УДК 378

П. В. Никитин[1], И. В. Фархшатов[1], М. В. Литвиненко[2]

[1]Межрегиональный открытый социальный институт, Йошкар-Ола
[2]Марийский государственный университет, Йошкар-Ола

ИГРОВЫЕ ТЕХНОЛОГИИ КАК ФАКТОР ПОВЫШЕНИЯ МОТИВАЦИИ ИЗУЧЕНИЯ ИНФОРМАТИКЕ

В статье описана методика обучения будущих специалистов в области информационных технологий (ИТ), в том числе и будущих учителей информатики, основам информационной безопасности на базе междисциплинарного подхода, практико-ориентируемых заданий и метода демонстрационных примеров, разработанных авторами с учетом современных тенденций в области информационной безопасности. Под информационной безопасностью в статье понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры. В результате обучения по описанной в статье методике студенты будут знать основные информационные угрозы, пути несанкционированного доступа к информации, каналы утечки, а также классификацию способов и средств защиты информации. В статье подробно описываются практические задания по каждой из дисциплин (программное обеспечение ЭВМ; информационные технологии; компьютерные сети, интернет- и мультимедиатехнологии; компьютерные сети и информационные системы; методы защиты информации), входящих в методическую систему обучения по данному направлению, которые разработаны авторами с учетом современных тенденций в области информационных технологий и защиты информации. Описанная методика была внедрена в процесс обучения будущих специалистов в области информационной безопасности, в том числе и будущих учителей информатики, в АНО ВПО «Межрегиональный открытый социальный университет» и ФГБОУ ВПО «Марийский государственный университет». Результаты эксперимента доказывают положительно влияние данной методики на качество обучения студентов в области информационной безопасности (формальные (физические, аппаратные, программные); неформальные (организационные, законодательные, морально-этические)).

Ключевые слова: методика обучения информатике; информационная безопасность; сетевые угрозы; безопасность сети; интернет; способы «взлома».

В соответствии ФГОС ООО, ФГОС С(П)ОО, формирование компетенций обучающихся в области информационно-коммуникационных технологий – поиск, построение и передача информации, знание основ информационной безопасности, умение безопасного использования средств информационно-коммуникационных технологий является важнейшей задачей образования [14, III, п. 14]. Следовательно, подготовке специалистов в области информационной безопасности необходимо уделять должное внимание. Отметим, что к данным специалистам можно отнести и учителей информатики.

Под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры [4, с. 20].

Будущий специалист в области информационных технологий, а также будущий учитель информатики должны знать основные информационные угрозы, пути несанкционированного доступа к информации, каналы утечки, а также классификацию способов и средств защиты информации. Под защитой информации будем понимать деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния [4, с. 21]. Выделяют следующие способы и средства защиты информации: формальные (физические, аппаратные, программные); неформальные (организационные, законодательные, морально-этические). Отметим,

что студенты должны знать не только теоретические основы данных вопросов, но и владеть практическими умениями и методикой обучения данной темы.

В настоящий момент времени, разработано много методических работ, посвященных информационной безопасности [1; 3; 4; 6; 13 и др.]. В данных работах очень хорошо описаны теоретические вопросы информационной безопасности, но недостаточно представлены практико-ориентируемые задания, которые можно реализовать в качестве лабораторных работ.

Также отметим, что среди условий реализации Федерального государственного стандарта основной образовательной программы ФГОС ООО [14, IV. п. 21] школа «должна обеспечивать для участников образовательного процесса возможность:

• организации сетевого взаимодействия общеобразовательных учреждений, направленного на повышение эффективности образовательного процесса;

• эффективного управления образовательным учреждением с использованием информационно-коммуникационных технологий, современных механизмов финансирования».

Таким образом, наличие в образовательном учреждении грамотно построенной защищенной локальной сети, в которой могут работать все участники образовательного процесса – учащиеся, педагоги, администрация, является насущной необходимостью. Следовательно, школе необходим специалист в области информационной безопасности. И если в больших школах, как правило, предусмотрена должность системного администратора, на которого возложено создание, администрирование и защита локальных вычислительных сетей, то в сельской школе, при небольшом количестве учеников, как правило, нет системного администратора, его роль выполняет учитель информатики.

Ключевой дисциплиной в области информационной безопасности является учебная дисциплина «Методы защиты информации», целью которой выступает ознакомление студентов с основными положениями теории защиты компьютерной информации, математическими моделями и стандартами. Основные разделы изучения, которые включает данная дисциплина, следующие: источники, риски и формы атак на информацию; политика безопасности; стандарты безопасности; криптографические модели; алгоритмы шифрования; модели безопасности основных ОС; администрирование сетей; алгоритмы аутентификации пользователей; многоуровневая защита корпоративных сетей; защита информации в сетях; требования к системам защиты информации. В принципе, изучение данных разделов вполне достаточно для студентов, но, как показывают результаты эксперимента, знания и тем более умения, полученные студентами в рамках данной дисциплины, не соответствуют современным требованиям, которые школа предъявляет специалистам в области информационной безопасности. По наблюдениям, из анкетирования и бесед со студентами, в первую очередь, это связано с избыточным теоретическим материалом, получаемым студентами, за небольшое количество времени, а также с недостаточностью практических заданий и демонстрационных примеров в области информационной безопасности, поэтому авторами статьи была разработана методическая система обучения данного направления, в основу которой входят междисциплинарная интеграция, практико-ориентируемые задания и метод демонстрационных примеров [9].

Первой дисциплиной, на которой происходит знакомство студентов с основами информационной безопасности, является дисциплина «Программное обеспечение ЭВМ» (в некоторых случаях «Информационные технологии» [11]). На данной дисциплине студенты знакомятся с теоретическими основами информационной безопасности, в частности, с основными информационными угрозами, с компьютерными вирусами и приемами борьбы с ними, с законодательными и административными уровнями информационной безопасности. Каждый из студентов, в рамках изучения дисциплины «Программное обеспечение ЭВМ», защищает реферат по теме «Пути несанкционированного получения информации (каналы утечки информации)». Отметим некоторые из тем рефератов:

• Применение подслушивающих устройств.

• Незаконное подключение к аппаратуре или линиям связи вычислительной системы.

• Злоумышленный вывод из строя механизмов защиты.

• Считывание данных в массивах других пользователей.

• Маскировка под зарегистрированного пользователя с помощью хищения паролей и других реквизитов разграничения доступа.

• Получение защищаемых данных с помощью серии разрешенных запросов и другие.

Написание рефератов идет с учетом современных тенденций, в качестве литературы рассматриваются не только классические научные учебники в области информационной безопасности,

но и популярные компьютерные журналы («Хакер», CHIP, «Информационная безопасность» и другие). Как показывает практика, студенты с удовольствием включаются в процесс обучения и уровень сформированности мотивации изучения данной темы сильно увеличивается.

На дисциплине «Компьютерные сети, интернет- и мультимедиатехнологии», в некоторых случаях «Компьютерные сети, информационные системы» будущие специалисты в области ИТ знакомятся с сетевыми угрозами, а также методами и средствами защиты информации в сети. Остановимся на данном вопросе более подробно.

Прежде чем приступить к вопросам безопасности сети, студенты должны научиться проектировать, создавать и администрировать локальную вычислительную сеть (ЛВС). Причем для построения ЛВС студентам предлагается использовать схему, которую потом они смогут использовать при работе в небольших школах, в центрах дополнительного образования и т. д. На рисунке 1 приведен пример модели ЛВС, предлагаемой студентам для построения.

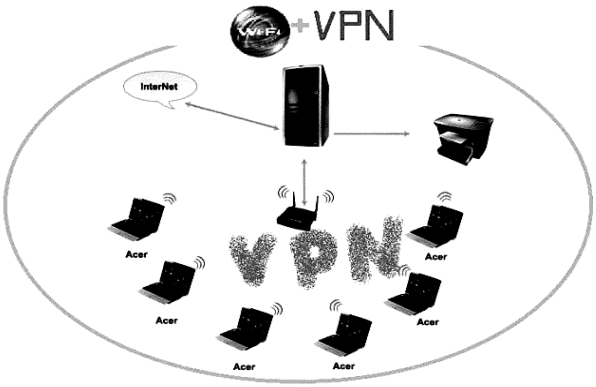

Рис. 1. Предлагаемая модель беспроводной локальной сети

Как видно из рисунка, будущие учителя информатики создают беспроводную ЛВС, используя технологию Wi-Fi. Кроме этого, при построении ЛВС применяется и VPN-подключение (виртуальная частная сеть), поэтому вначале будущие учителей информатики знакомятся с сетевым оборудованием, его настройками и характеристиками, после чего переходят к вопросам безопасности.

Студенты должны четко усвоить, что для беспроводной сети безопасность является столь же важным аспектом, как и для проводной. Прежде всего необходимо защитить переход из одной сети в другую, чтобы беспроводная сеть не стала потенциальным местом нежелательного проникновения в корпоративную сеть, где хранятся данные, которые ни в коем случае не должны попасть в чужие руки. Кроме того, требуется защита сети от несанкционированного доступа, также следует предотвратить простое «прослушивание» данных. Желательно, чтобы беспроводная локальная сеть, созданная на территории одной школы, вообще не была «слышна» за ее пределами.

Для защиты подобной сети, студенты учатся настраиваться VPN-сервер, брандмауэр, файловый сервер, антивирус и устанавливать права доступа, применимые к учителям и ученикам. При этом они знакомятся с основными функциями файлового сервера; создают надежную систему хранения данных, используя простейший вариант системы RAID (от англ. RAID – Rebundancy Array of Inexpensive Disks – избыточные массивы дешевых дисков) – *mirror*, так называемое «зеркало»; настраивают контроллер домена (центр авторизации пользователей), сервер корпоративного антивируса (место хранения и распространения обновлений антивируса), а также принт-сервер.

Для организации защиты информации в ЛВС студенты учатся использовать в основном стандартные средства, чаще всего распространяемые в образовательных учреждениях, такие как:

1) брандмауэр Windows;

2) «Антивирус Касперского Internet Security»;

3) Wi-Fi-роутер с защитой WPA2 PSK AES (Advanced Encryption Standard);

4) доменная система работы компьютеров;

5) VPN-сеть.

Отметим, что Wi-Fi-роутер с защитой WPA2 PSK AES (Advanced Encryption Standard) требует особых настроек, которые подробно рассматриваются в обучении. Каждое устройство сети оснащено собственным сетевым адресом MAC (Media Access Control), поэтому студенты должны прописать в роутере адреса только известных им устройств. При настройке Wi-Fi-сети они используют заранее определенные IP-адреса, которые прописывают в роутер. Кроме этого, будущие специалисты в области ИТ при настройке защищенной беспроводной сети учатся устанавливать пароль на роутер, скрывать вещание SSID (видимость сети) и устанавливать пароль на беспроводное соединение, использующего стандарт WPA2 PSK AES.

Далее, для успешной реализации ЛВС студенты настраивают пользовательские машины: выставляют IP-адреса; подключают их к беспроводной сети (ввод пароля); настраивают антивирусы; настраивают VPN-подключение.

После настройки всей беспроводной сети в целом требуется провести апробацию данной модели

и проверить устойчивость сети к попыткам взлома, чем и будут заниматься студенты на следующей дисциплине «Методы защиты информации». Одной из основных задач, решаемых студентами при атаках на сеть, – это выяснение возможных причин утечки информации. При многочисленных попытках удаленного взлома ЛВС через сеть Интернет студенты понимают, что основными причинами утечки информации служат необновленные версии операционной системы, антивирусных баз и программных модулей, откуда они делают вывод, что использование лицензионных продуктов является обязательным условием организации безопасности сети.

Также для проверки защищенности беспроводной сети и выяснения уязвимости системы студентам предлагается задание по попытке взлома сети. Причем, они должны это сделать двумя способами: первый – не имея ключа; второй – имея пароль от пользовательской машины нескольких пользователей: ученика, учителя и администратора.

В настоящее время Интернет переполнен предложениями способов взлома беспроводных сетей, но основными являются два:

1) метод ручного подбора;

2) брутфорс (от английского *brute force* — полный перебор или метод «грубой силы») – один из популярных методов взлома паролей на серверах и в различных программах.

Метод *брутфорс* заключается в том, что программа-взломщик пытается получить доступ к какой-либо программе или к сети Wi-Fi путем перебора паролей по критериям, заданным владельцем данного Wi-Fi. Способ взлома брутфорсом является достаточно долгим, но мощным, поэтому он остается на вооружении и по сей день, а с учетом все увеличивающихся мощностей компьютеров и пропускной способности интернет-каналов останется на вооружении еще на долгое время. Данный способ подбора хорош тем, что пароль взламывается, но на это может уйти много времени, поэтому, студенты понимают, что «сложный» пароль (заглавные и строчные символы, цифры, спецсимволы, немалая длина и т. п.) является одним из мощных средств защиты информации.

Будущие специалисты ИТ пытаются взломать сеть, и если это происходит (например, пароль состоит из простого набора букв), то данные, передающиеся по сети, они все равно не могут расшифровать, так как используется VPN (виртуальная сеть, защищенная паролем). Так как в Wi-Fi-роутере еще настроена адресация по IP и использованием MAC со скрытым SSID, то студенты убеждаются, что даже теоретически очень сложно взломать данную сеть. Но если вдруг злоумышленник получил доступ к одному из ноутбуков, то максимум, что он сможет сделать – это узнать имя беспроводной сети под учетной записью «Гость». Чтобы попасть в папку общего доступа на серверном компьютере, ему потребуется узнать пароль от пользователя Ученик. Для доступа к некоторым документам, журналам, научным статьям, хранящимся на сетевом диске, потребуется узнать пароль пользователя Учитель, поэтому пароли от учетных записей требуется хранить в секрете от учеников и при раскрытии такой информации требуется либо немедленная смена пароля, либо удаленная блокировка экрана с серверного компьютера. Кроме этого, студенты убеждаются, что для дополнительной защиты документов требуется устанавливать пароль на их редактирование или удаление, непосредственно в самих программах или в настройках папки общего доступа. И в последнем случае, если злоумышленник узнал пароль администратора на пользовательских машинах, то он сможет просмотреть, изменить или удалить лишь часть информации, которая находится в папке общего доступа; установить или удалить программы на пользовательском компьютере. Но для доступа к серверному компьютеру ему потребуется пароль, а он не тот, что установлен на пользовательских компьютерах. Чтобы получить логин и пароль для входа на роутер, злоумышленнику потребуется воспользоваться брутфорсом, что по времени у него займет от 1 минуты до многих лет (если пароль сложный).

Отметим, что на данной дисциплине будущие учителя информатики также знакомятся с основными криптографическими моделями, алгоритмами шифрования и аутентификации пользователей.

Следующей дисциплиной, связанной с подготовкой студентов в области информационной безопасности, является дисциплина «Информационные системы», («Распределенные информационные системы»). Одним из заданий на данной дисциплине является создание автоматизированной системы, позволяющей проводить обучение на базе сети (система дистанционного обучения) [10]. Здесь студенты должны организовать персонализацию доступа к информации пользователями и реализовать многоуровневую систему информационной безопасности. При этом в базе данных (СУБД MySQL), в соответствующих полях таблицы, где хранятся пароли пользователей, студенты ставят специальную хеш-функцию MD5, предназначенную для свертки входного массива любого размера

в битовую строку, что позволит обезопасить данные. Даже если злоумышленнику удастся взломать сервер с персональными данными, то вместо действительного пароля он увидит строку типа b10c8lb164e0544805b7e99be72e3fa5, которую необходимо будет расшифровать, на что уйдет много времени. Также на данной дисциплине они знакомятся с законодательными и морально-этическими нормами использования авторского права. Как правило, каждый из студентов регистрирует созданный им электронный образовательный ресурс в Федеральном государственном бюджетном научном учреждении «Институт управления образованием Российской академии образования» или в Роспатенте, после чего получает авторское свидетельство и информационную карту алгоритмов и программ [2; 7; 8; 12; 15 и др.], что свидетельствует о высокой степени усвоения материала в области авторского права.

Описанная методика была внедрена в процесс обучения будущих специалистов в области ИТ в АНО ВПО «Межрегиональный открытый социальный университет» и ФГБОУ ВПО «Марийский государственный университет». Результаты эксперимента доказывают положительное влияние данной методики на качество обучения студентов в области информационной безопасности. На рисунке 2 приведены результаты итогового среза студентов в области информационной безопасности. Контрольная группа (КГ) была составлена из студентов, занимающихся по традиционной системе, экспериментальную группу (ЭГ) составляли студенты, занимающиеся по описанной выше методике.

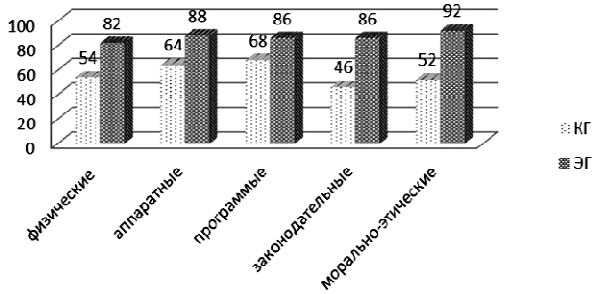

Рис. 2. Сравнительная характеристика уровня сформирпованности компетенций студентов в области информационной безопасности

Результаты итогового среза были обработаны методами математической статистики с помощью автоматизированной системы анализа результатов психолого-педагогических исследований [5]. Результаты проверки доказывают эффективность описанной методики обучения.

1. Бояров Е. Н. Концептуальные подходы к обучению специалиста информационной безопасности в университете: автореф. дис. ... канд. пед. наук. СПб., 2008. 151 с.

2. Васильев В. Г., Никитин П. В. Технологии скринкастинга: от теории до практики: электронное учебно-методическое пособие // Хроники объединенного фонда электронных ресурсов «Наука и образование». 2014. № 12. С. 98.

3. Галатенко В. А. Основы информационной безопасности. М.: Бином. Лаборатория знаний, 2012. 205 с.

4. Гафнер В. В. Информационная безопасность. Ростов-на-Дону: Феникс, 2010. 324 с.

5. Горохова Р. И., Никитин П. В. Возможности современных информационных технологий в педагогических исследованиях // Образовательные технологии и Общество (Educational Technology & Society): международный электронный журнал , 2012. Т. 15. № 2. С. 317–337. URL: http://ifets.ieee.org/russian/periodical/journal.html

6. Гриншкун В. В., Димов Е. Д. Принципы отбора содержания для обучения студентов вузов технологиям защиты информации в условиях фундаментализации образования // Вестник Российского университета дружбы народов. Сер. «Информатизация образования». 2012. № 3. С. 38–45.

7. Зайков А. С., Никитин П. В. Комплект учебно-методических материалов (компьютерные мотивационные игры) // Хроники объединенного фонда электронных ресурсов «Наука и образование». 2014. № 12. С. 97.

8. Захаров А. С., Никитин П. В., Фоминых И. А. Электронный образовательный ресурс «Кодирование информации» // Хроники объединенного фонда электронных ресурсов «Наука и образование». 2014. № 12. С. 94.

9. Никитин П. В. Организация индивидуального обучения будущих учителей информатики с применением современных информационных технологий // Образовательные технологии и Общество (Educational Technology & Society): международный электронный журнал , 2014. Т. 17. № 3. С. 569–583. URL: http://ifets.ieee.org/russian/periodical/journal.html

10. Никитин П. В., Мельникова А. И., Горохова Р. И. К вопросу о формировании предметных компетенций в области информационных технологий будущих учителей информатики // Вестник Московского государственного областного университета: электронный журнал . 2013. № 4. URL: http://www.evestnik-mgou.ru/Articles/View/487

11. Никитин П. В., Фоминых И. А., Горохова Р. И. Использование интеллектуальной обучающей системы при обучении студентов информационным технологиям // Вестник ИрГТУ, 2015. № 3. С. 24–30.

12. Подыганов А. С., Никитин П. В. Веб-технологии: от теории до практики: электронное учебно-методическое пособие // Хроники объединенного фонда электронных ресурсов «Наука и образование». 2014. № 12. С. 95.

13. Поляков В. П. Методическая система обучения информационной безопасности студентов вузов: автореф. дис. ... д-ра пед. наук. Н. Новгород, 2006. 47 с.

14. Федеральный государственный образовательный стандарт основного общего образования // Министерство образования и науки Российской Федерации. URL: минобрнауки.рф/документы/938/

15. Чешуина Н. В., Никитин П. В., Фоминых И. А. Электронный образовательный ресурс «Массивы: определение, задания, сортировка» // Хроники объединенного фонда электронных ресурсов «Наука и образование». 2014. № 12. С. 96.

1. Boyarov E. N. Kontseptual'nye podkhody k obucheniyu spetsialista informatsionnoi bezopasnosti v universitete: avtoref. dis. ... kand. ped. nauk, SPb., 2008, 151 p.

2. Vasil'ev V. G., Nikitin P. V. Tekhnologii skrinkastinga: ot teorii do praktiki: elektronnoe uchebno-metodicheskoe posobie, *Khroniki ob"edinennogo fonda elektronnykh resursov «Nauka i obrazovanie»*, 2014, No. 12, pp. 98.

3. Galatenko V. A. Osnovy informatsionnoi bezopasnosti, M.: Binom. Laboratoriya znanii, 2012, 205 p.

4. Gafner V. V. Informatsionnaya bezopasnost'. Rostov-na-Donu: Feniks, 2010, 324 p.

5. Gorokhova R. I., Nikitin P. V. Vozmozhnosti sovremennykh informatsionnykh tekhnologii v pedagogicheskikh issledovaniyakh, *Obrazovatel'nye tekhnologii i Obshchestvo* (*Educational Technology & Society*)*: mezhdunarodnyi elektronnyi zhurnal*, 2012, t. 15, No. 2. pp. 317–337. URL: http://ifets.ieee.org/russian/periodical/journal.html

6. Grinshkun V. V., Dimov E. D. Printsipy otbora soderzhaniya dlya obucheniya studentov vuzov tekhnologiyam zashchity informatsii v usloviyakh fundamentalizatsii obrazovaniya, *Vestnik Rossiiskogo universiteta druzhby narodov*, Ser. «Informatizatsiya obrazovaniya», 2012, No. 3, pp. 38–45.

7. Zaikov A. S., Nikitin P. V. Komplekt uchebno-metodicheskikh materialov (komp'yuternye motivatsionnye igry), *Khroniki ob"edinennogo fonda elektronnykh resursov «Nauka i obrazovanie»*, 2014, No. 12, p. 97.

8. Zakharov A. S., Nikitin P. V., Fominykh I. A. Elektronnyi obrazovatel'nyi resurs «Kodirovanie informatsii», *Khroniki ob"edinennogo fonda elektronnykh resursov «Nauka i obrazovanie»*, 2014, No. 12, p. 94.

9. Nikitin P. V. Organizatsiya individual'nogo obucheniya budushchikh uchitelei informatiki s primeneniem sovremennykh informatsionnykh tekhnologii, *Obrazovatel'nye tekhnologii i Obshchestvo* (*Educational Technology & Society*)*: mezhdunarodnyi elektronnyi zhurnal*, 2014, t. 17, No. 3, pp. 569–583, URL: http://ifets.ieee.org/russian/periodical/journal.html

10. Nikitin P. V., Mel'nikova A. I., Gorokhova R. I. K voprosu o formirovanii predmetnykh kompetentsii v oblasti informatsionnykh tekhnologii budushchikh uchitelei informatiki, *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta: elektronnyi zhurnal,* 2013, No. 4,URL: http://www.evestnik-mgou.ru/Articles/View/487

11. Nikitin P. V., Fominykh I. A., Gorokhova R. I. Ispol'zovanie intellektual'noi obuchayushchei sistemy pri obuchenii studentov informatsionnym tekhnologiyam, Vestnik IrGTU, 2015, No. 3, pp. 24–30.

12. Podyganov A. S., Nikitin P. V. Veb-tekhnologii: ot teorii do praktiki: elektronnoe uchebno-metodicheskoe posobie, *Khroniki ob"edinennogo fonda elektronnykh resursov «Nauka i obrazovanie»*, 2014, No. 12, p. 95.

13. Polyakov V. P. Metodicheskaya sistema obucheniya informatsionnoi bezopasnosti studentov vuzov: avtoref. dis. ... d-ra ped. nauk, N. Novgorod, 2006, 47 p.

14. Federal'nyi gosudarstvennyi obrazovatel'nyi standart osnovnogo obshchego obrazovaniya // Ministerstvo obrazovaniya i nauki Rossiiskoi Federatsii, URL: minobrnauki.rf/dokumenty/938/

15. Cheshuina N. V., Nikitin P. V., Fominykh I. A. Elektronnyi obrazovatel'nyi resurs «Massivy: opredelenie, zadaniya, sortirovka», *Khroniki ob"edinennogo fonda elektronnykh resursov «Nauka i obrazovanie»*, 2014, No. 12, p. 96.

Статья поступила в редакцию 20.09.2015 г

UDK 378

P. V. Nikitin[1], I. V. Farkhshatov[1], M. V. Litvinenko[2]

[1]Interregional Open Social Institute, Yoshkar-Ola
[2]Mari State University, Yoshkar-Ola

GAME TECHNOLOGIES AS A FACTOR FOR INCREASE THE MOTIVATION OF LEARNING COMPUTER SCIENCE

The article describes a technique of training of future specialists in the field of information technology (IT), including the future teachers, computer science basics of information security based on a multidisciplinary approach, practice-oriented tasks and method of demos developed by the authors in accordance with modern trends in the field of information security. The article reveals the concept of "information security" as the security of the information and supporting infrastructure against accidental or intentional, natural or man-made influences that can harm the owner or user of the information and supporting infrastructure. As a result of study, as described in the article, students will learn the basic information threat of unauthorized access to the path information leakage channels, as well as the classification of methods and means of information security. The article describes in detail the practical tasks on each of the disciplines (computer software, information technology, computer networks, Internet and multimedia technologies, computer networks and information systems, methods of information protection) included in the methodological training system of this specialization, and developed by the authors based on current trends in the field of information technology and information security. The technique described in the study has been implemented in the process of training of future specialists in the field of information security, including the future teachers of computer science, in the Interregional Open Social University, and Mari State University. The experimental results have a positive impact on the quality of this method of training students in the field of information security (formal (physical, hardware, software) and informal (organizational, legal, moral and ethical)).

Keywords: methods of teaching computer science, information security, network threats, network security, internet access, methods of hacking.