

# Информационная безопасность и защита информации

---

А.А. Малюк, И.Ю. Алексеева

## КУЛЬТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ЭЛЕМЕНТ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

В статье рассматриваются гуманитарные проблемы обеспечения информационной безопасности, связанные с этическими вопросами развития информационных технологий и формированием в обществе информационной культуры. Использован опыт преподавания соответствующих дисциплин в отечественных и зарубежных высших учебных заведениях.

*Ключевые слова:* информационная безопасность, гуманитарные проблемы информационной безопасности, информационная культура, этика в сфере информационных технологий.

Доктрина информационной безопасности Российской Федерации определяет информационную безопасность как состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере. Это определение, как видно, изначально носит комплексный характер. Только используя комплексный подход (по целям, средствам и организационным решениям), можно добиться прогресса в обеспечении безопасности.

Здесь уместно привести высказывание президента компании «Counterpane Systems» (США) Брюса Шнайера: «Тот, кто думает, что может решить проблемы безопасности с помощью технологии, не понимает ни проблем безопасности, ни проблем технологии».

---

© Малюк А.А., Алексеева И.Ю., 2016

Работа выполнена при финансовой поддержке РГНФ, проект № 15-03-00248: Проведение научных исследований по направлению «Формирование в обществе культуры информационной безопасности».

Очевидно, что обеспечение информационной безопасности – проблема многосторонняя и должна решаться всей совокупностью технологических, организационно-правовых и гуманитарных методов (прежде всего, морально-этических).

Такой взгляд на проблему информационной безопасности четко просматривается в позиции Совета Безопасности Российской Федерации. Секретарем Совета Безопасности в 2008 г. утверждены Основные направления научных исследований и Приоритетные проблемы в области обеспечения информационной безопасности Российской Федерации, которые делятся на три группы: гуманитарные проблемы, технические проблемы и проблемы кадрового обеспечения. Причем статистика инцидентов показывает, что удельный вес гуманитарных проблем достигает 80 %.

К числу наиболее острых на сегодняшний день гуманитарных проблем информационной безопасности большинство экспертов относит:

- исследование социально-психологических последствий широкого использования современных информационных технологий во всех сферах жизни общества;
- регулирование отношений и противодействие злоупотреблениям свободой слова в сети Интернет;
- правовое регулирование отношений в области противодействия преступлениям в сфере информационно-коммуникационных технологий;
- формирование системы международной информационной безопасности.

При рассмотрении данного списка проблем и современных тенденций в развитии и использовании новых информационных технологий может быть сформулирован перечень компетенций специалистов по защите информации в области гуманитарных аспектов проблемы, который выглядит следующим образом.

*Специалист по защите информации должен:*

а) знать:

- место и роль проблем информационной безопасности в становлении современного информационного общества;
- социально-психологические последствия внедрения и широкого распространения современных информационных технологий;
- нормы этики в сфере информационных технологий;
- проблемы обеспечения баланса интересов личности, общества и государства в информационной сфере;
- проблемы обеспечения информационно-психологической безопасности личности и общества;

б) уметь:

- поставить задачу разработки оптимальной организации службы защиты информации, учитывающей личностные особенности коллектива и психологию поведения его членов в условиях информационного общества;
- организовать систему обучения сотрудников основам информационной культуры и этики;

в) владеть:

- основными организационными и морально-этическими методами обеспечения информационной безопасности;
- навыками прикладной риторики в сфере обеспечения информационной безопасности.

Чтобы сформировать перечисленные компетенции, содержание соответствующего учебного курса должно включать следующие разделы.

1. Стратегия развития информационного общества в Российской Федерации.

2. Сохранение культурно-нравственных ценностей российского народа, русского языка как средства межнационального общения.

3. Информационная культура и этика.

4. Информационное обеспечение государственной политики.

5. Информационно-психологическая безопасность, психофизическое воздействие на личность и общество, информационное оружие.

6. Интернет и свобода слова, защита от вредоносного контента.

7. Социальные проблемы информационного общества, проблемы образования и воспитания.

8. Правовые проблемы развития информационного общества, защита интеллектуальной собственности

9. Преступления в сфере информационных технологий.

Сформулированные выше предложения были реализованы при формировании пилотного проекта в Национальном исследовательском ядерном университете «МИФИ».

При разработке технологии образовательного процесса по данному курсу использовались практически все современные достижения в области педагогики и психологии профессионального образования. Значительные усилия были сосредоточены на развитии креативности студентов, вовлечении их в дискуссию по различным вопросам в рамках семинаров и круглых столов.

Использовалась и такая форма, как организация мастер-классов ведущих ученых и специалистов. Значительную помощь в реализации этой части проекта оказали ученые Института философии РАН (при активном участии академика В.С. Степина). В качестве

примеров ниже приведены темы мастер-классов, проведенных за последние два года:

- «Информационно-динамическая модель баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения»;
- «Место и роль СМИ в решении задач информационного обеспечения государственной политики Российской Федерации»;
- «Информационная безопасность и политическая этика»;
- «Информационное пространство и проблема целостности российского государства»;
- «Национальные интересы России и информационное противостояние в современном мире».

Отдельного внимания потребовала организация семинарских занятий и подготовка итогового научного доклада. Именно на этот вид занятий возлагается задача по формированию компетенций будущих специалистов, связанных с развитием навыков организационного и морально-этического обеспечения мероприятий по защите информации, т. е. формированию в конечном счете культуры информационной безопасности.

Остановимся далее более подробно на проблеме преподавания разделов курса, связанных с этикой в сфере информационных технологий<sup>1</sup>. Это неслучайно, так как именно этические проблемы лежат в основе обеспечения культуры информационной безопасности.

Здесь уместно привести высказывание Патриарха Московского и Всея Руси Кирилла, который в одном из своих выступлений говорил: «...невозможно сегодня защитить нашу молодежь и детей от информации, которую они потребляют. Только внутри самого человека должны быть выстроены эти рубежи обороны. Человек должен быть достаточно открыт к восприятию того, что несет ему современный мир, и одновременно должен быть способным защитить самые сокровенные глубины своей жизни, сохраняя свою национальную, духовную, религиозную, культурную самобытность, а вместе с этой самобытностью сохраняя нравственную систему ценностей...».

Развитие информационно-коммуникационных технологий порождает новые контексты проблем нравственности и правил поведения. Проблема правил поведения в «киберпространстве» выглядит чрезвычайно сложной, если учитывать предоставляемые здесь возможности анонимности и неконтролируемости, с одной стороны, и многообразие участвующих в этом процессе социальных групп – с другой. В данном контексте особое значение приобретают различия в ценностных ориентирах таких групп, в представлениях о хорошем и плохом, о допустимом и недопустимом, разные спосо-

бы обращения со «своими» и «чужими». Нельзя не принимать во внимание и достаточно широко распространенного мнения, что в «вирте» должны утрачивать силу этические предписания, действующие в «реале».

Надежды на решение многих общественно важных проблем в информационной сфере сегодня зачастую связывают с совершенствованием правового регулирования. Однако если последнее сконцентрировано лишь на позитивном праве, писаных законах, игнорирующих сложившиеся представления о справедливости, социальных ценностях и этически приемлемых формах поведения, то расширение сферы его действия способно привести скорее к усилению конфликтов, чем к формированию устойчивого порядка. Ключевое значение в данных условиях приобретают вопросы этические, ибо, во-первых, по-настоящему действенным может быть лишь закон, базирующийся на прочных нравственных основаниях, а во-вторых, невозможно подвести под юридические нормы и проконтролировать все аспекты деятельности человека.

Каждая эпоха дает свои импульсы развитию нравственного сознания и создает трудности для такого развития. Вызовы, характерные для начала XXI в., не в последнюю очередь связаны с формированием глобального информационного пространства, позволяющего массам людей расширять свои представления о допустимых и рекомендуемых формах поведения. Аудио- и видеопродукция (в том числе, игровая индустрия) вносят свой вклад в широкое распространение образцов поведения, формально признаваемого не только безнравственным, но и противоправным. Это способствует распространению морального релятивизма – представления об относительном характере любых этических норм и неправомерности выдвижения абсолютных моральных императивов. Возведение финансово-экономической реальности в ранг основной, если не единственной, социальной реальности способствует тому, что разговоры о нравственных основаниях общества воспринимаются как несерьезные и даже неприличные. На фоне призывов к «толерантности» и «пониманию другого» задача «понимания себя» и общности, образуемой «мною» с «другими», выглядит в лучшем случае третьестепенной. Надежды на то, что распространение компьютерных технологий по всему миру позволит выработать согласованные стандарты поведения, которые могли бы стать основой глобальной этики, выглядят скорее наивными, чем имеющими веские основания. *Глобализация экономики и создание «глобального информационного общества» сопровождаются скорее разрушением ранее сложившихся этических систем, чем формированием глобального нравственного сознания.*

Еще в 1970-х годах авторы доклада президенту Франции<sup>2</sup> предсказывали, что *развитие информационно-коммуникационных технологий не оправдает надежд на объединение нации вокруг «огромного культурно однородного среднего класса»*. По мысли этих авторов, нарождающееся информационное общество будет менее четко социально структурировано и более полиморфно, чем общество индустриальное, это будет сложное общество культурных напряженностей и культурных конфликтов.

Серьезные расхождения в представлениях о поведении подобающем и недопустимом затрудняют сегодня совместную деятельность людей. *Все чаще возникает необходимость договариваться о правилах, формулировать установки, которые должны разделяться всеми членами той или иной организации или сообщества, принимать этические кодексы и устанавливать санкции за их нарушение.*

В упомянутом выше курсе «Гуманитарные проблемы информационной безопасности» при подготовке занятий по этике (имеющих и лекционную, и практическую составляющие) использовался опыт сотрудничества российских и американских ученых в рамках проекта «Инженерная этика для российских инженеров», выполнявшегося во второй половине 1990-х годов на базе Московского авиационного института и Института философии РАН.

Следует отметить, что когда речь идет о выборе между стратегиями «адаптации зарубежного» и «создания своего», в области гуманитарных наук он легче может быть сделан в пользу последнего. Позиция, определившая характер рассматриваемого курса, с самого начала основывалась на формулировании и осмыслении, прежде всего, тех проблем, которые являются актуальными здесь и сейчас. Знание о зарубежном опыте весьма желательно, но ценно оно скорее как повод для размышления, чем как базовая модель, которая нуждается лишь в некоторых модификациях с учетом особенностей страны.

Выполнить такую задачу, конечно же, непросто. Тем не менее движение своим путем может привести к интересным находкам. Например, можно построить курс, отталкиваясь от проблемы смысла жизни, а отсюда перейти к проблеме смысла профессиональной деятельности. В самом деле, почему интерес к проблеме смысла жизни нужно считать признаком «неправильности» русского человека? Не разумнее ли этот интерес легализовать, признать в качестве законного источника вдохновения человека философствующего, осмысливающего собственную деятельность и отношения с людьми по поводу этой деятельности?

Ситуативный анализ в курсе прикладной этики необходим, но следует ли стремиться к тому, чтобы он был столь же детальным,

как в американских курсах? Нужен ли «case» на каждом занятии? Почему бы не попробовать творческие задания – скажем, задание привести примеры профессионального поведения, соответствующего категорическому императиву И. Канта, а также примеры, противоречащие этому императиву (ситуации могут быть вымышленными, взятыми из жизни, из книг, кинофильмов и т. д.). Опыт показывает, что в ходе выполнения такого задания обе формулировки категорического императива («поступай только согласно такой максиме, руководствуясь которой ты в то же время можешь пожелать, чтобы она стала всеобщим законом» и «поступай так, чтобы ты всегда относился к человечеству и в своем лице, и в лице всякого другого как к цели и никогда не относился бы к нему только как к средству») усваиваются студентами удивительно легко, хотя раньше, в контексте общего курса философии, казались малопонятными и почти не связанными с реальными жизненными проблемами.

Мы знаем, что учение о профессиональном долге и нравственных обязательствах получило наиболее развитую форму в медицинской деонтологии (понимаемой обычно как врачебная и сестринская этика). Стоит ли будущему специалисту по защите информации иметь общее представление об этом виде профессиональной этики, основные принципы которой были сформулированы еще в V веке до н. э., и соотносить с ней нравственное содержание своей профессии, находя черты сходства и различия? Мы пришли к выводу, что стоит, даже если в условиях ограниченного учебного времени за рамками курса придется оставить некоторые вопросы, касающиеся деталей поведения специалиста, работающего в сфере информационных технологий.

Как уже отмечалось, в нашем случае курс этики в сфере информационных технологий является частью более обширного курса гуманитарных проблем информационной безопасности. Это дает возможность увидеть вопросы этики в общем контексте проблем информационной культуры, связать с темами творчества, места и роли техники в современном мире, обратить внимание на некоторые психологические аспекты. За курсом этики следует курс риторики в сфере информационных технологий. Включение этого курса в программу профессиональной подготовки мотивировано тем, что специалист по защите информации должен уметь формулировать и аргументировать свои предложения, убеждать руководство организации в необходимости принимать меры по защите информации, уметь работать с персоналом и т. д. В упражнениях по риторике используются, среди прочего, материалы из курса этики.

Разумеется, описываемый в данной статье опыт – только малая часть того опыта обсуждения в студенческой (и аспирантской) аудитории проблем профессиональной этики специалиста в области информационных технологий, который накоплен в стране к настоящему времени.

С марта 2010 г. приказом Министерства образования и науки РФ введен в действие Федеральный государственный стандарт высшего образования по направлению подготовки «Прикладная этика». Введение этого стандарта, безусловно, отвечает растущей потребности в систематической разработке вопросов этики профессий и сфер деятельности. Представляется, что важность этической подготовки как обязательной части профессионального образования в области ИКТ осознается преподавателями профильных дисциплин и руководством вузов, когда эти люди убеждают будущих специалистов в том, что познания в области этики им необходимы.

С 2014 г. мы живем в условиях информационно-психологической войны, которая является частью сложной системы экономических и финансовых войн, политического противоборства и вооруженных конфликтов на территории разных стран. «Стратегия национальной безопасности», принятая США в 2015 г.<sup>3</sup>, объявляет одной из главных угроз безопасности Соединенных Штатов так называемую «агрессию России», а условием обеспечения безопасности американского народа – мировое лидерство США, демонстрируемое, в частности, тем, что США «мобилизовали и возглавили международные усилия по наказанию России». Заявленное здесь стремление к глобальному лидерству органично сочетается с провозглашенной США еще в начале XXI в. установкой на «доминирование по всему спектру» («full-spectrum dominance»)<sup>4</sup>, предполагающей, что технологические достижения должны обеспечить превосходство в принятии решений. Одна из составляющих такого доминирования – информационное превосходство над любым возможным противником, конкурентом или оппонентом. Как заключает на основе анализа материалов государственных ведомств США Е.А. Роговский<sup>5</sup>, термину «информационное доминирование» соответствует целый набор способов информационного воздействия, в числе которых – информационный мониторинг, информационное давление и информационное сдерживание

Очевидно, что усилия по реализации подобного рода установок не могут не оказывать влияния на состояние глобального информационного пространства в целом и российских сегментов информационного пространства в частности. И это следует учитывать в разработке проблем культуры информационной безопасности для подготовки специалистов по защите информации.



- 
- <sup>1</sup> Малюк А.А., Полянская О.Ю., Алексеева И.Ю. Этика в сфере информационных технологий. М.: Горячая линия – Телеком, 2011.
- <sup>2</sup> Nora S., Mine A. The Computerisation of Society. A Report to the President of France. Cambridge; L., 1980.
- <sup>3</sup> National Security Strategy. Febr. 2015. The White House. Washington, 2015.
- <sup>4</sup> Garamone J. Joint Vision 2020 Emphasizes Full-spectrum Dominance // U.S. Department of Defense [Электронный ресурс]. URL: <http://archive.defense.gov/news/newsarticle.aspx?id=45289> (дата обращения: 15.06.2015).
- <sup>5</sup> Rogovskiy E.A. Американская стратегия информационного преобладания // Россия и Америка в XXI веке. Электронный научный журнал. 2009. № 3 [Электронный ресурс]. URL: <http://www.rusus.ru/?act=read&id=161> (дата обращения: 15.06.2015).