DOI: 10.17117/na.2016.04.03.159

Поступила (Received): 30.04.2016

<http://ucom.ru/doc/na.2016.04.03.159.pdf>**Провоторский А.О., Шипеева К.В.****Методы и средства обхода антивирусных систем, средств сетевой защиты, средств защиты операционных систем****Provotorskiy A.O., Shipeeva K.V.****Methods and means of round of anti-virus systems, means of network protection, means of protection of operating systems**

Наука идёт в ногу со временем, открывая всё новое, а также и злоумышленники не стоят на месте. В данной статье рассказывается о методах и средствах обхода антивирусных систем, средств сетевой защиты, средств защиты операционных систем – программных, технических и комбинированных

Ключевые слова: обход, защита операционных систем, безопасность

Провоторский Александр Олегович

Студент

Омский государственный технический университет

г. Омск, пр. Мира, 11

Шипеева Кристина Владимировна

Студент

Омский государственный технический университет

г. Омск, пр. Мира, 11

The science keeps up to date, opening all new, as well as malefactors don't stand still. In this article it is told about methods and means of round of anti-virus systems, means of network protection, means of protection of operating systems – program, technical and combined

Key words: round, protection of operating systems, safety

Provotorskiy Alexandr Olegovich

Student

Omsk state technical university

Omsk, Mira ave., 11

Shipeeva Christina Vladimirovna

Student

Omsk state technical university

Omsk, Mira ave., 11

Трудно себе представить современное общество без использования компьютерных технологий и сети Интернет. Все больше важной и ценной информации люди хранят на электронных носителях, обрабатывают на компьютерах и передают через локальные и глобальные сети.

Естественно, применяются определенные защитные механизмы, которые позволяют защищать от несанкционированного доступа наиболее важную информацию. И этому вопросу уделяют много внимания разработчики программного обеспечения, в том числе и антивирусных программ. Но также естественно, что существуют методы и средства обхода антивирусных систем, средств сетевой защиты, средств защиты ОС. Более того, данные вопросы прорабатываются на уровне правительств. Формируются или уже функционируют специальные группы специалистов, которые занимаются так называемыми кибератаками.

Условно все методы, средства и технологии обхода всех, как старых, так и самых современных, можно разделить на следующие группы:

1. Физические, технические или аппаратные средства. В данном случае речь идет о возможности проникновения в помещение, где располагается компьютер, его включение и банальное копирование необходимых сведений. Сюда же можно включить сканирующие устройства и приспособления, которые способны считывать информацию через Wi-Fi и так далее. Часто механизмы оснащаются алгоритмами, позволяющими убрать из фона «белый шум». Именно он чаще всего используется для защиты.

2. Программные средства. Среди них наиболее распространенными программами, позволяющими получить доступ к информации, являются так называемые вирусы. Все антивирусные программы работают по определенному алгоритму, отыскивая в коде тело вируса. Если удастся «спрятать» тело, обнаружить его будет очень сложно. Большой проблемой для взломщика, зачастую, становятся пароли, которые могут размещаться как на сетевых ресурсах, в том числе «облаках», так и на компьютерных носителях. В любом случае, можно разработать под конкретные условия эксплуатации «взломщик паролей». К сожалению, чаще всего эти программы уникальны и приспособлены для одного направления работы.

3. Комбинированные средства обхода защит. Речь идет о совместном использовании программных и аппаратных средств. Так, например, можно подключиться к кабелю физически и с помощью специального программного обеспечения получить доступ к нужной информации, отфильтровав ее в общем потоке.

4. Отдельно стоит выделить программы-дешифраторы. Сегодня многие физические лица (что уж говорить про компании и серьезные организации) используют самые разные методы и технологии шифрования. И сознание качественного программного продукта для осуществления дешифровки – верх мастерства специалистов.

Таким образом, как бы ни развивались технологии защиты информации, какие бы новые средства и методы не придумывались, всегда в ногу с ними будут совершенствоваться и кибер-преступники, шпионы и разведчики. Как говорил один известный ученый – любое действие рождает противодействие.

Список используемых источников:

1. Безбогов А.А., Яковлев А.В., Шамкин В.Н. Методы и средства защиты компьютерной информации Тамбов: издательство ТГТУ, 2006. С. 38.
2. Блинов А.М. Информационная безопасность. Ч. 1. 2010. С. 55-57.
3. Каторин Ю., Разумовский А., Спивак А. Защита информации техническими средствами. Санкт-Петербург, 2012. С. 95.