

## ОБУЧЕНИЕ УЧАЩИХСЯ ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СРЕДСТВАМИ ОБЛАЧНОГО АНТИВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

**Шевчук Михаил Валерьевич, кандидат физико-математических наук, доцент кафедры Вычислительной математики и методики преподавания информатики ГОУ ВПО «Московский государственный областной университет»**

✉ shevchukmv@gmail.com

**Шевченко Виктория Геннадьевна, аспирант кафедры Вычислительной математики и методики преподавания информатики ГОУ ВПО «Московский государственный областной университет»**

✉ shevchenkovg89@gmail.com

*В статье рассматриваются вопросы обеспечения информационной безопасности образовательного учреждения; вопросы выбора и использования современных антивирусных программных средств защиты информации. Наибольшее внимание в статье уделено проблеме обучения учащихся обеспечению информационной безопасности средствами облачного антивирусного программного обеспечения. Приведен обзор функциональных возможностей облачного антивирусного программного обеспечения, а также рассмотрены их возможности для обучения.*

**Ключевые слова:** антивирусное программное обеспечение, облачные технологии, информационная безопасность, PandaCloudAntivirus, Prevx, ImmundetAntivirus.

В настоящее время проблема обеспечения компьютерной и информационной безопасности современного образовательного учреждения является одной из наиболее актуальных при организации учебной деятельности учащихся. Количество современных информационных угроз отличается многообразием и стремительно пополняется и эволюционирует параллельно с появлением новых и значительным совершенствованием уже традиционно используемых в образовательных целях информационных и коммуникационных технологий. Несколько медленнее изменяется и, по возможности, учитывает происходящие изменения в сфере обеспечения информационной безопасности нормативно-правовая база, что, в свою очередь, способствует необходимости совершенствования и повышения эффективности методов и средств обеспечения компьютерной и информационной безопасности учебной деятельности учащихся, как в образовательном учреждении, так и за его пределами.

В современной школе информация и информационная инфраструктура являются главными компонентами учебного процесса. Учебные классы оснащаются компьютерной техникой и соответствующим про-

граммным обеспечением, бесппроблемное функционирование которого определяет качество полученных знаний и способствует успешному формированию необходимых компетенций учащихся.

С целью повышения уровня компьютерной и информационной безопасности в учебных учреждениях необходимо использовать различные программные средства, препятствующие нанесению материального ущерба в виде потери данных и морального вреда учащимся негативной информацией, непредназначенной для знакомства с ней несовершеннолетних пользователей. Для защиты рабочего окружения учебных персональных компьютеров используются различные программные и аппаратные средства, которые значительно повышают эффективность обеспечения информационной безопасности учебного рабочего места. К таким средствам традиционно относят идентификацию пользователя с помощью пароля, использование разнообразных средств программного и аппаратного шифрования и применение защитного программного обеспечения.

Для обеспечения компьютерной безопасности образовательного учреждения необходимо, в первую очередь, защищать персональные компьютеры от несанкционированного доступа, в частности, от вредоносного программного обеспечения, хакерских атак, программ-шпионов, рекламных программ, различных спам-рассылок. Инфицировать персональный компьютер различными вредоносными программами, которые могут привести к потере данных, можно при работе в сети Интернет, при установке приложений из ненадежных источников, а также при использовании непроверенных съемных накопителей. Наиболее распространенным способом предотвращения подобных проблем традиционно считается антивирусное программное обеспечение.

Существует большое количество антивирусных программ для защиты информации и предотвращения попадания в персональный компьютер вредоносного кода. Большинство распространенных антивирусных программ являются платными, хотя и стоят относительно недорого, но большинство антивирусов требуют регулярного продления лицензии каждые полгода или год, что значительно повышает эксплуатационные расходы на сопровождение работоспособного и относительно безопасного в плане информационной безопасности компьютерного класса. Существуют также и условно бесплатные антивирусные программы, которые не всегда являются достаточно эффективным средством при борьбе с вредоносными программами ввиду искусственно ограниченной функциональности. Кроме того, антивирусные базы бесплатных программ не всегда своевременно обновляются, что может повлечь определенные последствия, связанные с потерей информации или повреждением компьютерных программ. В качестве альтернативы подобным антивирусным программам предлагается использовать облачное антивирусное программное обеспечение, которое является бесплатным, либо условно бесплатным, но, несмотря на такие ограничения, в силу своей облачной сущности, поддерживают в актуальном состоянии и своевременно обновляют свои антивирусные базы. Наиболее

распространенными являются такие облачные антивирусные программы, как PandaCloudAntivirus, ImmunetFreeAntivirus и Prevx. Для использования перечисленных антивирусных программ необходимо загрузить с официального сайта на персональный компьютер соответствующий дистрибутив, установить его, после чего все базы и их обновления, а также проверка персонального компьютера и других носителей информации, подключаемых к нему, будут осуществляться в автоматическом режиме. Необходимым условием работы облачных антивирусных программ является наличие активного подключения к сети Интернет. Каждая из перечисленных облачных антивирусных программ имеет свои характерные особенности функционирования, которые необходимо учитывать при их выборе как в качестве инструмента защиты учебного рабочего места, так и в качестве объекта изучения на занятиях в учебном учреждении.

Рассмотрим особенности облачной антивирусной программы PandaCloudAntivirus [4]. В настройках программы размещены параметры сетевого соединения и функции, отвечающие за отправку подозрительных файлов в «облако». Другие настройки антивирусного сканера в PandaCloudAntivirus отсутствуют, так как все доверено автоматике, самостоятельно принимающей решения при обнаружении вирусов, руткитов, троянских программ и рекламных модулей, шпионского программного обеспечения, программ-шуток и прочих вредоносных приложений. Как и большинство антивирусных программ, PandaCloudAntivirus достаточно быстро сканирует файлы на наличие вредоносного программного обеспечения, а после сканирования программа отправляет зараженные объекты в специальную папку под названием «Карантин», из которой можно либо извлечь случайно попавшие туда файлы, либо окончательно удалить файлы, являющиеся вредоносными. При этом программа фиксирует все операции в файле отчета, который впоследствии можно экспортировать в формат CSV. Для каждого вредоносного файла, который антивирус не смог обезвредить, PandaCloudAntivirus показывает ссылки на веб-страницы с описанием методик удаления конкретного вируса или троянской программы вручную. Кроме того, антивирус имеет возможность использования URL- и веб-фильтрации, при помощи которой можно ограничить доступ учащихся к соответствующим вредоносным сайтам сети Интернет, что представляется достаточно удобным и в меру эффективным инструментом преподавателя для организации и регулирования сетевой активности учащихся в качестве дополнения к уже существующим системам защиты. Интерфейс программы переведен на более чем 20 языков, среди которых есть и русский язык, что является несомненным плюсом для использования данной программы в учебных учреждениях, а также при обучении работе с ней учащихся. Данная программа имеет также и платную версию, которая обладает дополнительными функциями [4] такими, как защита в публичных беспроводных сетях, автоматическая вакцинация съемных носителей информации, встроенный межсетевой экран, который позволяет осуществлять контроль и фильтрацию проходящих через негостевых пакетов в соответ-

ствии с заданными правилами. Основной задачей межсетевое экрана является защита компьютерных сетей или ее отдельных узлов от несанкционированного доступа, что при использовании в качестве защиты позволяет дополнительно усилить информационную безопасность учебного рабочего места, а при использовании данного программного продукта в качестве объекта изучения у учащихся появляется возможность познакомиться с подобным функционалом и научиться обеспечивать комплексную защиту своего рабочего места.

Антивирусная программа ImmunetFreeAntivirus также основана на технологии облачных вычислений и обладает аналогичной, как и у предыдущего программного продукта, возможностью поддержания актуального состояния своей антивирусной базы и обеспечивает своевременную загрузку и установку обновлений клиентской части облачной программы, а также предъявляет достаточно низкие системные требования к аппаратному обеспечению учебного рабочего места [2], что иногда может оказаться определяющим при выборе инструмента обеспечения информационной безопасности учебной деятельности учащихся в компьютерном классе. Бесплатный облачный антивирус ImmunetFree предназначен для работы с антивирусным программным обеспечением Symantec, AVG и McAfee [2], улучшая показатели их защиты, или антивирусная программа может работать самостоятельно, став единственным защитным программным обеспечением учебного компьютера. Антивирус поддерживает как полное, так и выборочное сканирование персонального компьютера и носителей информации. После окончания сканирования можно просмотреть отчеты о результатах сканирования. Антивирус ImmunetFree не имеет русскоязычного интерфейса, что немного усложняет работу с ним в качестве средства обучения, однако, при наличии интуитивно понятной интерфейсной части, данный недостаток антивирусной программы можно расценивать как дополнительную возможность пополнения словарного запаса учащихся специфическими английскими терминами из области информационной безопасности, что, несомненно, в перспективе положительным образом скажется на продуктивности дальнейшего знакомства и изучения нового и ранее незнакомого защитного программного обеспечения, в котором, даже в адаптированных для русскоязычных пользователей версиях программ, далеко не все термины, встречающиеся в интерфейсной части или в описании выявленных информационных угроз, переведены на русский язык. В противном случае, решить проблему неполного понимания учащимися англоязычного интерфейса программы могут эффективно помочь компьютерные словари или специализированные облачные сервисы перевода.

Платная версия облачной антивирусной программы ImmunetFreeAntivirus предоставляет защиту персонального компьютера и возможность его сканирования без обязательного подключения к сети Интернет, однако это не освобождает системных администраторов, лаборантов компьютерных классов или преподавателей и учащихся от необходимости регулярного обновления антивирусной базы данной программы.

Кроме того, платная версия имеет расширенные возможности по обнаружению вредоносного программного обеспечения в электронных письмах и архивных файлах, а также позволяет обнаруживать руткиты (от англ. rootkit).

Бесплатная версия облачной антивирусной программы Prevx [5], с которой объединил свои функциональные возможности антивирус WebrootSecureAnywhereAntivirus, имеет возможность сканировать на наличие вредоносного программного обеспечения только на одном системном локальном диске компьютера. Чтобы полностью проверить компьютер и съемные носители информации на наличие вредоносного и нежелательного программного обеспечения, необходимо приобрести полную версию данной облачной антивирусной программы. Кроме того, в бесплатной версии Prevx учащиеся имеют доступную возможность изучить на занятии некоторые специальные функции защитной программы, например, настроить эвристический анализатор, планировщик, модуль проверки файлов, блокирующий некоторые сайты при помощи надстройки для браузеров SafeOnline. Наличие в Prevx русскоязычного интерфейса облегчает работу с ним как преподавателям, так и учащимся и их родителям.

Выше были рассмотрены основные функциональные возможности некоторых облачных антивирусных программ, которые в той или иной степени влияют на их выбор и перспективность использования для образовательных целей, а также в качестве эффективных инструментов обеспечения информационной безопасности учебных рабочих мест в компьютерных классах.

Однако основным достоинством подобных облачных антивирусных программ можно считать то, что они являются, как правило, наименее требовательными к аппаратному обеспечению компьютерного класса, по сравнению с традиционным антивирусным программным обеспечением, устанавливаемым в качестве инструмента защиты на персональные компьютеры учебного учреждения, и для их использования необязательно иметь высокопроизводительные и дорогостоящие вычислительные машины, а обновление облачных антивирусных программ и проверка локальных дисков и прочих носителей информации будет происходить в автоматическом режиме, эффективно используя вычислительные ресурсы учебного персонального компьютера.

Помимо рассмотренных облачных антивирусных программ защитными функциями обладает также антивирусное облако Kaspersky Security Network [3], которое фиксирует и обрабатывает данные при переходе по сайтам сети Интернет, а также при установке программного обеспечения в случае обнаружения попыток заражения персонального компьютера вредоносным программным обеспечением или при подозрительной активности программ; затем обрабатывает эти данные и отправляет информацию в специальную базу, содержимое которой становится практически мгновенно доступно другим пользователям данного облачного сервиса. Такой подход позволяет сократить время на получение обновленных баз вирусных сигнала-

тур и экономить сетевой трафик, расходуемый при обновлении антивирусных программ, что иногда немаловажно для бюджета образовательного учреждения. При помощи облачных технологий Kaspersky Security Network реализует следующие функции: веб-фильтр, который позволяет проверять ссылки на веб-страницах; анти-фишинг, который предотвращает несанкционированный доступ к данным пользователя; анти-спам, который позволяет фильтровать письма на наличие рекламной, мошеннической и другой вредной информации; проверка программ на наличие потенциальных угроз.

Кроме того, в последнее время становится актуальным и необходимым использование антивирусного программного обеспечения и на распространенных мобильных платформах. Современные дети рождаются в век бурного развития компьютерных технологий и часто получают свой первый смартфон или планшетный компьютер уже с малых лет, поэтому проблема, связанная с необходимостью обеспечения информационной безопасности носимой электроники детей, а также их родителей, становится актуальной и выходит на первый план при появлении у них этих устройств.

Производители антивирусных программных средств стараются не отставать от развития и изменения приоритетов в области обеспечения информационной безопасности, и с этой целью выпускают и регулярно обновляют специальные версии своего антивирусного программного обеспечения и для мобильных платформ, например, для мобильной операционной системы Android, встроенная система безопасности которой регулярно подвергается испытанию со стороны многочисленных зловредных программ, распространяемых иногда даже через официальный магазин приложений. Подобные зловредные программы при определенном стечении обстоятельств могут добиться своих целей, что, как правило, может привести к нарушению штатной работоспособности мобильного устройства, угрозе личной информации или к некоторым финансовым потерям.

В этой ситуации, дополнительно к рекомендуемым разработчиками мобильной платформы мерам предосторожности при установке дополнительного программного обеспечения и при соблюдении элементарных правил безопасности при работе в сети Интернет, рекомендуется воспользоваться мобильными версиями антивирусных программ, обладающих практически той же функциональностью, что и версии для персональных компьютеров. В настоящее время наиболее распространенными антивирусными программами для мобильной платформы являются Kaspersky Internet Security, Dr.Web, McAfee Mobile Security и некоторые другие, менее известные защитные программы.

Антивирусу Dr.Web[1] стоит уделить особое внимание, так как данный антивирус обладает не только стандартными функциями, присутствующими традиционным антивирусам, но и имеет ряд характерных для мобильного защитного программного обеспечения функций: антиспам, антивор, функция, позволяющая помочь найти мобильный телефон при его уте-

ре, и, самое главное, URL-фильтр CloudChecker, представляющий из себя облачный инструмент для фильтрации, основной задачей которого является блокировка нежелательных ресурсов сети Интернет в браузере. С помощью фильтра CloudChecker можно заблокировать доступ к потенциально опасным и нежелательным веб-ресурсам, условно разделенным по следующим категориям: наркотики, известные источники вирусов, нецензурная лексика, терроризм, насилие, оружие, сайты для взрослых и другие.

Работе с антивирусными программами школьников обучают в 10-11 классах [6], но, как правило, количество теоретических занятий, отводимых на изучение данной темы, превышает количество практических занятий. На практических занятиях работа школьников с антивирусным программным обеспечением ограничивается часто лишь проверкой персонального компьютера и съемных дисков на наличие зараженных вирусами файлов и обновление антивирусной базы самой программы.

Разработанные практические работы [7,8] по использованию облачных антивирусных программ на занятиях, кроме проверки персонального компьютера и съемных дисков на вирусы, ориентированы в своей содержательной части и на установку дистрибутива антивируса на персональный компьютер, и на его настройку. Однако, при выполнении подобных заданий возникает небольшая сложность технического характера, связанная с наличием на учебном рабочем месте уже установленного антивирусного программного обеспечения, удаление или изменение которого, как правило, противоречит установленной политике безопасности организации учебной деятельности учащихся за персональными компьютерами. Для этих целей хорошо подходит программное обеспечение виртуальных машин с предустановленными заранее преподавателем операционными системами семейства Windows или Linux, в среде которых имеется практическая возможность полноценного изучения всех этапов установки, настройки и эксплуатации системного программного обеспечения, к которому, в том числе, и относятся облачные антивирусные программные средства. В этом случае не потребуются затратное выделение отдельных персональных компьютеров для учебных экспериментов учащихся с антивирусным программным обеспечением на занятиях, что позволяет считать использование виртуальных машин для учебных целей экономически эффективным и технически оправданным средством.

Таким образом, проблема обеспечения информационной безопасности учебной деятельности учащихся в образовательном учреждении и за его пределами, а также знакомство учащихся с основными методами и средствами ее безопасного осуществления становится актуальной и определяющей при организации эффективного процесса обучения. Решение данной проблемы образовательного учреждения невозможно без использования современных подходов и программных средств обеспечения информационной безопасности, в качестве которых успешно могут выступать антивирусные программные средства на основе облачных технологий, развитие которых в настоящее время переживает стремительный подъем и

актуальность применения которых, в свете изменяющегося соотношения используемых в учебном процессе традиционных персональных компьютеров и мобильных устройств в пользу последних, будет только повышаться.



### БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Официальный сайт антивируса Dr.Web. URL: <http://www.drweb.com/>(дата обращения: 21.04.2014)
2. Официальный сайт антивируса ImmundetAntivirus. URL: <http://www.immUNET.com/>(дата обращения: 21.04.2014)
3. Официальный сайт антивируса Kaspersky Internet Security. URL: <http://www.kaspersky.ru/>(дата обращения: 21.04.2014)
4. Официальный сайт антивируса PandaCloudAntivirus. URL: <http://www.cloudantivirus.com/>(дата обращения: 21.04.2014)
5. Официальный сайт антивируса Prex. URL: <http://prevx.com/>(дата обращения: 21.04.2014)
6. Семакин И.Г. Информатика и ИКТ. Базовый уровень: практикум для 10-11 класса / И.Г. Семакин, Е.К. Хеннер, Т.Ю. Шеина. - 3-е изд. испр. - М.: БИНОМ. Лаборатория знаний, 2010. - 295 с.
7. Шевчук М.В., Шевченко В.Г. Павлов К.С. Изучение методов обеспечения информационной безопасности с применением виртуальных машин и облачных технологий: учебное пособие. М.: Изд-во МГОУ, 2013.- 140 с.
8. Шевчук М.В., Шевченко В.Г. Технологии облачных вычислений: лабораторные работы по дисциплине «Информационные и коммуникационные технологии в науке и образовании» (учебное пособие). М.: Изд-во МГОУ, 2012.- 212 с.