ФОРМИРОВАНИЕ ЭФФЕКТИВНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЦИФРОВОМ ОБРАЗОВАТЕЛЬНОМ ПРОСТРАНСТВЕ

© Э. Д. Алисултанова, Д. С. Бицалов

ГГНТУ им. акад. М. Д. Миллионщикова, г. Грозный, Россия

Данная статья направлена на формирование эффективной системы защиты информации. В настоящее время ввиду совершенствования информационных технологий все более актуальной становится проблема защиты информации, так как вместе с улучшением методов защиты информации, к сожалению, развиваются и методы утечки информации. В данной статье рассмотрена одна из актуальных систем защиты информации, система ViPNet Client.

Программный комплекс ViPNet Client предназначен для защиты рабочих мест корпоративных пользователей. ViPNet Client надежно защищает от внешних и внутренних сетевых атак за счет фильтрации трафика. Кроме того, ПК ViPNet Client обеспечивает защищенную работу с корпоративными данными через зашифрованный канал, в том числе для удаленных пользователей.

Ключевые слова: интерфейс, ViPNet Client for Windows, пользователь, ключи шифрования, защита информации.

Целью исследования является формирование эффективной системы защиты информации.

Задачами исследования являются:

- изучение литературы систем защиты информации и выбор более подходящей системы защиты информации;
- анализ работы выбранной системы защиты информации;
- определение недостатков выбранной системы защиты информации;
- разработка программного обеспечения для устранения недостатков.

Характеристика комплекса задач, задачи и обоснование необходимости совершенствования системы обеспечения информационной безопасности

Изучив различные системы защиты информации, выбрали систему ViPNet Client.

Программный комплекс ViPNet Client предназначен для защиты рабочих мест корпоративных пользователей. ViPNet Client надежно защищает от внешних и вну-

тренних сетевых атак за счет фильтрации трафика. Кроме того, ПК ViPNet Client обеспечивает защищенную работу с корпоративными данными через зашифрованный канал, в том числе для удаленных пользователей. ViPNet Client поддерживает работу на компьютерных устройствах под управлением ОС Linux OS X и Microsoft Windows (рис. 1) [1].

Работа в корпоративной сети защищенной от внутреннего нарушителя. Соединение с ресурсами, сервисами а также другими пользователями осуществляется через каналы, функционирующие по принципу «точка-точка». Это позволяет надежно защитить информацию от других пользователей, в том числе внутри корпоративной сети.

Безопасная работа удаленного пользователя с корпоративными ресурсами и сервисами через защищенные каналы. Шифрование трафика защитит работу с внутренними ресурсами и сервисами вашей организации при передаче данных через Интернет.

Защищенное общение пользователей. Обеспечить защиту корпоративных пользователей также позволит совместное использова-

Рис. 1. Интерфейс ViPNet Client

ние ПК ViPNet Client с приложениями ViPNet Connect и ViPNet Деловая почта (данная возможность поддерживается определенными модификациями ViPNet Client).

Кроме того, ViPNet Client поддерживает защищенные каналы для корпоративных коммуникаций на основе сторонних решений, в

том числе IP-телефонии, видео-конференц-связи и так далее.

Защита виртуальной машины. ViPNet Client может работать на виртуальных машинах также допускается использование средств защиты ViPNet в VDI-средах.

Преимущества:

Высокая производительность шифрования и фильтрации трафика позволяет в реальном времени осуществлять защиту трафика служб голосовой и видеосвязи в сетях TCP/IP, а также обеспечивать одновременную работу с ресурсами разных сегментов корпоративной сети.

Равный доступ к ресурсам корпоративных информационных систем независимо от места и способа подключения пользователя к телекоммуникационной сети (при использовании решения ViPNet Network Security).

Защита канала не влияет на работу сторонних приложений на компьютере пользователя.

Ключи шифрования, политики безопасности и обновления ПО ViPNet доставляются

Рис. 2. Режимы работы ViPNet

Рис. 3. Схема подключения к компьютеру в локальной сети

на компьютер через надежный защищенный канал.

Система ViPNet использует 5 различных режимов работы (рис. 2):

Блокировать IP-пакеты всех соединений;

Блокировать все соединения, кроме разрешенных;

Пропускать все исходящие соединения, кроме запрещенных;

Пропускать все соединения;

Пропускать IP-пакеты без обработки [2].

При установке первого режима работы компьютер заблокирован абсолютно полностью от всех ПК, находящихся в сети и вне.

Второй режим позволяет подключаться компьютерам, которые изначально прописаны в списке разрешенных подключений.

Третий режим работает противоположно второму. Он допускает все подключения кроме тех, которые находятся в списке запрещенных подключений.

Четвертый режим работы пропускает все соединения, которые удовлетворяют настройкам фильтрации, заданной организацией.

При работе пятого режима проходят абсолютно все соединения.

Для более надежной защиты информации в приоритете используется именно второй ре-

жим работы. Чуть реже используются первый и третий режимы. И практически никогда не используются четвертый и пятый режимы, в целях защиты какой-либо информации.

Практика показывает, что пользователям необходимо подключаться удаленно к компьютерам, на которых установлена система ViPNet, но при определенных режимах работы системы безопасности это сделать невозможно. При этом пользователю не показывается каких-либо ошибок или предупреждений, что является большим недостатком, так как на выяснение причины отсутствия соединения компьютеров может уходить много времени. Попытка подключения изображена (на данной схеме рис. 3).

Было принято решение разработать улучшение для данной системы. Это улучшение представляет собой дополнительную программу, которая будет отслеживать входящие подключения к персональному компьютеру пользователя, и если это подключение будет из списка разрешенных тогда пользователю будет сообщаться о попытке подключения, после чего он может одобрить это подключение. В случае если подключение отсутствует в списке разрешенных, тогда это подключение игнорируется.

Рис. 4. Обновленная схема подключения к компьютеру в локальной сети

Данная программа будет выполнять следующие задачи:

упрощение работы пользователя с системой «ViPNet»;

сокращение рабочего времени на подключение по сети.

При наличии дополнительной программы схема подключения к ПК будет выглядеть следующим образом (рис. 4).

Комплекс программно-аппаратных средств обеспечения информационной безопасности и защиты информации предприятия

Программа реализована на языке python с помощью PyQt5 и SQLite.

Python является высокоуровневым языком программирования общего назначения. Он направлен на более комфортную работу разработчика, за счет чего повышается производительность его работы, и на читаемость кода. Синтаксис его ядра минималистичен, однако стандартная библиотека Python включает в себя множество полезных функций.

PyQt5 – это набор различных Python библиотек, с помощью которых создается графический интерфейс на базе платформы Qt5 от компании Digia.

PyQt5 доступен для Python 2 и Python 3.

Библиотека Qt является одной из самых мощных библиотек GUI (графического интерфейса пользователя).

PyQt5 реализован в виде набора python-модулей. Эта библиотека имеет более 620 классов и 6000 функций и методов.

Это мультиплатформенная библиотека. Работает она на всех основных операционных системах, в том числе Unix, Windows и Mac OS.

SQLite – это небольшая встраиваемая СУБД (система управления базами данных). Как известно, в своем развитии SQL устремился в разные стороны. Крупные производители начали дополнять разными расширениями. И хотя принимаются разные стандарты (SQL 92), в реальной жизни все крупные БД не поддерживают стандартов полностью и имеют что-то свое. Так вот, SQLite старается жить по принципу «минимальный, но полный набор». Она

вводит некие свои особенности, которые очень удобны, но не стандартны [3].

Программа напрямую работает с сетью. Реализовать это помогает модуль «socket». С помощью этого модуля программа будет принимать IP-адреса компьютеров, которые хотят подключиться к данному ПК. За счет SQLite в программе будут храниться все IP-адреса, которые входят в сеть. При получении IP-адреса, который хочет подключиться, начинается сверка адреса с уже существующими в базе данных. В случае наличия данного адреса в базе пользователь получает сообщение о попытке подключения к его компьютеру, и за ним остается право выбора – разрешить подключение или нет. Если же при сверке адресов программа не найдет его в своей базе, тогда данное подключение игнорируется, так как изначально оно запрещено.

При получении оповещения о попытке подключения пользователь вправе открыть компьютер в сети для удачного подключения. Если же с этим возникают трудности, пользователь может воспользоваться инструкцией, которую можно будет открыть в данном оповещении.

Средство криптографической защиты информации ViPNet Client выполняет функции VPN-клиента в сети ViPNet и обеспечивает защиту компьютера от несанкционированного доступа при работе в локальных или глобальных сетях. Программное обеспечение ViPNet Client может быть установлено для защиты трафика на любом компьютере с ОС Windows, будь то стационарный, удаленный, мобильный компьютер или сервер.

Системные требования

Процессор – Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.

Объем оперативной памяти – не менее 512 Мбайт (рекомендуется 1 Гбайт).

Свободное место на жестком диске – не менее 150 Мбайт (рекомендуется 250 Мбайт).

Сетевой адаптер или модем.

Операционная система – Windows XP SP3 (32-бит), Server 2003 (32-бит), Vista SP2 (32/64-бит), Server 2008 (32/64-бит), Windows 7 (32/64-бит), Server 2008 R2 (64-бит).

При использовании более ранних версий Windows, чем Windows 8, на компьютере должен быть установлен накопительный пакет обновления часовых поясов KB2570791.

Для операционной системы должен быть установлен последний пакет обновлений.

При использовании Internet Explorer – версия 6.0 или выше.

Ограничения

На компьютере не должно быть установлено никаких программ КриптоПро.

На компьютере должно быть установлено точное время.

Ядром программного обеспечения ViPNet является ViPNet-драйвер, основной функцией которого является фильтрация, шифрование и расшифрование входящих и исходящих IP-пакетов.

Каждый исходящий пакет обрабатывается ViPNet-драйвером одним из следующих способов:

- шифруется и отправляется;
- отправляется в исходном виде (без шифрования);
- блокируется (в соответствии с установленными сетевыми фильтрами).

Каждый входящий пакет обрабатывается следующим образом:

- пропускается (если он не зашифрован и это разрешено сетевыми фильтрами для нешифрованного трафика);
- расшифровывается (если пакет был зашифрован);
- блокируется (в соответствии с установленными сетевыми фильтрами).

ViPNet-драйвер работает между канальным уровнем и сетевым уровнем модели OSI, что позволяет осуществлять обработку IP-пакетов до того, как они будут обработаны стеком протоколов TCP/IP и переданы на прикладной уровень. Таким образом, ViPNet-драйвер защищает IP-трафик всех приложений, не нарушая привычный порядок работы пользователей.

Если для управления сетью ViPNet используется программа ViPNet Network Manager версии ниже 4.3 или ПО ViPNet Administrator версии ниже 4.4.1, то при первом запуске программы ViPNet Монитор стандартный сетевой экран Windows будет автоматически отключен. При использовании более поздних версий со-

стоянием сетевого экрана Windows управляет администратор сети ViPNet, поэтому при первом запуске программы ViPNet Монитор сетевой экран Windows будет включен или отключен в зависимости от настроек, заданных администратором сети ViPNet.

При добавлении установочных пакетов ViPNet Client и ViPNet CSP разной разрядности для каждого пакета на вкладке Общие в поле Название рекомендуется изменить заданное по умолчанию имя приложения, указав разрядность.

Обновление групповых политик на компьютерах пользователей может происходить не сразу, если на контроллере домена задан большой интервал времени для обновления политик. В этом случае вы можете инициировать немедленное обновление групповых политик, для этого в командной строке ОС Windows выполните команду `gpupdate`, а затем перезагрузите компьютеры пользователей.

На компьютерах пользователей установка ПО ViPNet Client будет выполняться в невидимом для пользователя режиме во время загрузки операционной системы. После установки программного обеспечения ViPNet Client и загрузки ОС на каждом сетевом узле появится сообщение с предложением установить дистрибутив ключей ViPNet.

Описание разработки программного обеспечения

Первый шаг в разработке данной программы – создать окно, в котором будут находиться кнопки и оповещение.

Для создания окна оповещения необходимо было задать размеры этого окна и указать его расположение на экране. Метод `setGeometry ()` делает две вещи: помещает окно на экран и устанавливает его размер. Первые два параметра `x` и `y` – это позиция окна. Третий – ширина, и четвертый – высота окна. На самом деле он сочетает в себе методы `resize ()` и `move ()` в одном методе. После этого я задаю название окна оповещения с помощью метода `setWindow Title ()`. Метод `show ()` отображает виджет на экране. Виджет сначала создается в памяти, и только потом (с помощью метода `show`) показывается на экране (рис. 5).


```

1      self.setGeometry(300, 300, 500, 200)
2      self.setWindowTitle('К вашему ПК хотят подключиться!')
3      self.show()
4
5
6  if __name__ == '__main__':
7
8      app = QApplication(sys.argv)
9      ex = Example()
10     sys.exit(app.exec_())
11

```

Рис. 5. Создание окна оповещения

```

16     def initUI(self, address):
17         lbl = QLabel('Пользователь' + str(address) + ' хочет подключиться к вашему ПК', self)
18         lbl.move(30, 50)
19

```

Рис. 6. Создание сообщения

```

19
20     qbtn1 = QPushButton('Ok', self)
21     qbtn1.clicked.connect(QCoreApplication.instance().quit)
22     qbtn1.resize(qbtn1.sizeHint())
23     qbtn1.move(100, 150)
24

```

Рис. 7. Создание кнопки

После создания самого окна я задаю сообщение, которое будет находиться в данном окне. В этом помогает метод `QLabel()`. Далее с помощью метода `move()` выбираю расположение сообщения в окне по координатам *x* и *y* (рис. 6).

Следующим пунктом является создание кнопок. Кнопка является экземпляром класса `QPushButton`. Первый параметр конструктора – название кнопки. Вторым параметром является родительский виджет. Родительский виджет является виджетом `Example`, который наследуется от `QWidget`.

Система обработки событий в `PyQt5` построена на механизме сигналов и слотов. Если мы нажмем на кнопку, вызовется сигнал “нажатие”. Слот может быть слот `Qt` или любая `Python` функция.

`QCoreApplication` содержит главный цикл обработки; он обрабатывает и диспетчеризирует все события. Метод `instance()` дает нам его текущий экземпляр.

Обратите внимание, что `QCoreApplication` создается с `QApplication`. Сигнал “нажатие” подключен к методу `quit()`, который завершает приложение. Коммуникация осуществляется между двумя объектами: отправителя и приемника. Отправитель – кнопка, приемник – объект приложения (рис. 7).

Данная программа работает с сетью с помощью модуля `socket`. Для работы с сокетами нужно импортировать сам модуль, после чего создать сокет (рис. 8).

```

7     import socket
8
9     sock = socket.socket()
10

```

Рис. 8. Создание сокета

Благодаря этому сокету теперь можно принимать соединения с помощью функции `accept`. Она ждет появление входящего соеди-

нения и возвращает связанный с ним сокет и адрес подключившегося. Адрес – массив, состоящий из IP-адреса и порта (рис. 9).

```
conn, addr = sock.accept()
```

Рис. 9. Отслеживание соединений

Данная программа имеет свою неповторимую базу данных, в которой будут храниться IP-адреса всех компьютеров, находящихся в сети. Для чего это нужно? Все просто, после того, как программа отследит IP-адрес подключаемого компьютера, она начинает искать этот адрес в своей базе. Пользователь, к которому идет подключение, получает оповещение только в том случае, если данный IP-адрес присутствует в базе данных. В противном случае подключение будет игнорироваться. Так

как изначально подключения блокируются, нет никакого смысла принудительно отвергать сторонние подключения.

Подключается данная база данных при помощи СУБД SQLite (рис. 10).

Здесь с помощью команды PRAGMA table_info (Addresses) я получаю информацию о своей таблице Addresses.

Интерфейс данной программы прост и понятен каждому. При попытке подключения пользователь увидит окно с сообщением о данном подключении и адрес подключаемого компьютера. Окно имеет две кнопки «Ок» и «Инструкция». Если пользователь достаточно опытен, он нажимает кнопку «Ок» (после чего сообщение закрывается) и дает доступ для данного компьютера. Если пользователь не знает, как дать доступ, он нажимает кнопку «Инструкция», после чего открывается пошаговая инструкция открытия доступа для данного компьютера. Инструкция довольно проста и

```
7 import sqlite3 as lite
8 import sys
9
10 con = lite.connect('test.db')
11
12 with con:
13     cur = con.cursor()
14     cur.execute('PRAGMA table_info(Addresses)')
15     data = cur.fetchall()
16
```

Рис. 10. Работа с БД

Рис. 11. Интерфейс программы на ОС Windows

Рис. 12. Интерфейс программы на ОС Linux

каждое действие расписано максимально подробно. При тестировании данной инструкции я сделал вывод, что с ней справится любой пользователь.

Данная программа может работать на различных версиях Windows, такие как:

- Microsoft Windows XP;
- Microsoft Windows Vista;
- Microsoft Windows 7;
- Microsoft Windows 10.

Также есть возможность работать с этой программой на Linux и OS X (рис. 11, 12).

ЛИТЕРАТУРА

1. Кабакова Н. В. Система защиты информации ViPNet. М.: ДМК Пресс, 2014. 392 с.
2. Баранова Е. К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. 2009. № 1 (49). С. 15-26.
3. Баранова Е. К. Методики анализа и оценки рисков информационной безопасности. Моделирование и анализ безопасности и риска в сложных системах // Труды Международной научной школы МА БР 2014 (Санкт-Петербург, 18-20 ноября 2014 г.). СПб., 2014. С. 132-138.
4. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. 544 с.
5. Ворона В. А., Тихонов В. А. Концептуальные основы создания и применения системы защиты объектов: Учебное пособие. Обеспечение безопасности объектов. Горячая линия-Телеком. М., 2012. 196 с.

THE FORMATION OF AN EFFECTIVE SYSTEM OF INFORMATION PROTECTION IN THE DIGITAL EDUCATIONAL SPACE

© E. D. Alisultanova, D. S. Bicalov

GSTOU named after acad. M. D. Millionshchikov, Grozny, Russia

This article is aimed at the formation of an effective system of information security. Currently, in view of the improvement of information technology, the problem of information security remains more urgent, as together with the improvement of information security methods, information leakage methods are unfortunately developing.

This article describes one of the current information security systems, ViPNet Client system.

The ViPNet Client servage software package is designed to protect the workplaces of corporate users. ViPNet Client podaressis protects the cigar from external and internal network attacks by filtering the representation of the traffic. In addition, the ViPNet Glukharev Client PC provides secure non-administrative work with corporate data shunning through an encrypted channel, including for remote eliminated users.

Key words: ViPNet Client interface panel for Windows, user, encryption keys, information protection

REFERENCES

1. Kabakova, N. V. (2014) Sistema zashhity informacii ViPNet [ViPNet Information Protection System]. M.: DMK Press, 392 p.
2. Baranova, E. K. (2009) 'Metodiki i programmnoe obespechenie dlja ocenki riskov v sfere informacionnoj bezopasnosti'. *Upravlenie riskom*. [Methods and software for risk assessment in the field of information security. Risk Management]. № 1 (49). Pp. 15-26.
3. Baranova, E. K. (2014) 'Metodiki analiza i ocenki riskov informacionnoj bezopasnosti. Modelirovanie i analiz bezopasnosti i riska v slozhnyh sistemah'. *Trudy Mezhdunarodnoj nauchnoj shkoly MA BR 2014, Saint-Petersburg, 18-20 november 2014.*) [Methods of analysis and assessment of information security risks. Modeling and analysis of safety and risk in complex systems. Transactions of the International Scientific School MA BR 2014]. S-P. Pp. 132-138.
4. Shangin, V. F. (2008) Zashhita kompjuternoj informacii. Effektivnye metody i sredstva [Protection of computer information. Effective methods and tools]. DMK Press. 554 p.
5. Vorona, V. A. and Tihonov, V. A. (2012) Konceptual'nye osnovy sozdaniya i primeneniya sistemy zashhity obektov: Uchebnoe posobie. Obespechenie bezopasnosti ob'ektov. Gorjachaja linija-Telekom [Conceptual framework for the creation and application of a system of object protection. Study guide. Ensuring the safety of objects. Hot line-Telecom]. M., 196p.