УДК 378.147:004.056.57

Особенности формирования информационной компетенции обучающихся нетехнических специальностей в части развития умений защиты информации от разрушающих программных воздействий

Бакулин Василий Михайлович

Кандидат физико-математических наук, доцент,
Волгоградская академия МВД России,
400089, Российская Федерация, Волгоград, ул. Историческая, 130;
e-mail: bvm@volgodom.ru

Еськин Дмитрий Леонтьевич

Кандидат физико-математических наук, доцент,
Волгоградская академия МВД России,
400089, Российская Федерация, Волгоград, ул. Историческая, 130;
e-mail: yd38@bk.ru

Аннотация

Работа имеет междисциплинарный характер и написана на стыке педагогики и информационной безопасности. В работе авторы рассматривают некоторые особенности формирования деятельностного компонента информационной компетенции, связанного с умением осуществлять защиту информации от разрушающих программных воздействий, у обучающихся, не обладающих глубокими техническими знаниями в области обеспечения информационной безопасности. Данный компонент информационной компетенции предлагается формировать в несколько этапов. На начальном этапе обучающимся необходимо получить теоретические знания и основные представления о различных видах вредоносного программного обеспечения. На следующем этапе целесообразным является изучение функциональных возможностей программ, предназначенных для защиты информации, в частности средств антивирусной защиты компьютерной системы. Для поиска путей решения проблемы выбора антивирусной программы на учебном занятии предлагается использовать такой интерактивный метод обучения как мозговой штурм. С целью обеспечения наибольшей эффективности учебного процесса и максимального охвата имеющегося на рынке антивирусного программного обеспечения при подготовке конкретных практических занятий целесообразно использовать программы виртуальных машин совместно с ознакомительными версиями антивирусных программ. Отдельное внимание следует уделить освоению программного обеспечения, предназначенного для восстановления удаленных файлов. В целях повышения эффективности образовательного процесса предлагается использование комбинированных методов освоения материала, таких как: мозговой штурм и классическое практическое занятие.

Для цитирования в научных исследованиях

Бакулин В.М., Еськин Д.Л. Особенности формирования информационной компетенции обучающихся нетехнических специальностей в части развития умений защиты информации от разрушающих программных воздействий // Педагогический журнал. 2017. Т. 7. № 6А. С. 133-140.

Ключевые слова

Информационная компетенция, защита информации, вредоносные программы, антивирусная защита, восстановление файлов.

Введение

В современном мире специалистам практически любых профессий в процессе осуществления своей профессиональной деятельности приходится иметь дело с различной компьютерной и телекоммуникационной техникой. Поэтому при обучении будущих специалистов необходимо уделить особое внимание формированию у них информационной компетенции.

Сегодня информационная компетентность может считаться ключевой компетенцией, т.е. необходимой человеку независимо от профильной подготовки [Санникова, Письменный, 60]. Поскольку информационная компетентность неразрывно связана с владением современными информационными технологиями, то ее формирование должно осуществляться с использованием методик, основанных на использовании компьютерной техники [Дусева, 2015, 133]. Достаточно значимым деятельностным компонентом информационной компетенции является умение использовать методы и средства обеспечения информационной безопасности в профессиональной деятельности. А в связи с тем, что одной из основных причин, приводящих к потере информации, является деструктивное действие вредоносного программного обеспечения, современный специалист должен уметь осуществлять защиту информации от разрушающих программных воздействий.

Основная часть

На начальном этапе формирования информационной компетенции в части организации защиты информации от разрушительного программного воздействия обучающимся необходимо получить теоретические знания и основные представления о различных видах вредоносного программного обеспечения.

На сегодняшний день наиболее распространенными и деструктивными вредоносными программами являются программы следующих типов: компьютерные вирусы, сетевые черви и троянские программы [Еременко, Сапелкин, Хитов, 2016].

Для понимания различий между указанными типами вредоносного программного обеспечения обучающиеся должны знать их принцип действия (распространения) и основные функциональные возможности.

Под компьютерными вирусами понимают программы, которые посредством записи себя в служебные разделы диска или внедрения своего исполнительного кода в другие прикладные программы способны самостоятельно распространяться в компьютерных системах. Отличительной особенностью вирусов является то, что они могут заразить отдельный компьютер, но, как правило, не могут самостоятельно распространяться через компьютерные сети.

Сетевыми червями называют вредоносные программы, которые способны самостоятельно распространяться в локальных и глобальных вычислительных сетях. В отличие от вирусов, которые распространяются бесконтрольно, черви выполняют заранее определенные действия.

Троянские программы – это вредоносные программы, которые маскируют свою деятельность под видом обычного прикладного программного обеспечения. В отличие от вирусов и червей, троянские программы не способны распространяться самостоятельно в компьютерных системах и сетях, поэтому данный вид вредоносных программ на начальном этапе заражения пытается любыми способами спровоцировать пользователя на запуск исполняемого файла троянской программы, или использует возможности сетевых червей для своей загрузки на рабочую станцию и последующего запуска.

На следующем этапе формирования информационной компетенции в части организации защиты информации от разрушительного программного воздействия является целесообразным изучение функциональных возможностей программ, предназначенных для защиты информации. Средства защиты информации от деструктивного и иного воздействия по своим функциональным возможностям можно схематично разбить на три вида:

7) Средства разграничения доступа к данным и ресурсам компьютерных систем посредством реализации механизмов идентификации и аутентификации пользователей;
8) Средства криптографического преобразования информации, хранимой в компьютерной системе и передаваемой через компьютерные сети;
9) Средства антивирусной защиты компьютерной системы.

Методика преподавания тем, предполагающих изучение первых двух видов программных средств, была рассмотрена нами в предыдущих работах [Еськин, Бакулин, 2015] и [Бакулин, Еськин, 2016], поэтому более подробно остановимся на освоении обучающимися средств антивирусной защиты.

Перед непосредственным выбором и освоением средств антивирусной защиты, обучающиеся должны понять сам принцип ее функционирования.

Основное назначение антивирусных программ – это обнаружение вредоносных программ и их удаление из компьютерной системы. Однако существует множество различных способов организации антивирусной защиты, отличающихся по сложности своей реализации и эффективности.

Для упрощения выбора обучающимся необходимого средства защиты рассмотрим несколько классификаций алгоритмов антивирусных программ.

Первая классификация касается реализации поиска угроз «нулевого дня», т.е. вредоносных программ еще неизвестных производителям антивирусов [Алиев, 2014, 27]:

1) Алгоритм реактивной защиты осуществляет поиск известных угроз по характерным участкам исполнительного кода (сигнатурам) вредоносных программ. Для реализации данного алгоритма необходимо, чтобы информация о вредоносных программах находилась в базе сигнатур антивируса.
2) Алгоритм проактивной защиты осуществляет поиск еще неизвестных угроз на основании определения особенностей исполнительного кода и функционального поведения программ, которые характерны для вредоносного программного обеспечения.

Вторая классификация основывается на том, как именно антивирусные программы анализируют потенциально опасные программы:

1) Алгоритм анализа исполнительного кода подозрительных или потенциально опасных программ;

2) Алгоритм анализа поведения подозрительных программ на предмет выполнения деструктивных или иных несанкционированных действий;
3) Алгоритм отслеживания изменений системных или иных важных файлов, проводимых подозрительными программами.

Также важной классификацией антивирусных программ является возможность их работы в различных режимах:

1) Режим монитора, когда антивирусная программа в режиме реального времени проверяет все запускаемые программы, передаваемые по компьютерной сети данные, а также отслеживает все подозрительные действия запущенных программ;
2) Режим сканера, когда антивирусная программа выполняет проверку указанных областей хранения данных и оперативной памяти компьютерной системы по команде пользователя или по расписанию.

Знание основных принципов работы антивирусных программ должно обучающимся в дальнейшем помочь с выбором конечного решения.

Ввиду того, что на сегодняшний день существует достаточно большое количество программного обеспечения, предназначенного для защиты персонального компьютера от вирусов, встает проблема выбора антивирусной программы. Немногочисленные тесты антивирусных программ, проводимые различными журналами по тематике информационных технологий, достаточно глубоко анализируют их, сравнивая совершенно различные параметры от удобства пользовательского интерфейса до цены. С другой стороны, как правило, данные тесты нельзя считать полноценными в части, качающейся тестирования именно антивирусной защиты, поскольку для этого необходимо располагать большой базой вредоносного программного обеспечения, соответствующими стендами и процедурами автоматизации тестирования [Панасенко, www].

Для поиска путей решения проблемы выбора антивирусной программы на учебном занятии на наш взгляд целесообразно использовать такой интерактивный метод обучения как мозговой штурм. Данный метод, направленный на генерирование идей по решению проблемы, основан на процессе совместного разрешения поставленных в ходе организованной дискуссии проблемных задач [Двуличанская, 2011, 13]. К основным достоинствам метода мозгового штурма относят активизацию деятельности всех его участников, поощрение творческого мышления, его синергетический эффект, когда в результате интерактивного взаимодействия между участниками чужие идеи дорабатываются, развиваются и дополняются [Измаилова, Кузнецова, 2013, 34].

Мозговой штурм проводится в три этапа: предварительный, этап генерирования идей и заключительный. На предварительном этапе педагогический работник знакомит обучающихся с правилами проведения мозгового штурма, формулирует проблемный вопрос, например, «Каким образом мы можем выбрать оптимальную антивирусную программу?», и отражает его на доске в качестве заголовка. На данном этапе целесообразно определить участника, который будет в дальнейшем фиксировать все предлагаемые идеи на доске. Этап генерирования идей является основным этапом мозгового штурма, во время которого его участники выдвигают идеи по решению стоящей перед ними проблемы. Участники могут предлагать идеи по очереди или бессистемно по усмотрению ведущего. В последнем случае идеи предлагаются свободно, однако есть риск, что не все участники будут вовлечены в процесс выдвижения идей. Все идеи, которые высказываются участниками, должны своевременно фиксироваться на доске.

На заключительном этапе подводятся итоги мозгового штурма. Все идеи систематизируются, группируются по каким-либо признакам и обобщаются. Далее происходит

оценивание идей, выбираются наиболее рациональные и оригинальные, в процессе обсуждения определяется оптимальная идея. В итоге составляется окончательный список практически используемых идей.

Применительно к развитию у обучающихся умений использования средств антивирусной защиты, как одного из этапов формирования у них информационных компетенций, мозговой штурм будет полезен для определения оптимальных критериев отбора антивирусного программного обеспечения, которое им в дальнейшем предлагается освоить. В этом случае освоение средств антивирусной защиты может происходить в два этапа. На первом этапе обучающиеся в форме мозгового штурма осуществляют поиск оптимального для заданных условий программного обеспечения. На втором этапе обучающиеся непосредственно знакомятся с функциональными возможностями выбранных на первом этапе программ.

Для обеспечения наибольшей эффективности учебного процесса и максимального охвата, имеющегося на рынке антивирусных программ при подготовке конкретных практических занятий, предлагается использовать программы «виртуальных машин» совместно с ознакомительными версиями антивирусных программ. Такой подход позволяет обезопасить учебные рабочие станции от неосторожных действий обучающихся и, в то же время, дает полную свободу действий в изучении функциональных возможностей используемого программного обеспечения [Бакулин, Еськин, 2016].

Иногда в результате деструктивного действия вредоносного программного обеспечения оказываются удалены файлы пользователя. В этом случае при отсутствии актуальных резервных копий файлов пользователь рискует лишиться важной для него информации в виде текстовых документов, фотоархивов и т.п. Возможна и обратная ситуация, когда нужные пользователю файлы были удалены антивирусной программой, работающей в режиме максимальной защиты, поскольку были расценены ей как подозрительные. Кроме того, файлы могут быть удалены самим пользователем случайно или в результате действия третьих лиц. Вне зависимости от причин, которые привели к удалению файлов, возникает необходимость их восстановления. В связи с этим задача развития у обучающихся умения восстанавливать удаленные файлы в рамках формирования элементов информационной компетенции является достаточно важной.

С целью развития указанного умения на практическом занятии предлагается выполнить задание по восстановлению удаленных файлов с помощью специализированного программного обеспечения. В качестве программы для восстановления можно использовать утилиту Recuva. Данная программа способна восстанавливать файлы с жестких дисков компьютера, с цифровых фотокамер и MP3-плееров, а также с портативных USB-накопителей [Крупин, www]. Несомненным достоинством данной утилиты является и то, что она распространяется на бесплатной основе.

Перед выполнением практического задания следует акцентировать внимание обучающихся на том, что при удалении файла происходит удаление ссылки на него в таблице разделов файловой системы, при этом технически содержимое самого файла сохраняется. При дальнейшей работе с диском на участки, на которых хранится содержимое удаленного файла, может быть записана другая информация. Поэтому важно сразу после обнаружения пропажи файла прекратить работу с разделом диска, с которого он был удален.

Подводя итог, следует акцентировать внимание обучающихся на том, что ни одно программное средство, предназначенное для защиты информации от разрушающего воздействия вредоносных компьютерных программ, не может гарантировать стопроцентную

защиту. Поэтому важно, чтобы пользователь сам проявлял осторожность, не запускал файлы и не открывал электронные письма, полученные из сомнительных источников.

Заключение

На основании вышеизложенного можно сделать следующие выводы.

При формировании информационной компетенции у обучающихся нетехнических специальностей основной упор должен делаться в обзорно-ознакомительном направлении.

В процессе получения практических навыков защиты информации от разрушающих программных воздействий следует использовать программное обеспечение, которое в освоении не требует специальной технической подготовки обучающихся.

Использование комбинированных методов освоения материала, например, мозгового штурма и классического практического занятия, может существенно повысить эффективность образовательного процесса.

Библиография

1. Алиев А.Т. Проактивные системы защиты от вредоносного программного обеспечения // Известия ЮФУ. Технические науки. 2014. № 2 (151). С. 26-33.
2. Бакулин В.М., Еськин Д.Л. Методика преподавания темы «Организация парольной защиты в файловых системах» для обучающихся нетехнических специальностей // Современные наукоемкие технологии. 2016. № 8-2. С. 290-293.
3. Двуличанская Н.Н. Интерактивные методы обучения как средство формирования ключевых компетенций // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2011. № 4. С. 13.
4. Дусева Н.Ю. Компьютерная среда формирования информационных компетенций у иностранных слушателей // Вестник Волгоградской академии МВД России. 2015. № 2 (33). С. 131-136.
5. Еременко С.П., Сапелкин А.И., Хитов С.Б. Классификация вредоносных программ // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2016. № 3. С. 55-61.
6. Еськин Д.Л., Бакулин В.М. Оптимизация обучения по теме «Основы криптографии» обучающихся юридических специальностей // Современные проблемы науки и образования. 2015. № 6-0. С. 380.
7. Измаилова Э.А., Кузнецова Ю.А. Метод мозгового штурма // Модели, системы, сети в экономике, технике, природе и обществе. 2013. № 2 (6). С. 32-35.
8. Крупин А. Восстановление утраченного. URL: http://old.computerra.ru/ terralab/softerra/409841
9. Панасенко А. Современная антивирусная индустрия и ее проблемы. URL: https://www.anti-malware.ru/node/84
10. Санникова С.В., Письменный Е.В. Ключевые компетенции личности в контексте болонского процесса // Вестник Южно-Уральского государственного университета. Серия: Образование. Педагогические науки. 2009. № 24 (157). С. 57-62.

The features of the formation of information competence of students of non-technical specialties in terms of information protection skills development against destructive software impacts

Vasilii M. Bakulin

PhD in Physics and Mathematics, Associate Professor,
Volgograd Academy of the Internal Affairs Ministry of the Russian Federation,
400089, 130 Istoricheskaya st., Volgograd, Russian Federation;
e-mail: bvm@volgodom.ru

Dmitrii L. Es'kin

PhD in Physics and Mathematics, Associate Professor,
Volgograd Academy of the Internal Affairs Ministry of the Russian Federation,
400089, 130 Istoricheskaya st., Volgograd, Russian Federation;
e-mail: yd38@bk.ru

Abstract

The work has interdisciplinary nature and is written at the intersection of pedagogy and information security. The authors consider some features of the formation of an activity component of information competence related to the ability to protect information from destructive program influences in students who do not have deep technical knowledge in the field of information security. This component of information competence is proposed to be formed in several stages. At the initial stage, students need to obtain theoretical knowledge and basic ideas about various types of malicious software. The next step is to study the functionality of programs designed to protect information, in particular, the means of antivirus protection of a computer system. To find ways to solve the problem of selecting an antivirus program in a training session, it is proposed to use such an interactive method of training as brainstorming. In order to ensure the maximum efficiency of the educational process and the maximum coverage of the antivirus software available on the market in preparing specific practical exercises, it is advisable to use virtual machine programs in conjunction with evaluation versions of anti-virus software. Particular attention should be paid to the development of software designed to recover deleted files. In order to increase the effectiveness of the educational process, it is proposed to use combined methods of mastering the material, such as: brainstorming and classical practical exercises.

For citation

Bakulin V.M., Es'kin D.L. (2017) Osobennosti formirovaniya informatsionnoi kompetentsii obuchayushchikhsya netekhnicheskikh spetsial'nostei v chasti razvitiya umenii zashchity informatsii ot razrushayushchikh programmnykh vozdeistvii [The features of the formation of information competence of students of non-technical specialties in terms of information protection skills development against destructive software impacts]. *Pedagogicheskii zhurnal* [Pedagogical Journal], 7 (6A), pp. 133-140.

Keywords

Information competence, information protection, malware, antivirus protection, file recovery.

References

1. Aliev A.T. (2014) Proaktivnye sistemy zashchity ot vredonosnogo programmnogo obespecheniya [Proactive malware protection systems]. *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering sciences], 2, pp. 26-33.
2. Bakulin V.M., Es'kin D.L. (2016) Metodika prepodavaniya temy «Organizatsiya parol'noi zashchity v failovykh sistemakh» dlya obuchayushchikhsya netekhnicheskikh spetsial'nostei [The technique of training of the theme «Organization of password protection in file systems» for students of non-technical specialties]. *Sovremennye naukoemkie tekhnologii* [Modern high technologies], 8-2, pp. 290-293.
3. Dvulichanskaya N.N. (2011) Interaktivnye metody obucheniya kak sredstvo formirovaniya klyuchevykh kompetentsii [Interactive training methods as a means of forming key competences]. *Nauka i obrazovanie: nauchnoe izdanie MGTU im. N.E. Baumana* [Science and Education: Scientific edition of Bauman MSTU], 4, pp. 13.

4. Duseva N.Yu. (2015) Komp'yuternaya sreda formirovaniya informatsionnykh kompetentsii u inostrannykh slushatelei [Computer environment as a means to develop information competences among foreign students]. *Vestnik Volgogradskoi akademii MVD Rossii* [Volgograd Academy of the Russian Internal Affairs Ministry's Digest], 2, pp. 131-136.
5. Eremenko S.P., Sapelkin A.I., Khitov S.B. (2016) Klassifikatsiya vredonosnykh program [Classification of malware]. *Nauchno-analiticheskii zhurnal Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoi protivopozharnoi sluzhby MChS Rossii* [Bulletin of of Saint Petersburg University of the state fire service of EMERCOM of Russia], 3, pp. 55-61.
6. Es'kin D.L., Bakulin V.M. (2015) Optimizatsiya obucheniya po teme «Osnovy kriptografii» obuchayushchikhsya yuridicheskikh spetsial'nostei [Optimization of training on «Basics of cryptography» students of legal professions]. *Sovremennye problemy nauki i obrazovaniya* [Modern problems of science and education], 6-0, pp. 380.
7. Izmailova E.A., Kuznetsova Yu.A. (2013) Metod mozgovogo shturma [The method of brainstorming]. *Modeli, sistemy, seti v ekonomike, tekhnike, prirode i obshchestve* [Models, systems, networks in Economics, technic, nature and society], 2, pp. 32-35.
8. Krupin A. *Vosstanovlenie utrachennogo* [Recovering lost]. Available at: http://old.computerra.ru/terralab/softerra/409841 (Accessed 05/11/17).
9. Panasenko A. *Sovremennaya antivirusnaya industriya i ee problemy* [Modern anti-virus industry and its problems]. Available at: https://www.anti-malware.ru/node/84 (Accessed 06/11/17).
10. Sannikova S.V., Pis'mennyi E.V. Klyuchevye kompetentsii lichnosti v kontekste bolonskogo protsessa [Personal key competences in the context of bologna process]. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta* [Bulletin of the South Ural State University], 4, pp. 57-62.