СОВЕРШЕНСТВОВАНИЕ ПРОФИЛАКТИКИ КИБЕРПРЕСТУПЛЕНИЙ ПОСРЕДСТВОМ ПОВЫШЕНИЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАСЕЛЕНИЯ

Ё.Кудратов
самостоятельный соискатель.

https://doi.org/10.5281/zenodo.23743999

Аннотация. *В статье исследуются вопросы профилактики киберпреступлений через повышение культуры информационной безопасности населения. Рассмотрены понятие и структура культуры информационной безопасности, криминологическая характеристика наиболее распространенных киберпреступлений против граждан и роль методов социальной инженерии в их совершении. Обосновывается положение о том, что значительная часть киберпреступлений становится возможной не из-за технических уязвимостей, а вследствие недостаточной цифровой грамотности пользователей. На основе анализа зарубежного опыта предложена многоуровневая модель формирования культуры информационной безопасности, включающая систему непрерывного образования, информационные кампании, государственно-частное партнерство и механизмы оперативного оповещения.*

Ключевые слова: *киберпреступность, информационная безопасность, культура информационной безопасности, социальная инженерия, фишинг, мошенничество, цифровая гигиена, профилактика, государственно-частное партнерство.*

Цифровая трансформация, охватившая практически все сферы жизни общества, открыла перед гражданами широкие возможности: дистанционные банковские услуги, электронная торговля, онлайн-образование, получение государственных услуг через электронные порталы. В Республике Узбекистан развитие цифровой экономики и электронного правительства определено одним из приоритетов государственной политики [6]. Вместе с тем цифровизация создала и новые риски. Киберпреступность сегодня относится к наиболее динамично растущим видам преступности как в мире, так и в нашей стране.

Особенностью киберпреступлений является их трансграничный и дистанционный характер: преступник и потерпевший не встречаются лично, преступление может совершаться с территории другого государства, а цифровые следы относительно легко скрыть. Это существенно затрудняет раскрытие таких преступлений и возмещение причиненного ущерба [8; 16]. Следовательно, ключевое значение приобретает предупреждение преступлений — недопущение того, чтобы гражданин стал жертвой.

В Республике Узбекистан сформирована правовая база в сфере обеспечения информационной безопасности. Принят Закон «О кибербезопасности» [1], действуют законы «Об информатизации» [2] и «О персональных данных» [3]. В Уголовный кодекс включена специальная глава XX¹ «Преступления в сфере информационных технологий», а мошенничество с использованием компьютерной техники квалифицируется как отягчающее обстоятельство в рамках статьи 168 [4]. Однако правовые и технические меры сами по себе не способны предотвратить преступления, совершаемые посредством обмана самого пользователя.

Цель настоящей статьи — обосновать роль культуры информационной безопасности населения в профилактике киберпреступлений и разработать предложения

по ее повышению. Методологическую основу исследования составили общенаучные методы анализа и синтеза, сравнительно-правовой и системный методы, а также обобщение данных международных исследований.

Под культурой информационной безопасности в настоящей статье понимается совокупность знаний, ценностей, установок и устойчивых моделей поведения личности, обеспечивающих осознанное распознавание угроз в цифровой среде и защиту от них собственной информации, денежных средств и прав. Европейское агентство по кибербезопасности (ENISA) подчеркивает, что культура кибербезопасности проявляется не столько в знаниях, сколько в повседневном поведении людей и в том, насколько безопасное поведение стало для них привычным [12].

В структуре культуры информационной безопасности можно выделить следующие компоненты:

- **когнитивный** — знания об основных видах угроз, способах мошенничества, правах пользователя и порядке действий при инциденте;
- **ценностно-мотивационный** — понимание ценности персональных данных, осознание личной ответственности за собственную безопасность;
- **поведенческий** — устойчивые навыки безопасного поведения: использование надежных паролей и двухфакторной аутентификации, проверка ссылок и источников, отказ от передачи кодов подтверждения третьим лицам;
- **критический** — способность критически оценивать поступающую информацию, распознавать манипуляции и попытки психологического давления.

Европейская рамка цифровых компетенций граждан (DigComp) выделяет безопасность — защиту устройств, персональных данных, здоровья и благополучия в цифровой среде — в качестве одной из пяти базовых областей цифровой компетентности [17]. Это подтверждает, что информационная безопасность является неотъемлемой частью цифровой грамотности каждого гражданина, а не узкопрофессиональной сферой специалистов.

С позиции теории рутинной активности Л. Коэна и М. Фелсона преступление происходит при совпадении трех элементов: мотивированного преступника, подходящей цели и отсутствия способного охранителя [15]. В цифровой среде мотивированных преступников и потенциальных целей неограниченно много, а роль «охранителя» в значительной мере выполняет сам пользователь: его знания, внимательность и навыки. Повышение культуры информационной безопасности, таким образом, делает пользователя «трудной целью» и разрывает цепочку условий, необходимых для совершения преступления.

Данный подход согласуется с концепцией ситуационной профилактики, направленной на увеличение усилий и риска для преступника и снижение его выгоды. Если значительная часть граждан будет знать, что банк никогда не запрашивает код из SMS, «стоимость» мошеннической схемы для преступника резко возрастет, а ее эффективность снизится.

Международные исследования инцидентов информационной безопасности последовательно показывают, что в большинстве случаев утечек данных и мошенничества решающую роль играет человеческий фактор — ошибки, невнимательность или обман пользователя [14]. Самые совершенные технические средства защиты оказываются бесполезными, если пользователь сам сообщает злоумышленнику пароль или код

подтверждения. Именно поэтому профилактика киберпреступлений не может ограничиваться техническими и правовыми мерами и должна включать целенаправленное формирование безопасного поведения населения.

Анализ правоприменительной практики позволяет выделить наиболее распространенные виды киберпреступлений, направленных против граждан:

1. **Хищение средств с банковских карт** путем получения обманным путем реквизитов карты и одноразовых кодов подтверждения. Злоумышленник звонит или пишет от имени банка, платежной системы или правоохранительного органа и под различными предлогами («подозрительная операция», «блокировка карты», «обновление данных») выманивает у потерпевшего код.
2. **Фишинг** — создание поддельных сайтов, внешне неотличимых от сайтов банков, государственных порталов, интернет-магазинов, и рассылка ссылок на них с целью получения логинов, паролей и платежных данных.
3. **Мошенничество в сфере электронной торговли** — фиктивные интернет-магазины и объявления, требующие предоплаты за несуществующий товар.
4. **Инвестиционные и криптовалютные схемы** — привлечение средств под обещание сверхвысокой доходности, в том числе через поддельные торговые платформы.
5. **Захват аккаунтов** в социальных сетях и мессенжерах с последующей рассылкой от имени владельца просьб о денежной помощи его знакомым.
6. **Мошенничество с фиктивным трудоустройством и онлайн-кредитами** — требование оплаты за «оформление», «страховку» или «проверку» до получения работы или займа.
7. **Распространение вредоносных приложений**, маскирующихся под полезные программы и предоставляющих злоумышленнику доступ к SMS, банковским приложениям и персональным данным.

Большинство указанных деяний квалифицируется по статье 168 Уголовного кодекса (мошенничество), а также по статьям главы XX[1], предусматривающим ответственность за несанкционированный доступ к компьютерной информации, создание и распространение вредоносных программ и иные преступления в сфере информационных технологий [4].

Общей чертой большинства перечисленных преступлений является то, что они основаны не на техническом взломе, а на психологическом воздействии на человека. Потерпевший сам, добровольно передает преступнику информацию или переводит деньги. Такой метод получил название социальной инженерии [9; 10].

Социальная инженерия эксплуатирует универсальные механизмы человеческого поведения, описанные в психологии влияния [11]:

- **авторитет** — злоумышленник представляется сотрудником банка, правоохранительного органа, налоговой службы, что снижает критичность восприятия;
- **срочность и страх** — «на ваше имя оформляется кредит», «ваша карта будет заблокирована через пять минут»; в состоянии стресса человек действует импульсивно;
- **дефицит и выгода** — «выигрыш», «бонус», «только сегодня»; ожидание выгоды подавляет осторожность;

- **доверие и социальное доказательство** — сообщение приходит от знакомого (со взломанного аккаунта) или сопровождается отзывами «довольных клиентов»;
- **забота о близких** — «ваш родственник попал в беду, срочно нужны деньги».

Современные мошенники используют заранее подготовленные сценарии, подменные номера телефонов, персональные данные жертвы, полученные из утечек, что делает их обращения убедительными. Развитие технологий синтеза голоса и изображения создает дополнительные риски: возникают схемы, в которых злоумышленник имитирует голос или видеоизображение знакомого человека.

Уязвимость к киберпреступлениям различается в зависимости от возрастных и социальных групп.

Лица старшего возраста позднее начали пользоваться цифровыми сервисами и нередко не знают базовых правил: что банк никогда не запрашивает код из SMS, что нельзя устанавливать приложения по просьбе собеседника. Им свойственно доверие к лицам, представляющимся должностными лицами.

Молодежь активно пользуется технологиями, однако склонна недооценивать риски: публикует личную информацию в социальных сетях, устанавливает непроверенные приложения, откликается на предложения «легкого заработка». Кроме того, молодые люди нередко сами вовлекаются в преступные схемы — например, передают за вознаграждение свои банковские карты третьим лицам («дропы»), не осознавая, что тем самым становятся соучастниками.

Граждане с невысоким уровнем дохода более восприимчивы к предложениям кредитов, работы и «инвестиций» с высокой доходностью.

Типичными поведенческими ошибками пользователей являются: использование одного и того же пароля для разных сервисов; отказ от двухфакторной аутентификации; установка приложений из неофициальных источников; переход по ссылкам из сообщений без проверки адреса сайта; публикация персональных данных (номер телефона, дата рождения, фотографии документов) в открытом доступе. Многие пользователи не знают, куда и в каком порядке следует обращаться при совершении в отношении них киберпреступления, и как быстро заблокировать карту или аккаунт.

Значительная часть киберпреступлений остается за пределами официальной статистики. Потерпевшие нередко не обращаются в правоохранительные органы из-за стыда, небольшой суммы ущерба, неверия в возможность раскрытия или незнания порядка обращения. Высокая латентность искажает реальную картину киберпреступности, затрудняет выявление новых схем и снижает эффективность профилактики, поскольку сведения о новых способах мошенничества поступают с опозданием.

В Республике Узбекистан разъяснительная работа ведется органами внутренних дел, коммерческими банками, операторами мобильной связи, средствами массовой информации. Вместе с тем она носит в значительной мере разрозненный характер: каждое ведомство и организация действуют самостоятельно, единые стандарты и сообщения отсутствуют, эффективность кампаний не измеряется. В системе образования вопросы информационной безопасности рассматриваются фрагментарно, в основном в рамках курса информатики, с упором на технические, а не поведенческие аспекты. Работа с

наиболее уязвимыми группами — пожилыми гражданами и жителями сельской местности — ведется недостаточно системно.

Европейский союз. Европейское агентство по кибербезопасности (ENISA) ежегодно в октябре проводит Европейский месяц кибербезопасности — общеевропейскую информационную кампанию, в рамках которой государства-члены, частные компании и общественные организации реализуют мероприятия по повышению осведомленности граждан. ENISA разработало методические рекомендации по формированию культуры кибербезопасности, подчеркивающие необходимость опоры на поведенческие науки, ориентации на конкретные целевые группы и обязательного измерения результатов [12]. Рамка цифровых компетенций DigComp используется государствами ЕС при разработке образовательных программ для всех возрастов [17].

Великобритания. Национальный центр кибербезопасности (NCSC) реализует общенациональную кампанию «Cyber Aware», в которой сведены к нескольким простым и понятным действиям ключевые рекомендации для граждан: надежный пароль для электронной почты, двухфакторная аутентификация, регулярное обновление устройств, резервное копирование данных. Действует единый национальный центр приема сообщений о мошенничестве и киберпреступлениях (Action Fraud), что упрощает обращение потерпевших и позволяет аккумулировать сведения о новых схемах.

Сингапур. В Сингапуре полиция совместно с Национальным советом по предупреждению преступности разработала мобильное приложение ScamShield, которое фильтрует мошеннические звонки и сообщения на основе базы номеров, по которым поступали жалобы, и позволяет пользователю быстро сообщать о подозрительных обращениях. Параллельно проводятся масштабные информационные кампании, а банки обязаны внедрять дополнительные меры защиты клиентов, включая задержку и дополнительное подтверждение операций, совершаемых после смены настроек безопасности.

Австралия. Комиссия по конкуренции и защите прав потребителей Австралии ведет портал Scamwatch, на котором публикуются актуальные сведения о мошеннических схемах, принимаются сообщения граждан и регулярно издаются аналитические обзоры, используемые для корректировки профилактической работы.

Во многих странах вопросы безопасного поведения в интернете включены в школьные программы начиная с младших классов. ЮНЕСКО разработало модельную программу медиа- и информационной грамотности для педагогов и учащихся, рассматривающую в том числе вопросы приватности, безопасности и критического восприятия информации [13].

Обобщение зарубежного опыта позволяет выделить следующие принципы эффективной профилактики: простота и конкретность сообщений; ориентация на целевые группы; системное партнерство государства, банков и операторов связи; наличие единого и удобного канала для сообщений о мошенничестве; оперативное информирование о новых схемах; обязательная оценка результатов.

Направления повышения культуры информационной безопасности населения Республики Узбекистан. *Национальная концепция.* Представляется целесообразной разработка национальной концепции (программы) повышения культуры информационной безопасности населения, определяющей цели, целевые группы, ответственных исполнителей, механизмы координации и показатели эффективности. Координацию ее

реализации можно возложить на уполномоченный орган в сфере кибербезопасности с участием органов внутренних дел, образования, Центрального банка, коммерческих банков и операторов связи [1; 5].

Формирование культуры информационной безопасности должно охватывать все уровни образования [7]:

- **дошкольное и начальное образование** — в игровой форме усваиваются простые правила: не общаться с незнакомыми в сети, не сообщать адрес и номер телефона, рассказывать взрослым о неприятных ситуациях;
- **общее среднее образование** — в рамках информатики или отдельного модуля изучаются безопасность паролей, распознавание фишинга, защита персональных данных, кибербуллинг, правовые последствия участия в мошеннических схемах (в том числе передачи своих банковских карт третьим лицам);
- **профессиональное и высшее образование** — для всех направлений вводится общеобразовательный курс «Основы информационной безопасности» или «Медиаграмотность»;
- **образование взрослых** — практические занятия на базе махалли, библиотек, информационно-ресурсных центров, центров обслуживания населения.

Ключевое требование — практическая направленность обучения: упражнения на распознавание поддельных сообщений и сайтов, моделирование ситуаций «звонок от банка», отработка алгоритма действий при инциденте.

Необходимо также включить модуль по информационной безопасности в программы переподготовки и повышения квалификации педагогических кадров и обеспечить учителей готовыми методическими материалами.

Информационные кампании для взрослого населения должны строиться на следующих принципах: краткие и однозначные сообщения с призывом к конкретному действию («Банк никогда не спрашивает код из SMS. Спрашивают — это мошенник»); выбор каналов с учетом целевой группы (короткие видео в социальных сетях для молодежи; телевидение, радио, встречи в махалле — для пожилых); использование реальных историй потерпевших с их согласия и без раскрытия личности [3]; регулярное обновление содержания с учетом новых схем; измерение осведомленности населения до и после кампаний.

Банки, платежные системы и операторы мобильной связи находятся в постоянном контакте с гражданами и располагают техническими возможностями для профилактики. Целесообразно: закрепить обязанность банков предоставлять клиентам при подключении дистанционного обслуживания краткую памятку по безопасности; расширить применение механизмов дополнительного подтверждения и временной задержки нетипичных операций; предусмотреть оперативный обмен информацией о мошеннических номерах и счетах между правоохранительными органами, банками и операторами связи; упростить процедуру блокировки номеров, используемых в мошеннических целях.

Целесообразно создать единую онлайн-платформу (и короткий номер), через которую граждане могут сообщить о киберпреступлении или подозрительном обращении. Поступающие сведения должны анализироваться для выявления новых схем, а информация о них — оперативно доводиться до населения через СМИ, социальные сети, мобильные приложения банков. Это одновременно снизит латентность киберпреступлений и повысит оперативность профилактики.

Для пожилых граждан необходимы практические занятия в махалле с участием волонтеров из числа студентов, а также вовлечение членов семьи в обучение старших родственников. Для молодежи — разъяснение уголовно-правовых последствий передачи банковских карт и участия в мошеннических схемах в качестве «дропов».

Проведенное исследование позволяет сформулировать следующие выводы.

Во-первых, киберпреступления против граждан в подавляющем большинстве случаев совершаются не путем технического взлома, а с использованием методов социальной инженерии, эксплуатирующих доверие к авторитету, страх, срочность и ожидание выгоды. Поэтому пользователь является одновременно главным объектом атаки и главным звеном защиты.

Во-вторых, культура информационной безопасности представляет собой не только сумму знаний, но и систему ценностей, установок и устойчивых поведенческих навыков. Ее формирование требует длительной, систематической и адресной работы, а не разовых мероприятий.

В-третьих, уязвимость к киберпреступлениям различается в зависимости от возраста и социального положения: пожилые граждане нуждаются прежде всего в базовых правилах и практических навыках, молодежь — в понимании рисков и правовых последствий собственного поведения.

В-четвертых, профилактическая работа в Республике Узбекистан ведется разрозненно, без единых стандартов, координации и оценки эффективности; высокий уровень латентности киберпреступлений затрудняет своевременное выявление новых схем.

В-пятых, зарубежный опыт демонстрирует эффективность комплексного подхода, сочетающего простые и понятные информационные кампании, системное партнерство государства, банков и операторов связи, единые каналы приема сообщений и обучение на всех уровнях образования.

На основе изложенного предлагается:

1. Разработать национальную концепцию повышения культуры информационной безопасности населения с четким распределением задач и показателями эффективности.
2. Внедрить практико-ориентированные модули по информационной безопасности на всех уровнях системы образования и в программы повышения квалификации педагогов.
3. Проводить регулярные информационные кампании, ориентированные на конкретные целевые группы, с измерением их результатов.
4. Закрепить механизмы государственно-частного партнерства с банками, платежными системами и операторами связи, включая обмен информацией о мошеннических номерах и счетах и дополнительную защиту нетипичных операций.
5. Создать единую платформу для сообщений о киберпреступлениях и оперативного оповещения населения о новых схемах.
6. Организовать адресную работу с пожилыми гражданами и молодежью на базе махалли и учебных заведений.

Осознание каждым гражданином того, что он является первым и главным защитником собственной безопасности в цифровой среде, должно стать основой государственной политики в сфере профилактики киберпреступлений.

Список литературы

1. Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 г. № ЗРУ-764.
2. Закон Республики Узбекистан «Об информатизации» от 11 декабря 2003 г. № 560-II.
3. Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 г. № ЗРУ-547.
4. Уголовный кодекс Республики Узбекистан (утвержден Законом Республики Узбекистан от 22 сентября 1994 г.).
5. Закон Республики Узбекистан «О профилактике правонарушений» от 14 мая 2014 г. № ЗРУ-371.
6. Указ Президента Республики Узбекистан «О Стратегии развития Нового Узбекистана на 2022–2026 годы» от 28 января 2022 г. № УП-60.
7. Закон Республики Узбекистан «Об образовании» от 23 сентября 2020 г. № ЗРУ-637.
8. Конвенция Совета Европы о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.).
9. Hadnagy C. Social Engineering: The Science of Human Hacking. 2nd ed. Indianapolis: Wiley, 2018.
10. Mitnick K. D., Simon W. L. The Art of Deception: Controlling the Human Element of Security. Indianapolis: Wiley, 2002.
11. Cialdini R. B. Influence: The Psychology of Persuasion. Rev. ed. New York: Harper Business, 2006.
12. ENISA. Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. Heraklion: European Union Agency for Cybersecurity, 2018.
13. UNESCO. Media and Information Literate Citizens: Think Critically, Click Wisely! (Media and Information Literacy Curriculum for Educators and Learners). Paris: UNESCO, 2021.
14. Verizon. Data Breach Investigations Report (ежегодные выпуски).
15. Cohen L. E., Felson M. Social Change and Crime Rate Trends: A Routine Activity Approach // American Sociological Review. 1979. Vol. 44, No. 4. P. 588–608.
16. United Nations Office on Drugs and Crime. Comprehensive Study on Cybercrime (Draft). Vienna: UNODC, 2013.
17. Vuorikari R., Kluzer S., Punie Y. DigComp 2.2: The Digital Competence Framework for Citizens. Luxembourg: Publications Office of the European Union, 2022.