

УДК 004.056

DOI: 10.35750/2071-8284-2019-3-181-187

А.В. Костюк

кандидат технических наук, доцент

Санкт-Петербургский военный институт

войск национальной гвардии Российской Федерации

Российская Федерация, 198206, Санкт-Петербург, ул. Лётчика Пилютова, д. 1

ORCID: 0000-0002-5642-2443. E-mail: kostyuk.anatoliy.2015@mail.ru

С.А. Бобонец

кандидат военных наук, доцент

Санкт-Петербургский военный институт

войск национальной гвардии Российской Федерации

Российская Федерация, 198206, Санкт-Петербург, ул. Лётчика Пилютова, д. 1

ORCID: 0000-0002-1756-3390. E-mail: sbobon@mail.ru

А.И. Примакин

доктор технических наук, профессор

Санкт-Петербургский университет МВД России

Российская Федерация, 198206, Санкт-Петербург, ул. Лётчика Пилютова, д. 1

ORCID: 0000-0001-8411-300X. E-mail: a.primakin@mail.ru

Подходы к обеспечению информационной безопасности электронного обучения

Аннотация: В статье отмечается, что доступность информационных ресурсов глобальной сети и средств массовой информации создаёт угрозы зависимости от негативной, противоречивой или агрессивной информации, поэтому одной из актуальных задач является обеспечение информационной безопасности электронного обучения. Несмотря на очевидные достижения в использовании технологии электронного обучения, пока ещё педагогическому аспекту данного вида обучения не уделяется должного внимания. Установлено, что внедрение информационных технологий в образовательную деятельность без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз. Рассматривается решение задачи обеспечения безопасности электронного обучения в двух направлениях: обеспечение безопасности информационных процессов и ограничение доступа личности к информации, представляющей собой угрозу её жизнедеятельности. Проанализированы угрозы, оказывающие влияние на информационную безопасность электронного обучения. Обосновывается применение современных педагогических и информационных технологий в качестве средств обеспечения информационной безопасности обучения в сети.

Ключевые слова: электронное обучение, информационная безопасность, безопасность электронного обучения, технологии обучения, педагогические технологии.

Для цитирования: Костюк А.В., Бобонец С.А., Примакин А.И. Подходы к обеспечению информационной безопасности электронного обучения // Вестник Санкт-Петербургского университета МВД России. – 2019. – № 3 (83). – С. 181-187. DOI: 10.35750/2071-8284-2019-3-181-187.

Anatoliy V. Kostyuk

Cand. Sci. (Tech.), Docent

Saint-Petersburg Military Institute of the Forces of the National Guard of the Russian Federation

1, Letchika Pilyutova str., Saint-Petersburg, 198206, Russian Federation

ORCID: 0000-0002-5642-2443. E-mail: kostyuk.anatoliy.2015@mail.ru

Sergey A. Bobonets

Cand. Sci. (Mil.), Docent

Saint-Petersburg Military Institute of the Forces of the National Guard of the Russian Federation

1, Letchika Pilyutova str., Saint-Petersburg, 198206, Russian Federation

ORCID: 0000-0002-1756-3390. E-mail: sbobon@mail.ru

Alexey I. Primakin

Dr. Sci. (Tech.), Professor

Saint-Petersburg University of MIA of Russia

1, Letchika Pilyutova str., Saint-Petersburg, 198206, Russian Federation

ORCID: 0000-0001-8411-300X. E-mail: a.primakin@mail.ru

Approaches to ensuring information security of e-learning

Annotation: The article notes that accessibility to information resources of the global network and mass media creates threats of dependence on negative, contradictory or aggressive information, therefore, one of the urgent tasks is to ensure its information security. Despite the obvious achievements of using e-learning technology, they do not pay enough attention to the pedagogical aspect of this type of training. It has been established that the introduction of information technologies into educational activities without linking to ensuring information security significantly increases the likelihood of information threats. We consider the solution to the problem of ensuring the security of e-learning in two directions: ensuring the security of information processes and limiting an individual's access to information that represents a threat to their life. Analyzed the threats that affect the information security of e-learning. The use of modern pedagogical and information technologies as a means of ensuring information security training in the network is substantiated.

Keywords: e-learning, information security, e-learning security, teaching technologies, pedagogical technologies.

For citation: Kostyuk A.V., Bobonets S.A., Primakin A.I. Approaches to ensuring information security of e-learning // Vestnik of St. Petersburg University of the Ministry of Internal Affairs of Russia. – 2019. – № 3 (83). – P. 181-187. DOI: 10.35750/2071-8284-2019-3-181-187.

Информационные и телекоммуникационные технологии на современном этапе стремительно проникают во все сферы образовательной деятельности. Данному процессу содействуют как внешние факторы, которые связаны с процессом информатизации общества, так и внутренние, обусловленные распространением в образовательных организациях современной компьютерной техники и программного обеспечения. Также этому способствует принятие государственных и межгосударственных программ информатизации образования и осознания необходимости информатизации у большинства участников образовательной деятельности [1].

Благодаря глобальной сети, человек получает возможность учиться и совершенствовать свои знания на протяжении всей жизни. Однако доступность информационных ресурсов

глобальной сети и средств массовой информации создаёт угрозы обретения зависимости от негативной, противоречивой или агрессивной информации. Таким образом, информатизация современного общества создаёт не только благоприятные информационные условия для образовательной деятельности и развития личности, но и определённые проблемы в области информационной безопасности.

Следовательно, одной из актуальных задач, стоящих перед современным обществом, является обеспечение его информационной безопасности [2]. Решение данной задачи осуществляется в двух направлениях: обеспечение безопасности информационных процессов и ограничение доступа личности к информации, представляющей угрозу её жизнедеятельности.

Быстрое развитие информационно-телекоммуникационных технологий (ИКТ) открывает дополнительные возможности в образовательном процессе. Вследствие этого в современных условиях наблюдается устойчивая тенденция интеграции образовательных и информационных технологий. Наиболее отчётливо это заметно в технологиях электронного обучения.

Несмотря на достижения использования технологии электронного обучения, необходимо отметить, что большая часть и разработчиков, и преподавателей не уделяют должного внимания педагогическому аспекту данного вида обучения [3; 4].

В основе электронного обучения лежит самостоятельная образовательная деятельность обучающихся, которые имеют возможность пользоваться дополнительными информационными ресурсами, размещёнными, как в глобальной сети Интернет, так и в электронной образовательной среде.

В связи с широким распространением сети Интернет часто приходится говорить не об ограничении доступа личности к опасной информации, а наоборот, о ситуациях, когда контакт пользователя с опасной информацией является результатом не его действий, а несанкционированного, вредоносного проникновения такой информации к личности.

Негативные социально-психологические последствия проявляются в том, что у личности начинают размываться как нравственные ценности, так и способности различать иллюзорное и реальное. Ещё более серьёзную опасность, чем «псевдореальность», представляет повальное увлечение подрастающего поколения новыми технологиями, поскольку в этом возрасте затруднено распознавание истинности происходящего.

Отсутствие цензуры в глобальной сети создаёт кроме социальной также и педагогическую проблему, поскольку информационные ресурсы Интернета используются в образовательном процессе любой формы получения образования. В Доктрине информационной безопасности РФ¹ отмечается, что «практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления

информационных угроз» [4]. В документе также обращается внимание на то, что возникают новые способы противозаконной деятельности, в том числе с применением информационных, коммуникационных и высоких технологий [4].

Как следствие, появляется проблема обеспечения информационной безопасности (ИБ), без решения которой невозможно осуществлять полноценное развитие личности в условиях информатизации образования. В настоящее время образовательное сообщество пришло к выводу о необходимости обучения противодействию манипулированию сознанием обучающихся. Уточним понимание используемых терминов «информационная безопасность» и «технология».

Анализ научных источников свидетельствует о наличии различных подходов к трактовке и определению термина «информационная безопасность». В Доктрине информационной безопасности РФ указывается, что информационная безопасность характеризует «состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз»². В этом же документе отмечается, что состояние ИБ в области технологий и образования «характеризуется и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомлённостью граждан в вопросах обеспечения личной информационной безопасности»³. Поэтому дальнейшее развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности, и повышение уровня обученности граждан в вопросах обеспечения личной информационной безопасности становится одним из важных направлений государственной политики в сфере информационной безопасности.

Анализ литературных источников позволяет сделать вывод о том, что информационная безопасность, формирование взаимодействия и коммуникации участников образовательного процесса во многом зависят от педагогических технологий, используемых в образовательной деятельности [3; 5].

Термин «технология» в современной педагогике появился благодаря бурному развитию

¹ Утверждена Указом Президента РФ от 5 декабря 2016 г. № 646.

² Об утверждении Доктрины информационной безопасности Российской Федерации Указ Президента РФ от 5 декабря 2016 г. № 646.

³ Там же.

научно-технического прогресса, в том числе и информатизации общества, а также желанию преподавателей добиваться в своей профессиональной работе ожидаемых результатов [6].

В настоящее время отсутствует устоявшаяся ёмкая и однозначная формулировка определения технологии обучения. К примеру, некоторые авторы истолковывают технологию обучения как инструмент для достижения ожидаемых дидактических целей, отмечая, что она всегда является составной частью образовательного процесса и в этом смысле развивает классическую дидактику. Другие авторы рассматривают технологию в качестве совокупности этапов, обеспечивающих достижение дидактических задач, а по своему содержанию технологию представляют объединением форм, методов и средств обучения, которое реализует эффективное достижение заранее установленных учебных целей. Третьи представляют технологию обучения как совокупность методико-организационных действий преподавателя, обращённую на оптимизацию образовательного процесса посредством технических и информационных средств обучения.

Анализ определений, представленных в разнообразных научных и других источниках, свидетельствует, что основная часть исследователей соглашается с тем, что технология обучения является средством, обеспечивающим оптимальное построение и реализацию образовательного процесса.

Данный тезис является важнейшим, так как именно в нахождении наилучших способов гарантированного достижения установленных образовательных целей и заключается главный смысл технологизации образовательного процесса. Следовательно, технологический подход к обучению в условиях информатизации общества предполагает такое проектирование образовательного процесса, которое обеспечивало бы гарантированное достижение дидактических целей, основываясь на исходных установках (образовательные ориентиры, цели и содержание обучения).

Технология обучения, на наш взгляд, может трактоваться как логически выстроенная совокупность педагогических действий, операций и процедур, которые обеспечат гарантированное получение ожидаемого результата обучения в изменяющихся условиях образовательного процесса. Примерами современных педагогических

технологий являются кейс-метод, метод проектов, метод дискуссий, ситуационный анализ, ролевые и деловые игры и др.

Проведённый анализ свидетельствует, что современные педагогические технологии необходимо рассматривать и как средство информационной безопасности обучающихся, и как условие для обеспечения информационной безопасности образовательных ресурсов [3; 7].

Кроме того, анализ современной научно-педагогической литературы свидетельствует, что у некоторой части специалистов вызывают сомнения достигнутые результаты электронного обучения, адекватность электронных ресурсов, защита интеллектуальной собственности и др. [6].

Исследования, проведённые учёными В.И. Зуевым и Е.П. Чирко, показывают, что существуют серьёзные угрозы безопасности нормального функционирования системы электронного обучения. Среди таких угроз необходимо выделить следующие [6]:

- неадекватность электронных образовательных ресурсов и повреждение их целостности;
- несанкционированный доступ к электронным образовательным ресурсам [5];
- атаки на информационные сервисы и службы;
- изменения, вносимые в механизмы тестирования.

Присоединяясь к сомнениям относительно достигнутых результатов электронного обучения и их достоверности, авторы обращают внимание на источники психолого-педагогических факторов риска. К таким источникам они причисляют информационные ресурсы, информационную образовательную среду, обучающегося. Особое внимание обращают на риски, напрямую связанные с человеческим фактором: обучающимися, обслуживающим персоналом и преподавательским составом.

В своих исследованиях В.И. Зуев и Е.П. Чирко отмечают, что безопасность электронного обучения следует обеспечивать в трёх взаимосвязанных областях, оказывающих отрицательное влияние на качество электронного обучения. Предлагаемая информационная модель безопасности электронного обучения в пространственном представлении является сочетанием трёх плоскостей, ассоциированных соответственно с коммуникационной средой, электронными об-

разовательными ресурсами, персоналом и обучающимися [4].

Проанализируем некоторые из сторон предложенной информационной модели безопасности, которые включают в себя преподавателей, обучающихся и обслуживающий персонал. В рассматриваемой модели целесообразно выделить ряд факторов, напрямую связанных с обеспечением информационной безопасности электронного обучения:

– какую степень самостоятельности проявляет обучающийся в процессе своего обучения и выполнения заданий?

– кто в действительности тестируется и взаимодействует с преподавателем?

– какими навыками публичного выступления или диспута будет обладать обучающийся?

– в какой степени осуществлена защита авторских прав разработчика контента (образовательные ресурсы, контрольные и тестовые материалы, индивидуальные задания), который размещается в информационной образовательной среде или на сайте в глобальной сети?

– насколько соответствуют действительности ссылки обучающегося на свои работы в телекоммуникационной сети, отказ в обслуживании?..

Следует отметить, что особенности электронного обучения оказывают значительное влияние на отбор и структурирование образовательного контента. Это объясняется тем, что одной из ключевых специфических черт, присущих электронной форме обучения, является интерактивность, способствующая реализации информационно-коммуникационных технологий (ИКТ) [4; 8]. Именно современные ИКТ позволяют реализовать комфортное взаимодействие участников образовательного процесса. Кроме того, важными достоинствами электронной формы обучения являются простота и удобство реализации инновационных методов обучения, различных видов контроля, как автоматизированного, так и открытого, вопрос индивидуализации обучения.

Различные творческие задания, скрупулёзно подобранные ссылки на достоверные источники интернет-ресурсов, а также интерактивные формы коммуникации друг с другом и с педагогом содействуют повышению качества образовательного процесса и защищённости обучающихся от искажённой информации глобальной сети.

В настоящее время необходимость решения задачи обеспечения информационной безопасности электронного обучения не вызывает сомнений как у преподавателей, так и у обслуживающего персонала [8; 9]. На основании наблюдений и обобщения рассмотренных выше сторон информационной модели безопасности можно утверждать, что информационная безопасность преимущественно определяется имеющимися у обучающегося критическим мышлением и информационной культурой, а также уровнем информационной компетентности преподавателей. Кроме того, следует отметить, что на информационную безопасность электронной формы обучения оказывают существенное влияние и другие факторы, среди которых – организация электронной образовательной среды, используемые формы и организация обучения, педагогические технологии, а также задачи и содержание курса [4; 10].

В настоящее время важно не только создавать условия информационной безопасности образовательного процесса как в очной, так и в дистанционной форме обучения, но и формировать информационную безопасность на любом этапе обучения, начиная с дошкольного возраста. Можно утверждать, что на современном этапе информатизации общества сформированность информационной безопасности обучающегося в основном зависит от способности выявлять и определять степень информационной угрозы; предугадывать последствия информационной угрозы и вырабатывать контрдействия [5].

При рассмотрении угроз со стороны основных источников информации – телевидения и Интернета – следует акцентировать внимание на существовании различных типов угроз и их конкретных примерах, рассматривать документальные случаи их проявления и последствий. Немаловажным является изучение юридической стороны обеспечения информационной безопасности, тех нормативных актов, которые обеспечивают её реализацию и предусматривают ответственность за её нарушение: обучающиеся должны понимать, что сеть Интернет – это тоже часть социума, и преступления в виртуальном пространстве так же недопустимы, как и в пространстве реальном. Процесс такого воспитания целесообразно строить, основываясь на принципах добровольного принятия общепринятых норм поведения, через активное включение молодёжи в выполнение обще-

ственно полезной и личностно-развивающей деятельности. Именно такое погружение даёт возможность найти то общее нравственное начало для современной молодёжи и «остального» общества, которому она пытается себя противопоставить, вовлекаясь в антисоциальную деятельность в виртуальном пространстве.

Одним из приёмов повышения мотивации обучающихся и стимулирования их познавательного интереса является их личное участие в исследовательской деятельности. Следствием такой деятельности является превращение обучающихся из пассивных наблюдателей, что является характерным для нынешнего поколения, в активно познающих окружающую их действительность. Не вызывает сомнения, что только непосредственное участие в тех или иных ситуациях способствует усвоению нравственных основ социального поведения. Для этого при изучении вопросов обеспечения информационной безопасности необходимо ставить перед обучающимися задачи, не только требующие поиска ответа в учебнике или сети Интернет, но и побуждающие их к глубокому изучению поставленной проблемы, ее анализу в контексте своей личной жизненной ситуации, поиску путей решения проблемы и их обоснования, правовой и нравственной оценке ситуации. Важным фактором при организации подобной деятельности обучающихся является исключение или минимизация формализма, формирование заинтересованности как в самом процессе исследований, так и в получении конечного результата. В ходе таких исследований важно также создавать повышенную заинтересованность обучающихся в изучаемом материале и формировать критическое отношение к информационным ресурсам.

Поэтому, чтобы ответить на ключевой вопрос, как быть и какие шаги предпринимать для обеспечения безопасности личности в современном обществе, идущим по пути информатизации, следует, на наш взгляд, выделить ряд направлений, реализация которых будет способствовать обеспечению безопасности личности:

- целесообразно прийти к единой трактовке ключевых понятий и терминов, которые используются в области обеспечения информационной безопасности личности;

- выработать общие подходы к решению проблем, вызванных разрушающим воздействием информации на психику личности, на

индивидуальное и общественное сознание и на политико-идеологическую сферу;

- разработать и принять международные законодательные акты, обеспечивающие регулирование информационных отношений в области использования конфиденциальной информации как в компьютерных сетях, так и в информационных системах общего доступа, которые реально или потенциально могут использоваться в деструктивных и криминальных целях [11].

Одним из важнейших факторов решения проблемы обеспечения информационной безопасности является подготовка преподавательского состава, обладающего новыми педагогическими и информационными технологиями, с учётом специфики электронного обучения.

В современных условиях информационно-коммуникационные технологии выступают как средства обучения, реализующие определённые педагогические технологии. Для обеспечения ИБ курса электронного обучения преподаватель должен обладать необходимыми навыками безопасной организации и проведения дискуссий, ролевых и деловых игр, электронной лекции, телеконференции, видеоконференции, вебинара и т. д. [5].

Таким образом, пути решения проблемы информационной безопасности подрастающего поколения лежат в том числе и в педагогической области. Преподаватель, владеющий педагогическим мастерством, а следовательно, и педагогическими технологиями, способен организовать образовательный процесс так, чтобы развивать информационную грамотность, формировать навыки критического мышления, готовить сознание обучающихся к противодействию угрозам деструктивной информации.

В условиях информатизации образовательной деятельности проблема обучения вопросам обеспечения ИБ как обучающихся, так и преподавателей выдвигается на первый план. Вследствие этого в профессиональную подготовку обучающихся, а также в программу повышения квалификации и преподавателей, и обслуживающего персонала необходимо включить темы по информационной безопасности с соответствующей профессиональной направленностью. Профессиональную компетентность участников электронного обучения необходимо оценивать с учётом обеспечения информационной безопасности образовательного процесса.

Список литературы

1. Бушмелева Н. А., Разова Е. В. Формирование компетенций в области информационной безопасности в системе высшего педагогического образования // Научно-методический электронный журнал «Концепт». – 2017. – Т. 2. – С. 537–544. – URL: <http://e-koncept.ru/2017/570106.htm>.
2. Арутюнов В. В. Современные проблемы и задачи обеспечения информационной безопасности. // Вестник Московского финансово-юридического университета. – 2016. – № 2. – С. 213–222.
3. Костюк А. В., Бобонец С. А. Информационная безопасность электронного обучения // ООО «Консалтинговая компания Юком». Научный альманах. – 2016. – № 8-1 (22). – С. 129–132.
4. Смолян Г. Л. Сетевые информационные технологии и проблемы безопасности личности // Информационное общество. – 1999. – Вып. 1. – С. 21–25.
5. Зуев В. И. Безопасность электронного обучения / Совершенствование подготовки IT-специалистов по направлению «Прикладная информатика для инновационной экономики». – Москва: Московский университет экономики, статистики и информатики, 2010. – С. 81–85.
6. Гамова О. В. Обучение основам информационной безопасности на уроках информатики в системе образовательных организаций, реализующих программы среднего профессионального образования // Научная дискуссия: вопросы педагогики и психологии, 2017. – № 3 (60). – С. 34–43.
7. Колгатнин А. Г. Информационная безопасность в системах открытого образования // Образовательные технологии и общество, – 2014. – № 4 (21). – С. 112–118.
8. Башлыкова А. А., Каменщиков А. А., Олейников А. Я. О подходах к разработке профилей интероперабельности в военной области // Информационные технологии и вычислительные системы. – 2016. – № 12. – С. 112–121.
9. Мalyuk А. А., Полянская О. Ю. Зарубежный опыт формирования в обществе культуры информационной безопасности // Безопасность информационных технологий. – 2016. – № 4. – С. 25–37.
10. Владимиров В. А. Информационная безопасность личности // Молодой учёный. – 2015. – № 11. – С. 1294–1298.

References

1. *Bushmeleva N. A., Razova Ye. V. Formirovaniye kompetentsiy v oblasti informatsionnoy bezopasnosti v sisteme vysshego pedagogicheskogo obrazovaniya [Elektronnyy resurs] // Nauchno-metodicheskiy elektronnyy zhurnal «Kontsept». – 2017. – T. 2. – S. 537–544. – URL: <http://e-koncept.ru/2017/570106.htm> (data obrashcheniya: 10.07.2019).*
2. *Arutyunov V. V. Sovremennyye problemy i zadachi obespecheniya informatsionnoy bezopasnosti. // Vestnik Moskovskogo finansovo-yuridicheskogo universiteta. – 2016. – № 2. – S. 213–222.*
3. *Kostyuk A. V., Bobonets S. A. Informatsionnaya bezopasnost' elektronno go obucheniya // ООО «Konsaltingovaya kompaniya Yukom», Nauchnyy al'manakh. – 2016. – № 8-1 (22). – S. 129–132.*
4. *Smolyan G. L. Setevyye informatsionnyye tekhnologii i problemy bezopasnosti lichnosti // Informatsionnoye obshchestvo. – 1999. – Vyp. 1. – S. 21–25.*
5. *Zuyev V. I. Bezopasnost' elektronno go obucheniya / Sovershenstvovaniye podgotovki IT-spetsialistov po napravleniyu «Prikladnaya informatika dlya innovatsionnoy ekonomiki». – Moskva: Moskovskiy universitet ekonomiki, statistiki i informatiki, 2010. – S. 81–85.*
6. *Gamova O. V. Obucheniye osnovam informatsionnoy bezopasnosti na urokakh informatiki v sisteme obrazovatel'nykh organizatsiy, realizuyushchikh programmy srednego professional'nogo obrazovaniya // Nauchnaya diskussiya: voprosy pedagogiki i psikhologii. – 2017. – № 3 (60) – S. 34–43.*
7. *Kolgatnin A. G. Informatsionnaya bezopasnost' v sistemakh otkrytogo obrazovaniya // Obrazovatel'nyye tekhnologii i obshchestvo. – 2014. – № 4 (21). – S. 112–118.*
8. *Bashlykova A. A., Kamenshchikov A. A., Oleynikov A. Ya. O podkhodakh k razrabotke profiley interoperabel'nosti v voyennoy oblasti // Informatsionnyye tekhnologii i vychislitel'nyye sistemy. – 2016. – № 12. – S. 112–121.*
9. *Malyuk A. A., Polyanskaya O. Yu. Zarubezhnyy opyt formirovaniya v obshchestve kul'tury informatsionnoy bezopasnosti // Bezopasnost' informatsionnykh tekhnologiy. – 2016. – № 4. – S. 25–37.*
10. *Vladimirov V. A. Informatsionnaya bezopasnost' lichnosti // Molodoy uchenyy. – 2015. – № 11. – S. 1294–1298.*