Основой ТАУ является метод пространства состояний, с помощью которого отдельные системы описываются во времени в виде векторных дифференциальных уравнений.

Применение научно-методологического аппарата ТАУ позволяет:

определить статические и динамические свойства системы;

описать основные законы управления в виде математических зависимостей, в соответствии с которыми вырабатываются управляющие воздействия;

исследовать переходные процессы в системе, их качество и влияние на дальнейшее поведение управляемой системы;

исследовать устойчивость и управляемость системы;

наглядно представить процессы функционирования системы методом фазовой плоскости (пространства).

Таким образом, представление и исследование процесса защиты информации в ИССН как объекта управления в рамках системного анализа – теории автоматического управления позволит определить его параметры (характеристики) и выявить присущие ему особенности, которые должны в полной мере учитываться при создании автоматизированных средств и систем управления защитой информации в ИССН. Это необходимо для проведения моделирования процессов защиты информации в ИССН в различных условиях их функционирования в целях определения оптимальности и эффективности применения различных способов управления защитой информации посредством программно-технических средств (средств автоматизации).

УДК 339

М.С. Маскина, О.В. Степанова

О БЕЗОПАСНОСТИ БЕСКОНТАКТНЫХ ПЛАТЕЖЕЙ

На сегодняшний день в мире существуют разные способы оплаты услуг, наиболее новым из которых является бесконтактный платеж. Самыми известными бесконтактными системами оплаты в России являются: MasterCard PayPass, Visa PayWave, Apple Pay, Samsung Pay. Их создатели заявляют, что технология бесконтактных платежей не только является прогрессивной, но и считается самой безопасной. В данной статье попытаемся разобраться, действительно ли бесконтактные платежи настолько безопасны.

Все вышеперечисленные системы оплаты работают на технологии связи, действующей на малых расстояниях, – NFC (Near Field Communication). Это высокочастотная, беспроводная связь малого радиуса,

работающая на частоте 13,56 МГц при скорости передачи данных 424 кбит/с на расстоянии до 10 см, предназначена для бесконтактного обмена информацией. В бесконтактные карты MasterCard PayPass и Visa PayWave встроен чип NFC, который позволяет провести операцию оплаты, если банковскую карточку поднести к считывающему устройству на близкое расстояние. Это очень удобно, так как процесс оплаты занимает немного времени, так как подтверждение платежа не требуется, если сумма покупки не превышает 1 000 рублей.

На данный момент Apple Pay поддерживает технологию NFC пока лишь с картами платежной системы MasterCard. Достаточно лишь сфотографировать или внести данные карты на смартфон iPhone, чтобы он стал платежным средством. Безопасность Apple Pay базируется на трех составляющих: биометрическом сенсоре Touch ID, чипе NFC и чипе Secure Element, который хранит в себе, не передавая и не копируя, информацию о банковских картах. Каждая транзакция получает уникальный код – токен, который передается терминалу вместо индивидуального номера карты. Чтобы произвести оплату, ее нужно подтвердить PIN-кодом или срабатыванием Touch ID независимо от суммы покупки. В случае кражи или потери смартфона iPhone все платежи можно запретить через программу Find My iPhone.

В отличие от Apple Pay платежный сервис Samsung Pay обеспечивает и работу по бесконтактной технологии, и связь по магнитной полосе. В смартфон Samsung помимо чипа NFC встроен магнитный чип MST (Magnetic Secure Transmission), который создает сигнал, идентичный сигналу пластиковой карты при ее взаимодействии с терминалами оплаты. Смартфоны с сервисом Samsung Pay создают магнитное поле, сходное с сигналом магнитной полосы банковской карты, и поддерживают обе ведущие платежные системы Visa и MasterCard.

Система безопасности Samsung Pay имеет также два принципа действия. На магнитных терминалах при каждом соединении чип генерирует индивидуальный код – токен, чтобы терминал считывал именно его, а не уникальный номер карты. При работе с NFC программа использует потоковое шифрование данных и алгоритм Serpent (змея), который оперативно распознает несанкционированный доступ. Samsung Pay использует безопасную среду Samsung Knox, которая проверяет смартфон на наличие уязвимостей и при их нахождении автоматически отключает Samsung Pay. В случае кражи или потери смартфона можно запретить проводить платежи через программу Samsung Find My Mobile.

В теории безопасность бесконтактных платежных технологий обеспечена вполне, но так ли это в действительности? Рассмотрим подробнее уровни защиты.

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