Дата поступления рукописи в редакцию: 25.12.2025 г.
Дата принятия рукописи в печать: 25.02.2026 г.
DOI: 10.24412/2224-9133-2026-1-528-533

ШАРЛОВА Марина Николаевна,
подполковник полиции, старший преподаватель кафедры административного права и административной деятельности ОВД, Ставропольского филиала Краснодарского университета МВД России,
e-mail: charlova2017@yandex.ru

СОЦИАЛЬНАЯ БЕЗОПАСНОСТЬ В КИБЕРПРОСТРАНСТВЕ: МЕХАНИЗМЫ РАСПОЗНАВАНИЯ ЛОЖНОЙ ИНФОРМАЦИИ И МЕРЫ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Аннотация. *В научной статье анализируются особенности социальной безопасности в киберпространстве. Отмечается, что в киберпространствах пересекаются социальная, информационная, экономическая и психологическая безопасность личности и социальных групп. Анализируются технологии нарушения социальной безопасности в киберпространстве: вирусы, кибермошенничество, фейк, фишинг и др. Выявляются проблемы обеспечения социальной безопасности в киберпространстве, а именно, сложность выявления источников угроз и их авторства, трудности в определении времени наступления угроз, неосознание и непонимание пользователями опасности от их действий. Отмечается несколько популярных способов обмана в киберпространстве. Автором предлагаются правила, придерживаясь которых, получится уберечь себя и своих близких от угроз в современном информационном пространстве.*

Ключевые слова: *интернет, гаджет, киберпространство, информация, телефонное мошенничество, фейк, фишинг, дипфейк, кибератаки.*

SHARLOVA Marina Nikolaevna
Lieutenant Colonel of Police, Senior Lecturer at the Department of Administrative Law and Administrative Activities of the Interior Ministry, Stavropol Branch of the Krasnodar University of the Ministry of Internal Affairs of Russia

SOCIAL SECURITY IN CYBERSPACE: MECHANISMS FOR DETECTING FALSE INFORMATION AND PROTECTION MEASURES IN INFORMATION SYSTEMS

Annotation. *The article analyzes the features of social security in cyberspace. It is noted that social, informational, economic and psychological security of individuals and social groups intersect in cyberspaces. The article analyzes technologies for violating social security in cyberspace: viruses, cyberbullying, fake, phishing, etc. The problems of ensuring social security in cyberspace are revealed, namely, the difficulty of identifying the sources of threats and their authorship, difficulties in determining the time of the threat, and users' lack of awareness and understanding of the danger from their actions. There are several popular ways of cheating in cyberspace. The author suggests rules, adhering to which, it will be possible to protect yourself and your loved ones from threats in the modern information space.*

Key words: *Internet, gadget, cyberspace, information, phone fraud, fake, phishing, deepfake, cyber attacks.*

В современном мире сложно представить человека без смартфона в руках, умных часов на запястье и аккаунта в глобальной сети. Интернет и социальные сети стали неотъемлемой частью жизни людей. Всемирная паутина, объединяющая пользователей в одном информационном пространстве, дает нам безграничные возможности. Узнавать новости с разных уголков планеты, совершать покупки в любое время суток, общаться с родными и близкими на рас-

стоянии, заводить новые знакомства, работать, не выходя из дома – все это теперь можно делать «в пару кликов» с персонального компьютера или смартфона.

Однако вместе с положительными аспектами, которые преподносит цифровая среда, есть и соответствующие риски. Раньше главной проблемой человека был поиск информации – сегодня ее фильтрация. Практически любое электронное устройство не принадлежит его владельцу в полной мере.

Главная задача современного мобильного телефона – собирать информацию о пользователе и управлять его вниманием. Чем интенсивнее используется смартфон, тем больше он знает о своем владельце. Данные собирают производители электронных устройств, платформ, а также легальные и вредоносные приложения. Рискам цифрового мира подвержен как сам смартфон с установленными на нем программами, сервисами, банковскими счетами, паролями, так и сознание пользователя мобильного гаджета. Характер информационных угроз многообразен – от развития интернет - зависимости до прямых атак на психику человека. Именно поэтому важно современному владельцу смартфона соблюдать цифровую гигиену.

Анализ данных о преступности в Российской Федерации, за период с января по декабрь 2024 года свидетельствует о сохранении стабильной обстановки [4].

Тем не менее, сохраняется тенденция к увеличению количества преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Отмечается увеличение на 23,5% по сравнению с аналогичным периодом 2023 года. Раскрываемость тяжких и особо тяжких деяний этой категории составляет 42,3%. Положительная динамика наблюдается в сфере мошенничеств с электронными платежами: их число сократилось на 56%.

В контексте спецоперации против Российской Федерации наблюдается беспрецедентная по масштабам борьба в информационном пространстве сети Интернет. Имеет место осуществление скоординированных атак из различных географических точек. Более 35 тысяч информационных ресурсов находятся под постоянным наблюдением государственных органов.

Согласно прогнозам, атаки программ-вымогателей сохранят статус основной киберугрозы в Российской Федерации как в 2024, так и в 2025 году. Защита информационных систем должна быть обеспечена от широкого спектра угроз, включая, помимо программ-вымогателей, вредоносное программное обеспечение, утечки данных, фишинг, DDoS-атаки и спамом. Ввиду сложности киберугроз и многообразия векторов атак, необходима комплексная стратегия защиты, включающая проактивные меры по обеспечению безопасности периметра, электронной почты, выявление уязвимостей и теневых активов, а также применение решений Threat Intelligence для превентивного предотвращения кибератак.

Поговорим о действиях, направленных на выявления ложных высказываний, фейков, схем манипуляции ложной информацией.

Распространение ложной информации в глобальной сети с каждым днем возрастает все сильнее, а вместе с этим растет и необходимость в ее распознании и пресечении. При помощи различных манипулятивных техник мошенники вербуют пользователей для получения собственной выгоды. Искусство применения психологических уловок с технологическими приемами, используя электронную коммуникацию, получило название социальная инженерия или социотехника.

Социальная инженерия – набор приемов психологической манипуляции, вынуждающие жертву сделать то, что нужно мошеннику-манипулятору. Владелец смартфона беспрекословно выполняет необходимые требования, так как полностью доверяет злоумышленнику. Социотехника применяется сегодня практически во всех видах сетевых манипуляций.

Киберугрозы включают в себя множество видов атак, такие как фишинг, вредные приложения, вирусы и трояны, телефонное мошенничество, платные подписки, вовлечение в массовые движения, фейки и многое другое.

Одной из первых разновидностей мошенничества в Сети стал фишинг. Фишинг (от английского fishing – рыбная ловля) – различные приемы для получения доступа к паролю и логину пользователя обычно при помощи поддельных сайтов, писем на электронную почту. Мошенник обычно требует обновить данные на сайте иначе доступ к странице, аккаунту будет не доступен больше.

Вредные приложения. Цель подобных сомнительных сервисов одна – получение экономической выгоды. Различают три основных типа таких приложений:

1. Фальшивые приложения – мимикрия под популярные платформы, связанные с платежными системами. Вредоносная программа при помощи прямого участия пользователя завладевает паролями, номерами счетов для дальнейшей кражи денежных средств с банковского счета, мобильного телефона.
2. Вымогатели – «локеры» и шифровальщики, блокирующие смартфон и требующие денежное вознаграждение за разблокировку. Под видом «хорошего» приложения пользователь устанавливает ловушку на свое цифровое устройство.

3. «Денежные пиявки» – программы со скрытой подпиской, пользующиеся экосистемой магазинов приложений и легкомыслием пользователя.

Вирусы и трояны. Целью вредоносных программ является незаметное проникновение на устройство пользователя для дальнейшего хищения данных, создания трафика на сайты, рассылки спама. Получить вирус на электронное устройство можно довольно простыми способами: открыть электронное письмо или приложенный файл, зайти на зараженный сайт, установить неизвестное приложение.

Телефонные мошенники. Мобильный вишинг - звонки от злоумышленников с целью получить финансовую или персональную информацию от наивного пользователя.

Рассмотрим типовые ситуации в сфере мобильных мошенничеств:

1. «Некогда объяснять». Мошенник звонит человеку, представляясь как родственник или близкий друг, и просит о срочной помощи – перевести деньги на карту, но объяснять, что случилось, нет времени.
2. Звонок из банка. Один из самых распространенных способов телефонных мошенничеств – это звонок якобы сотрудника из банка. Злоумышленник, используя различные приемы социотехники, пытается получить нужную ему информацию: номер карты, окончание срока ее действия, CSV-код, а далее просит подтвердить смс-код, только что поступивший на номер телефона клиента банка. Пока наивный пользователь думает, что сотрудничает с представителем банка, последний в свою очередь уже имеет доступ к банковскому счету. Поводы для звонка различны, от оповещения попытки снятия денежных средств до поздравления о выигрыше в лотерею.
3. Навязчивые расспросы. Мошенники звонят пользователю и начинают задавать вопросы с целью записать голос оппонента. Киберпреступники в ходе диалога вынуждают ответить «да» и назвать свои имя, отчество, фамилию. Данных сведений достаточно, чтобы пройти процедуру идентификации в банке.
4. Платные подписки операторов. Существуют два вида подписок на контент: открытые (легальные) и скрытые (нелегальные). При первом варианте подписок пользователь самостоятельно выбирает, тратить деньги на приобретение их или нет. Второй вариант подразумевает, что человек не знает о подключенных подписках и замечает данный факт лишь в момент списания денег.
5. Массовые движения. Пользователей глобальной сети Интернет постоянно привлекают к участию в тестах, заданиях, квестах, не несущих большой смысловой нагрузки, но обязательно подталкивающих к дальнейшему распространению среди друзей и близких. Организаторы завлекают участников яркими заголовками: «Проверьте свой IQ, если решите 9 из 10 заданий, верно, ваш интеллект выше 110», «Узнай, кем ты был в прошлой жизни», «Слово, которое ты найдешь первым в таблице, определит твой будущий год». Довольно частое явление в Сети – флешмобы. Участнику необходимо выполнить какое-либо действие: выложить свое фото десятилетней давности, облиться холодной водой (Ice Bucket Challenge), рассказать про самый неловкий случай из жизни и передать эстафету следующим. Несомненно, большая часть организаторов хотят заработать на бурном обсуждении массовых движений и их распространении, получая трафик и деньги с рекламы.
6. Фейки. Фейк – дезинформация в социальных сетях и средствах массовой информации. Фейк может быть как частичной, так и полной фальшивкой. По сравнению с обычными новостями, фейки распространяются в разы быстрее и имеют больший охват аудитории, а значит, и больше денег за рекламу. Связан данный феномен с тем, что поддельные новости имеют яркие, запоминающиеся, привлекающие внимание заголовки. Распространение непроверенной информации не что иное, как способ привлечь интерес пользователей, попытка стать известнее, заработок на наивных пользователях. С развитием технологий создание фейковой информации стало в разы легче. При помощи нейросетей сегодня можно создать подделку в любом формате: фото, видео, аудио.

Дипфейк – синтез контента, в котором на исходное изображение накладываются различные подмены. Например, заменяют лицо, мимику, движения на фото, аудиодорожки в видео. Лживые новости и посты в Сети становится практически невозможно отличить от настоящих.

7. Фишинг (Phishing) – представляет собой форму киберпреступности, целью которой является незаконное получение конфиденциальных данных пользователей, таких как идентификационные данные для входа в систему, номера телефонов и банковские реквизиты. Злоумышленники регулярно рассылают письма и сообщения с вирусами и ссылками на поддельные сайты, чтобы

получить пароли, номера банковских карт и другие личные данные пользователей. Такое интернет-мошенничество называется фишингом. Чаще всего фишинг реализуется с помощью электронной почты и социальных сетей.

Сегодня злоумышленники пользуются разнообразными способами обмана пользователей телефонов. Вишинг – это голосовой фишинг (от слияния двух слов «voice» и «phishing»), вид мошенничества с использованием социальной инженерии.

Вишинг – представляет собой форму телефонного мошенничества, характеризующуюся обманными действиями, направленными на получение денежных средств или конфиденциальных данных клиентов банковских учреждений. Чаще всего мошенники представляются сотрудниками банка или госструктур (МВД России, ФСБ России, Центробанка, Прокуратуры и представителями других организаций).

Отметим несколько популярных способов обмана, которые рекомендуется запомнить:

1. Похожий на известный, но содержащий незначительные отличия адрес компании.

Действие: не следует считать истинной информацию от таких адресатов.

2. Призывы произвести срочные, неотложные действия немедленно.

Действие: Не использовать гиперссылки в письмах от не доверенных адресатов для перехода по ним.

3. Фишинговые ссылки в теле писем.

Действие: Не использовать гиперссылки в письмах от недоверенных адресатов для перехода по ним.

4. Подозрительный файл в виде вложения к письму.

Действие: Всегда сканировать с помощью антивируса файлы, полученные от неизвестных отправителей.

5. Небрежный вид сайта электронного магазина, обещание выигрышей и значительное отличие цен на товары в меньшую сторону.

Действие: не оставлять свои контактные данные, данные банковских карт. Отказаться от использования сайта.

6. Требование заплатить незначительную сумму для получения крупного денежного вознаграждения (выигрыша, заработка, приза и т.п.).

Действие: отказаться от использования сервиса, сайта, не оставлять регистрационные данные.

7. Незначительные отличия в электронном адресе сайта в Web обозревателе – результат опечатки при вводе легитимного адреса.

Действие: проверьте электронный адрес сайта в адресной строке прежде чем вводить логин и пароль на форме ввода.

8. Гиперссылки в сообщении от имени банка или других компаний.

Действие: не переходить по гиперссылкам из сообщений.

9. Хвалебные отзывы о выигрыше денег или призов на сайте.

Действие: найти отзывы об организаторе акции на официальных новостных порталах, дополнительно изучить репутацию сайта. При отсутствии сведений– отказаться от посещения.

10. Сообщения с просьбой о незамедлительной помощи в социальных сетях от аккаунтов друзей (или с просьбой участвовать в голосовании за знакомого, родственника и т.п.).

Действия: связаться с людьми, с аккаунтов которых поступают подобные запросы по альтернативным каналам связи (стационарный, сотовый телефоны) для уточнения информации, не принимать спонтанных решений.

Таким образом, для парирования различных угроз при подозрении на наличие мошеннических действий или манипуляций в электронных сообщениях, звонках на мобильные телефоны, на электронных сайтах следует использовать выше приведенные тактики.

К дополнительным рекомендациям пользователям информационных систем, направленные на минимизацию рисков реализации угроз безопасности информации, следует отнести регулярное создание резервных копий важной информации и хранение резервных носителей в отключенном от информационной системы состоянии. Такой подход позволит сохранить ранее скопированные файлы при вирусном заражении компьютера или повреждении информационной системы шифровальщиком.

Общая рекомендация по нейтрализации атак, использующих методы социальной инженерии, в том числе использующие современные мессенджеры Telegram, Whatsapp, заключается в организации оперативной проверки поступающей информации через другие источники и альтернативные каналы связи. Сюда же следует отнести рекомендацию не разглашать различные персональные данные, данные банковских карт при поступлении подозрительных телефонных звонков, а также на малоизвестных сайтах интернет-магазинов, платежных систем и т.п., так как они могут оказаться фейковыми. Данный подход позволит сохранить конфиденциальность персональных данных.

Для того чтобы не попадаться на уловки мошенников в Сети необходимо знать основные

правила, придерживаясь которых, получится уберечь себя и своих близких от угроз в современном информационном пространстве:

1. Выстроить и сохранить личный информационный суверенитет.

Сегодня важно уметь выстроить и сохранить личный информационный суверенитет. Личный информационный суверенитет – способность человека сохранять самостоятельность мышления, не впадать в цифровую зависимость, не поддаваться манипуляциям в Сети. У большинства людей в наши дни выработалось «клиповое сознание» - восприятие мира только через короткие яркие образы. Пользователи Сети не могут долго сосредоточиться на чем-то одном, им постоянно необходимо переключаться с одной вкладки на другую. Жертвы данного феномена не могут читать длинные тексты или смотреть видео дольше 1-2 минут – начинают уставать. Это позволяет вербовщикам и мошенникам, используя одни и те же приемы, многократно обрабатывать пользователей. Избавиться от клипового мышления довольно трудно, так как для этого требуется заставлять себя концентрироваться на долговременных задачах.

2. Не доверять незнакомцам. Любой человек в Сети, с которым не было личных встреч в реальной жизни – незнакомец. Люди в цифровом пространстве не всегда те, за кого себя выдают, поэтому следует внимательнее относиться к тем, кого добавлять в друзья и с кем вступать в диалог. Мошенники пользуются преимуществом анонимности в Интернете и под видом защитников природы, представителей благотворительных фондов, сотрудников банков просят совершить переводы денежных средств.
3. Использовать хороший антивирус и регулярно обновлять его. Защитное программное обеспечение способно уберечь от многих проблем, связанных с кражей персональной информации, а также защитит цифровое устройство от электронных рисков.
4. Помнить о том, что из Интернета практически невозможно ничего удалить. Все, что попало в сеть остается там навсегда. Стоит следить за контентом, загружаемым в Интернет, любая компрометирующая информация может быть использована против ее владельца. Все фото, видео, сообщения, попавшие в цифровую среду, – публичные или могут стать публичными.
5. Использовать надежные пароли и многофакторную (двухфакторную) аутентификацию. Пароль должен соответствовать требованиям сложности, включающим использование букв верхнего и нижнего регистра, цифр и специальных символов. Не допускается использование легко угадываемых последовательностей символов и персональных данных в качестве пароля. Идентичные пароли на нескольких платформах ставят под угрозу их безопасность. Вторым фактором аутентификации может выступать, например, одноразовый код, присылаемый на личный номер сотовой связи в виде СМС.
6. Не переходить по неизвестным ссылкам. Яркая реклама на сайтах, призывы перейти по ссылке, прикрепленной к видео или посту, и продолжить просмотр могут таить под собой две главные опасности: похищение персональных данных и скрытую установку вредоносных программ.
7. Не скачивать приложения, музыку, кинофильмы, игры из сомнительных источников. Устанавливать различные программы и сервисы следует только из официальных лицензионных онлайн-магазинов или с сайтов разработчиков. Скачивая приложения из непроверенных информационных ресурсов, пользователь рискует занести вирус на свое электронное устройство.
8. Проверять информацию, полученную от незнакомых лиц или из неизвестных сообществ, страниц в Интернете. Всегда необходимо помнить о том, что в информационном потоке новостей и постов нередко встречаются и фейки. Нужно быть осторожным, развивать критичность мышления, искать и сохранять проверенные источники сведений, чтобы не попадаться на всевозможные махинации и злоупотребления.
9. Не разглашать персональной информации. Номера телефонов, банковских счетов, адрес, паспортные данные и другие личные сведения следует сохранять в тайне от цифрового мира. Для регистрации на различных онлайн-платформах рекомендуется использовать второй (альтернативный), не привязанный к банковским картам, номер телефона.

Соблюдение всех правил цифровой гигиены не может гарантировать полную безопасность в виртуальной реальности. Эффективное оружие против мошенников в Сети – это способность критически анализировать поступающую информацию; постоянная работа над повышением практических навыков, позволяющих отличать действительные факты от фейков.

При работе с различными информационными системами следует использовать про-

граммное обеспечение из доверенных источников, сертифицированное антивирусное программное обеспечение с актуальными базами вирусных сигнатур, при необходимости иметь на компьютере систему обнаружения атак, агентов мониторинга систем SIEM, DLP, SOAR. Данный подход позволит комплексно использовать имеющиеся современные системы защиты.

Список литературы:

[1] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года. – URL: https://мвд.рф/reports/item/48913905?ysclid=m50n6hwn84557964792. (Дата обращения 20.12.2025)

[2] Центр по компьютерным инцидентам фиксирует более 170 кибератак на РФ ежедневно. – URL: https://www.interfax.ru/digital/903202. (Дата обращения 22.12.2025)

[3] Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учебное пособие : в 2 ч. /А.В. Аносов [и др.] – Москва : Академия управления МВД России, 2019.–Ч. 1.– С. 208.

[4] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года. – URL: https://мвд.рф/reports/item/48913905?ysclid=m50n6hwn84557964792.

References:

[1] Brief description of the state of crime in the Russian Federation for January - December 2024. - URL: https://мвд.рф/reports/item/48913905?ysclid=m50n6hwn84557964792. (Date accessed 20.12.2025)

[2] The Computer Incident Center records more than 170 cyber attacks on the Russian Federation daily. – URL: https://www.interfax.ru/digital/903202. (Accessed 22.12.2025)

[3] A.V. Anosov. Activities of the internal affairs bodies to combat crimes committed using information, communication and high technologies: textbook: 2 hours/A.V. Anosov [et al.] - Moscow: Academy of Management of the Ministry of Internal Affairs of Russia, 2019.-Ch. 1. - S. 208.

[4] Brief description of the state of crime in the Russian Federation for January - December 2024. – URL: https://мвд.рф/reports/item/48913905?ysclid=m50n6hwn84557964792.