Кушнир Светлана Ивановна
канд. ист. наук, доцент, доцент
ФКОУ ВО «Воронежский институт
Федеральной службы исполнения наказаний»
г. Воронеж, Воронежская область
Кушнир Михаил Станиславович
студент
ФГБОУ ВО «Воронежский государственный
университет инженерных технологий»
г. Воронеж, Воронежская область

НЕКОТОРЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПОСЛЕДСТВИЯ ИХ ИГНОРИРОВАНИЯ

Аннотация*: информационная безопасность является одной из составляющих безопасности человека в современных условиях. Однако сложно говорить о решении проблемы информационной безопасности, если нет ее четких критериев, нет четких требований к этике такой безопасности, а личное пространство человека в цифровую эпоху находится под угрозой.*

Ключевые слова*: цифровое общество, глобализация, информационная безопасность, личная информация.*

В современном обществе существует множество проблем информационной безопасности, назовем лишь некоторые из них.

Кибератаки и хакеры: злоумышленники могут взламывать компьютерные системы, похищать конфиденциальные данные или провоцировать кибератаки.

Фишинг и мошенничество: киберпреступники могут использовать фишинговые письма или веб-сайты для обмана людей и получения их личной информации.

Утечки данных: крупные организации могут столкнуться с утечками данных, когда конфиденциальная информация становится доступной для посторонних лиц.

Недостаточная защита персональных данных: с множеством сервисов онлайн существует риск утечки или неправомерного использования личной информации пользователей.

Социальная инженерия: злоумышленники могут использовать манипулятивные методы, чтобы обмануть людей и получить доступ к важной информации.

Нехватка осведомленности и обучения: многие люди не осознают угрозы информационной безопасности и не знают, как защитить себя и свои данные.

Эти проблемы требуют постоянного внимания и улучшения в области информационной безопасности.

Но еще одной важной проблемой является Этическая проблема информационной безопасности. Дело в том, что информационная безопасность является таким состоянием информационной системы, которая не несет угроз окружающим людям и не представляет опасности для них. А этика сохранения тайны является важнейшим компонентом информационной безопасности.

На протяжении столетий вопросам сохранения чужой информации (читай тайны) уделялось огромное внимание, придавалось особое значение. Основная проблема здесь заключается в следующем: насколько информация должна быть скрыта или наоборот – насколько информацию возможно раскрыть? В какой области лежат критерии раскрытия информации и каковы они?

Некоторое время назад общество вступило в информационную эпоху своего развития. Эти изменения тотчас указали на этический коллапс в информационной среде в рамках морально-институциональных границ дозволенности информационной неприкосновенности человека в условиях развития глобальной информационной цивилизации [1].

Не удивительно, что самое широкое развитие правовые и этические проблемы сохранности личной информации приобрели именно в период становления информационного общества, в эпоху глобализации.

Этическая проблема информационной безопасности заключается в том, что использование информации и технологий без соблюдения этических норм мо-

жет привести к негативным последствиям для людей, организаций и общества в целом. Некоторые аспекты этой проблемы включают:

Нарушение приватности: несанкционированный доступ или использование чужих персональных данных без согласия является нарушением приватности и этически неприемлемо.

Манипуляция информацией: использование лживой или искаженной информации с целью манипулирования мнением общественности или достижения личных целей создает этические проблемы.

Конфликт интересов: в сфере информационной безопасности могут возникать ситуации, когда интересы различных сторон (например, компаний, государства, отдельных лиц) сталкиваются, и необходимо принимать этически обоснованные решения.

Ответственность за использование информации: люди и организации, имеющие доступ к конфиденциальной информации, несут ответственность за безопасное и этичное использование этой информации, чтобы избежать нанесения вреда другим.

Технологические последствия: развитие новых технологий, таких как искусственный интеллект или биометрическая идентификация, создает этические дилеммы в области защиты данных и личной приватности.

Ключевым аспектом в решении этических проблем информационной безопасности является соблюдение принципов прозрачности, справедливости, ответственности и уважения к приватности и правам других людей.

Личная жизнь является одним из аспектов жизни частной – это самое потаенное, это любые формы крайнего уединения, ухода в свой собственный внутренний мир. И этическим объектом защиты в данном случае выступают как мысли, так и чувства человека, которые крайне сложно оценить и измерить всесторонним образом. Поэтому именно этика не столько защищает от физических посягательств и насилия, сколько оберегает душевное и нравственное спокойствие, создавая «зону психологической безопасности» [2].

В период бурного генезиса информационного общества важный характер приобретают проблемы гарантии информационной неприкосновенности границ частной жизни как некой существенной доли свободы каждой личности.

Если недооценить важность вопросов информационной безопасности, то можно получить социальные, экономические и, наконец, политические катастрофические последствия. Поэтому многие ученые, чья деятельность так или иначе связана с информационной безопасностью делают вывод о необходимости формирования системы глобальной информационной безопасности. При этом отмечается, что существование такой системы невозможно без формирования особой информационной культуры социума [3].

Несоблюдение этических принципов информационной безопасности может привести к серьезным последствиям как для отдельных лиц, так и для организаций и общества в целом. Некоторые из потенциальных угроз в случае нарушения этических принципов:

Утечка конфиденциальной информации: несанкционированный доступ к важным данным и их утечка может привести к серьезным последствиям, таким как финансовые потери, повреждение репутации и ущерб для отношений с клиентами и партнерами.

Кража личных данных: использование личной информации без согласия владельца может привести к краже идентификационных данных, мошенничеству, а также нарушению приватности личной жизни.

Нарушение законов: несоблюдение этических норм может привести к нарушению законодательства о защите данных и привести к юридическим последствиям, таким как штрафы или судебные иски.

Повышенный риск кибератак: ненадлежащая защита информационных систем от киберугроз может способствовать уязвимостям и повысить риск кибератак, что может привести к серьезным последствиям для организации и ее клиентов.

Подрыв репутации: нарушение этических принципов информационной безопасности может нанести значительный ущерб репутации организации или

индивида, что может привести к потере доверия со стороны клиентов, партнеров и общественности.

Эти угрозы подчеркивают важность соблюдения этических принципов информационной безопасности и необходимость принятия мер по обеспечению безопасности данных и защите приватности.

В настоящих условиях также имеют значение техническая грамотность, культура и этика поведения человека, которые должны соответствовать существующей модели информационной безопасности.

Информационная этика является постоянно развивающейся областью исследований, которая включает в себя оценку отношений между фактами, теориями, политикой и ценностями в плане быстрого развития информационных технологий. Информационная этика занимается анализом социальных и личных воздействий информационных технологий. Глобальные проблемы информационной этики возникают в связи с отсутствием ясности в вопросах о том, каковы этические ограничения создания и применения информационной технологии, а также, как следует вести себя в условиях, когда информационные технологии предоставляют обществу и личности новые возможности в выборе действий. Проблемы искусственного интеллекта, генной инженерии и клонирования также входят в сферу информационной этики.

Список литературы

1. Кушнир С.И. Этические аспекты информационной безопасности / С.И. Кушнир, М.С. Кушнир // Актуальные вопросы гуманитарных и социальных наук: от теории к практике: материалы Всероссийской научно-практической конференции с международным участием. – Чебоксары, 2023. – С. 91–93. – EDN PBFZIM

2. Атаманов Г.А. О необходимости философского обоснования проблемы информационной безопасности / Г.А. Атаманов // Власть и воздействие на массовое сознание. – Пенза: РИО ПГСХА, 2007. – С. 84–87.

3. Астахова Л.В. Информационная безопасность: герменевтический подход / Л.В. Астахова. – М.: РАН, 2010. – 185 с. – EDN RVMWXT

4. Догучаева С.М. Анализ современных проблем информационной безопасности в российских компаниях / С. М. Догучаева // Риск: ресурсы, информация, снабжение, конкуренция. – 2022. – №2. – С. 65–68. EDN JXIBRK