И. И. Ашмарин, Н. М. Никифорова

ЭТИКА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

«ЭТИКА (греч. Ethika, от ethos — привычка, нрав) — философская наука, объектом которой является *мораль*. Термин "ЭТИКА" был введен Аристотелем. Начиная с древности ЭТИКУ было принято считать практической философией в отличие от собственно теоретического знания о мире. Всякое теоретическое знание имеет в конечном счете практическое значение… и содержит мировоззренческую сторону, так или иначе обосновывает цели *практической деятельности* (курсив наш. — *И. А., Н. Н.*). Специфика ЭТИКИ состоит в том, что указанные цели формируются здесь в форме идей о должном…» [1].

Именно наличие одной из ориентаций нормативной этики на моральное упорядочение практической деятельности человека определяет неизбежность коррекции и модификации свода этических норм, а в нашем случае и формирования принципиально новых норм, обусловленных появлением новых областей человеческой деятельности и, соответственно, новых социальных страт. Особенно это выразилось в этике конца XX в. с ее поворотом к прикладной этике — этике науки, биоэтике, этике бизнеса, этике деловых отношений и т. д.

И здесь достаточно остро встала проблема взаимоотношения между корпоративной и универсальной (исторически сложившейся общечеловеческой) этикой. Это — социальная ответственность представителей корпоративных страт, применение (а иногда и применимость) общих устоявшихся этических норм к конкретным ситуациям принятия решения. Здесь уместно еще раз сослаться на уже процитированный философский словарь: «Этика объективно оказалась перед необходимостью выбора между возвышенными, но лишенными жизненных соков моральными идеалами и реальной, но лишенной моральных достоинств жизнью» [1]. В ситуациях такого выбора на сегодняшний день в бизнесе, например, существуют два наиболее распространенных принципа построения этической аргументации — принцип утилитаризма и принцип нравственного императива [2].

Принцип утилитаризма: Действие считается морально оправданным, если оно приносит или имеет тенденцию принести максимальную пользу максимальному числу лиц. Суммарная польза сопоставляется с объемом причиняемого ущерба. И если ущерб перевешивает, решение является неэтичным. Если же все альтернативные действия причиняют ту или иную степень ущерба, то выбирается «наименьшее зло».

Принцип нравственного императива: Моральные решения не должны зависеть от конкретного результата.

Можно сказать, что *принцип нравственного императива* — это что-то вроде этического «безусловного рефлекса» как для индивида, так и для любой социальной, в том числе профессиональной или корпоративной, страты. В то же время *принцип утилитаризма* — это «условный рефлекс» на противоречия (повторим уже приведенную выше цитату из философского словаря) «между возвышенными, но лишенными жизненных соков моральными идеалами и реальной, но лишенной моральных достоинств жизнью».

Уже с первого взгляда на эти два принципа обнаруживается их отчетливая оппозиция — оппозиция целей и средств, желаемого и действительного, должного и реального. При этом мы молчаливо предполагаем, что средства и реальность в этой оппозиции находятся в рамках закона. Молчаливо — потому, что все, что выходит за эти рамки, попадает в зону не этических, а юридических норм. Т. е. сегодня (как, впрочем, и не только сегодня) этические нормы особенно важны и необходимы на той пограничной полосе, где общество уже начинает осуждать, а закон еще не начал наказывать. Такая полоса, например, сформировалась в сетевом интернет-сообществе, которое живет по законам своей уже сложившейся — «сетевой» — этики, законам, которые реально существуют в жизни сообщества,

но в правовом поле еще не конституированы. При этом наказания для нарушителей этой этики вполне ощутимы — нарушителю, как правило, закрывают доступ в социальную сеть, на форум и т. д.

Этика в приложении к юридическим и профессиональным аспектам информационной безопасности представляет собой особые стандарты поведения. Многие организации, признавая необходимость этического кода, или правил поведения, разрабатывают основные положения специально для отрасли, компании, руководства и персонала.

Современные зарубежные источники рассматривают преимущественно два стандарта, которые, не являясь законами, диктуют минимальные требования к поведению профессионалов в области защиты информации.

Один из них, (ISC) Code of Ethics, имеет преамбулу и четыре канонических правила.

В первой предусмотрены защита безопасности государства, верность руководителю и членам сообщества на основе следования самым высоким этическим нормам поведения.

Именно исполнение этих требований составляет основное условие сертификации профессионалов в защите информации, которые обязаны подписывать соглашение о готовности исполнять требуемый этический код. Они также обязаны придерживаться правил, требующих от профессионалов защиты интересов общества, государства и его инфраструктуры. Профессионал обязан действовать благородно, честно, справедливо, ответственно и в рамках закона.

Порядочность (integrity) становится не столько нормой личного поведения, сколько профессиональной оценкой исполнения служебных обязанностей, которые не могут исполняться должным образом, если остальные члены организации сомневаются в мотивах поведения исполнителя.

Имея обязанности перед обществом, профессионал выполняет особые обязательства перед своим нанимателем, обеспечивая ему честное и квалифицированное обслуживание.

Понятие «профессионал — специалист в области защиты информационной безопасности» постоянно развивается и изменяется, что требует от профессионала постоянного развития и расширения его знаний.

Работа в сети Интернет должна опираться на положение документа «Ethics and the Internet (RFC) 1087», который лежит в основе всех кодексов поведения и политик. Этот документ перечисляет запреты на действия, которые определяются как «неприемлемые и неэтичные» для профессионала, такие как неавторизованный доступ к ресурсам, разрушения в Сети, использование чужих ресурсов, нарушение целостности информации, нарушение права на конфиденциальность.

Есть четкая перекличка в заповедях компьютерной этики Commandments of Computer Ethics с Commandments of the Bible. Их формулировки отсылают нас к исходным положениям классических учений об этике, начиная с «Thou shalt not harm other people», «Thou shalt not steal», «Thou shalt not bear false witness» и т. п., формулируя их применительно к веку информационных технологий и требуя их неукоснительного исполнения.

Таким образом, профессиональная этика специалиста по защите информации возвращает нас к представлению об этике как норме обязательного поведения определенного класса и профессии (lawers, clergy, medical doctors, financiers).

Современность придает понятию «professional ethics» новый смысл, без усвоения которого невозможна работа в сфере информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. Философский словарь / Под ред. И. Т. Фролова. 7-е изд. М.: Республика, 2001. — 700 с.
2. Этика делового общения // Википедия. URL: http://ru.wikipedia.org/wiki/ (дата обращения — 09.06.12 г.).