О НЕОБХОДИМОСТИ ПРЕПОДАВАНИЯ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» НА ГУМАНИТАРНЫХ ФАКУЛЬТЕТАХ ВУЗОВ

СИМАВОРЯН С. Ж.

NECESSITY OF INFORMATION SECURITY TEACHING AT HUMANITARIAN FACULTIES OF HIGHER EDUCATIONAL ESTABLISHMENT

SIMAVORYAN S. ZH.

The article brings in Internet cyber threats analysis. Wide use of IT-equipment by students demands their regular protection against unauthorized access to the stored and processed information. Authors state that this problem can be solved by students' information security increase.

В данной статье приводится анализ киберугроз в сети интернет. Широкое использование средств ВТ студентами требует их регулярной защиты от несанкционированного доступа к хранимой и обрабатываемой в них информации. Авторы утверждают, что эту задачу можно решить путем расширения грамотности студентов в области информационной безопасности.

Keywords: cyber threat, information security, teaching, humanitarian faculty.

Ключевые слова: киберугроза, защита информации, информационная безопасность, преподавание, гуманитарный факультет.

УДК 004.78

На сегодняшний день стало совершенно ясно, что Интернет имеет большой потенциал, предоставляет новые возможности улучшения высшего и среднего образования. Интернет – довольно сложный механизм, для пользования которым нужны навыки пользования, умение обращаться с информацией и, что самое главное, постоянно защищаться от всех угроз, идущих из Интернета. Вопросу использования Интернета в вузах уже несколько лет уделяют внимание специалисты самого разного уровня. Все они единодушно сходятся во мнении, что Интернет стимулирует процесс развития интеллектуальных способностей и самостоятельного мышления студентов, предоставляя массу дополнительной информации. В то же время отмечается, что Интернет является лишь средством в учебном процессе и использование Интернет-технологий должно полностью контролироваться пользователем, при этом к пользователю предъявляются следующие требования: компьютерная грамотность и знание Интернет-технологий, организация работы по поиску и анализу необходимой информации, а также контроль за доступом к информации (пользователь должен уметь защищать информацию, хранящуюся в его компьютере, и не стать инструментом в руках киберпреступников).

Использование Интернета только в качестве инструмента образования не защищает пользователя от киберугроз. Заведя ICQ для переписки с одногруппниками (одноклассниками), студент с той же легкостью может оказаться жертвой спам-атаки или киберпреследования, как и человек, использующий мессенджеры для развлечения.

Информированность о виртуальных угрозах требуется всем, кто взаимодействует с Интернетом, вне зависимости от ресурсов, которые он посещает. Конечно, риск подхватить компьютерный вирус у пользователя, посещающего электронные библиотеки меньше, чем у посетителя порносайтов, но полностью исключать подобную возможность нельзя.

Например, многие преподаватели пользуются электронной почтой для связи со студентами. Иногда их электронные адреса публикуются на сайтах вузов или студенческих форумах. Этим может воспользоваться злоумышленник, замаскировавшись под студента: отправить письмо с вредоносным вложением, носящим безобидное название «моя курсовая работа». Киберпреступник, ориентированный на получение крупной материальной прибыли, конечно, скорее взломает базу адресов крупной компании. А вот злопамятный студент, обладающий навыками программирования, вполне может попытаться «отомстить» за собственную некомпетентность в изучаемом предмете, на которую Вы ему указали. Перестать открывать письма студентов из боязни перед их содержимым – означает потерять одно из преимуществ использования Интернет коммуникаций в процессе обучения. Намного лучше уметь защищать свой компьютер от угроз извне.

1. Анализ киберугроз в 2009–2010 годах.

Развитие информационных технологий в 2009-2010 гг. всецело было направлено на повышение эффективности работы в условиях экономического кризиса, практически охватившего все сферы экономики. Но, к сожалению, по данным МВД России с развитием информационных технологий увеличилась киберпреступность [3, 6, 7]. Деятельность киберпреступников была сконцентрирована на «зарабатывании» денег (можно сказать, на мошенническом зарабатывании денег). Поскольку в жестких экономических условиях люди стали относиться к своим финансам более внимательно и осторожно, для того чтобы заставить их раскошелиться, злоумышленникам пришлось разрабатывать новые программы обмана людей. Прежде всего стоит отметить, что вредоносные программы стали более интеллектуальными и самостоятельными. Такие программы могут обходить системы антивирусной защиты, определять установленные на компьютер операционную систему, браузер или другое ПО, необходимое для их работы. Например, так называемые браузерные баннеры продемонстрировали достаточно широкий радиус поражения браузеров, включая Internet Explorer, Mozilla, Firefox и Opera. Как поясняют эксперты, эти программы распространяются с сайтов, содержащих скрипты, которые определяют используемую программную среду и в зависимости от этого производят загрузку соответствующей вредоносной программы. После активизации подобных приложений на экране компьютера появляется «баннер», который из-за своих размеров практически парализует работу браузера. Для удаления этого «баннера» требуется отправить платное SMS-сообщение. Быстрый и удобный способ оплаты товаров и услуг с помощью SMS-сообщений также успешно использовался блокировщиками Windows (Trojan, Winlock). Упрекнув пользователя в незаконном использовании операционной системы или другого ПО, блокировщики требовали от жертвы отправить платное SMS для восстановления работоспособности системы. Еще одним ярким примером программы-вымогателя стал Trojan.Encoder, который при попадании в систему шифрует документы пользователя, после чего предлагает заплатить автору вируса за получение утилиты дешифровки. В целом, как отмечают эксперты, троянские программы-вымогатели стали одним из самых популярных видов вредоносных программ 2009–2010 гг. Начиная с мая 2009 года, стало увеличиваться число фальшивых антивирусов. Данные программы имитируют работу антивирусных программ, сообщая пользователю об обнаруженных угрозах, после чего предлагают вылечить систему или приобрести полную версию продукта. Для распространения псевдоантивирусов мошенники, как правило, используют спам-рассылки, взломанные сайты и рекламу в интернете. Фальшивые антивирусные программы остаются привлекательным источником доходов для вирусописателей в силу простоты их разработки, отлаженной системы распространения и высоких доходов. Наверняка они получат распространение и в будущем году. Помимо троянских программ, широкую известность в 2010 г. приобрели сетевые черви, использующие уязвимости Windows-систем. Несмотря на предпринятые производителем популярной ОС меры по выпуску соответствующих патчей, активность этого вредоносного семейства на сегодняшний

день остается на достаточно высоком уровне.

В течение 2009 г. изменялись и совершенствовались средства распространения вирусов, а также способы их сокрытия в системе. Вирусописатели продолжили эксперименты в области социальной инженерии, где наиболее удачными примерами стали массовые атаки на пользователей социальных сетей. В течение этого года было зарегистрировано множество атак на социальные сети во всем мире, в том числе и на российские «В Контакте» и «Одноклассники». Одним из последних громких событий стала атака на социальную сеть «В Контакте», в результате которой в руки злоумышленников попали десятки тысяч аккаунтов. Применение руткит-технологий для всевозможных способов защиты от обнаружения антивирусными средствами стало одним из основных направлений развития вредоносных программ. Самые последние модификации руткита Backdoor способны обходить практически все современные поведенческие анализаторы. По версии компании Dr.Web в 2009 г. в почтовом трафике были обнаружены такие вредоносные программы, как:

1. Trojan.DownLoad.47256
2. Win32.HLLM.Beagle
3. Trojan.DownLoad.36339
4. Trojan.Fakealert.5115
5. Trojan.DownLoad.37236
6. Win32.HLLM.MyDoom.33808
7. Trojan.Fakealert.5238
8. Trojan.Packed.683
9. Trojan.MulDrop.40896
10. Trojan.PWS.Panda.122
11. Win32.HLLM.MyDoom.based
12. Trojan.DownLoad.50246
13. Win32.HLLM.MyDoom.44
14. Trojan.Botnetlog.9
15. Trojan.Packed.2915
16. Trojan.MulDrop.19648
17. Win32.HLLM.Netsky.based
18. Trojan.Fakealert.5825
19. Trojan.Fakealert.5356
20. Win32.HLLM.Netsky.35328

А на компьютерах пользователей были обнаружены такие вредоносные программы, как:

1. Trojan.DownLoad.47256
2. Win32.HLLW.Gavir.ini
3. Win32.HLLW.Shadow.based
4. Win32.HLLM.Beagle
5. Trojan.Fakealert.5115
6. Trojan.DownLoad.36339
7. Win32.HLLM.Generic.440
8. Trojan.Fakealert.5238
9. DDoS.Kardraw
10. Win32.HLLM.Netsky.35328
11. JS.Nimda
12. Win32.Virut.14
13. Trojan.MulDrop.16727
14. Trojan.Botnetlog.9
15. Win32.Virut.5
16. Win32.HLLW.Autoruner.5555
17. W97M.Thus
18. Win32.Alman
19. Win32.Sector.17
20. Win32.HLLM.MyDoom.49.

По мнению вирусных аналитиков, в 2009 г. вредоносные программы развивались в двух направлениях:

1) к финансовой цели, что привело к продолжению работ над мошенническими и шпионскими программами;

2) к большему охвату операционных систем и браузеров, что продолжило разработку новых руткит-технологий и усовершенствование приемов из области социнженерии. Эксперты считают, что рост популярности смартфонов будет подогревать интерес злоумышленников к соответствующим мобильным платформам. Вместе с тем, на сегодняшний день доля вредоносных программ в общем объеме вредоносного трафика невелика, и в силу многообразия мобильных платформ в ближайшее больших потрясений не ожидается.

2010 г. ознаменовался значительным ростом активности эксплуатации уязвимости CVE-2010-2568 [5]. Она используется как нашумевшим в конце июля сетевым червем Worm.Win32.Stuxnet, так и троянцем-дроппером, устанавливающим на зараженный компьютер последнюю модификацию заражающего вируса Sality – Virus.Win32.Sality.ag. Как и ожидалось, злоумышленники сразу же «взяли в оборот» новую дыру в наиболее популярной в настоящее время версии ОС Microsoft Windows. Но уже второго августа Microsoft был выпущен патч MS10-046, закрывающий уязвимость. Это обновление идет с пометкой «Critical», что означает обязательную установку всем пользователям системы.

На компьютерах пользователей обнаружены следующие вредоносные программы:

1. В первой таблице представлен TOP 20 вредоносных и потенциально нежелательных программ, которые были обнаружены и обезврежены на компьютерах пользователей.

Позиция	Вредоносная программа	Количество зараженных компьютеров
1	Net-Worm.Win32.Kido.ir	280087
2	Virus.Win32.Sality.aa	172770
3	Net-Worm.Win32.Kido.ih	153825
4	Net-Worm.Win32.Kido.iq	107156
5	Trojan.JS.Agent.bhr	106796
6	Exploit.JS.Agent.bab	90465
7	Worm.Win32.FlyStudio.cu	75394
8	Virus.Win32.Virut.ce	68010
9	Exploit.Win32.CVE-2010-2568.d	52193
10	Trojan-Downloader.Win32.VB.eql	48440
11	P2P-Worm.Win32.Palevo.arxz	42145
12	Exploit.Win32.CVE-2010-2568.b	40385
13	Worm.Win32.Mabezat.b	38252
14	Worm.Win32.VBNA.b	37461
15	AdWare.WinLNK.Agent.a	37240
16	Virus.Win32.Sality.ag	36144
17	Trojan-Dropper.Win32.Sality.r	32352
18	Trojan.Win32.Autoit.ci	31391
19	Trojan-Dropper.Win32.Flystud.yo	29475
20	Packed.Win32.Krap.ao	29309

Сетевой червь Kido (1-е, 3-е, 4-е место) и заражающие вирусы Virus.Win32.Virut.ce (8-е место), Virus.Win32.Sality.aa (2-е место) уверенно удерживают свои позиции. Это же относится и к эксплойтам, эксплуатирующим уязвимость CVE-2010-0806 – Trojan.JS.Agent.bhr (5-е место) и Exploit.JS.Agent.bab (6-е место). Новая уязвимость LNK-ярлыков Windows обозначена как CVE-2010-2568. Эта уязвимость стала популярной у злоумышленников: в рейтинг попали сразу три зловреда, так или иначе связанные с CVE-2010-2568. Два из них – эксплойты Exploit.Win32.CVE-2010-2568.d (9-е место) и Exploit.Win32.CVE-2010-2568.b (12-е место), непосредственно эксплуатирующие уязвимость. Третий, Trojan-Dropper.Win32.Sality.r (17-е место), использует эту уязвимость для своего

распространения. Он генерирует уязвимые LNK-ярлыки с названиями, привлекательными для пользователей, и распространяет их по локальной сети. Когда пользователь открывает папку, содержащую такой ярлык, происходит запуск зловреда. Основная задача Trojan-Dropper.Win32.Sality.r – установить в систему последнюю модификацию заражающего вируса Sality-Virus.Win32.Sality.ag (16-е место).

Что интересно, оба эксплойта к уязвимости CVE-2010-2568, попавшие в рейтинг, чаще всего детектируются на компьютерах пользователей в России, Индии и Бразилии. Если Индия – это основной источник распространения червя Stuxnet (первого зловреда, использующего данную уязвимость), то с Россией не все понятно.

Географическое распределение Trojan-Dropper.Win32.Sality.r аналогично распределению эксплойтов и приводится на рис. 1 [5].

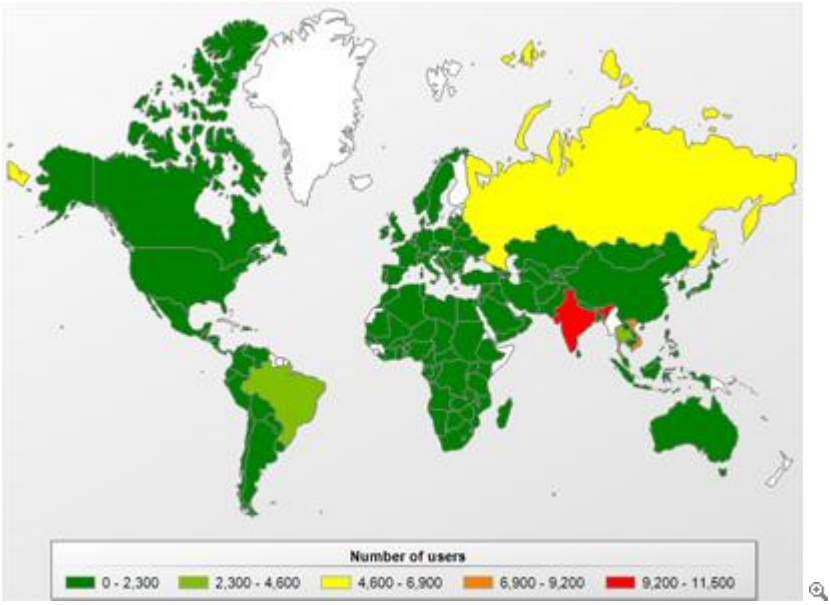

Рис. 1. Географическое распределение срабатываний на эксплойт Explot.Win32.CVE-2010-2568.d

Еще один новичок рейтинга – очередной представитель рекламных программ. На этот раз в TOP 20 попал AdWare.WinLNK.Agent.a (15-е место). Он представляет собой ярлык, при запуске которого происходит переход по рекламной ссылке. Сам ярлык устанавливается различными рекламными программами.

В рейтинге появился новый представитель зловредов, использующих скриптовый язык AutoIt – Trojan. Win32. Autoit.ci (18-е место). Попала в двадцатку и новая модификация P2P-червя Palevo – P2P-Worm.Win32.Palevo.arxz (11-е место). Оба семейства мы описывали в предыдущих обзорах. Они выполняют множество деструктивных действий: в частности, прописываются в автозагрузку, пытаются скачать и запустить другие вредоносные программы, распространяются через локальную сеть.

Попали в рейтинг и два представителя вредоносных упаковщиков: Packed. Win32. Krap.ao (20-е место), Worm.Win32.VBNA.b (14-е место). Оба они защищают упакованные зловреды от детектирования. А упаковывать они могут практически любые вредоносные программы, начиная от фальшивых антивирусов и кончая мощными бэкдорами, такими, как Backdoor.Win32.Blakken.

2. Вторая таблица характеризует обстановку в интернете. В этот рейтинг попадают вредоносные программы, обнаруженные на веб-страницах, а также те зловреды, которые пытались загрузиться с веб-страниц на компьютеры пользователей.

Позиция	Вредоносная программа	Число уникальных попыток загрузки
1	Trojan-Downloader.Java.Agent.ft	135755
2	Exploit.JS.Agent.bab	127561
3	Exploit.HTML.CVE-2010-1885.a	85502
4	Trojan.JS.Agent.bhr	67061
5	AdWare.Win32.FunWeb.ds	60129
6	Exploit.HTML.CVE-2010-1885.c	57988
7	AdWare.Win32.FunWeb.di	50928
8	AdWare.Win32.FunWeb.q	50504
9	Exploit.HTML.HCP.b	46874
10	Exploit.Java.CVE-2010-0886.a	45844
11	Trojan-Downloader.VBS.Agent.zs	37578
12	Trojan.JS.Redirector.cq	37479
13	Trojan-Clicker.JS.Iframe.fq	35181
14	AdWare.Win32.FunWeb.ci	33073
15	Exploit.Java.CVE-2010-0094.a	30062
16	Exploit.JS.Pdfka.cop	29588
17	Exploit.HTML.CVE-2010-1885.d	28396
18	Exploit.JS.CVE-2010-0806.b	26990
19	AdWare.Win32.FunWeb.fb	26350
20	Exploit.HTML.CVE-2010-1885.b	25820

В таблице приведены двадцать уязвимостей, из которых двенадцать эксплойтов, которые относятся к шести разным уязвимостям.

Наибольшую популярность у злоумышленников снискала уязвимость CVE-2010-1885. Ее используют сразу пять эксплойтов из TOP 20: Exploit.HTML.CVE-2010-1885.a (3-е место), Exploit.HTML.CVE-2010-1885.c (6-е место), Exploit.HTML.HCP.b (9-е место), Exploit.HTML.CVE-2010-1885.d (17-е место) и Exploit.HTML.CVE-2010-1885.b (20-е место). Уязвимость CVE-2010-1885 использует недоработку в центре справки и поддержки Windows и позволяет исполнять вредоносный код на системах Windows XP и Windows 2003. По-видимому, популярность этих систем и привела к росту числа эксплойтов для этой бреши в MS Windows.

По популярности вслед за уязвимостью CVE-2010-1885 следует CVE-2010-0806, которая не собирается сдавать своих позиций. Ее используют три разных

эксплойта из TOP 20: два скрипта, известные нам по предыдущим двадцаткам, – Exploit.JS.Agent.bab (2-е место) и Trojan. JS.Agent.bhr (4-е место) – и новичок рейтинга Exploit.JS.CVE-2010-0806.b (18-е место).

Еще три эксплойта из TOP 20 используют уязвимости в ПО, работающем на движке Java. Первое место занимает эксплойт Trojan-Downloader.Java.Agent.ft, который использует довольно старую уязвимость CVE-2009-3867. Exploit.Java.CVE-2010-0886.a (10-е место), эксплуатирующий соответственно CVE-2010-0886. Интересно, что в августе 2010 г. появился первый эксплойт к уязвимости CVE-2010-0094, обнаруженной еще в начале апреля 2010 г. В Exploit.Java.CVE-2010-0094.a (15-е место) происходит ряд вызовов функций, которые в конечном итоге приводят к выполнению вредоносного кода, его графическое распространение приводится на рис. 2 [5].

Этот эксплойт в августе использовался злоумышленниками только в развитых странах – США, Германии, Великобритании. Возможно, это связано с тем, что в этих странах популярны программы, использующие Java.

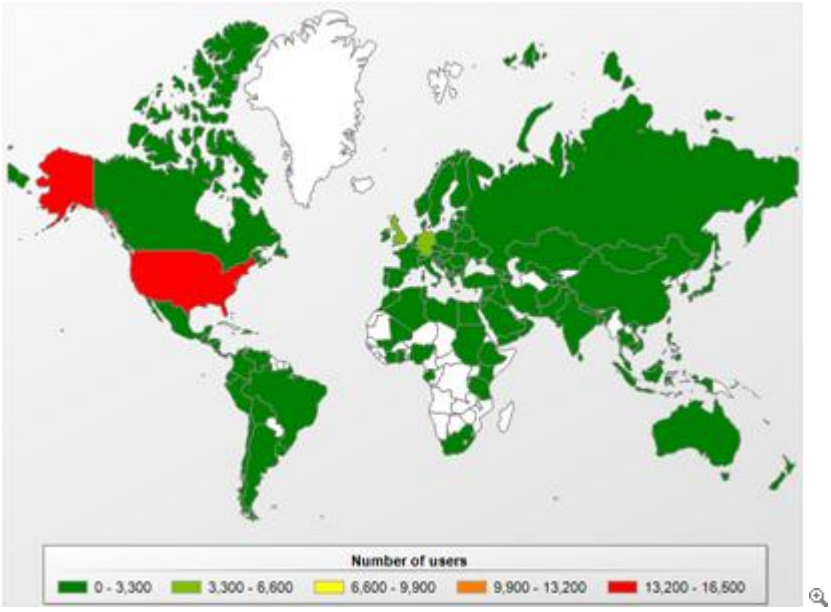

Рис. 2. Географическое распространение Exploit. Java.CVE-2010-0094.a

Еще один эксплойт – Exploit. JS.Pdfka.cop (16-е место) – довольно обычный и использует особенности PDF-документа для выполнения зловредного кода.

Новичок рейтинга Trojan-Clicker. JS.Iframe.fq (13-е место) относится к категории вредоносных скриптов, перенаправляющих браузер жертвы по вредоносной ссылке с помощью HTML-тэга “<iframe>”. Еще два вредоносных скрипта – Trojan-Downloader.VBS.Agent.zs (11-е место) и Trojan.JS.Redirector.cq (12-е место) – также заслуживают особого внимания.

Не теряют своей популярности рекламные программы. AdWare.Win32.-FunWeb вытеснила своих июльских конкурентов Shopper.l и Boran.z. В августе 2010 г. сразу пять представителей семейства FunWeb попали в двадцатку. Из них три модификации – “ds”, “ci”, “q” (5-е, 14-е и 8-е место соответственно), а “fb” и “di” (19-е и 7-е место).

2. Решение задачи борьбы с киберпреступностью.

Проблему противодействия кибер-угрозам необходимо решать сразу на трех уровнях [4]. Так, на уровне государства киберпреступность должна снижаться за счет принятия законодательных актов. В первую очередь это касается ужесточения наказания за подобные преступления. Сейчас оно непростительно мягкое – 2–3 года лишения свободы, в отличие от других стран, где за такие нарушения полагается 10–15 лет заключения с конфискацией имущества, такое неадекватно слабое наказание поощряет

преступника к повторным действиям, более изощренным. Кроме того, на уровне государства должны решаться вопросы о том, какой контент можно определить как «нежелательный» или «спорный». В рамках правовой системы в МВД России предлагают сделать эту функцию предметом рассмотрения суда, а не отдавать на откуп властных структур.

Второй уровень противодействия киберпреступникам – уровень провайдера. По мнению «Лаборатории Касперского», именно провайдеры должны заниматься фильтрацией трафика от вирусов и спама, как входящего, так и, что немаловажно, исходящего. В случае, если от пользователя идет зараженный трафик, он должен быть заблокирован до того момента, пока его компьютер не будет вылечен. Здесь провайдерам необходимо самостоятельно фильтровать так называемый «спорный и нежелательный контент», к которому в первую очередь относятся сайты с детской порнографией, сайты, пропагандирующие фашизм, экстремизм, религиозную или расовую ненависть.

Во-первых, доступ к нежелательным адресам можно блокировать с помощью специальных программ. Как правило, этот способ применяется в учебных заведениях, но он не гарантирует стопроцентной защиты, поскольку злоумышленники моментально создают новые сайты.

Более действенная мера – прекращение работы самого ресурса. Солидные провайдеры при заключении договора, как правило, включают в соглашение пункт, предусматривающий закрытие сайтов запрещенного содержания, например, электронные письма с угрозами; угрожающие (неприличные) сеансы мгновенных сообщений; агрессивные сообщения по мобильной связи; вебсайты, созданные, чтобы осмеивать других; отправление сообщения от лица другого человека; пересылка личных сообщений, фотографий или видеосъемок другим пользователям. Прекратить работу сайта можно также по решению суда, правда, это более длительная процедура.

На третьем уровне борьбы с киберпреступностью должны стоять сами пользователи и общественные организации, в том числе вузы и другие учебные заведения. Их задача – грамотное обучение основам информационной безопасности при пользовании компьютером.

Защищаться и быть защищенным в сети Интернет – неотъемлемое конституционное право каждого гражданина России, который имеет право на защиту от агрессивного контента, от злоумышленников любых мастей.

Современное развитие средств вычислительной техники, их разнообразие и доступность по цене позволили практически каждому студенту иметь дома собственный компьютер. Известно, что каждый студент по-разному воспринимает и осваивает знания, связанные с защитой персональных данных, хранящихся в собственном компьютере. Так, например, дисциплина «Информационная безопасность» в СГУТиКД преподается лишь только на факультете информационных технологий и математики. Студенты данного факультета по окончании вышеназванного курса становятся грамотными специалистами в области защиты информации.

Цель изучения дисциплины – приобретение студентами теоретических знаний и практических навыков по организационному обеспечению защиты информации.

Данный курс является одним из основных курсов специальной профессиональной подготовки специалистов в области защиты информации и информационной безопасности и связан с правовыми, экономическими и техническими дисциплинами по теории и методологии защиты информации.

Компьютеризация общества, внедрение и развитие новейших информационных и телекоммуникационных технологий позволяют по-новому взглянуть на образовательный процесс в гуманитарных факультетах, а именно: наряду с преподаванием некоторых предметов по математике и информатике необходимо преподавать и предмет по защите информации и информационной безопасности.

Информационная безопасность является одной из новых дисциплин, преподаваемых на базе высшего и среднего профессионального образования. Данная дисциплина достаточно сложная и объемная, поэтому использование информационных технологий дает возможность студентам осваивать материал в

соответствии с их индивидуальными возможностями и запросами, а преподавателю позволяет:

- сократить время на изложение теоретического материала;
- повысить глубину и прочность знаний, уровень развития учащихся;
- индивидуализировать и дифференцировать процесс обучения;
- стимулировать познавательную активность и самостоятельность;
- активизировать развитие творческих способностей учащегося.

Под информационной технологией обучения понимают совокупность форм организации взаимодействия преподавателя и обучаемого в рамках учебного процесса на базе ВТ, комплекс программно-инструментальных средств ЭВМ в поддержку этого взаимодействия и методику его использования.

В СГУТиКД на факультете ФИТиМ учебный процесс преподавания дисциплины «Информационная безопасность» строится как единый цикл занятий, каждое из которых предполагает использование той или иной информационной технологии, включающий электронные учебники, обучающие компьютерные программы, мультимедийные презентации, лабораторные и практические работы с использованием ПК, видеофильмы, материалы для интерактивной доски. Преподаваемые таким образом занятия дают возможность студентам ФИТиМа самостоятельно изучать теоретический материал, приобретать практические навыки по защите информации одновременно с получением теоретических знаний, повторять практические действия необходимое для каждого студента количество раз, использовать для закрепления и повторения материала презентации уроков, совершенствовать свои умения и навыки по организации защиты информации.

Представленные выше факторы дают возможность усилить интерес к преподаваемой дисциплине, выявить наиболее заинтересованных обучающихся студентов, усилить наглядность дисциплины и повысить качество обучения, повысить качество полученных практических навыков, предоставить возможность индивидуального обучения каждого студента.

Таким образом, преподавание дисциплины «Информационная безопасность» на всех факультетах вуза действительно является актуальным и экономически востребованным предметом. Не зря в народе говорится: «Защищен – значит, вооружен».

Литература

1. Галанов А.Б. Система действий ученика и учителя на уроке с использованием телекоммуникационных технологий // Интернет-журнал «Эйдос». 2005. 29 апр. http://www.eidos.ru/journal/2005/0529-03.htm (дата обращения 10.11.2010).
2. Зайцева О.Б. Информационная компетентность учителя образовательной области «Технология». Педагогика № 7. 2004.
3. Режим доступа: www.mvd.ru/news/27701/ (дата обращения 10.11.2010).
4. Режим доступа: http://www.sdteam.com/4/?start=140 (дата обращения 10.11.2010).
5. Режим доступа: http://www.securelist.com/ru/analysis/208050651/Reyting_ vredonosnykh_programm_avgust_2010 (дата обращения 10.11.2010).
6. Режим доступа: http:// www.whatis.ru/razn/razn34.shtml (дата обращения 10.11.2010).
7. Режим доступа: http:// www.inosmi.ru/social/20101007/16343… (дата обращения 10.11.2010).

Сведения об авторе:

Симаворян Симон Жоржевич, канд. тех. наук, доцент кафедры общей математики СГУТиКД (Сочи).