УДК 004.056

А.Р. Мацылевич

ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ КАК ОБЪЕКТ УПРАВЛЕНИЯ

Среди информационных сетей различного назначения можно выделить информационные сети специального назначения (ИССН), которые функционируют в интересах ведомств и органов, входящих в состав сил обеспечения национальной безопасности Республики Беларусь. Специфика ИССН определена назначением, условиями функционирования, природой угроз безопасности информации, а также тяжестью последствий их реализации. Реализация данных угроз может нанести ущерб не только владельцу ИССН, но и национальной безопасности Республики Беларусь.

В своем развитии информационные системы и сети, в том числе ИССН, достигли такого уровня, что человек по своим психофизиологическим возможностям уже не в состоянии адекватно и оперативно противодействовать угрозам безопасности информации, существенно снижая эффективность защиты информации. Необходимость использования ресурсоемких интерфейсов («машина – человек – машина») обуславливает зависимость процессов защиты информации от таких характеристик человека, как мотивация, профессиональная подготовленность, усталость, отвлеченность, эмоциональность и др., которые могут способствовать блокированию системы защиты информации в ИССН (влияние так называемого человеческого фактора). Более того, неквалифицированные действия человека по управлению защитой информации являются внутренней угрозой безопасности информации в ИССН.

Максимально возможное исключение человеческого фактора из процессов защиты информации достигается при применении программно-технических средств, реализующих функции управления защитой информации (средства и системы управления защитой информации). Автоматизация процессов управления защитой информации позволяет наиболее эффективно решать задачи как единого управления защитой информации, так и защиты информации в ИССН.

В настоящее время концептуально и методологически наиболее изучены вопросы применения средств защиты информации, в меньшей мере вопросы применения средств контроля эффективности защиты информации. Концептуальные положения создания и применения средств управления защитой информации и, более того, систем автоматизированного управления защитой информации в ИССН разработаны недостаточно полно.

ИССН являются сложными организационно-техническими системами, в которых объединены элементы различной природы (антропогенной и техногенной). Поэтому, несмотря на тщательное изучение технических и организационных систем, возникла необходимость автоматизированного управления новыми типами систем – организационно-техническими. Наличие человека как элемента в системе, элемента в подсистеме управления (лицо, принимающее решение по защите информации) не позволяет в полной мере применять традиционные методы формирования управляющих воздействий (касающихся исключительно организационных или технических систем).

По причине недостаточной изученности вопросов управления защитой информации подсистема защиты информации в ИССН традиционно рассматривается в основном как организационная система. Поэтому в защите информации преобладают меры правового или организационного характера. Применение технических мер, связанных с внедрением средств вычислительной техники, в первую очередь касается криптографического преобразования информации и защиты информации от утечки по техническим каналам.

В настоящее время созданы подходы и условия для формирования эффективно функционирующих систем управления организационно-техническими процессами, к классу которых относится защита информации. Основополагающим при этом является адекватное представление о защите информации как об объекте управления, то есть определены назначение, цели функционирования, структура, основные параметры (характеристики), способы управления, критерий оптимальности и эффективности управления.

Задачу адекватного представления о защите информации как об объекте управления целесообразно решать в рамках системного анализа, наиболее конструктивного направления, используемого для практических приложений теории систем к задачам управления. Описание защиты информации как объекта управления и в то же время как системы осуществляется в понятиях системного анализа.

Описание защиты информации как объекта управления позволяет провести дальнейшее исследование управления защитой информации в рамках теории автоматического управления (ТАУ). Теория автоматического управления входит в состав дисциплин, образующих науку об управлении. Изначально ТАУ предназначалась для исследования процессов управления техническими объектами. В последнее время ТАУ используют для изучения статики и динамики не только технических объектов, но и организационных, организационно-технических.

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.