УДК 008

Вавилова Елена Юрьевна

Vavilova Elena Yurievna

Кандидат филос. наук, доцент кафедры «Гуманитарные науки»

Candidate of Philosophical Sciences, Associate Professor of Humanities Department,

Кузин Артём Викторович

Kuzin Artem Viktorovich

Старший преподаватель кафедры «Информационные системы и технологии»

Senior Lecturer of the Department of Information Systems and Technologies,

Изварина Анастасия Антоновна

Izvarina Anastasia Antonovna

Студент

Student,

ФГБОУ ВО «Ярославский государственный технический университет»

Yaroslavl State Technical University

Ярославль, Россия

Yaroslavl, Russia

БЕЗОПАСНОСТЬ КАК КОНСТАНТА СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ РАЗРАБОТОК

SECURITY AS A CONSTANT OF MODERN INFORMATION DEVELOPMENTS

Аннотация: В современном мире огромное значение приобрело сочетание гуманистических нравственных ценностей с практикой информационной безопасности. Информационная безопасность – комплекс технико-административных мер, направленных на поддержание в цифровом пространстве ценностей конфиденциальности, целостности, доступности, подлинности, этичности контента. С конца XX века стало развиваться многокомпонентное поле информационной безопасности. В нем выделяются основные взаимосвязанные части: физическая, инфо-технологическая, социо-психологическая, прогностическая.

Abstract: In the modern world, the combination of humanistic moral values with the practice of information security has become of great importance. Information security is a set of technical and administrative measures aimed at maintaining the values of confidentiality, integrity, accessibility, authenticity, and ethics of content in the digital space. Since the end of the XX century, the multicomponent field of information security has been developing. It highlights the main interrelated parts: physical, info-technological, socio-psychological, prognostic.
Ключевые слова: информационная безопасность, современные технологии, общество.
Key words: information security, modern technologies, society.

Глобальная цифровизация современного общества подтверждает, что прогресс невозможен без информационного обмена. Развитие последнего традиционно было связано с вопросами безопасности передаваемых или сохраняемых данных.

В соответствии с комплексом документов РФ, регулирующих вопросы безопасности, «под информационной безопасностью понимается состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере» [2, с. 132]. Шире, информационная безопасность – комплекс технико-административных мер, направленных на поддержание в цифровом пространстве ценностей конфиденциальности, целостности, подлинности, этичности контента. Сюда же входят меры, направленные на предотвращение доступа к конфиденциальной информации третьими лицами, ее хранение и разработка адекватных сред для передачи данных. Вопросами обеспечения физической сохранности данных занимается безопасность критической информационной инфраструктуры. Проблемами безопасности в компьютерных сетях занимается кибербезопасность – дисциплина, изучающая угрозы сети Интернет, этику «веб-сёрфинга», сокрытие личности, защитные протоколы и др.

Следует понимать, что в современном мире информация существует как в цифровой, так и в «нецифровой» форме, и обращение к тому или иному виду информации подразумевает различные методы ее обработки, передачи и хранения. Исторически информация в любой форме подразделяется на

общедоступную и конфиденциальную. Конкретное наполнение, количество и качество этих категорий информации социально обусловлено. Именно процессы, производимые над конфиденциальной информацией, породили ряд методов, которые послужили началом развития информационной безопасности. Если же глобально понимать информацию как продукт психофизической деятельности интеллектуальной системы, то выделяются несколько этапов в изменении понимания рисков и обеспечения качества безопасности данных.

Простейшие способы физической защиты данных применялись еще в древности: охрана, перевод на редкие языки, тайные кабинеты, использование доверенных лиц и т. п. В 1816 году появляется электро- и радиосвязь. Набирает популярность кодировка сообщений с помощью сигнала и его последующие декодирование. С 1935 года появляются радиолокационные и гидроакустические средства. Когда в 1946 году поваляется электронно-вычислительная машина или компьютер, люди понятия не имели, как защищать хранящуюся в нем информацию. Отсюда доступ к данной технологии ограничивался физическим доступом к оборудованию. В 1970-х годах появляются средства коммуникации с широким спектром задач. Но и угрозы стали гораздо серьезнее. Выделилась группа людей, которая при желании могла наносить ущерб информационной безопасности отдельных пользователей (хакеры). Общество и государство не могло игнорировать появившуюся сферу правонарушений и преступности, поэтому формируется информационное право. 1980-е годы выявили качественно новые возможности человечества – от все ускоряющегося совершенствования технологий до полетов в космос. При этом выяснилось, что нет идеально работающих компьютерных программ и моделей поведения пользователей, которые гарантируют абсолютную безопасность.

С конца XX века стала важна оценка потенциальной безопасности любых инновационных технологий. Среди таких систем наиболее активно исследуются те, которые способны самостоятельно генерировать информацию. Во-первых, это разработки и продвижение искусственного интеллекта. Прогностически его относят к подобным человеческому разуму системам, основанных на нечетких

множествах и нейронных сетях. Во-вторых, сложные генераторы псевдослучайных чисел. Они также могут относится к системам, порождающим информацию, хотя и с большой натяжкой. Псевдослучайными они называются, потому что существуют некие правила (формула), которая в большей степени определяет, какое значение будет сгенерировано. Встречаются также аппаратные генераторы (истинно) случайных чисел, в основе которых лежат различные физические процессы. В-третьих, существует пространство дополненных реальностей. Виртуальную реальность мы исключаем – в ней уже все продумано, новая информация, формально, не возникает. Другое дело системы, которые выводят на интерфейс информацию в режиме реального времени, дополняя картину окружающего мира. Например, нашлемный HUD летчика-истребителя, выдающий траекторию движения, приборную скорость, угол атаки и захват цели. На основании получаемых данных, пилот принимает какое-то решение, и таким образом в процессе появляется новая информация, которую также нужно оценивать. В окружающем нас поле обмена контентом уже сложились требования к цифровым технологиям, которые сводятся к доминантам работоспособности, применимости, эффективности, законности, этичности, безопасности. Указанные позиции относятся как к уже существующим технологиям, так и к разрабатываемым инновационным многокомпонентным системам.

Сейчас много внимания с позиции прогнозов безопасности привлекают нейросети и нейроинтеграционные технологии – как заявка на радикальное изменение человеческого бытия. Нейротехнологии могут оказывать влияние на человеческий мозг непосредственно, поэтому оценка их опасности/безопасности, пользы/вреда для человечества актуально противоречива (табл. 1).

Таблица 1

Дискуссионные вопросы нейротехнологий

Новшество	Прогрессивный компонент	Потенциальные риски

Установка импланта в мозг человека	Лечение психических и иных заболеваний, активация/блокирование зон мозга по медицинским показаниям.	Ошибки при взаимодействии с мозгом человека. Нехватка знаний об анатомии и физиологии высшей нервной деятельности человека.
Управление имплантом через интерфейс носимого устройства (смартфон, часы)	Непосредственное отслеживание и управление своим физическим состоянием.	Утрата устройства, завладение им третьими лицами, возможность злонамеренного использования. Как будет осуществляться управление в условиях отсутствия или некачественной работы Интернет-сетей?
Использование нейроинтерфейсов различного спектра	Лечение нейродегеративных заболеваний, возможность для физически неполноценных людей управлять гаджетами [1, с. 350].	Краткосрочность, большое влияние индивидуальных факторов, возможность вмешательства третьих лиц. Необходимость постоянного обновления составляющих терапевтической системы.

Таким образом, с конца XX века стали развиваться системно связанные направления информационной инновационной безопасности, включающие следующие компоненты:

- физический компонент защиты и охраны субъекта и объекта информационного процесса;

- инфо-технологический компонент информационной безопасности;
- социо-психологический компонент снижения рисков при работе с информацией, использовании и передаче разного рода данных;
- предупреждающее проектирование архитектуры информационной безопасности и снижения рисков.

Библиографический список:

1. Свааб Дик. Наш креативный мозг. Как человек и мир творят друг друга / Пер. Д.В. Сильвестрова. Спб.: Изд-во И. Лимбаха, 2020. 512 с.

2. Цвык И.В. Компьютерная этика и проблемы интеллектуальной безопасности // Вестник РУДН, Серия «Философия». 2013, № 3. С. 125-133. Режим доступа: https://cyberleninka.ru/article/n/kompyternaya-etica-i-problemy-intellectualnoy-bezopasnosti/viewer (дата обращения 13.01.2021).