Первый уровень защиты – физический, суть которого заключается в том, что при совершении оплаты посредством NFC карту или смартфон нужно поднести на достаточно близкое расстояние (до 10 см) к считывающему устройству. Это условие действия бесконтактных технологий удалось обойти исследователям из британского Университета Суррея. Они продемонстрировали возможность считывания данных по технологии NFC на расстоянии до 80 см с помощью компактного сканера, которых позволяет таким образом незаметно забирать деньги в местах большого скопления людей. Другим путем пошли испанские хакеры Риккардо Родригес и Хосе Вилла, которые создали концепт вируса для операционной системы Android, превращающий смартфон в ретранслятор NFC-сигнала. При нахождении бесконтактной карты рядом с таким смартфоном злоумышленнику поступает сигнал о возможности проведения транзакции, создается мост между банковской картой и телефонами жертвы и хакера посредством связи сети Интернет. Таким образом, мошенник может расплатиться на ближайшем терминале со своего телефона, используя чужую карту.

Второй уровень защиты – криптография. Бесконтактные транзакции защищены стандартом EMV (Europay MasterCard Visa). Если магнитную дорожку можно просто скопировать, то с чипом аналогичные действия не совершаются. При каждом запросе терминала микросхема генерирует одноразовый ключ, который можно перехватить, но он уже не подойдет для следующего платежа.

Третий уровень защиты – сумма покупки. Существуют ограничения максимальной суммы единовременного списания денежных средств с бесконтактных карт, которые задает банк-эквайер. В России этот предел равен 1 000 рублей, при превышении его терминал просит ввести PIN-подтверждение для совершения покупки. К Apple Pay и Samsung Pay это не относится: для проведения платежа всегда требуется подтверждение. Британские исследователи Ньюкаслского университета сообщили, что обнаружили в платежной системе Visa недостаток: если запросить платеж в иностранной валюте, то пороговое ограничение не действует, хотя представители Visa позднее опровергли эту информацию.

Из вышесказанного следует, что существует возможность снятия посторонним лицом денег с банковских карт через бесконтактные платежи. Технологии Apple Pay и Samsung Pay являются самыми безопасными, так как предусматривают запрос PIN-кода или срабатывание Touch ID при проведении любой транзакции, независимо от суммы покупки. Но и эти технологии не обеспечивают полной безопасности бесконтактных платежей, ибо существует вирус, который автоматически устанавливает в операционной системе телефона приложения злоумышленников. На сегодняшний день более защищенной считается Apple Pay из-за существования некоторых ограничений: оплата принимается лишь в немногих учреждениях, система работает с одной платежной системой.

Судя по темпам внедрения бесконтактных платежных систем, все эти возможные угрозы не слишком пугают банки – очевидно, выгода превышает потери. Точнее, потери при бесконтактном мошенничестве пока незначительны, и банки могут компенсировать их безболезненно для себя. Таким образом, можно сказать, что самый простой и доступный способ безналичной оплаты является достаточно небезопасным. Так что о сохранности своих денежных средств лучше позаботиться самому, а не надеяться на обещания разработчиков новых систем.

УДК 343.32

А.М. Пановицын

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ЦЕЛЯХ ПРЕСЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ РАДИКАЛЬНЫХ ПОЛИТИЗИРОВАННЫХ ФОРМИРОВАНИЙ

Доступный мобильный интернет не только способствует социально-политическому и экономическому развитию общества, но и несет вполне реальные угрозы. Так, поиск кандидатов в радикальные группировки, их вербовка и соответствующая идейная и психологическая обработка все чаще осуществляются посредством сети Интернет. Ресурсы глобальной сети позволяют радикальным организациям оказывать массовое пропагандистское воздействие, особенно на молодое поколение, которое, являясь основным потребителем интернет-контента, еще не имеет твердых социальных позиций, политических взглядов и убеждений. Об эффективности данной работы свидетельствует статистика возраста лиц, задерживаемых при проведении политических акций за совершение противоправных действий на территориях нашего и сопредельных государств.

Сегодня в сети Интернет достаточно оппозиционных сайтов и информационных ресурсов, исключающих терпимость и толерантность, призывающих к публичному выражению своих политических и общественных взглядов путем проведения уличных акций, несанкционированных массовых мероприятий и других провокационных действий возле зданий государственных органов, посольств и консульских учреждений, крупных промышленных предприятий и организаций, в других местах массового скопления граждан. Члены радикальных формирований не собираются вести диалог с властями, не признают

компромиссов и не видят безопасных способов решения возникающих социальных и политических проблем, поэтому неизменной целью данных мероприятий является дестабилизация социально-политической обстановки в стране и организация массовых беспорядков, как показали события, предшествующие несанкционированным массовым мероприятиям, запланированным на 26 марта 2017 г. в Минске.

Проведение таких акций требует от органов внутренних дел Республики Беларусь и внутренних войск Министерства внутренних дел Республики Беларусь усиленных мер по охране общественного порядка и обеспечению общественной безопасности, а также поиска новых эффективных мер пресечения деятельности радикальных политизированных формирований.

В настоящее время в целях ограничения влияния радикальных политизированных формирований проводятся профилактические мероприятия, в том числе направленные на ограничение свободного доступа к ресурсам, содержащим социально-опасный контент. Данная работа, хоть и является эффективной, не может устранить имеющуюся угрозу, так как вместо удаленного контента появляется новый, адреса ссылок на материалы пропагандистского характера периодически меняются, информация размещается на серверах частных зарубежных компаний, напрямую не связанных с радикальным организациями, но уклоняющихся от взаимодействия с государственными службами.

Наряду с применяемыми методами профилактики сегодня предпринимаются дополнительные меры по ликвидации радикальных формирований путем выявления и привлечения к ответственности лиц, непосредственно занимающихся как вербовкой, подготовкой и организацией политических провокаций, так и поиском спонсоров и покровителей. В этих целях используются имеющиеся в распоряжении правоохранительных органов Республики Беларусь специализированные программно-технические комплексы UFED компании Celebrite, предназначенные для проведения криминалистических исследований устройств сотовой связи.

Устройства мобильной связи из-за своей компактности и функциональности являются наиболее распространенными средствами поиска информации и коммуникации в сети Интернет. Поэтому благодаря данным, находящимся в них, можно установить лиц, являющихся членами радикальных организаций и несущих потенциальную и реальную угрозу обществу. Следовательно, при задержании активных участников радикальных формирований, подозреваемых в совершении преступных действий, целесообразно изымать имеющиеся у них средства мобильной связи для проведения криминалистического исследования в целях получения вещественных доказательств преступной деятельности и установления соучастников, заказчиков и организаторов преступлений.

При проведении исследований средств связи особая роль должна отводиться сведениям, полученным из электронной почты, мобильных браузеров, интернет-мессенджеров, социальных сетей, специализированных форумов и чатов, навигационных приложений и других коммуникационных программ. Абоненты сетей сотовой связи, используя веб-браузеры, читают новости, посещают веб-сайты, совершают финансовые операции, следят за социальными сетями и т. д. При этом любая их сетевая активность оставляет следы в операционной системе и приложениях мобильного устройства. Проведение экспертного исследования мобильных веб-браузеров позволяет узнать: историю браузера, историю поиска; проанализировать закладки, временные файлы; изучить содержание сохраненных страниц и файлов, cookies; установить сохраненные пароли и имена пользователя; определить геолокационные данные местонахождения абонента.

Исследование интернет-мессенджера, в свою очередь, способствует установлению: истории групповых и приватных бесед (включая неавторизованные контакты, группы контактов); списка контактов с фотографиями, полями и заметками; полной информации о звонке посредством IP-телефонии: имени адресата или владельца телефонного номера, длительности разговора; текста отправленных сообщений, номера телефона получателя, временной метки и стоимости; деталей учетной записи: имени, адреса, телефонного номера, адреса электронной почты, даты рождения, другой пользовательской информации; геоданных события.

Кроме того, оперативный интерес при исследовании устройств сотовой связи могут представлять временные файлы, сохраненные фото, видео- или аудиозаписи, сделанные владельцем телефона, которые приняты другими абонентами или переданы им либо разыскиваются в сети Интернет подозреваемым. К примеру, мультимедийный контент может быть посвящен изготовлению простейших зажигательных гранат, взрывных устройств или тактике противодействия правоохранительным органам. Анализ навигационных приложений мобильного устройства дает возможность изучить маршруты и поисковые запросы пользователя, определить места, которые разыскивал или посещал подозреваемый.

Определенный интерес с точки зрения получения фактических сведений представляет возможность восстановления удаленных сообщений. В изъятых устройствах в большинстве случаев можно восстановить SMS- и MMS-переписку, сообщения электронной почты и другие сообщения в зависимости от типа устройства. Кроме того, используя специальные утилиты для просмотра данных, эксперты могут анализировать вложения и технические данные сообщений. В результате подобного исследования появляется возможность установить полный круг общения подозреваемого за счет сведений, полученных из элек-

тронной почты, социальных сетей, приложений IP-телефонии, чатов, форумов, SMS- и MMS-сообщений и т. п. Возможность восстановления переписки позволяет выявить возможных соучастников и организаторов проводимых акций, установить лиц, осуществляющих руководство и финансирование радикальных организаций.

Кроме того, извлеченные из мобильных устройств геолокационные сведения, совмещенные с данными операторов электросвязи, позволяют определить места проживания и подготовки членов радикальных организации, расположение возможных схронов оружия и боеприпасов.

Все вышеизложенное свидетельствует о возможности повышении качества работы правоохранительных органов по пресечению деятельности радикальных политизированных формирований за счет внедрения современных информационных технологий и технических средств.

УДК 621.391.01

А.С. Поляков, Д.В. Белый

ПРОСТОЙ СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ОШИБОК ПРИ ПЕРЕДАЧЕ ПО ЛИНИЯМ СВЯЗИ

Несмотря на серьезные достижения в области создания надежных каналов связи, проблема зашиты информации от ошибок при ее передаче остается достаточно актуальной. В настоящее время для решения этой задачи используются различные методы кодирования/декодирования информации, которые достаточно сложны, трудоемки при реализации и не всегда соответствуют требованиям по производительности (быстродействию). Наиболее простой способ обнаружения и исправления ошибок основан на операции вычисления четности единичных символов в строках и столбцах бинарной матрицы, представляющей собой передаваемую информацию. При кодировании двухмерных кодов этот способ позволяет определять адреса ошибок, но при условии, что и в столбцах, и в строках бинарной матрицы имеются только одиночные ошибки.

Предлагаемый ниже способ устранения ошибок основан на использовании результатов проверок четности по четырем координатам бинарной матрицы: строкам, столбцам, главным диагоналям и вспомогательным диагоналям.

Под главными диагоналями понимается как основная главная диагональ матрицы, так и все параллельные ей диагонали, рассматриваемые как непрерывные цепочки элементов матрицы, начинающиеся в первой строке и проходящие в направлении «сверху – вниз – направо» через все строки матрицы до достижения крайнего правого элемента

предыдущей строки с переходом на левый элемент следующей строки. Нумерация элементов новой строки начинается с номера, который был последним в предыдущей строке. На рисунке 1 элементы основной главной диагонали обозначены цифрой 1, а номера остальных главных диагоналей – цифрами, расположенными в верхних левых углах элементов матрицы.

Под вспомогательными диагоналями подразумеваются основная вспомогательная диагональ матрицы и все параллельные ей диагонали, проходящие в направлении «сверху – вниз – налево», начиная с первой строки матрицы и заканчивая последней строкой. С крайнего левого элемента строки происходит переход на крайний правый элемент следующей строки. Номера вспомогательных диагоналей на рисунке выделены курсивом и размещены в нижних правых углах элементов матрицы. Номера диагоналей на рисунке соответствуют номерам столбцов в первой строке матрицы: *b* – номера главных диагоналей в прямом направлении, *b̲* – номера вспомогательных диагоналей, *d* – номера главных диагоналей (расположены в верхних левых углах элементов матрицы), *d̲* – номера вспомогательных диагоналей (расположены в правых нижних углах элементов матрицы), *a* – номера строк матрицы.

		d						n	d		
b		1	2	3	4	5	6	7	8	9	10
b̲		9	8	7	6	5	4	3	2	1	Ln
a	1	1 9	2 8	3 7	4 6	5 5	6 4	7 3	8 2	9 1	
	2	9 8	1 7	2 6	3 ▼ 5	4 4	5 3	6 2	7 1	8 9	■
	3	8 7	9 6	1 5	2 4	3 3	4 2	5 1	6 9	7 1	
	4	7 ▼ 6	8 5	9 4	1 3	2 2	3 1	4 9	5 8	6 7	■
	5	6 5	7 4	8 ▼ 3	9 2	1 1	2 9	3 8	4 ▼ 7	5 6	
m	6	5 4	6 3	7 2	8 1	9 9	1 8	2 7	3 6	4 5	
MD	7	4 ■ 3	5 2	6 1	7 ■ 9	8■ 8	9 7	1 6	2 5	3■ 4	
AD̲	8	2	1	9	8	■7	■6	■ 5	4	■ 3	
Cln	9	■		■	■				■		

Размещение номеров диагоналей и проверочных символов четности