мая N рабочими станциями. В случае перегрузки $\Lambda^{\text{Т}} > \Lambda^{\text{П}}$ секцией управления выполняется регулирование нагрузки для каждой РС $l_i^{\text{Т}} \to l_i^{\text{Р}}$, где $l_i^{\text{Р}}$ – значение регулируемой нагрузки i-й РС, устраняющее перегрузку канала связи $\sum_{i=1}^{N} l_i^{\text{Р}} \le \Lambda^{\text{П}}$.

Программная реализация секции управления позволяет устанавливать различные политики ограничения трафика абонентов, учитывая их приоритеты, т. е. $l_i^{\text{Р}}$ может определяться для каждой i-й РС в соответствии с политикой приоритетов передачи данных, установленной в сети, для каждой РС.

Возможность измерять трафик канала передачи данных сервера в реальном масштабе времени позволяет оперативно обнаруживать и устранять перегрузку сети, что позволяет избежать проблемы монополизации канала связи отдельными абонентами сети.

Таким образом, предложенный метод управления информационным трафиком протокола TCP обладает высокой оперативностью управления загрузкой каналов связи путем постоянного поддержания суммарной нагрузки на канал ниже порогового уровня, что позволяет устранить причину блокировок и потери информационных кадров. Программная реализация метода позволяет гибко изменять политики ограничения избыточного трафика абонентов с учетом их приоритетов и заданного для них уровня качества обслуживания. Достоинством метода является его независимость от операционной среды, что связано с тем, что протокол TCP встроен во все современные сетевые операционные системы.

А.Н. Лепехин

ДЕЯТЕЛЬНОСТЬ ОРГАНОВ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В БАНКОВСКОЙ СФЕРЕ

На протяжении последних пяти лет отмечается рост выявленных правоохранительными органами фактов хищений денежных средств из банкоматов с использованием банковских пластиковых карт. Примерно половина из них совершена при помощи поддельных банковских пластиковых карт, в том числе карт, эмиттированных банками иностранных государств и ввезенных преступниками на территорию Республики Беларусь. Кроме того, имеются факты разбойных нападений на структурные подразделения банков, кражи денежных средств из банкоматов путем их повреждения. Указанные факторы оказывают негативное влияние на легальный оборот информации в банковской сфере, ее защиту и связаны с обеспечением информационной безопасности в банковской системе в целом.

Анализ практики расследования уголовных дел по фактам неправомерного использования персональной финансовой информации для совершения хищений показывает, что причинами вышеуказанных преступных посягательств являются:

невысокая профессиональная подготовка работников банковской системы;

ненадлежащий уровень оснащения объектов, осуществляющих расчетно-кассовое обслуживание, техническими средствами и системами защиты информации;

расположение банковских объектов, в том числе банкоматов, в местах, не обеспечивающих безопасность и сохранность имущества;

отсутствие либо несовершенство систем видеонаблюдения, что не способствует предотвращению преступных посягательств и препятствует изобличению виновных лиц при привлечении их к уголовной ответственности.

Кроме того, за последнее время существенно увеличилось число преступлений, связанных с часто забываемыми в банкомате банковскими картами, находящимися в активированном состоянии. Однако в качестве средства профилактики указанной группы правонарушений наличие системы голосового оповещения о необходимости забрать карту после завершения банковской операции в большинстве банкоматов отсутствует.

Как показывает практика расследования по уголовным делам, связанным с хищениями в банковской сфере, органы предварительного расследования сталкиваются с рядом организационных недостатков в работе банковских учреждений, устранение которых могло бы оказать существенную помощь в раскрытии и расследования указанных преступлений:

банковские объекты, в том числе банкоматы, не всегда расположены в общественных местах (помещениях субъектов хозяйствования), которые находятся в зонах патрулирования правоохранительных органов либо оснащены системами видеонаблюдения;

прилегающая к банкоматам территория не должным образом оснащена аппаратурой видеонаблюдения с высоким разрешением и более длительным периодом хранения информации;

недостаточный профессиональный уровень работников банков (операционный персонал), а также характер проводимой разъяснительной работы при заключении договоров банковского обслуживания;

неиспользование возможности средств массовой информации для освещения негативных последствий небрежного использования и ос-

тавления банковских пластиковых карт их владельцами в банкоматах в целях профилактики хищений.

Одним из частых фактов совершения хищений в банковской сфере является случай, когда преступник в ходе непродолжительного времени общения с человеком, пользуясь моментом, когда тот находится в состоянии алкогольного опьянения, похищает его банковскую пластиковую карту, предварительно узнав или подглядев ее PIN-код. После чего направляется к банкомату или объектам розничной торговли, где оплата производится с использованием пластиковых банковских карт, и путем ввода уже известного ему PIN-кода совершает хищение денежных средств потерпевшего.

Реализацию преступного замысла облегчает то, что при предоставлении банковской пластиковой карты в местах розничной торговли сотрудники объекта торговли не предпринимают никаких мер по идентификации личности, предоставляющей пластиковую карту (кроме ввода PIN-кода) (это недостаточно четко оговорено в ведомственных нормативных актах, регулирующих процесс использования пластиковых карт в данных предприятиях).

В целях решения уголовно-процессуальных задач сотрудниками органа предварительного расследования в ходе следствия по указанным фактам проводится ряд следственных действий, направленных на выявление лиц, совершивших преступление: выемка видеозаписи камер видеонаблюдения банкоматов, а также в тех местах, где проводится розничная торговля; допрос лиц, осуществлявших выдачу товара или денежных средств по представленной похищенной банковской пластиковой карте, с целью уточнения примет преступника; опознание лиц, которые использовали похищенные пластиковые карты либо им пособничали; назначение различных экспертиз в зависимости от обстоятельств совершенного преступления в данной сфере. Это далеко неполный перечень следственных действий и иных мероприятий, которые следователь выполняет в ходе расследования уголовных дел по вышеуказанным фактам.

В соответствии со ст. 199 УПК Республики Беларусь в целях профилактики совершения преступлений в банковской сфере и обеспечения безопасности информации следователем выносятся представления об устранении нарушений закона, причин и условий, способствовавших совершению преступления, которые направляются в учреждения, где недостаточно обеспечена безопасность проводимых банковских операций как непосредственно с деньгами, так и посредством пластиковых банковских карт. Кроме того, выносятся представления в отношении конкретных лиц, которые не должным образом обеспечивают выполнение своих должностных обязанностей, связанных с осуществлением операций с пластиковыми банковскими картами и соблюдением установленного порядка их совершения.

Таким образом, деятельность органов предварительного расследования в целях обеспечения безопасности информации в банковской сфере направлена как на раскрытие и расследование фактов преступных посягательств на банковскую систему и хранящуюся в ней информацию, так и на профилактику указанных фактов.

Д.В. Лукашонок, **И.Н. Цырельчук**

ПРИНЦИПЫ ПОСТРОЕНИЯ ЗАЩИЩЕННОЙ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ОРГАНИЗАЦИИ

Основу любой организации оставляет локальная вычислительная сеть (ЛВС), по которой передается информация, предназначенная как для открытого использования, так и ограниченного распространения. Возникает проблема построения защищенной ЛВС с учетом действующего законодательства Республики Беларусь. Рассмотрим решение данной проблемы на примере.

Введем следующие ограничения: ЛВС построена по топологии звезда на базе контроллера домена, все коммутационное оборудование является управляемым, для разграничения доступа между различными подсетями будем использовать аппаратный брандмауэр, ЛВС расположена в пределах одного здания (этажа) и не имеет смежных с другими организациями стен, межэтажные перекрытия защите не подлежат, в ЛВС не обрабатывается информация, отнесенная в установленном порядке к государственным секретам или для служебного пользования, физическая защита оборудования (пожарно-охранная сигнализация, системы автоматического пожаротушения, системы контроля и управления доступом) функционирует надлежащим образом.

Работу организации могут нарушить: физический отказ оборудования (серверов, персональных компьютеров (ПК), кабельной сети, сети электропитания и т. п.); умышленные и неумышленные попытки несанкционированного доступа (НСД) (сотрудниками и посетителями организации, из ЛВС организации, из внешних сетей); программный сбой (вследствие запуска вредоносного исполняемого и (или) интерпретируемого кода, физических ошибок оборудования и т. п.).

Они требуют правильных технических решений организации построения ЛВС. Физический отказ требует использования резервирования критически важных узлов системы, резервное копирование информации ПК и серверов. Для исключения аварийного отключения серверов вследствие нарушения работы сети электропитания необходимо использовать источники бесперебойного питания, которые позволят обеспечить корректное завершение их работы.