ФИЛОСОФСКИЕ НАУКИ

КРАТКИЙ АНАЛИЗ ОСНОВНЫХ МЕР ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Манжуева Оксана Михайловна
Док. филос. наук, доцент кафедры информационно-коммуникационных технологий ФГБОУ ВО ВСГИК, г. Улан-Удэ
Костылева Ольга Петровна
Преподаватель ГАПОУ РБ БРМТИТ, г. Северобайкальск

АННОТАЦИЯ: в статье рассматриваются основные меры обеспечения информационной безопасности: экономические методы, технические средства, правовые и морально-этические меры. Проведен краткий анализ эффективности их применения, на основании чего сделан вывод об особой роли морально-этических мер. Авторы доказывают, что морально-этические меры, являющиеся первым и последним рубежом в построении системы защиты информационной безопасности.

ANNOTATION: the article examines the main measures to ensure information security: economic methods, technical means, legal and moral and ethical measures. The analysis of the effect of their application is carried out, a conclusion is made about the role of moral and ethical measures. The authors argue that moral and ethical measures are the first and last stage in the construction of the information security protection system.

Ключевые слова: информационной безопасность, экономические методы, технические средства, правовые меры, морально-этические меры.

Key words: information security, economic methods, technical means, legal measures, moral and ethical measures.

В литературе существует широкая классификация методов и средств по обеспечению защиты безопасности в информационных системах. Под системой защиты информации предполагают сумму специальных служб, методов, средств, мероприятий по обеспечению защиты безопасности системы и циркулирующей в ней информации. В число основных способов обеспечения защиты информационных систем относят мероприятия организационного, правового, инженерно-технического, программно-аппаратного и криптографического характера [2]. Необходимо отметить, что значительно реже в число указанных мер включают морально-этические методы [2; 8].

Доктрина информационной безопасности Российской Федерации, в качестве основных мер по обеспечению безопасности выделяет правовые, организационно-технические и экономические.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя: разработку программ обеспечения информационной безопасности РФ и определение порядка их финансирования; совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

В свою очередь, технические средства защиты информации заключаются в аппаратном и программном обеспечении, входящем в состав автоматизированной системы. Организационные или, иначе, административные меры представляют собой меры защиты, регулирующие рабочие действия автоматизированной системы обработки информации, правила использования ресурсов, работу персонала.

Здесь стоит заметить, что организационные меры защиты информации, скорее, необходимы для обеспечения эффективного поддержания каких-либо других видов средств защиты, но обеспечить необходимый уровень безопасности, основываясь исключительно на административных мерах.

Технические средства, развиваемые в одном или нескольких направлениях, требующие определенного программного обеспечения, в известном смысле определяют деятельность по технической защите информационных систем. Но необходимо отметить, как показала практика, возможность построить эффективную и бесперебойно функционирующую систему на основе одних технических средств защиты исключена. Эффективность функционирования системы защиты информационной безопасности зависит от суммы объективных и субъективных характеристик, одна из которых – степень качества аппаратного и программного обеспечения, заложенного в ее основе.

Качество технической защиты, образующей каркас системы безопасности, определено, прежде всего, профессиональными и личностными характеристиками индивида: ошибки и недостатки, как в компьютерных программах, так и в аппаратных средствах – неизбежный спутник информационной технологии, повышение качества – это никогда не прекращающийся процесс. Изложенное выше говорит о необходимости постоянной работы с персоналом организации в целях повышения образователь-

ного уровня, формирования благоприятной психологической атмосферы в коллективе и воспитания определенных морально-этических установок. Гипотеза о создании абсолютно надежных технических и физических средств защиты, отсекающих всякую вероятность существования открытого канала утечки информации, всегда оставляет возможность воздействия на сотрудников организации, обеспечивающих бесперебойное функционирование системы. Слаженную эффективную работу этих специалистов по обеспечению корректной работы технологических средств защиты В. Ю. Гайкович и Д. В. Ершов справедливо называют «ядром безопасности» всей системы [2].

Таким образом, на качество технической защиты, образующей каркас системы безопасности, сильное влияние оказывает человеческий фактор [1, С. 188; 3; 6, С. 71]. Прочность системы безопасности обусловлена стойкостью и профессионализмом коллектива, а повышение ее уровня происходит за счет законодательных и морально-этических мер. При этом самые совершенные законы и эффективнейшая кадровая политика не являются достаточными для конечного решения проблем защиты.

Правовые меры защиты предоставляют собой действующие национальные законы и нормативные акты, определяющие основные правила действий в информационной среде, ответственность за их правонарушения, тем самым препятствующие противозаконному применению информационных технологий и обеспечивающие сдерживающие условия с целью предотвращения девиантного поведения.

На взгляд авторов, морально-этические меры противодействия в системе информационной безопасности требуют обязательного внедрения в практику защиты информации, а также должного уровня изучения, поскольку невнимательное отношение к данной группе методов является серьезным упущением при построении системы защиты политики безопасности. Морально-этические меры противодействия в определенном отношении универсальны, поскольку принципиально применимы на всех уровнях защиты от несанкционированного доступа к автоматизированной системе и информации.

Морально-этические меры задают правила обращения с информацией и накладывают определенную степень ответственности за их несоблюдение. Различают два направления: создание и поддержание в обществе негативного отношения к нарушениям и нарушителям по отношению к информационной безопасности, в том числе и карательного характера. Второе заключается в координации действий, направленных на повышение уровня образованности и информированности общества в области информационной безопасности. Необходимо заметить, что морально-этические и правовые меры противодействия в некотором смысле являются универсальными мерами на всех этапах построения системы защиты. В одних случаях они являются единственным способом защиты информации от неправомерных действий: злоупотребления служебным положением при работе с информацией, защита открытой информации от незаконного тиражирования и т. д. В других случаях люди просто не совершают противоправных действий не потому, что это технически сложно или невозможно, а потому, что подобные действия выходят за рамки допустимых норм в обществе, они осуждаются и, более того, наказываются.

Юридическая ответственность за правонарушения в информационной сфере, на первый взгляд, кажется одним из эффективнейших способов регулирования общественных отношений. Но реальность такова, что на правовом уровне вопросы гражданско-правовой ответственности за нарушения информационной безопасности не находят своего отражения, развитие законодательства в данной области весьма отстает от темпов роста технологий и числа преступлений в информационной среде [5; 7].

Еще одна причина касается координации характера направления разработки и применения законодательных мер. Такая новая область деятельности, как информационная безопасность, требует применения мер скорее не карательного характера, а, в первую очередь, с нашей точки зрения, разъяснительного: в подобной ситуации важно научить, оказать помощь, чем запретить и наказать. Сегодня общество должно ясно осознать всю важность проблемы, увидеть и понять возможные пути решения поставленных задач. В этой связи необходимо скоординировать усилия научного, учебного и производственного плана. От государства в частности и общества в целом, прежде всего, требуются интеллектуальные вложения, направленные на формирование морально-этических установок функционирования в информационной среде.

Таким образом, принципиально невозможно построить абсолютно (идеально) надежную систему защиты информационной безопасности. Кроме того, систему защиты безопасности невозможно построить, основываясь исключительно на организационно-технических и экономических средствах. В первую очередь, прочность системы безопасности определяется стойкостью и профессионализмом персонала, а повышение ее уровня происходит за счет законодательных и морально-этических мер.

При этом важно отметить, что самые совершенные законы и эффективнейшая кадровая политика не являются достаточными для конечного решения проблем защиты. Поскольку всякий человек, даже обладающий абсолютной надежностью, не застрахован от неумышленного случайного нарушения. Кроме того, достаточно сложно воспитать такого уровня персонал, в отношении которого невозможно предпринять различные усилия, вынуждающие обойти предписания. В данной ситуации острую актуальность приобретают морально-этические меры, являющиеся первым и последним рубежом в построении системы защиты информационной безопасности. В процессе обеспе-

чения информационной безопасности как социального явления в качестве главного фактора построения системы защиты и регулятора деятельности человека в информационной среде выступают морально-этические принципы и ответственность каждого, основанные на принятых правилах поведения в обществе и подкрепленные мерами законодательного характера на государственном уровне. Подобный подход, основанный на приоритете морально-этических мер в процессе обеспечения информационной безопасности, на наш взгляд, позволит найти новые направления повышения эффективности системы защиты.

Литература:

1. Благодатских В. А. Стандартизация разработки программных средств. М.: Финансы и статистика, 2006. – 283 с;

2. Гайкович В. Ю., Ершов Д. В. Основы безопасности информационных технологий. М.: МИФИ, 1995. – 96 с.

3. Деминг Э. Выход из кризиса. Новая парадигма управления людьми, системами и процессами. М.: «Альпина Паблишер», 2011. – 417 с.

4. Евдокимов К. Н. К вопросу о причинах компьютерной преступности в России // Известия ИГЭА. – Иркутск, 2010. – № 6. – С. 167-170.

5. Макаренко С. И. Информационная безопасность. Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.

6. Миллер Г. У. Качественная программа: будущее информационной технологии. М.: ИНИОН РАН, 1993. – С. 63-75.

7. Стюгин М. А. Защита систем от исследования. Методы и модели построения защищенных систем и управления информацией в конфликте. М.: РРГУ, 2011. – 132 с.

8. Хофман Л. Дж. Современные методы защиты информации: пер. с англ. М.: Сов. Радио, 1980. – 264 с.