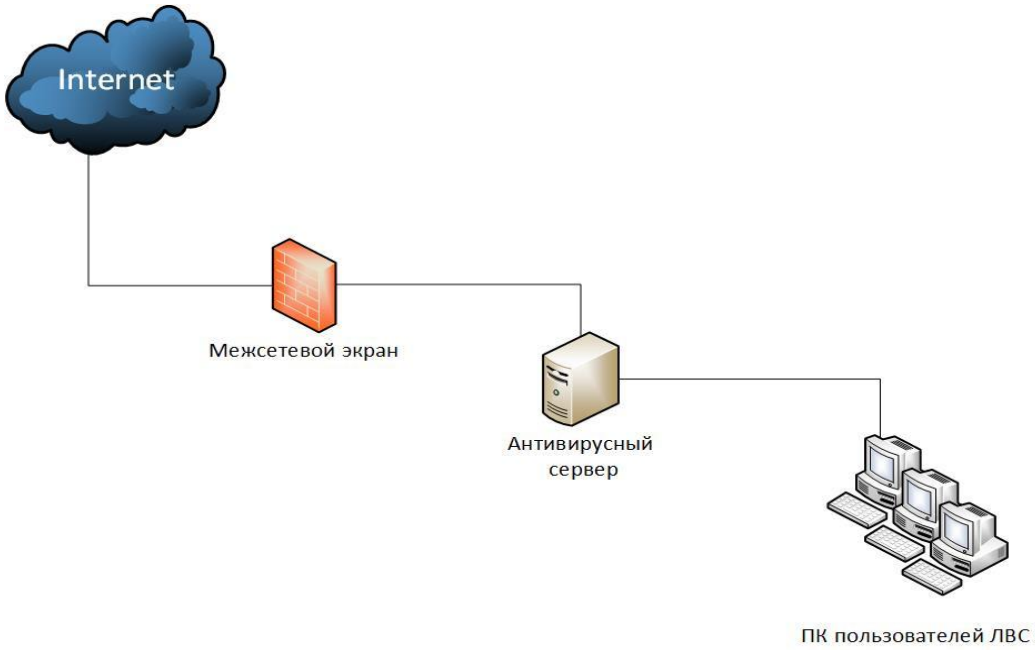

Рисунок 1 – Система антивирусной защиты ЛВС предприятия водного транспорта

Работоспособность ЛВС предприятия водного транспорта значительно зависит от степени ее противостояния угрозам заражения КВ. При этом — применение для целей информационного обмена каналов внешних вычислительных сетей, в том числе — глобальной сети Интернет, предполагает срочную и эффективную защиту от КВ. Наилучшим образом она может быть решена путем создания в составе ЛВС предприятия системы антивирусной защиты (АВЗ), представленной на рисунке 1; надежность системы АВЗ будет определяться не только технологией, реализованной в антивирусном программном обеспечении (ПО), а также — организационными мероприятиями, определяющими эффективное его применение.

Защита ЛВС предприятия водного транспорта от КВ предполагает постоянный и непрерывный контроль состояния системы АВЗ. Данную задачу способны решить пакеты

антивирусного ПО; присутствие этих пакетов во всех сегментах ЛВС является необходимым, но недостаточным условием противостояния угрозам заражения КВ. Причина — нерегулярное обновление пакетов антивирусного ПО ведет к «устареванию» системы АВЗ, что равносильно ее отсутствию в отдельные временные промежутки. При этом — система АВЗ выполняет следующие контрольные функции:

а) контроль обновления пакетов антивирусного ПО на серверах и ПЭВМ;

б) контроль включенности программы «монитор» пакетов антивирусного ПО на серверах и ПЭВМ;

в) контроль безошибочности настройки пакетов антивирусного ПО, а также — выполнение пользователями ПЭВМ регламента их применения;

г) контроль сроков действий лицензий пакетов антивирусного ПО;

д) контроль функционирования пакетов антивирусного ПО на серверах и ПЭВМ дистанционно с автоматизированного рабочего места (АРМ) администратора системы АВЗ;

е) контроль резервного копирования «критичной» информации;

ж) контроль проверочных мероприятий внешних носителей информации в подразделениях;

з) контроль функционирования системы АВЗ на серверах и ПЭВМ в подразделениях.

Вслед за Роберт И.В., под персональной электронно-вычислительной машиной (ПЭВМ) будем понимать ЭВМ, которую может эксплуатировать непрофессиональный пользователь без помощи профессионального программиста [2,3]. ПЭВМ характеризуется: развитым человеко-машинным интерфейсом, обеспечивающим простоту управления; малогабаритными носителями информации; малыми габаритами и массами; малым энергопотреблением; большим количеством прикладных программ для многих областей применения. Таким образом, ПЭВМ — персональные компьютеры (ПК).

Функционирование системы АВЗ предприятия водного транспорта предполагает комплексное противодействие угрозам заражения КВ. Это предусматривает согласованное проведение правовых, организационных, а также программно-технических мероприятий с целью обеспечения защиты от КВ:

1) Обнаружение и локализацию уязвимостей, где существуют угрозы заражения КВ; это даст возможность ликвидировать основания вероятного прохождения вирусных атак.

2) Обнаружение и локализацию атак КВ в положенное время.

3) Обнаружение и локализацию последствий угроз КВ; это обеспечит минимальный ущерб при реализации угроз заражения КВ.

При этом реализация данных мероприятий на предприятии водного транспорта возможна при наличии:

1) Нормативно-методического обеспечения системы АВЗ. Это предусматривает формирование внутреннего регламента эксплуатации системы АВЗ, как составной части «политики» информационной безопасности (ИБ) предприятия.

2) Кадрового обеспечения системы АВЗ. Это предусматривает обучение работников предприятия по образовательной программе повышения квалификации, направленной на формирование компетентности относительно эксплуатации системы АВЗ.

3) Программно-аппаратного обеспечения системы АВЗ. Это предусматривает наличие в составе системы АВЗ комплекса программно-аппаратных средств:

а) Средства выявления КВ — базовая составляющая системы АВЗ; они обнаруживают различные КВ на уровнях ПЭВМ, серверов и сетевых шлюзов. С целью выявления КВ применяются сигнатурные и эвристические методы. При выявлении КВ оповещаются

пользователи ПЭВМ, а также работники предприятия, отвечающие за защиту информации; при этом происходит также удаление выявленных КВ из зараженных файлов. С целью обеспечения эффективности защиты от КВ, средства их выявления должны создаваться на антивирусных ядрах разных изготовителей, что позволит проверять файлы или электронную почту разными средствами; а также обеспечит высокую надежность работы всей системы АВЗ за счет возможности дублирования функционала сканирующих ядер.

б) Средства определения уязвимостей обеспечивают возможность нахождения технологических, а также эксплуатационных уязвимостей ЛВС предприятия при помощи сетевого сканирования: ПЭВМ, серверного оборудования и средств коммуникации. С этой целью применяются активные и пассивные методы сбора информации. После этого формируется информационное сообщение об обнаруженных уязвимостях, а также методах их устранения.

в) Средства защиты от спама блокируют почтовые сообщения рекламного характера. При этом входящие почтовые сообщения из глобальной вычислительной сети Интернет изначально проходят через контекстный фильтр, а лишь затем попадают на почтовый сервер предприятия.

г) Средства управления системой АВЗ решают следующие вопросы: удаленная установка и удаление антивирусного ПО на серверах и ПЭВМ; удаленное управление комплексом программно-аппаратных средств; подсистем ЛВС предприятия с целью обеспечения автоматизации информационной деятельности, а также оперативности принятия решений по защите от КВ; сбор и анализ информационных потоков, поступающих из других сетей.

Этапы построения системы антивирусной защиты ЛВС предприятия водного транспорта включают:

1) Аудит информационной безопасности системы.
2) Обучение персонала.
3) Пусконаладочные работы.
4) Разработка проекта системы.
5) Техническое сопровождение системы.
6) Формирование требований к системе.

Заключение. Эксплуатация системы антивирусной защиты ЛВС предприятия водного транспорта предполагает ее модернизацию; при этом необходимо поэтапное создание и внедрение взаимосвязанных модулей (функциональных подсистем), обеспечивающих защиту от КВ. Модульный принцип построения сделает систему более гибкой, а также позволит заменить или модернизировать каждую функциональную подсистему, не затрагивая остальные её модули.

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 (психолого-педагогические и технологические аспекты) /И. В. Роберт — Москва : Изд-во Института информатизации образования Российской академии образования, 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.