# АДАПТАЦИЯ ИНФРАСТРУКТУРНЫХ РЕШЕНИЙ ТРЕБОВАНИЯМ К БЕЗОПАСНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ

*А.Ю. Дедов*
Алтайский государственный университет, г. Барнаул

В настоящее время жизненный цикл любого программного продукта стремительно сокращается. Это положительно влияет на безопасность, так как новые версии исправляют значительную часть ошибок старых. Кроме того, улучшается и совершенствуется функционал. Недостатком частых обновлений является конечная стоимость использования продукта (необходимость приобретения новых версий), а если речь идет о сертифицированном ПО, возникает вопрос дополнительной сертификации обновлений.

На российском рынке в сфере защиты информации регуляторами выступают Федеральная служба по техническому и ээкспортному контролю (ФСТЭК), Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Их требования защиты соответствуют информации, обрабатываемой в системе. Так, например, для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе необходимо соответствующими сертификатами закрепить отсутствие НДВ в используемом ПО.

Актуальность данной темы растет с каждым годом – программы финансирования не учитывают постоянно меняющийся рынок программного обеспечения, что приводит к ситуациям, когда организации продолжают пользоваться устаревшими продуктами, на которые истек срок поддержки вендора. Так, например, Microsoft Windows XP начала выпускаться еще в 2001 году, основная поддержка продукта была остановлена в апреле 2009 года, расширенная – в апреле 2014 года. По статистике компании Net Applications, в феврале 2017 года эта операционная система находилась на третьем месте по популярности в мире с долей 8,45 %, уступая только Windows 7 (48,41 %) и Windows 10 (25,19 %) [1], рис.1.

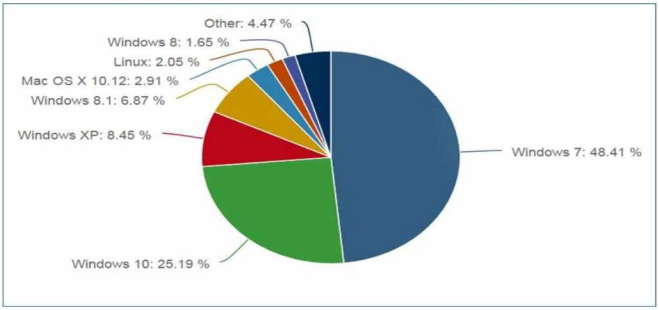


Рис. 1. Доля распределения рынка ОС по состоянию на 2017 г.

В то же время ведущие российские производители ПО для защиты информации и средств криптографической защиты прекращают поддержку Windows XP в своих продуктах. Компания ИнфоТеКС – поставщик ПО ViPNet Client для Windows, в обновленной версии ViPNet Client 4 уже не указывает устаревшую систему в качестве официально поддерживаемой [2]. Несмотря на то, что обратная совместимость версий 3.х и 4.х обеспечена технологией, сертификат соответствия ФСБ России № СФ/525-2952 на ПК ViPNet Client 3.2 заканчивается 20.08.2018 г. а для систем класса КС2 и КС1 сертификат прекратил свое действие 30.11.2017 г., что означает невозможность построения систем класса КС2 и выше на имеющемся оборудовании. Сети КС3 не удовлетворяют потребностям многих организаций, обрабатывающих персональные данные. Компания «Код безопасности» в новом продукте Secret Net Studio также отказалась от поддержки Windows XP.

Для повышения уровня защищенности сетей необходимо максимально снизить роль неподдерживаемого оборудования и перенести его функционал на поддерживаемые сертифицированные решения. Предлагается защищать систему с двух сторон сервера терминалов:

- Использование терминального клиента и средств защиты терминальных подключений для защиты изнутри;
- Использование шлюзовых координаторов для шифрования для защиты снаружи.

Полноценно решить проблему устаревшего софта поможет только его обновление, но как временную меру для повышения безопасности в ряде задач можно использовать защищенные терминальные подключения. Терминальный клиент после установления связи с терминальным сервером пересылает на

последний вводимые данные (нажатия клавиш, перемещения мыши) и, возможно, предоставляет доступ к локальным ресурсам (например, принтер, дисковые ресурсы, устройство чтения смарт-карт, локальные порты (COM/LPT)). Терминальный сервер предоставляет среду для работы (терминальная сессия), в которой исполняются приложения пользователя. Результат работы сервера передается на клиента, как правило, это изображение для монитора и звук (при его наличии).

Современные СЗИ поддерживают большинство распространенных версий серверных операционных систем и предоставляют функционал защиты терминальных подключений. В зависимости от выбранного ПО можно организовать защиту неограниченного числа терминальных клиентов. Так, например, сервер терминалов Dallas Lock требует лицензирования каждого отдельного подключения, а Secret Net Studio может осуществлять защиту любого числа клиентов в рамках одной лицензии.

Для обеспечения криптографической защиты трафика в условиях использования неподдерживаемых систем, рекомендуется использовать шлюзовые кординаторы, устанавливаемые на границу защищаемого периметра. Это снижает удобство пользования открытым интернетом, но позволяет осуществлять передачу данных по защищенным каналам с использованием шифрования по ГОСТ 28147-89 на ключах шифрования 256 бит и при наличии всех действующих сертификатов на оборудование. Шлюзовые координаторы используются в качестве серверного решения шифрования. За невозможностью использования персонального межсетевого экрана и СКЗИ на большом числе машин, существует вариант использования отдельного устройства, которое будет шифровать трафик, выходящий за периметр сети, производить его фильтрацию и маршрутизацию, а также, при необходимости, обеспечивать агрегирование интерфейсов и балансировку нагрузки[3].

Модернизация парка ИТ любой организации требует больших финансовых инвестиций. По данным портала TAdviser, только АИС ПФР (сопоставимая с исследуемой в научной работе) в 2015 году требовало 22 млрд. рублей на развитие автоматизированной информационной системы [4]. Оценка в 28% машин с устаревшей системой показывает, что в условиях недостаточности финансирования необходимо применять альтернативные способы и возможности работы, не нарушая при этом действующего законодательства РФ.

**Библиографический список**

1. Microsoft возобновила поддержку операционной системы Windows XP [Электронный ресурс]. – Режим доступа: https://3dnews.ru/950045 – Заглавие с экрана. – (Дата обращения: 01.02.2018).
2. ViPNet Client версия 4 [Электронный ресурс]. – Режим доступа: https://infotecs.ru/product/vipnet-client-.html – Заглавие с экрана. – (Дата обращения: 02.02.2018).
3. ViPNet Coordinator HW1000 версия 4 [Электронный ресурс]. – Режим доступа: https://infotecs.ru/product/vipnet-coordinator-hw-1000.html – Заглавие с экрана. – (Дата обращения: 02.02.2018).
4. 10 самых дорогих ИТ-систем в госсекторе России сегодня [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Государственные_ИТ-гиганты:_10_самых_дорогих_информационных_систем_современной_России – Заглавие с экрана. – (Дата обращения: 02.02.2018).