ФЕДЕРАЛЬНЫЙ ИНТЕРНЕТ-ЭКЗАМЕН ДЛЯ ВЫПУСКНИКОВ БАКАЛАВРИАТА И СПЕЦИАЛИТЕТА (ФИЭБ)

НАПРАВЛЕНИЕ ПОДГОТОВКИ
09.03.04 ПРОГРАММНАЯ ИНЖЕНЕРИЯ

ПРИМЕРЫ ЗАДАНИЙ ПИМ

ЧАСТЬ 1 ПИМ

Дисциплина «Базы данных»

Задание (установите соответствие между нумерованными объектами в формулировке задания и вариантами ответов)

Установите соответствие между ключевыми словами оператора SELECT и их функциями.
1. FROM
2. DISTINCT
3. ORDER BY
4. GROUP BY
5. WHERE

Варианты ответов:
1) отбирает для результата необходимые группы по условию предиката
2) отбирает неповторяющиеся строки для результата
3) отбирает для результата строки по условию предиката
4) указывает таблицы или представления для выборки
5) выводит результирующий набор в указанном порядке
6) группирует одинаковые значения в указанных столбцах

Дисциплина «Информационная безопасность»

Задание (укажите не менее двух вариантов ответов)

К алгоритмам, требующим, чтобы отправитель и получатель обменивались секретным ключом, используемым для обеспечения конфиденциальности сообщений, относятся …

Варианты ответов:
1) алгоритм из ГОСТ 28147-89
2) алгоритм Диффи – Хеллмана
3) алгоритм «Кузнечик»
4) SHA-2
5) RSA

Дисциплина «Искусственный интеллект»

Задание (установите правильную последовательность в предложенной совокупности ответов)

Установите последовательность шагов при реализации метода структурного распознавания.

Варианты ответов:
1) применение в рамках структурного подхода других методов распознавания
2) построение адекватного описания объектов распознавания
3) обучение для вывода грамматики
4) реализация процесса распознавания посредством процедур синтаксического анализа
5) выбор грамматики

Дисциплина «Компьютерные сети»
Задание (введите ответ в поле)

Технологии WIFI описаны в стандарте IEEE 802. …
(В ответе введите двузначное число.)

Введите ответ

Дисциплина «Метрология и качество программного обеспечения»
Задание (введите ответ в поле)

К метрикам первой группы относятся метрики оценки отклонения от нормы характеристик исходных проектных материалов, которые устанавливают полноту заданных технических характеристик исходного … (Введите слово в форме соответствующего падежа.)

Введите ответ

Дисциплина «Операционные системы»
Задание (установите правильную последовательность в предложенной совокупности ответов)

Установите последовательность событий, происходящих при обращении к виртуальному адресу на странице, отсутствующей в памяти.

Варианты ответов:
1) виртуальный адрес поступает в менеджер памяти
2) обеспечивается наличие свободного страничного фрейма
3) менеджер памяти формирует физический адрес и подает его на шину адреса
4) генерируется исключение по отсутствию страницы
5) требуемая страница читается в память с диска

Дисциплина «Программирование»
Задание (укажите не менее двух вариантов ответов)

Операторами, внутри которых может применяться оператор continue, являются …

Варианты ответов:
1) цикл while
2) оператор выбора switch
3) цикл do…while
4) цикл for
5) условный оператор if

Дисциплина «Структуры и алгоритмы обработки данных»
Задание (элементы доступны для перетаскивания)

Установите соответствие между алгоритмом и временем его работы.

1. Алгоритм Флойда –
2. Алгоритм Дейкстры –

Варианты ответов:
1) $O(n^3)$
2) $O(n)$
3) $O(n^2)$

Дисциплина «Управление программными проектами»

Задание (укажите не менее двух вариантов ответов)

Верными утверждениями, относящимися к V-образной модели жизненного цикла информационной системы, являются следующие …

Варианты ответов:

1) позволяет лучше контролировать результат на предмет его соответствия ожиданиям, поскольку сфокусирована на тестировании

2) приспособлена к возможным изменениям требований заказчика

3) предусматривает внесение изменений в требования на разных этапах жизненного цикла

4) дает возможность значительно повысить качество программного обеспечения за счет своей ориентации на тестирование

5) является модификацией каскадной модели и обладает многими ее недостатками

ЧАСТЬ 2 ПИМ

Кейс-задание
(Тип задач профессиональной деятельности: научно-исследовательский)

Задание
Необходимо разработать информационную систему для магазина компьютерных игр. Пользователями информационной системы являются: администратор, сотрудник магазина, покупатель.
В информационной системе должны быть реализованы следующие функции:
1) просмотр и управление данными о пользователях (администратор);
2) просмотр и управление данными об играх (наименование, год выпуска, жанр, цена, компания-производитель, системные требования: видеокарта, оперативная память, процессор, операционная система, наличие русской версии, принадлежность к серии, номер игры в серии, возможность сетевой игры) (сотрудник);
3) просмотр и поиск игр по различным критериям (сотрудник и покупатель);
4) покупка игр в офлайн (сотрудник) или онлайн (покупатель), приложение должно разрабатываться с учетом требований к информационной безопасности онлайновых покупок;
5) помощь покупателю в выборе компьютерной игры на основе его пожеланий:
- сформировать набор желаемых параметров путем опроса покупателя и определить наличие желаемого набора у имеющихся в продаже игр;
- предложить пользователю выбрать понравившиеся ему игры и определить для имеющихся в продаже игр соответствие предпочтениям пользователя.
Приложение должно разрабатываться с учетом требований к информационной безопасности онлайн-покупок.

Краткое содержание информации	Имя файла	Скачать файл
Информационная безопасность электронных платежных систем	1k1_Pril1	PDF

Подзадача 1 (укажите не менее двух вариантов ответов)

Поскольку набор желаемых параметров при поиске игр весьма широк, разработчики информационной системы приняли решение сформировать для каждой имеющейся игры единую строку-описание путем соединения всех ее параметров, а затем решать задачу подбора подходящих игр как поиск наибольшего числа подстрок – пожеланий покупателя, содержащихся в строках описаний игр.
Алгоритмами поиска, которые могут быть применены для этой цели, являются …

Варианты ответов:
1) алгоритм Вагнера – Фишера
2) алгоритм Кнута – Морриса – Пратта
3) алгоритм Дейкстры
4) алгоритм Рабина – Карпа
5) алгоритм Бойера – Мура
6) алгоритм Укконена

Подзадача 2 (укажите не менее двух вариантов ответов)

Основными угрозами безопасности электронной платежной системы являются …
При решении задания используйте файл 1k1_Pril1.

Варианты ответов:
1) внутренние нарушители при обработке информации внутри банка или оператора, когда данные могут оказаться доступными сотрудникам

2) перехват интернет-трафика между участниками обмена электронными сообщениями о финансовых транзакциях (банками, операторами платежных кошельков, банкоматами, клиентами)

3) невозможность гарантированного определения взаимной подлинности участников транзакций

4) возможность участников транзакции отказаться от авторства поручения на отправку средств или сообщения

5) DDoS-атаки на сетевые сервисы электронной платежной системы

Подзадача 3 (укажите не менее двух вариантов ответов)

Для реализации прямого вывода в экспертной системе магазина компьютерных игр, когда по результатам опроса пользователя по различным параметрам игры определяется наличие желаемых параметров у предлагаемых магазином игр, можно использовать продукционную модель. В продукционной системе знания представляются совокупностью правил вывода вида «ЕСЛИ (условия-посылки), ТО (действия-заключения)». Продукционные порождающие правила являются очень удобной моделью знаний для представления связей между состоянием проблемы и действиями, которые необходимо предпринять для ее решения.
К компонентам продукционных систем относятся …

Варианты ответов:

1) память правил
2) база данных
3) база правил
4) компилятор правил
5) интерпретатор правил

Подзадача 4 (установите правильную последовательность в предложенной совокупности ответов)

Для чтения данных об играх и записи предпочтений в экспертной системе магазина компьютерных игр предложено использовать фреймовую модель представления знаний. Фреймовые модели обеспечивают требования связанности и структурированности за счет свойств наследования и вложенности, которыми обладают фреймы. В качестве фреймов и их экземпляров можно представить базу игр, где для каждой игры должны храниться необходимые данные.
Установите правильную последовательность шагов при построении фреймовой модели представления знаний.

Варианты ответов:

1) определить абстрактные объекты и понятия предметной области
2) добавить фреймы-объекты сценариев и сцен
3) задать конкретные объекты предметной области
4) определить набор возможных ситуаций
5) описать динамику развития ситуаций через набор сцен

Подзадача 5 (укажите не менее двух вариантов ответов)

Файлы информационной системы магазина предполагается хранить в файловой системе NTFS. Как полагают разработчики, эта файловая система удовлетворяет всем требованиям к защите данных, позволяя задать разрешения и запреты различных прав доступа к файлу для каждой группы пользователей и для каждого пользователя.
Относительно защиты данных в системе NTFS истинными являются следующие утверждения …

Варианты ответов:

1) если для пользователя задано разрешение права доступа к файлу, но для одной из его групп задан запрет, то действует запрет

2) набор разрешений для пользователя определяется как дизъюнкция разрешений, заданных для него самого и для всех его групп

3) права доступа, заданные для конкретного пользователя, имеют преимущество над правами доступа групп, к которым он принадлежит

4) право доступа на запись в файл включает также право на чтение этого файла

5) если для пользователя и его групп не задан ни запрет, ни разрешение права доступа к файлу, то это равносильно запрету

ПРИЛОЖЕНИЯ К КЕЙС-ЗАДАНИЮ

Приложение 1k1_Pril1

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

Вопросы безопасности электронных платежных систем являются сложной задачей для финансового сектора и регуляторов. Существуют две серьезные проблемы – несанкционированные списания средств с банковских карт или счетов юридических лиц и общая гарантия сохранности платежей, совершаемых через небанковские системы переводы платежей. Принимаемые в последние годы меры смогли сделать электронные переводы более безопасными.

Как работает ЭПС

Под термином «электронная платежная система» (ЭПС) понимается система расчетов, при которой платежи проводятся по интернет-каналам, традиционной обработки платежных поручений не происходит.

Под это определение попадают:

- расчеты посредством банковских карт традиционных систем Visa, MasterCard, «Мир». Здесь при абсолютной гарантии защиты трансакций возникает проблема несанкционированных списаний в результате перехвата трафика или получения номеров карт;
- программы межбанковских расчетов по электронным каналам связи, в том числе быстрых платежей, осуществляемых банками по номерам телефонов;
- расчеты через электронные кошельки (Яндекс.Деньги и другие);
- расчеты через инфраструктуру мобильных операторов и другие современные решения.

В Банке России организовано несколько моделей платежей по Интернету. Это программа внутрирегиональных расчетов по сети Интернет (ВЭР) и межрегиональных электронных расчетов (МЭР). Для крупных срочных платежей в России в 2007 году создана идеология банковских срочных платежей (БЭСП). Она является аналогом европейской программы RTGS. Подключенные к ней банки переводят друг другу крупные суммы с целью перечисления клиентам в течение одного операционного дня.

Информационная безопасность электронных платежных систем обеспечивается требованиями, предъявляемыми к банкам-участникам:

- наличие корреспондентского счета в ЦБ РФ;
- действующая лицензия на осуществление банковской деятельности;
- отсутствие просроченных долгов перед ЦБ РФ;
- обмен сообщениями по установленному механизму коммуникации с Банком России на основе договора;
- соответствие ИС банка техническим требованиям и требованиям по ИБ кредитных организаций, предъявляемым ЦБ РФ.

Требования формулируются в Положениях Банка России и являются обязательными для исполнения. Отказ от выполнения требований может привести к полному или частичному отключению банка от технологии БЭСП.

Общие принципы ИБ механизмов дистанционных переводов

Если говорить об защите от несанкционированных переводов ЭПС в общем, то вне зависимости от уровня каждой конкретной модели к ним действуют единообразные требования.

Среди наиболее уязвимых мест:

- интернет-трафик между участниками обмена электронными сообщениями о финансовых трансакциях (банками, операторами платежных кошельков, банкоматами, клиентами);
- обработка информации внутри банка или оператора (например, Яндекс.Денег), когда данные могут оказаться доступными сотрудникам;

- постоянная доступность систем платежей для клиентов, отсутствие сбоев в их работе и на линии связи.

Наличие этих уязвимостей вынуждает банки и операторов обеспечивать защиту трафика при пересылке доступными способами (передача по защищенным каналам, шифрование) и разрабатывать модели аутентификации отправителя и получателя средств.

При этом в работе банка или оператора платежей возникают проблемы:

- определение взаимной подлинности участников трансакции при установлении соединения;
- обеспечение конфиденциальности и подлинности платежных поручений, отправляемых по интернету, и других документов;
- защита процесса отправки, формирование доказательств отправления и получения документов;
- обеспечение исполнения документа (например, постоянное нахождение остатка на корреспондентском счете банка, позволяющее организовать платеж).

Банк и оператор ЭПС обязаны реализовать механизмы защиты клиентов от несанкционированных списаний денежных средств, конкретные требования к которым определяются политиками операторов и регламентами ЦБ РФ:

- управление доступом клиента, сотрудников оператора и получателя, создание механизма аутентификации;
- контроль подлинности и целостности информации в сообщении;
- обеспечение конфиденциальности сведений в процессе передачи;
- невозможность отказаться от авторства поручения на отправку средств или сообщения;
- гарантии доступа к ресурсам и неутраты сообщения в пути, его доставки;
- невозможность оператора или банка отказаться от исполнения поручения на перевод или платеж;
- сохранение данных по поручениям и сообщениям.

Для осуществления платежей посредством банковских карт международные системы переводов применяют собственные меры ИБ межкарточных переводов, корреспондирующие с требованиями Банка России. Для иных операторов безбумажных платежей, совершающих более 6 миллионов переводов в год, работает программа сертификации Qualified Security Assessor (QSA).

В России работают представительства нескольких организаций, имеющих право на выдачу сертификата, и он будет предоставлен, если оператор соответствует следующим требованиям:

- его деятельность соответствует международному стандарту Payment Card Industry Data Security Standard (PCI DSS);
- оператор сервиса платежей получил сертификат на соответствие международным требованиям к менеджменту ИБ кредитных организаций в сфере разработки, внедрения и сопровождения программных средств ISO/IEC 27001:2005;
- оператор работает с использованием электронно-цифровой подписи (ЭП);
- шифрование осуществляется разрешенными средствами криптографической защиты, разработанными организациями, имеющими лицензии на право осуществления деятельности по предоставлению, техническому обслуживанию криптографических средств.

Стандарт защиты информации в индустрии платежных карт PCI DSS был разработан международными операторами платежных карт Visa и MasterCard. В него входит 12 детально описанных требований, согласно которым должна обеспечиваться защита платежных систем.

Рекомендации ЦБ РФ

В последние годы ЦБ РФ от рекомендаций организациям финансового сектора по обеспечению защиты денежной системы перешел к непререкаемым требованиям, обязательным для выполнения и сопровождающимся внесением изменений в законы и подзаконные нормативные акты. Теперь информацию о каждой зафиксированной хакерской атаке и о том, что она готовится, он должен получать в течение трех часов.

Сведения необходимо передавать в FinCERT (Центр мониторинга и реагирования на компьютерные атаки в финансовой сфере, подразделение ЦБР). Передаются все данные, связанные с покушением на совершение несанкционированного перевода денежных средств со счетов компаний и физических лиц. Большинство банков и организаций финансового сектора уже подключены к системе горячего реагирования ФинЦЕРТ, если этого не произошло, сведения направляются по e-mail, без гарантии его своевременного прочтения и регистрации. С этим связаны сложности: такое сообщение обязательно должно быть подписано ЭП, но, если киберпреступникам удалось разрушить важный сектор многоэшелонированной защиты банка, удостоверить сообщение ЭЦП окажется сложно.

В стандарте обеспечения информационной безопасности электронных платежных систем ЦБ РФ закрепил несколько обязательных требований:

- компьютер, подключенный к системе, не должен быть доступен из локальной сети банка (п. 5 Постановления ЦБ РФ №672-П);
- компьютер, отправляющий платежи на корреспондентский счет ЦБ РФ на обработку, должен постоянно мониториться с целью выявления несанкционированного вмешательства в программное обеспечение или подключения к сторонним серверам.

Интересно, что регулятор не требует от банка обязательного информирования о DDoS-атаках и других ситуациях, касающихся защиты системы обработки платежей самого финансового учреждения. Но все рекомендации, связанные с защитой от несанкционированных переводов и вмешательством в работу ЭПС любого уровня, как национального, так и международного, должны выполняться неукоснительно. Банки заявили после выхода рекомендаций о глобальном изменении правил игры, ранее они не сообщали о хакерских атаках по двум причинам:

- из страха репутационных рисков;
- из боязни быть оштрафованными за несоблюдение требований ИБ и правил корпоративного поведения.

Сейчас меры воздействия на банки за отказ от соблюдения требований регулятора более жесткие, чем просто штрафы. Одна из них отключение финансовой организации-нарушителя от системы банковских срочных платежей (БЭСП). Размер штрафа, согласно ст. 74 Закона «О Центральном Банке», может составить до 1 % от уставного капитала банка. Например, размер штрафа для такого финансового учреждения, как Сбербанк, может составить 670 миллионов рублей.

Положение 672-П

В рамках регулирования деятельности банков по обеспечению безопасности для клиентов электронных платежных систем Банком России в апреле 2019 года издано Положение № 672-П «О требованиях к защите информации в платежной системе Банка России». Основным посылом сообщения стала обязанность банков к середине 2021 года полностью выполнить требования ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций». Проверка выполнения действий этого и предыдущего Постановления № 552-П происходит во время проведения ежегодных аудиторских проверок и проверок ЦБР, а дополнительной гарантией соблюдения требований становится включение их в качестве обязательств кредитной организации в ее договор с Банком России.

Помимо требований к обеспечению информационной безопасности электронных платежных систем, Стандарт содержит требования по обеспечению защиты данных, пересылаемых в рамках программы передачи финансовых сообщений (СПФС).

Требования ГОСТа касаются защиты двух механизмов отправления платежей:

- сервиса срочного перевода и сервиса несрочного перевода (ССНП);
- сервиса быстрых платежей (СБП).

Сформулированы требования к размещению объектов информационной инфраструктуры при осуществлении переводов денежных средств. Необходимо использовать разные сегменты сети и АРМ для организации формирования электронных сообщений о переводе средств и для контроля реквизитов этих сообщений. Кроме того, нужно следующее:

- обеспечить использование криптографических средств защиты информации высокого уровня;

- двухсторонняя аутентификация информации должна обеспечиваться на уровне требований ГОСТ Р ИСО/МЭК 7498-1-99;
- организовать регистрацию данных обо всех действиях клиентов со своими средствами с целью своевременного информирования Банка России о случаях несанкционированных списаний;
- для обмена информацией с Банком России о совершении платежей необходимо использовать отдельное рабочее место, оборудованное в соответствии с требованиями Стандарта.

Каждый участник системы переводов в целях обеспечения защиты электронных платежных систем обязан принять пакет внутренней организационно-распорядительной документации, описывающий:

- процесс защиты данных при управлении доступом к ним;
- порядок обеспечения физической и программной защиты ИС любого уровня;
- контроль целостности и защищенности инфраструктуры, сети организации, осуществляющей переводы;
- использование антивирусных средств и способов защиты от внедрения вредоносного кода;
- защиту от утечек данных;
- управление инцидентами информационной безопасности;
- защиту среды виртуализации;
- защиту информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств.

Нормы Постановления обязывают банки усилить внимание к собственным пробелам системы защиты, отказаться от самостоятельно разработанного программного обеспечения и перейти на единую системную концепцию безопасности платежей.

Яндекс.Деньги и другие платежные системы

Российские пользователи электронного кошелька Яндекс.Деньги часто интересуются, как именно устроены меры защиты платежей в ней. Платежный сервис использует следующие алгоритмы защиты:

- шифрование передаваемых данных с использованием криптоалгоритма RSA с хэшированием. Шифрование происходит на стороне отправителя средств, длина ключа составляет 1024 бит. Этот же метод шифрования применяют WebMoney и PayPal. Для сравнения, менее известная в России программа E-Port использует шифрование через SSL-протокол версии 3.0., что даже при применении 128-битного ключа оставляет место для уязвимостей;
- заверение трансакций подписью процессингового центра;
- применение сложного механизма аутентификации. Сначала пользователь вводит пароль, затем его подлинность проверяет программа-кошелек, для совершения платежей можно использовать смс-пароли;
- соединение происходит по протоколам HTTPS с использованием защищенного сертификата SSL;
- хранение всей информации организовано на защищенных серверах;
- от записи данные защищаются специальными программными решениями;
- используется программа «Яндекс.Кошелек», повышающая защиту трансакций.

В качестве одного из дополнительных решений введен код протекции, только при знании его получатель может забрать перевод, совершенный через оператора. Это позволяет избежать риска фишинга и отправки платежей неподтвержденным получателям.

Платежные приложения

Отдельным вопросом безопасности электронных платежных систем становится защита платежных приложений, таких как Apple Pay и Samsung Pay. ЦБ РФ, вводя регулирующие правила для иностранных операторов, часто входит в конфликт с уже разработанными и действующими нормами безопасности, чем может затруднить доступ российских граждан к этим ресурсам. Но своевременная реакция профессионального сообщества помогла внести изменения в новые регуляторные требования, и сервисы остались доступными для российских граждан.

Создаваемая система быстрых платежей (СБП), начало действия которой приходится на 28 января 2019 года, позволяющая отправлять деньги по номеру телефона, также имеет свои правила безопасности, утверждаемые регулятором. Для подключения к СБП от кредитных и финансовых организаций требуется:

- установить ПО с максимальной степенью защиты, рекомендуемое регулятором, или доработать собственное ПО в соответствии с требованиями и техническими спецификациями;
- провести тестовые испытания взаимодействия.

Сейчас в СБП уже зарегистрировалось более 30 участников, среди них 10 крупнейших банков страны. За промедление в подключении к СБП Сбербанк был оштрафован на 1 миллион рублей, что стало важным индикатором для других участников рынка. Центробанк предупредил операторов платежей о существовании рисков атаки с целью сбора персональных данных клиентов. В письме, разосланном банкам, сообщается, что основным направлением атаки стал «автоматизированный или ручной процесс сбора информации о клиентах банков – участников СБП. Злоумышленник, используя имеющиеся данные идентификатора клиента (номер его мобильного телефона), теперь может получить дополнительную информацию об этом человеке, например, имя, отчество и первую букву фамилии, а также названия нескольких банков, где у него есть открытые счета». Полученные номера телефонов злоумышленники могут использовать для организации массовых звонков клиентам банков с целью получения паролей от личных кабинетов и других данных.

Центробанк предлагает следующий механизм борьбы с угрозой: Национальная система платежных карт, являющаяся операционно-клиринговым центром СБП, проводит круглосуточный мониторинг операций и блокирует в системе номера подозрительных телефонов, с которых осуществляется массовый перебор. Помимо блокировки номеров ЦБ будет сообщать банкам об IP-адресах, с которых пытался осуществляться массовый перебор.

От принципа работы платежной системы и модели угроз зависят и способы защиты. Реализация рекомендуемых регулятором мер безопасности должна привести к повышению защищенности электронных платежей, снижению количества несанкционированных финансовых трансакций и списаний с банковских карт. Безопасность средств граждан целиком и полностью зависит от готовности банков и операторов выполнять требования регуляторов.