А. А. Зубрилин, К. Ю. Терешкина,
Мордовский государственный педагогический институт им. М. Е. Евсевьева, г. Саранск

ОСОБЕННОСТИ ОБУЧЕНИЯ БАКАЛАВРОВ ПЕДАГОГИЧЕСКОГО ОБРАЗОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

Аннотация
В статье приводится авторское видение обучения информационной безопасности бакалавров педагогического образования. Выделяется то содержание, которое должно быть усвоено ими в ходе изучения одноименной дисциплины.
Ключевые слова: информационная безопасность, информационные угрозы, педагогическое образование, бакалавриат, практические занятия.

Телекоммуникационные технологии, незаметно войдя в нашу жизнь, существенно видоизменили информационную деятельность пользователей: ускорился обмен сообщениями, стало проще находить информацию, принимать участие в различных мероприятиях, совершать онлайн-платежи — и все это без непосредственного физического контакта. Перемещение в пространстве для пользователей сейчас уже не является обязательным, чтобы решить ту или иную задачу. В то же время современные пользователи перестают задумываться над теми проблемами, с которыми они могут столкнуться в виртуальной реальности под названием Интернет [2, 3]. Они беспечно вводят свои паспортные или учетные данные, номера телефонов на сайты, которые, по их мнению, помогут заработать или получить необходимую информацию. В результате необдуманных действий происходит утечка конфиденциальной информации, а сам пользователь становится жертвой злоумышленников. Указанная проблема решается разными способами. Так, чтобы обучить пользователей безопасной работе с информационными ресурсами в сети Интернет и на персональном компьютере, в высших учебных заведениях вводится специальная дисциплина либо даже профиль (например, «Информационная безопасность», «Организация и технология защиты информации», «Информационная безопасность телекоммуникационных систем»), где студенты знакомятся с информационными угрозами и обучаются находить способы их предотвращения или предупреждения. В идеале обучать информационной безопасности нужно комплексно, в смежных дисциплинах [4].

Актуален, на наш взгляд, вопрос о том, *какими знаниями и умениями в области информационной безопасности должны обладать бакалавры педагогического образования как педагоги, готовые обучать подрастающее поколение в школах безопасной работе с информационными ресурсами*. В настоящей статье мы покажем собственное видение подготовки бакалавров педагогического образования в отмеченной области деятельности человека.

Проведя анализ дисциплин, изучаемых бакалаврами педагогического образования в вузах России в области обеспечения безопасной работы с информационными ресурсами, мы пришли к выводу, что подобная дисциплина в учебных планах

* Статья написана в рамках исследования «Информационная безопасность в контексте виртуализации российского общества», финансируемого за счет средств гранта на проведение научно-исследовательских работ по приоритетным направлениям научной деятельности вузов — партнеров по сетевому взаимодействию (МГПИ — ЮУрГГБУ).

Контактная информация

Зубрилин Андрей Анатольевич, канд. филос. наук, доцент кафедры информатики и вычислительной техники Мордовского государственного педагогического института им. М. Е. Евсевьева, г. Саранск; *адрес:* 430007, Республика Мордовия, г. Саранск, ул. Студенческая, д. 11а; *телефон:* (8342) 33-92-84; *e-mail:* azubrilin@mail.ru

Терешкина Кристина Юрьевна, магистрант физико-математического факультета Мордовского государственного педагогического института им. М. Е. Евсевьева, г. Саранск; *адрес:* 430007, Республика Мордовия, г. Саранск, ул. Студенческая, д. 11а; *телефон:* (8342) 33-92-84; *e-mail:* tereshkina_kyu@mail.ru

A. A. Zubrilin, K. Yu. Tereshkina,
Mordovian State Pedagogical Institute named after M. E. Evsevjev, Saransk

FEATURES OF TRAINING BACHELORS OF TEACHER EDUCATION IN INFORMATION SECURITY

Abstract
The article gives the author's vision of training bachelors of teacher education in information security. The content that needs to be internalized by students in the course of studying the discipline of the same title is allocated.
Keywords: information security, information threats, teacher education, baccalaureate, workshops.

имеет название «Информационная безопасность» или «Методы и средства защиты информации». Анализ их содержания показал, что большая часть времени отводится общим вопросам организации информационной безопасности с обязательным рассмотрением соответствующих нормативных документов. Также в рамках лекционного курса прорабатываются вопросы криптографической защиты и, в редких случаях, способы устранения уязвимостей компьютерных систем (например, изучаются программно-технические методы защиты, аутентификация пользователей и т. д.). Лекционный курс преимущественно поддерживается лабораторными работами, которые в основном связаны с криптографической защитой информации и рассмотрением алгоритмов шифрования (RSA, DES и т. д.). Иногда лекции подкрепляются не лабораторным практикумом, а семинарскими занятиями.

По нашему мнению, содержание дисциплины «Информационная безопасность» должно быть существенно расширено, как, например, это представлено в статье Ю. И. Богатыревой [1], и в него следует включить вопросы, связанные с информационными угрозами современности:

- антивирусная безопасность;
- противодействие взлому компьютерных систем;
- обеспечение защиты информации посредством шифрования данных (криптографическая защита);
- противодействие методам социальной инженерии;
- DoS- и DDoS-атаки.

Перечисленные вопросы имеет смысл рассматривать сквозь призму правовых аспектов информационной безопасности. В частности, можно решать ситуационные задачи [5], через которые студенты осознают собственную ответственность за возможные правонарушения.

Мы рекомендуем подкреплять лекции именно семинарскими занятиями, на которых обсуждаются общие и частные вопросы, посвященные информационной безопасности, предлагаются к просмотру тематические видеофрагменты, рассматриваются методы предотвращения информационных угроз.

Выносимые на обсуждение вопросы в зависимости от специфики аудитории могут корректироваться. Возможные вопросы приведены в таблице.

Таблица

Тематическое планирование семинарских занятий по изучению информационной безопасности

№ п/п	Тема семинара	Содержание темы (вопросы для обсуждения)
1	Правовые вопросы, связанные с информационной безопасностью	Правовое регулирование в области информационной безопасности. Законы о преступлениях в сфере информационных технологий. Авторское право. Пути доказательства авторства. Интеллектуальная собственность. Способы защиты интеллектуальной собственности. Лицензионное программное обеспечение. Компьютерное пиратство и законодательная ответственность за него
2	Нормативные документы, касающиеся государственной тайны	Государственная тайна. Ответственность за разглашение государственной тайны. Состояние законодательства РФ в области сохранения государственной тайны. Примеры нарушения государственной тайны
3	Программные и аппаратные средства по противодействию взлому ПК	Несанкционированный доступ к аппаратным средствам компьютера и средства ограничения доступа. Взлом экранной заставки Windows и пароля BIOS. Способы предотвращения взлома. Взлом операционной системы посредством носителей информации. Способы защиты. Ограничение доступа к USB-накопителям. Разграничение доступа в локальных сетях. Взлом учетных записей пользователей локальной сети. Способы предотвращения взлома
4	DoS- и DDoS-атаки как инструмент ограничения доступа к сетевому ресурсу	Технология проведения DoS- и DDoS-атак (перенаправление трафика, навязывание длинной сетевой маски и др.). Способы предотвращения DoS- и DDoS-атак. Пассивная и активная оборона при защите сервера от атак. Программные средства и информационные ресурсы для отражения DoS- и DDoS-атак
5	Комплексная защита сетевого компьютера от информационных угроз	Проблемы выбора защитного программного обеспечения. Хакинг и антихакинг. Хакерские технологии. Противодействие хакингу. Обзор программных средств для защиты объектов операционной системы от хакинга
6	Брандмауэр как инструмент антихакинга	Брандмауэр (межсетевой экран, firewall) и его назначение. Технология отражения атак брандмауэром. Настройка встроенного брандмауэра Windows. Характеристики специализированных брандмауэров. Критерии отбора брандмауэров для практического использования
7	Приложения по обнаружению вторжения на ПК и защите от него	Проактивные системы защиты компьютера. Системы контроля целостности данных. Борьба с потенциально опасными программами
8	Антивирусные программные средства офисного и домашнего назначения	Вредоносное программное обеспечение и пути его попадания в компьютер пользователя. Компьютерная реклама как инструмент заражения компьютера. Клавиатурные шпионы (кейлоггеры). Функциональные возможности антивирусных программных средств. Онлайн-антивирусы

Окончание таблицы

№ п/п	Тема семинара	Содержание темы (вопросы для обсуждения)
9	Парольная защита	Пароль как средство ограничения доступа к ресурсу. Требования к выбору пароля. Хранители паролей. Программы восстановления (взлома) паролей. Брутфорс
10	Программы шифрования данных	Шифрование данных и его назначение. Алгоритмы и стандарты шифрования. Архивирование файлов с паролем как инструмент защиты от несанкционированного доступа. Криптография и ее методы шифрования информации. Восстановление данных
11	Социальная инженерия и ее методы	Обзор методов социальной инженерии. Антропогенные инструменты защиты от методов социальной инженерии. Обратная социальная инженерия. Мошенничество в Интернете
12	Электронная валюта	Электронная наличность. Обзор платежных онлайн-систем. Опасности при работе с электронной наличностью. Проблемы электронной оплаты. Способы заработка в Интернете
13	Социальные сети как информационная угроза	Социальная сеть как инструмент сбора информации о гражданине. Инициируемые и не инициируемые пользователем угрозы в социальных сетях. Меры защиты от угроз в социальной сети
14	Дети и Интернет	Компьютерные программы для защиты детей от информационных угроз Интернета. Фильтрация данных. Программы контентной фильтрации
15	Политика информационной безопасности и ее организация в локальной сети	Настройка безопасности групповой работы с информационными ресурсами в локальной сети. Локальная политика безопасности. Авторизация и ее задачи. Настройка аудита сетевых ресурсов. Работа с журналом безопасности. Защита локальной сети от взлома. Сниффинг

Предлагаемые к изучению темы не являются жестко связанными друг с другом. Поэтому в зависимости от количества часов, выделяемых на изучение дисциплины, преподаватель может выбирать конкретные темы на свое усмотрение.

Обязательным компонентом обучения информационной безопасности является просмотр видеофрагментов с их дальнейшим обсуждением.

Практикоориентированность дисциплины обеспечивается за счет выполнения индивидуальных творческих заданий, где бакалаврам следует в домашних условиях установить на своих компьютерах защитное программное обеспечение и настроить его на оптимальную работу. В качестве отчета преподавателю представляется документ, оформленный по заданной схеме. При выполнении данного задания у бакалавров формируются навыки инсталляции программного продукта, его настройки, выяснения возможных причин сбоев в работе и т. д.

Обучение информационной безопасности бакалавров педагогического образования в предложенном нами варианте (лекции и семинары, подкрепленные самостоятельной внеаудиторной работой) позволит:

- более широко охватить спектр возможных информационных угроз;
- подробно рассмотреть методы противодействия угрозам;
- сформировать умения по применению защитного программного обеспечения;
- добиться овладения студентами методами противодействия психологическому воздействию.

В зависимости от появления новой информационной угрозы можно путем незначительных изменений корректировать содержание дисциплины, тем самым модернизируя его.

Литература

1. *Богатырева Ю. И.* Педагогическая деятельность и обеспечение информационной безопасности личности // Информатика и образование. 2013. № 2.

2. *Зубрилин А. А.* Информационные угрозы Интернета: светлое будущее или темное настоящее // Информатика в школе. 2010. № 7.

3. *Зубрилин А. А., Александрова Р. И.* Эмигрировавшие в Интернет // Человек. 2002. № 4.

4. *Никитин В. П.* Методические особенности обучения будущих учителей информатики основам информационной безопасности // Информатика и образование. 2015. № 10.

5. *Семенова З. В.* Ситуационные задачи в теме «Правовые аспекты информационной безопасности» // Информатика и образование. 2008. № 2.