В. П. Гайдук[1], В. А. Шапцев[2]
[1]НКО СЮНВ «ЮНОВА», г. Тюмень
[2]Тюменский государственный университет, г. Тюмень

К ВОПРОСУ О СОЗДАНИИ В РОССИИ ЦИФРОВОЙ ПОЛИЦИИ. ТЕХНОЛОГИЧЕСКИЙ АСПЕКТ

Аннотация. Обосновывается актуальность фундаментального решения проблемы засорения (экологической чистоты) Web-среды России. Такие технологии как информационные агенты, актуальные и точные данные — модель реальности, хакерские приемы агрессии сайтов и рабочих мест и др. позволяют при достаточной политической воле государства, адекватном финансировании и профессионализме разработчиков сделать жизнедеятельность в цифровой инфраструктуре эффективной: с высокой производительностью, без вреда здоровью, благополучию и с жизнерадостным настроением. Предлагаемое средство – активная цифровая силовая структура и адекватное законодательство.

Ключевые слова: информационная экология человека**,** цифровая инфраструктура России, эффективная жизнедеятельность, актуальные данные – модель реальности, цифровое право, цифровая полиция.

Насыщенность информационного поля (корректнее, потока сообщений и данных на) каждого человека экспоненциально растет. Совокупность эффектов и последствий этого процесса сформулировано как проблематика информационной экологии (обзор в [1]). В поддержку информационной активности граждан с 01.10.2019 г. в ГК РФ действует статья 141.1, закрепляющая понятие «цифровое право». «Согласно документу, цифровые права представляют собой «обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы». Оборот цифровых прав (осуществление, передача, залог, ограничение распоряжения и пр.) допускается только с помощью внесения записей в информационную систему без обращения к третьему лицу» [2].

С другой стороны, экологически деструктивна растущая цифровая преступность [3]. Информационная безопасность как «набор процедур и инструментов, которые обеспечивают всестороннюю защиту конфиденциальной корпоративной информации от неправильного

использования, несанкционированного доступа, искажения или уничтожения» [4], занимает пассивную позицию (только защиту) в отношении цифровой преступности, направленной прежде всего на отдельно взятого гражданина. Необходимо постоянно действующее силовое воздействие на потоки сообщений к человеку и на их источники, включая создателей и владельцев этих источников.

В этой связи в рамках цифровой трансформации [5] («фундаментального переосмысления клиентского опыта») актуально направление разработок по поддержке активной, цифровой, силовой деятельности государства в Web-среде, обеспечивающей «эффективную жизнедеятельность» [6] граждан.

Объем публикации не позволяет развернуть обсуждение всех нюансов такой деятельности. Здесь авторы лишь анонсируют само направление и формулируют локальную концепцию ее технологической основы.

Анонсированное выше исследование имеет целью защищенность каждого гражданина от информационной агрессии и одурачивания злоумышленниками, владеющими цифровыми технологиями и преступными намерениями. Предметом исследования являются адекватные **силовые цифровые технологии**, формулировки **соответствующих законодательных инициатив**, **организационные формы** осуществления соответствующей деятельности.

Методы исследования: обобщение фактов агрессии рабочего места пользователя компьютера и гаджета, моделирование и конструктивный анализ множества сценариев преступных информационных атак пользователей, дискуссии на встречах со специалистами как ИТ-сферы, так и силовых ведомств, системный синтез полицейской цифровой платформы (ПЦП), семантически корректное использование терминологии.

Локальным результатом системных размышлений на выбранную тему является следующая концепция технологии полицейского надзора, в частности (табл. 1).

У инфо-агента, например, имеется набор данных об оригинальном(ых) сайте(ах) (в частности, копия его части), с которым и сравниваются подозреваемые. Возможна и некоторая имитация действия клиента с ним в процессе идентификации подозрительного цифрового объекта.

Таблица 1

Концептуальный сценарий полицейского надзора в цифровой среде по факту, например, «мошеннический сайт» Сбера

№	*Действие*	*Исполнитель*	*Примечание*
1	*2*	*3*	*4*
1.	Создание специального информационного агента [7]	ИТ-специалист	Есть адекватные инструменты [7]
2.	Добавление инфо-агенту свойств глубокого проникновения	Доброжелательный хакер	
3.	Запуск инфо-агента в интернет	Дежурный оператор	
4.	Идентификация подозрительных цифровых объектов	Дежурный цифровой аналитик, интеллектный [8] модуль ПЦП	При несовпадении образов оригинала и объекта — решение: фейк, правда, доисследовать
5.	Анализ и классификация фактов (фейков) и результатов доисследования	Цифровой полицейский-аналитик с участием интеллектного компонента ПЦП	
6.	Формулирование проекта решения	- “ -	Воздействие на источник и обращение в суд по его владельцу
7.	Утверждение решения	ЛПР	
8.	Исполнение решения (блокирование сайта, штрафование и пр.)	Ответственное лицо	
Инфо-агенты могут работать непрерывно. По мере накопления опыта они и ПЦП совершенствуются			

Авторы понимают неглубокую проработанность идеи. Цель выступления — обратить внимание молодых ИТ-профессионалов, особенно по информационной безопасности; юристов и сотрудников силовых структур; органов власти на актуальность и возможность начала работ в рассматриваемом направлении с учетом развитости

новейших цифровых технологий и актуальности борьбы с цифровыми преступлениями и цифровой агрессией.

Разумеется, начало работ требует соответствующей воли лиц, принимающих решения, и наличия источника достаточного финансирования.

СПИСОК ЛИТЕРАТУРЫ

1. Евкова А. Проблематика информационной экологии. — URL: https://www. evkova.org/esse/problematika-informatsionnoj-ekologii (дата обращения 25.04.2023).
2. Волуйская М. В чем суть нового закона о цифровых правах? URL: https://aif.ru/society/law/chto_takoe_zakon_o_cifrovyh_pravah (дата обращения: 25.04.2023).
3. Поляков И.В. Цифровая преступность: проблемы понятийного аппарата, систематизации и правоприменительной практики // Проблемы правоохранительной деятельности. — 2020. — № 4. — С. 21-25.
4. Общие сведения об информационной безопасности (InfoSec). — URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-information-security-infosec (дата обращения: 25.04.2023).
5. Что такое цифровая трансформация? — URL: https://www.sap.com/cis/insights/ digital-transformation.html (дата обращения: 23.01.2021).
6. Шапцев В.А. Концепция человекоподобного диалога с цифровой инфраструктурой организации (на примере роли профессора университета) // Математическое и информационное моделирование. Вып. 19: материалы Всероссийской конференции молодых ученых. Тюмень, 17-21 мая 2021 г.). — С. 457-469. — URL: https://elib.utmn.ru/jspui/handle/ru-tsu/7220. (дата обращения 01.04.2023).
7. Пихтовникова И.В., Шапцев В.А. Обзор источников сведений по методологии «информационный агент» // Математическое и информационное моделирование: сборн. науч. трудов. Вып. 15, ч. 1. Тюмень: Изд-во ТюмГУ, 2017. — С. 295-306. (дата обращения: 01.04.2023).
8. Васильев С.Н., Жерлов А.К., Федосов Е.А., Федунов Б.Е. Интеллектное управление динамическими системами. — Москва: Физико-математическая литература, 2000. — 352 с.