DOI 10.37882/2223-2966.2023.7-2.26

# МЕТОДЫ И МОДЕЛИ ПОВЫШЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ УДАЛЕННЫХ ЗАПРОСОВ НА ИСПОЛНЕНИЕ ТРАНЗАКЦИЙ

***Савельев Иван Андреевич***
*к.т.н., Финансовый университет при Правительстве РФ, г. Москва*
*IASavelyev@fa.ru*

*Аннотация*. В настоящее время из-за совершенствования алгоритмов обработки больших данных, а также существенного удешевления вычислительной мощности серверного оборудования становятся всё более доступными, и, следовательно, популярными технологии фальсификации запросов на исполнение транзакций. В статье рассматриваются методы и модели повышения уровня защищенности удаленных запросов на исполнение транзакций. Представлена структура процессингового центра, основные его уязвимости, и методы обеспечения сетевой безопасности.

*Ключевые слова*: кибербезопасность, обеспечение конфиденциальности и целостности транзакций, принцип интероперабельности.

## ON THE PROSPECTS FOR THE INTRODUCTION OF BIOMETRIC INFORMATION INTO A GRAPHICAL SPEECH SIGNAL FORMAT

***I. Savelyev***

*Summary*: Currently, due to the improvement of algorithms for processing big data, as well as a significant reduction in the cost of computing power of server equipment, technologies for falsifying requests for transaction execution are becoming more and more accessible, and, consequently, popular. The article discusses methods and models for increasing the security level of remote transaction execution requests. The structure of the processing center, its main vulnerabilities, and methods of ensuring cybersecurity are presented.

*Keywords*: cybersecurity, ensuring confidentiality and integrity of transactions, the principle of interactivity.

## Введение

Учитывая огромную скорость развития компьютерной техники и самих технологий во всем мире, становится сложно угадать темпы их развития не только на ближайшее десятилетие, но и на год вперед. Несмотря на это главные направления развития хорошо прогнозируются. Например, одно из таких заманчивых в развитии на рынке направлений по предоставлению процессинговых услуг является решение, получившее признание и широкое применение в различных гигантских корпорациях. Оно вырастало из периода начального этапа развития компьютерных сетей и систем удаленного доступа на базе терминальных станций. Тогда пользователям была предоставлена возможность управления электронно-вычислительными ресурсами основного компьютера с использованием удаленного доступа через терминальные станции, которые были подключены по общему, как правило, открытому каналу передачи данных. Любой пользователь мог зарегистрироваться на центральном компьютере и получить определенные права на доступ.

Такая система удаленного доступа применяется и по сей день, однако современные тенденции развития интернет-технологий позволили передвинуть всю систему на следующую ступень. Во всем аналогичная технология получила широкое распространение. Сейчас она известна «тонкий клиент». Эта технология основана на технологии удаленного доступа между терминалом и главным компьютером, распределенной сетью (процессинговый центр). Чтобы получить доступ к своим ресурсам, пользователю требуется пройти регистрацию и аутентификацию на главной машине. При передаче информации о действиях пользователя с клавиатуры или сенсорного экрана от терминала к серверу, в ответ приходят изменения на экране удаленного терминала. Такой доступ гарантирует безопасность при получении процессинговых услуг. Данный подход обладает множеством плюсов, которые возможно использовать при повышении сетевой безопасности серверов процессингового центра (ПЦ).

Такой подход дает возможность не рассматривать защиту от вирусов терминалов, защиту от угроз появления дыр в безопасности, недекларированных возможностей программного обеспечения, НСД к информации, хранящейся на сервере. Использование централизованного управления доступом к терминалам с удаленным доступом к открытым сессиям пользователей и администрирование терминалов существенно упрощает функции администрирования сети. С экономической точки зрения, установленные на сервер программы можно разместить на всех тонких клиентах, не приобретая дополнительных лицензионных соглашений, что очень выгодно для крупных процессинговых центров. Еще одним крупным преимуществом становится то, что важные данные, в том числе персонального характера (номера карт, данные авторизации) нельзя сохранить на внешних информационных носителях при отсутствии специализирован-

ных средств, предоставляемые администраторами сети в специальных случаях. Все это позволяет сделать вывод о нулевой вероятности утечки критических данных с сервера ПЦ. Однако эта технология нуждается в специальной защите серверных приложений, другими словами, все компоненты программ, размещенные на сервере, требуют максимальной степени защиты от НСД.

Основополагающими факторами обеспечения безопасности удаленных запросов на исполнение транзакций предоставляемых услуг ПЦ. Стоит понимать, что все рассмотренное составляет лишь обобщение накопившегося практического опыта целого мира. Разумеется, каждый процессинговый центр, имеет характерные черты и особенности, поэтому и задачи по осуществлению безопасного его функционирования обладают своей спецификой. Каждый процессинговый центр выполняет обработку персональных данных с карт владельцев, а значит репутация и надежность ПЦ тесно связаны с уровнем безопасности внутренних систем. Теперь становится понятно, почему необходимо затрачивать столько ресурсов на достижение целей по обеспечению должного уровня устойчивости к отказам систем при круглосуточном обслуживании клиентов, так и на поддержание уровня защиты данных, обрабатываемых в ПЦ.

## Структура процессингового центра

В любом определении сказано, что процессинговый центр является юридическим лицом или его структурным подразделением, которое обеспечивает взаимодействие информации и специальных технологий между участниками электронных расчетов.

В России же понятие ПЦ, часто применятся к организациям, которые выпускают и обслуживают пластиковые карты, в первую очередь, это организации кредитно-финансовой сферы.

Почти все отечественные банки, выпускающие пластиковые карты, в том числе МИР, организуют свои банковские ПЦ, являющиеся структурными подразделениями, позволяющие осуществлять взаимодействие информации и специальных технологий между участниками электронных расчетов, и проводящие обработку операций с картами внутри своей сети.

Так каждая система расчета банковскими картами учитывает собственные условия для процессинговых центров.

Главным условием любых платежных систем является требование их сертификации их третьей стороны.

ПЦ на территории Российской Федерации должен иметь лицензии от федеральной службы безопасности на деятельность по услугам шифрования данных в международных системах платежей с банковскими картами и должное техническое обслуживание средств шифрования, которые также используются в интернациональных системах платежей.

Периферийное устройство (ПУ), или автоматическая кассовая машина (АТМ), используется для:
- — приема и выдачи бумажных денежных средств;
- — создания документированной информации об операциях с банковскими картами;
- — предоставления информации по текущему счету;
- — проведения электронных платежей.

Главная задача периферийного устройства ПЦ состоит в предоставлении наличных денежных средств и дополнительных услуг, в том числе:
- — учет баланса по банковскому счету;
- — прием денежных средств на депозитный счет;
- — осуществление платежных операций с распечаткой документов;
- — дистанционное обслуживание лицевого счета по карточному субсчету.

У любого устройства ПЦ всегда присутствуют:
- — аппаратное компьютерное средство с многозадачной ОС, тем самым оно классифицируется по первому классу;
- — совмещенное устройство для распознавания и работы с магнитными, оптическими или интеллектуальными картами;
- — устройство для выдачи бумажных денежных средств.

Перечисленные элементы компактно размещены в едином защищенном корпусе.

В ПУ встроены процессор, дисплей (часто сенсорный), блок клавиатуры и устройство для считывания персональных данных с карт владельца. Чтобы пройти идентификацию, пользователь помещает свою карту в специальный приемник — ридер, а с клавиатуры набирает код из 4-х цифр (ПИН-код). Только потом ПУ позволяет открыть сессию для работы в личным кабинетом или выполнить выдачу наличных.

Купюры, предназначенные для выдачи клиенту, держатся в защищенных кассетах, хоть и защищены не так хорошо, как сейфы — их можно вскрыть только при помощи специального оборудования.

Часто на банкоматы устанавливают вспомогательные устройства, которые хоть и увеличивают номинальную стоимость, зато существенно повышают уровень защищенности (web-камеры, оборудование для дистанционной консультации, криптографические средства защиты,

бесперебойным блочным питанием и пр.) В комплекте от производителей включено специальное ПО с базовыми исполнительными модулями для создания систем мониторинга, непосредственно встраиваемых в банкоматы.

## Уязвимости периферийного устройства

Уязвимости ПУ логически можно разделить на высокоуровневые и низкоуровневые

Высокоуровневые уязвимости ПУ связаны с проблемами построения защищенных систем, высокоуровневого платежного ПО, расположенного на терминале и промежуточных узлах между терминалом и банком. К данным компонентам ПУ применяются требования международных стандартов пластиковых карточек PCI DSS, PCI PA-DSS. [3]

Требования к криптографической стойкости алгоритмов шифрования, ключей шифрования, процессам начальной загрузки, смене и обновления ключей шифрования, периодам смены операционных и мастер-ключей и др. определены в стандарте PCI PTS.

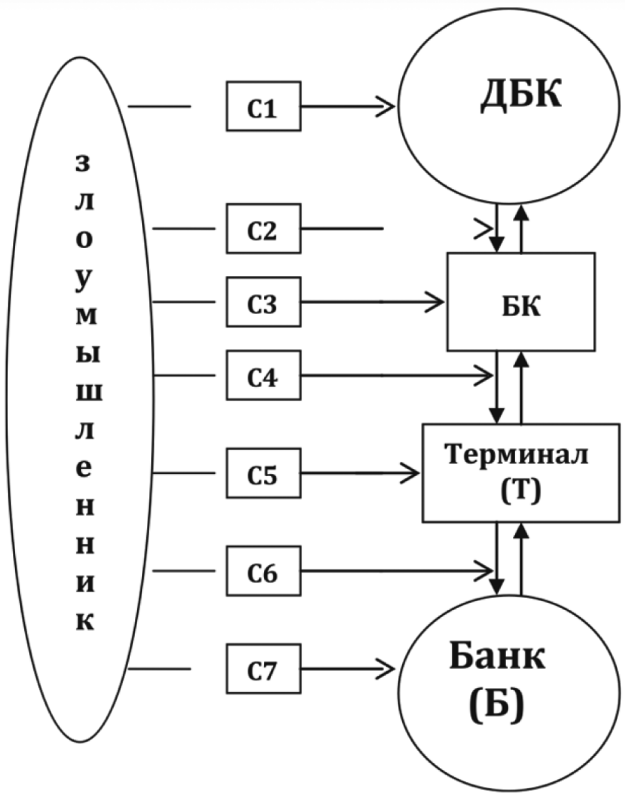


Рис. 1. Группы уязвимостей

Оборудование, взаимодействующие с банковскими картами (БК) и данными БК (ДБК), устройство ввода PIN-кода и чтения БК должно быть сертифицировано в соответствии с требованиями PCI PTS POI, оборудование банка, обрабатывающее транзакции от терминалов, сертифицируется в соответствии с требованиями PCI HSM.

Низкоуровневые уязвимости ПУ связаны с неразвитой культурой владения и использования БК, неразвитыми и малоэффективными методами противодействия мошенничеству основанному на уязвимостях С1 ... С5.

Существует ряд рекомендаций по использованию БК, вводу PIN-кода, однако их эффективность не удовлетворяет современному уровню технических решений по хищению персональной информации ДБК.

Так как низкоуровневые уязвимости напрямую зависят от владельцев БК, никак не затрагивая функциональные возможности ПУ и сетевой среды ПЦ, то их рассмотрение не попадает в рамки темы, которая рассматривается. Другими словами, одна из главных задач сводится к безопасности сетевой передачи данных. [1]

В таблице 1 указаны объекты и относящиеся к ним потенциальные уязвимости.

## Уровень безопасности в сети

Все имеющиеся меры, используемые в целях поддержания безопасности сети, состоят из 4 взаимосвязанных уровней:

— сетевой;
— пользовательский;
— транспортный;
— приложений.

Все уровни тесно взаимосвязаны между собой, а в некоторых случаях одни включают в себя другие. Следует обратить внимание, что дифференциация проводилась условно, ведь существуют комплексные системы, в которых указанные выше уровни интегрированы в один цельный.

Однако следует учесть, что все организационные уровни безопасности в сети имеются в любом процессинговом центре, поэтому каждый требует отдельного рассмотрения.

## Сетевой уровень безопасности

Текущий уровень включает технические средства, обеспечивающие надежное прохождение информации среди всех зон процессингового центра. На рисунке 2 представлен типовой вариант сетевой схемы ПЦ, где сетевая структура имеет разделение по зонам. Эти зоны взаимоувязаны при помощи специальных технических средств (маршрутизаторов и коммутаторов), которые выполняют роль перераспределяющих элементов сети между зонами. А межсетевой экран (далее МЭ) выполняет роль пограничника, пропускающего входящие и исходящие пакеты. Нередко эти устройства совмещаются в единое устройство, имеющем возможность настройки ограничений пропускной способности траффика.

Таблица 1.

Соотношение уязвимостей объектов

| № | Объекты | Уязвимости | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 1 | ДБК | Потеря БК | Сообщение PIN-кода третьим лицам | Потеря БК вместе с PIN-кодом | Смена PIN-кода на заведомо слабый | Хранение PIN-кода вместе с БК |
| 2 | ДБК + БК | Передача БК третьим лицам | Использование БК не по назначению | Сообщение номера БК (PAN номера карты) третьим лицам | Сообщение кодов подтверждения / отмены транзакций по БК третьим лицам | Сообщение кодов CVV2,CVC27 третьим лицам |
| 3 | БК | Размагничивание данных, хранимых на магнитной полосе БК | Физическое повреждение поверхности БК | Ограниченный срок эксплуатации БК вследствие «слабого» принципа хранения данных | Изменение данных, хранимых на магнитной полосе БК | Отсутствие подписи ДБК на БК |
| 4 | БК + ПУ | Скимминговое устройство считывания БК | Накладная клавиатура ввода PIN кода | Видео наблюдение процесса аутентификации — ввода PIN кода БК | Подслушивание нажатий клавиш PIN клавиатуры | Подглядывание процесса аутентификации ввода PIN кода БК |
| 5 | ПУ | Подмена терминала | Перехват управления терминалом | Замена устройства считывания БК | Замена клавиатуры ввода PIN кода | Перевод клавиатуры ввода PIN кода в небезопасный режим работы |
| 6 | ПУ + ПЦ | Атака «Man in the middle» | Атака типа «Replay» | Небезопасная/ устаревшая технология передачи ключей шифрования | Использование не криптостойких ключей шифрования | Использование не сертифицированного шифрующего оборудования |
| 7 | ПЦ | Небезопасная передача PIN кода и БК к ДБК | Небезопасная технология первичного ввода ключей шифрования | Небезопасная/ не сертифицированная технология смены ключей шифрования | Не регламентированные интервалы смены ключей шифрования | Уязвимости в физических модулях безопасности — HSM |

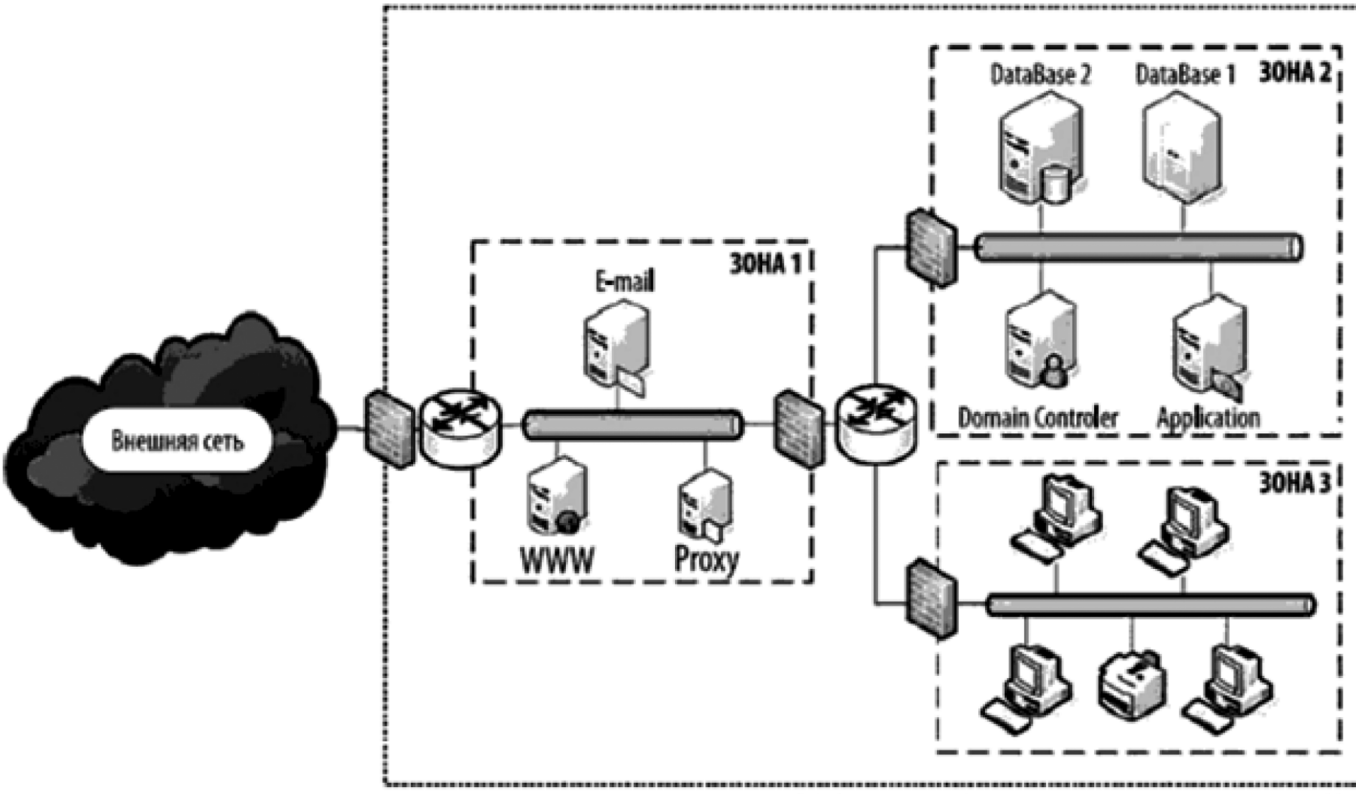


Рис. 2. Сетевая инфраструктура

Такое зональное разделение позволяет не только увеличить уровень защищенности ПЦ, но и сделать удобнее механизм управления списком контроля доступа. Мы видим, что первая зона отвечает за размещение приложений на сервере из вне которая носит название Демилитаризованная Зона или DMZ. Размещенные на сервере приложения могут включать в себе различные службы, начиная от интернет-банкинга, заканчивая электронной почтой. Ограничение доступа к сетевым службам снаружи устанавливается при помощи сетевого экрана, который пропускает только разрешенный администратором траффик.

Во второй зоне располагаются процессинговые серверы, отвечающие за работоспособность всего ПЦ. Здесь хранятся серверы БД, в качестве архива процессов авторизации и ячейки дальнейших счетов. Также здесь размещаются серверы для уровня приложений, обладающие доступом к серверам БД и выполняющих процесс авторизации соединений. Еще в этой зоне могут быть расположены средства накопления отчетной информации и управляющие уровнем доступа приложений серверы. Данная зона наиболее привлекательна для нарушителей, а значит, ее защита будет целью номер 1. Чтобы повысить уровень защиты, следует включить дополнительные МЭ и брандмауэры на каждом средстве. Для наиболее важных элементов требуется установить аудит доступа к данным. Настраивая политику безопасности в серверной зоне, важно отключить или заблокировать доступ ко всем ненужным процессам и второстепенным приложениям, которые могут использоваться как бреши в системе защиты злоумышленниками. Например, у серверов БД должен отсутствовать доступ по сети к ОС. Либо оставить доступ к БД только по защищенным каналам передачи, используя надежные протоколы. Полезными могут быть системы обнаружения вторжений (сканеры портов), которые позволяют преждевременно ограничить сетевой доступ при выявлении потенциально опасных данных в трафике (при попытках осуществления атак на сервер). Наиболее часто атакам подвергаются маршрутизаторы и МЭ. В целях повышения надежности, следует грамотно настроить интерфейс управления. По умолчанию интерфейс без подключений к сети, а настройка с других невозможна.

В третьей зоне находятся места работы сотрудников центра. Она выделена в одну сеть, потому что безопасность управления сотрудниками очень специфична и требует особого контроля. Ведь тут совмещены рабочие места с офисным оборудованием, таким как устройства ввода/вывода бумажной информации, телефонные сети и пр. Для каждого сотрудника должен быть настроен доступ в соответствии с дискреционной политикой безопасности.

### Пользовательский уровень безопасности

Что касается безопасности на этом уровне, то она осуществляется путем распределения доступа ко всем ресурсам на основе пользовательских групп.

Каждая ОС настроить разграничение доступа к данным для любого зарегистрированного пользователя или процесса. Значит, любой зарегистрированный пользователь или системный процесс получит строго заданные права на основе должностных инструкций, сформированные и предоставленные в бумажной форме. Удобнее, если у сотрудника будет совмещение ролей и обязанностей. Каждая роль обладает своими полномочиями, в соответствии с которыми открывается доступ.

Служебные процессы можно отнести к пользователю или группе пользователей. Администратором можно назначить целую группу, предварительно включив необходимых пользователей.

Каждый сотрудник должен обладать своей учетной записью, которую он использует для регистрации в сети процессингового центра. И эту же учетную запись можно использовать уже внутри сети для работы с принтером или факсом.

Разрабатывая политику безопасности, каждый сотрудник должен соблюдать правила хранения и использования личных данных для входа в сеть. Требуется заранее прописать условия на запрет передачи паролей третьей стороне. Разрабатывая политику, требуется задать безопасный подход по формированию формы и длинны пароля, сложность и частоту изменения.

Пароли создаются с длинной, равной или превышающей 8 символов, используя разные регистры, буквы и цифры. А частота изменения пароля снижает вероятность его взлома методом подбора. Хорошие результаты на практике показывает и такой метод, как ограничение числа попыток ввода пароля, которое варьируется в диапазоне от 3 до 5).

В качестве дополнительной меры по защите могут использоваться средства идентификации и аутентификации. Например, цифровые сертификаты значительно увеличивают защищенность системы от попыток взлома. А двухфакторная аутентификация дает возможность исключить раскрытие данных учетной записи в случае взлома пароля методом подбора. Еще можно добавить использование биометрических данных в качестве ключей.

Сделав анализ, можно сказать, что безопасность на уровне пользователей является еще одним препятствием для злоумышленника, позволяющее разграничи-

вать ресурсы пользователей в соответствии с политикой безопасности внутри процессингового центра.

### Безопасность на транспортном уровне

Если рассматривать следующий уровень — транспортный, то важно заметить, что он лишь выполняет контролирование функций уровня сети на функционирующих узлах приема и передачи в процессинговом центре. Задача этого уровня заключается в проверке целостности всех пакетов данных, их последовательности, маршрута, время отправки и получения, распознавание и фиксацию данных об отправке. Почти все современные угрозы видны здесь как на ладони.

Гарантировать целостность при передаче данных может лишь шифрование служебной и основной информации. Только обладатели секретного ключа получают доступ к зашифрованным данным.

Правда стоит заметить, что данные методы защиты не могут противостоять уничтожению, перенаправлению или задержке передаваемой информации. Чтобы этого избежать, требуется дублировать передачу данных по другим защищенным каналам параллельно.

### Безопасность уровня приложений

Перечисленные выше меры существенно повышают безопасность сети.

Однако следует отметить такое понятие как интероперабельность, то есть способность двух или более систем, или компонентов к обмену информацией и к использованию информации, полученной в результате обмена [4]. Общая модель обеспечения интероперабельности состоит из:

Организационной интероперабельности (интероперабельность бизнес-процессов). Способность систем достигать общих целей на уровне бизнес-процессов.

Семантической интероперабельности. На данном уровне стоит задача описания структур данных, т.е. содержательную сторону обмениваемой информации. Это способность любых взаимодействующих систем одинаковым образом понимать смысл передаваемой информации.

Технической интероперабельности. Описывает вопросы использования общих форматов и протоколов для представления и передачи информации (TCP/IP, UDP, HTTP, SSL).

Отсутствия интероперабельности.

Перечисленные выше меры существенно повышают безопасность сети. Несмотря на защищенное функционирование данных на сетевом и уровне приложений, есть вероятность утечки конфиденциальных данных через дыры в прикладном ПО. Нарушитель может получить доступ к персональным данным, даже не нарушая ни один параметр защиты процессингового центра.

Поэтому, безопасность на данном уровне имеет высокий приоритет из всех компонентов защиты целого процессингового центра.

На вопрос о том, какие меры нужно использовать для защиты, легко ответит международный стандарт PA DSS, который подробно разъясняет все требования к ПО, которое обрабатывает данные карт. Когда был принят данный стандарт, то каждый поставщик стал обязан обладать сертификатом соответствия этому международному стандарту. Сертификат предъявляется в процессе проведения проверки на соответствие требованиям.

Например, одним из таких требований в PA DSS — это отсутствие в открытом виде информации о картах платежных систем (код безопасности CVV2/CVC2, информацию о сроках действия, номера карт и пр.)

Соответственный уровень обеспечения безопасности достигается путем обновлений важных областей ОС и систем БД. Данный шаг позволяет своевременно закрывать бреши.

Следующим шагом является методичное обновление ПО на МЭ и средствах маршрутизации. А при наличии платформ обнаружения вторжений, регулярно обновлять и их базы сигнатур.

Однако не все так просто с обновлениями главных сетевых узлов. Практика показывает, что нередки случаи вывода из строя или временно приостановке деятельности при реализации обновлений. Поэтому с целью снизить такой риск предлагается провести тестирование в безопасной среде (они носят название «песочниц»), где отслеживается реакция системы на данное нововведение. Из-за огромного объема системы ПЦ, проведение тестовых мероприятий часто занимает немало времени, доходя даже до нескольких недель или одного месяца. На стадии такого тестирования, необходимо включить ряд дополнительных мер для поддержания безопасности.

Если же тестирование проводится на серверах системы ПЦ требуется подготовка и осуществление тестирования на соответствующих элементах, для которых разработаны эти обновления. Проведение тестов строго должно проходить один законченный цикл транзакций, во избежание непредвиденных ошибок и сбоев при дальнейшей работе.

Еще одним обязательным компонентом зашиты является установка и функционирование программ поиска вирусной активности. Антивирусы устанавливаются на каждую из рабочих станций центра. Соответственно следует своевременно обновлять базы данных сигнатур.

Особую роль играют отчеты о работе или log-files. Ведь наша система состоит из нескольких больших элементов, поэтому требуется уделять больше внимания именно процессу записи и создания отчетов. На данный момент существует богатый выбор программ, предназначенных для решений в данной области.

Такое ПО осуществляет комплексный сбор и анализ данных по всем источникам:

— любые ОС;
— системы управления БД;
— средства маршрутизации и защиты сетей;
— программы-антивирусы;
— прикладные компоненты.

## Заключение

Перечисленный арсенал средств дает возможность не только своевременно устранять бреши в системе защиты, но и предупреждать их. А централизованный сбор информации после аудита доступа к элементам дет возможность составить хронологию атак, с последующим их предупреждением.

Соответственно следует защищать серверную часть централизованного сбора журналов log-файлов. Отчеты с сервера защищаются от модификации и удаления, без требуемых прав доступа. Время хранения этих отчетов для процессингового центра достигает 2–3 месяцев. После архивирования отчетов следует вычислить контрольные суммы с последующим документированием на бумаге.

Можно сделать вывод, что поддержание безопасности процессингового центра выливается в многостороннюю задачу, комплексное решение которой нуждается в тщательном анализе всех данных от этапа разработки до внедрения.

ЛИТЕРАТУРА

1. Ларионова С.Л. Информационная безопасность дистанционного банковского обслуживания: Учебное пособие. М. Издательство «Прометей», 2022.
2. Положение ЦБ РФ декабрь 2004 г. № 266-П «Об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт» (ред. от 21 сентября 2006 г.) (Зарегистрировано в Минюсте РФ 25 марта 2005 г. № 6431).
3. Состояние и перспективы защиты персональной информации держателя банковской карты при совершении трансакций через терминал [Электронный ресурс] — https://elibrary.ru/download/elibrary_20248757_23547189.pdf — 27.03.2023
4. Концепция обеспечения интероперабельности в электронной коммерции [Электронный ресурс]— https://cyberleninka.ru/article/n/kontseptsiya-obespecheniya-interoperabelnosti-v-oblasti-elektronnoy-kommertsii — 27.03.23


Журнал «Современная наука: актуальные проблемы теории и практики»