СИСТЕМА КОНТРОЛЯ ДОСТУПА НА ОСНОВЕ БИОМЕТРИЧЕСКИХ ПАРАМЕТРОВ

Шибко А. Л., студент
Русанов В. А., студент,
Голешов В. А., студент
Войтехович А. Д., студентка
Шейна А. Д., студент
Епимашко И. Р., студент

Институт информационных технологий, Белорусский Государственный Университет Информатики и Радиоэлектроники, г. Минск

Abstract. *In the last decades thanks to rapid information technology development the international community entered an era of forming of new information space which is created on the basis of a computerization and network telecommunications. This objective phenomenon of modern reality is followed by increase of volumes of the socially important information used in management systems by organizational systems for the purpose of rationalization of their activity. Level of informatization of management processes became one of the most important indicators of the social and economic progress made by the state and the separate organization. Reliable authorization and authentication become necessary attributes of everyday life*
Keywords: *information technology, biometric lock, software.*

Введение. В последние десятилетия благодаря стремительному развитию информационных технологий мировое сообщество вступило в эпоху формирования нового информационного пространства, которое создается на базе компьютеризации и сетевых телекоммуникаций. Это объективное явление современной действительности сопровождается нарастанием объемов социально значимой информации, используемой в системах управления организационными системами с целью рационализации их деятельности.

Результаты и обсуждение. Уровень информатизации процессов управления стал одним из наиболее важных показателей социально-экономического прогресса, достигнутого государством и отдельной организацией. С качественной стороны увеличение объемов информации, используемой в решении задач управления организациями, приводит к рационализации человеческого труда и росту благосостояния. Информационные технологии используются во множестве сфер деятельности человека, в том числе и в системе управления.

На сегодняшний день биометрия имеет ряд развивающихся направлений, каждое из которых имеет свои предпочтительные технические приложения. В исследованиях по биометрической тематике активное участие принимают десятки научных центров при университетах, ряд правительственных организаций и сотни коммерческих фирм. Сформировался специфический рынок биометрических аппаратных устройств и программных продуктов, а также услуг по поддержке, тестированию и адаптации этих биометрических продуктов. Существующие продукты можно разделить на две ветви.

К первой, следует отнести группу, которая, построена на анализе статических образов личности, данных от рождения и хорошо наблюдаемых окружающими.

Ко второй, относят устройства и программные средства, построенные на анализе динамических образов личности. Динамические образы личности отражают особенности характерных для нее быстрых подсознательных движений в процессе воспроизведения контрольного слова рукописным почерком или в процессе произнесения контрольного слова голосом пользователя.

Надежная авторизация и аутентификация становятся необходимыми атрибутами повседневной жизни: сегодня люди используют их при совершении самых обычных действий, например, при посадке на самолет, проведении финансовых операций или, когда просто забирают ребенка из детского сада. Права авторизации почти всегда принадлежат одному человеку или небольшой группе людей. Верификация личности становится трудной задачей, когда требуется высокая точность, то есть низкая вероятность ошибок. Кроме того, пользователь не должен иметь возможность впоследствии отрицать проведенную им операцию

и одновременно испытывать как можно меньше неудобств при прохождении процедуры аутентификации.

Одним из первых и самых надежных методов идентификации личности является использование рисунка кровеносных сосудов глазного дна. Вены и артерии, снабжающие глаз кровью, хорошо видны при подсветке глазного дна внешним источником света. Процедура идентификации личности сводится к тому, что человек наблюдает сквозь специальный окуляр удаленную световую точку, при этом осуществляется инфракрасная подсветка его глазного дна, и на нем выделяется дерево кровеносных сосудов.

Уникальность рисунка радужной оболочки обусловлена генотипом личности, и существенные отличия радужной оболочки наблюдаются даже у близнецов. Обнаружено, что при ряде заболеваний на радужной оболочке появляются характерные пигментные пятна и изменения цвета. Для ослабления влияния состояния здоровья на результаты идентификации личности в технических системах используются только черно-белые изображения высокого разрешения. Уникальность рисунка радужной оболочки глаза позволяет фирмам выпускать целый класс весьма надежных систем для биометрической идентификации личности. Этот класс систем захватывает видеоизображение глаза на расстоянии 20–30 сантиметров от видеокамеры, осуществляет автоматическое выделение зрачка и радужной оболочки.

Идентификация личности по особенностям геометрии кисти руки Системы идентификации по силуэту кисти руки появились одними из первых. Кожа человека состоит из двух слоев, при этом нижний слой образует множество выступов, в вершине которых имеются отверстия выходных протоков потовых желез. На основной части кожи выступы располагаются хаотично, и они трудно наблюдаемы. На отдельных участках кожи конечностей папилляры строго упорядочены в линии (гребни), образующие уникальные папиллярные узоры.

Одним из перспективных направлений развития технологии биометрической идентификации личности является использование индивидуальных особенностей геометрии лица. Принцип работы устройств этого класса крайне прост: миниатюрная видеокамера вводит изображение лица находящегося перед компьютером человека. Программное обеспечение сравнивает введенный портрет с хранящимся в памяти эталоном. Некоторые системы дополнительно осуществляют архивирование вводимых изображений для возможного в будущем разбора конфликтных ситуаций.

Для двухмерных систем изготовление муляжа-фотографии не является сложной технической проблемой. Существенные технические трудности при изготовлении муляжа возникают при использовании трехмерных биометрических систем, способных по перепадам яркости отраженного света восстанавливать трехмерную геометрию лица. Такие системы способны компенсировать неопределенность расположения источника освещенности по отношению к идентифицируемому лицу, а также неопределенность положения лица по отношению к видеокамере. Обмануть этот класс систем можно только объемной маской, точно воспроизводящей трехмерную геометрию лица оригинала.

На рисунке ниже представлены примеры отличительных индивидуальных характеристик.

Рис. 1. Отличительные индивидуальные характеристики: физиологические (отпечаток пальца) и поведенческие (подпись)

В биометрии различают два аутентификационных метода:

1) Верификация, основанная на биометрическом параметре и на уникальном идентификаторе, который выделяет конкретного человека (например, идентификационный номер), то есть этот метод основан на комбинации аутентификационных приемов.

2) Идентификация, в отличие то верификации, основана только на биометрических измерениях. При этом измеренные параметры сравниваются со всеми записями из базы зарегистрированных пользователей, а не с одной из них, выбранной на основании какого-то идентификатора.

Биометрическая идентификация может рассматриваться как «чистая» биометрическая аутентификация, но ее гораздо сложнее применять из-за сложности поиска в биометрической базе данных: каждый из биометрических образцов должен быть сопоставлен каждой записью из базы данных. Такая система требует высокой эффективности при сопоставлении огромного количества биометрических репрезентаций и нахождении нужного параметра. Верификационные системы, с другой стороны, совершают только одно или несколько сопоставлений 1:1.

Рис. 2. Три основных способа подтверждения личности человека

Единая биометрическая система (ЕБС) — цифровая платформа, разработанная компанией "Ростелеком" по инициативе Министерства связи и массовых коммуникаций РФ и Центрального Банка РФ, идентификации по голосу и изображению лица.

Рис. 3. Единая биометрическая система

Традиционные методы аутентификации требуют от пользователя определенных временных затрат, они не всегда удобны и небезопасны. Несмотря на все усилия разработчиков, подавляющее большинство современных технологий подвержено взломам, подмене данных и фальсификации. Биометрия — более простой с точки зрения пользователей способ аутентификации. Не нужно запоминать пароли или носить с собой некие устройства, а также решать проблемы с безопасным хранением, регулярной сменой и восстановлением идентификационных данных в случае утери или компрометации. С другой стороны, биометрия — наиболее дорогостоящий и сложный в реализации метод аутентификации.

Разработанное приложение, удовлетворяет следующим требованиям:

– модуль аутентификации, который позволяет реализовать процедуру безопасного входа для систем и приборов, таких как смартфоны, компьютеры, дома, автомобили и т.д.;

– разработать распределенную сеть аутентификации, построенную на базе блокчейна и предоставляющую надежную безопасную аутентификацию зарегистрированных в сети пользователей в любой точке мира. Она станет глобальной базой данных для аутентификации самых разных сервисов и может играть роль универсального идентификатора там, где необходимо подтверждение личности;

– внешним накопителем будет являться — жесткий диск с биометрической идентификацией и аутентификаций, который обеспечивает безопасное хранение данных, извлечение которых возможно только в присутствии пользователя, владеющего данными.

К любой разработке прилагается полный пакет документации, который включает в себя описание системы, руководства пользователей и алгоритмы работы. При разработке программного средства необходимо понимать процесс взаимодействия пользователей с системой. Для упрощения понимания процесса работы программного средства разработан алгоритм работы, который изображен на рисунке 4.

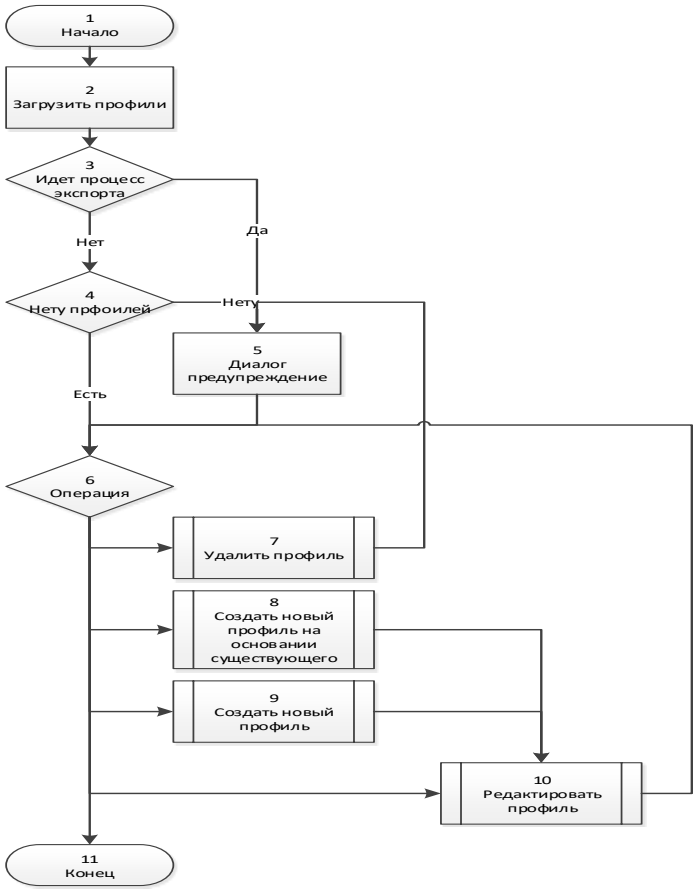

Рис. 4. Алгоритм работы

Язык, используемый для разработки - Xamarin — это фреймворк для кроссплатформенной разработки мобильных приложений (iOS, Android, Windows Phone) с использованием языка C#. Фреймворк состоит из нескольких основных частей:

– Xamarin.IOS — библиотека классов для C#, предоставляющая разработчику доступ к iOS SDK;

– Xamarin.Android — библиотека классов для C#, предоставляющая разработчику доступ к Android SDK;

– Компиляторы для iOS и Android;

– IDE Xamarin Studio;

– Плагин для Visual Studio.

Xamarin уникален тем, что он сочетает в себе все возможности родных платформ и добавляет ряд собственных мощных функций, в том числе:

1. Полное связывание для базовых SDK - Xamarin содержит привязки для почти всех базовых платформ SDK как в iOS, так и в Android. Кроме того, эти привязки строго типизированы, что означает, что их легко ориентировать и использовать, а также обеспечить надежную проверку типа компиляции и во время разработки. Это приводит к уменьшению количества ошибок во время выполнения и приложений более высокого качества.

2. Objective-C, Java, C и C ++ Interop - Xamarin предоставляет средства для непосредственного вызова библиотек Objective-C, Java, C и C ++, что дает вам возможность использовать широкий набор стороннего кода, который уже создан. Это позволяет использовать существующие библиотеки iOS и Android, написанные на Objective-C, Java или C / C ++. Кроме того, Xamarin предлагает связывание проектов, которые позволяют легко связывать собственные библиотеки Objective-C и Java с использованием декларативного синтаксиса.

3. Современные языковые конструкции - приложения Xamarin написаны на современном языке C #, который включает в себя значительные улучшения по сравнению с Objective-C и Java, такие как *динамические языковые функции*, *функциональные конструкции,* такие как *Lambdas, LINQ*, функции *параллельного программирования*, сложные *Generics* и многое другое.

4. Удивительная библиотека базового класса (BCL) - приложения Xamarin используют .NET BCL, массивную коллекцию классов, которые имеют исчерпывающие и упрощенные функции, такие как мощная поддержка XML, базы данных, Serialization, IO, String и Networking, просто для того, чтобы назвать несколько. Кроме того, существующий код C # может быть скомпилирован для использования в приложениях, который обеспечивает доступ к тысячам и тысячам библиотек, которые позволят вам делать то, что еще не описано в BCL.

5. Современная интегрированная среда разработки (IDE) - Xamarin использует Visual Studio для Mac в Mac OS X и Visual Studio в Windows. Это и современные IDE, которые включают такие функции, как автоматическое завершение кода, сложная система управления проектами и решениями, обширная библиотека шаблонов проектов, интегрированный источник управления и многие другие.

6. Поддержка мобильной кросс-платформы - Xamarin предлагает сложную кросс-платформенную поддержку для трех основных мобильных платформ iOS, Android и Windows Phone. Приложения могут быть написаны для совместного использования до 90% их кода, библиотека Xamarin. Mobile предлагает унифицированный API для доступа к общим ресурсам на всех трех платформах. Это значительно сокращает затраты на разработку и время выхода на рынок для мобильных разработчиков, ориентированных на три самых популярных мобильных платформы.

Для асинхронной разработки Xamarin предоставляет возможность использовать как классы из пространства имен System.Threading.Thread и System.Threading.ThreadPool, так и полный спектр возможностей, предоставляемых Task Parallel Library. Если разбивать приложение на слои, то получается такая схема:

– Data Layer (DL) – Хранилище данных, например, база SqlLite или xml-файлы;

– Data Access Layer (DAL) – Обертка над хранилищем для осуществления CRUD-операций;

– Business Layer (BL) – Слой, содержащий бизнес-логику приложения;

– Service Access Layer (SAL) – Слой, отвечающий за взаимодействие с удаленными сервисами (Rest, Json, WCF);

– Application Layer (AL) – Слой, содержащий платформозависимый код, другими словами, это код, который зависит от библиотек monotouch.dll или monodroid.dll;

– User Interface Layer (UI) – Слой пользовательского интерфейса.

Кроссплатформенными являются все слои, расположенные выше Application Layer. Доля переносимого кода достаточно сильно зависит от самого приложения, но, на мой взгляд, она вряд ли может превысить 50-60%. Инженеры Xamarin это понимают, поэтому стремятся к увеличению этой доли. В качестве достижений в решении этой проблемы можно рассматривать библиотеку Xamarin.Mobile. Она предоставляет единый для различных платформ API для работы с камерой, контактами и гео-локацией. Но использование этой библиотеки никак не ограничивает вас в применении платформозависимого API, например, с помощью механизма делегатов.

В iOS компилятор Xamarin's Ahead-of-Time (AOT) компилирует Xamarin.iOS-приложения непосредственно на собственный код сборки ARM. На Android компилятор Xamarin компилируется до промежуточного языка (IL), который затем «Just-in-Time» (JIT) скомпилирован в собственную сборку при запуске приложения.

Функциональное моделирование является важнейшим элементом концептуального анализа, который выполняется на начальном этапе проектирования любого ПС. Разработка и анализ функциональной модели позволяет достаточно глубоко погрузиться в предметную область, выявить функции, которые должно выполнять ПС и определить связи и взаимодействия между ними.

Наиболее подходящей методологией является IDEF0. Функциональная модель разрабатывается как некоторый набор диаграмм, текстов и глоссария.

Первая диаграмма называемая верхней или контекстной (TOP) – диаграммой, имеет только один прямоугольник Activity, который символизирует работу системы в целом. Все связи на этой диаграмме являются связями моделируемой системы со средой функционирования. Каждая Activity, начиная с Activity TOP диаграммы, может быть декомпозирована на субфункции, представляемые несколькими Activities.

Контекстная диаграмма, представленная на рисунках 5 и 6, дает общее описание системы и факторы влияющее на нее. После создания контекстной диаграммы начинается ее декомпозиция.

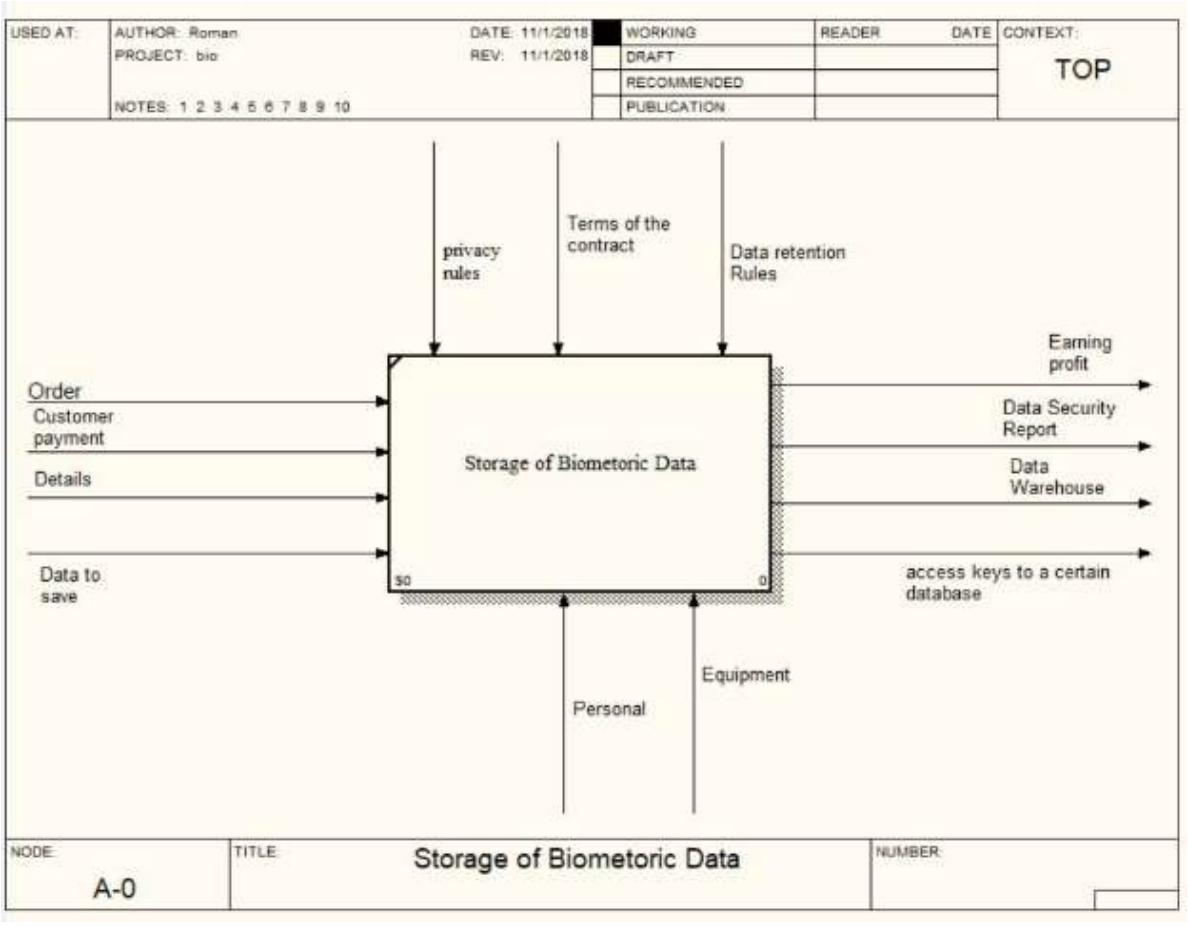

Рис. 5. Контекстная диаграмма

Данная контекстная диаграмма описывает бизнес-процесс IP-телефонии, механизмами которого являются Администратор и Пользователь, а элементами управления – Законодательство, Уставные документы и Внутренние распоряжения.

Бизнес-процесс имеет следующие входные данные:

- Авторизация;
- Информация о пользователях;
- Биометрические данные.

На выходе бизнес-процесса будут следующие ресурсы:
- Отчеты;
- Измененная БД;
- Статистическая информация.

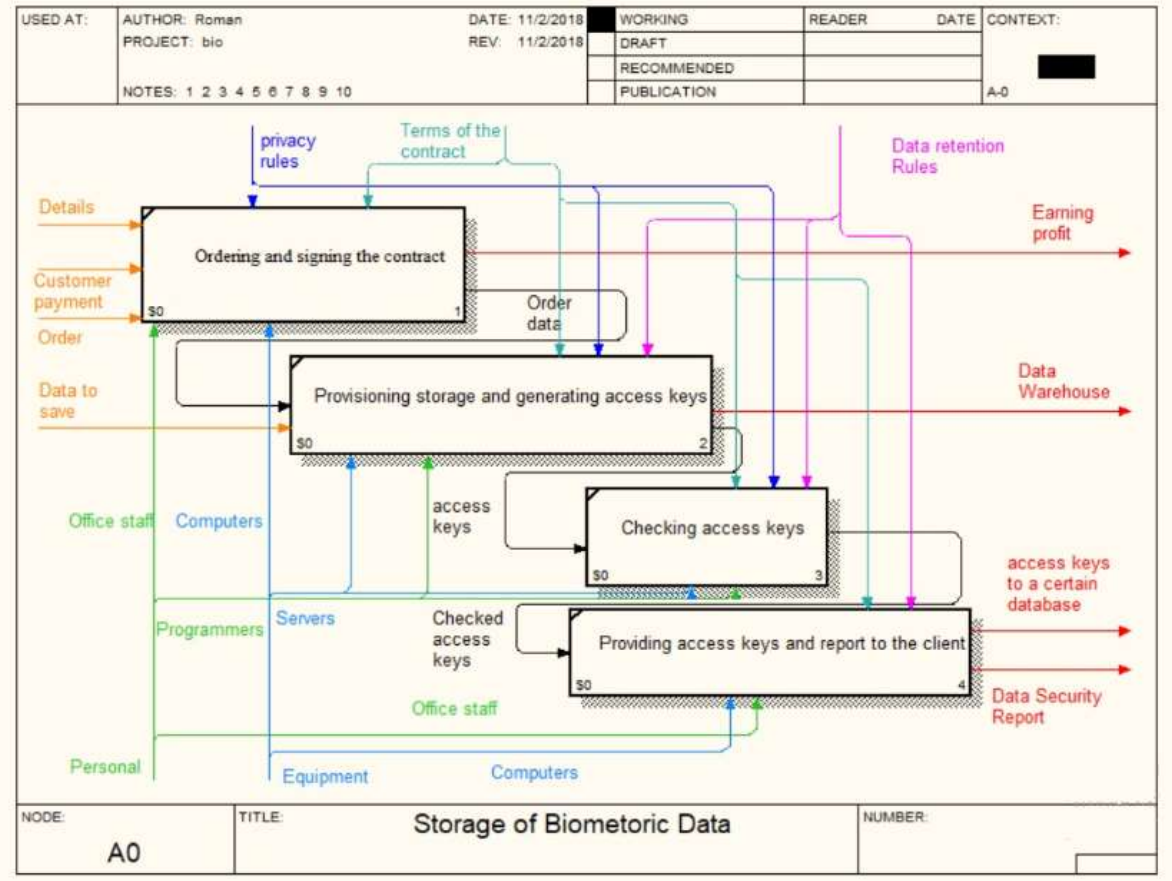

Рис. 6. Декомпозиция

Декомпозиция первого уровня описывает основные возможности механизмов Системы и Администратора. Где изначально происходит вход в систему, затем идентификация (в подсистеме определяется верность введенных идентификационных данных – логин и пароль). Далее Администратор, получив права имеет возможность влиять на изменения БД и отправлять измененную БД на обработку запросов и сохранение изменений Системой. После выполненных этапов существует возможность вывода отчетов и отображения обновленной информации.

Физическое проектирование базы данных – процесс подготовки описания реализации базы данных на вторичных запоминающих устройствах; на этом этапе рассматриваются основные отношения, организация файлов и индексов, предназначенных для обеспечения эффективного доступа к данным, а также все связанные с этим ограничения целостности и средства защиты [11].

Физическое проектирование является третьим и последним этапом создания проекта базы данных, при выполнении которого проектировщик принимает решения о способах реализации разрабатываемой базы данных. Во время предыдущего этапа проектирования была определена логическая структура базы данных (которая описывает отношения и ограничения в рассматриваемой прикладной области). Хотя эта структура не зависит от конкретной целевой СУБД, она создается с учетом выбранной модели хранения данных. Однако, приступая к физическому проектированию базы данных, прежде всего необходимо выбрать конкретную целевую СУБД. Поэтому физическое проектирование неразрывно связано с конкретной СУБД.

Между логическим и физическим проектированием существует постоянная обратная связь, так как решения, принимаемые на этапе физического проектирования с целью повышения производительности системы, способны повлиять на структуру логической модели данных.

Как правило, основной целью физического проектирования базы данных является описание способа физической реализации логического проекта базы данных.

В IT индустрии, нельзя игнорировать веб-угрозы и связанные с ними методы защиты. Количество уязвимостей, обнаруживаемых в веб-приложениях, намного больше, нежели количество уязвимостей, обнаруживаемых на сетевом уровне.

Угрозы, по значимости, расположились следующим образом:

1. внедрение кода (Injection);
2. межсайтовый скриптинг (Cross-Site Scripting);
3. ошибки аутентификации и управления сеансами (Broken Authentication and Session Management);
4. небезопасные прямые ссылки на объекты (Insecure Direct Object References);
5. межсайтовая подделка запросов (Cross-Site Request Forgery);
6. неправильная конфигурация окружения (Security Misconfiguration);
7. небезопасное хранение данных (Insecure Cryptographic Storage);
8. ошибки разграничения доступа (Failure to Restrict URL Access);
9. недостаточная защита транспортного уровня (Insufficient Transport Layer Protection);
10. непроверенные перенаправления (Unvalidated Redirects and Forwards).

Injection. Дефекты внедрения кода, такие как SQL, OS и LDAP, имеют место, когда неподтвержденные данные посылаются в интерпретатор в виде части команды или запроса. Злонамеренные данные атакующего могут обмануть интерпретатор и заставить его выполнить непреднамеренные команды, либо получить несанкционированный доступ к данным.

Cross-Site Scripting (XSS). Уязвимости данного типа имеют место, когда приложение берет неподтвержденные данные и отправляет их веб-браузеру пользователя без надлежащей проверки и экранирования. XSS позволяет атакующему выполнять сценарии в браузере жертвы, что может привести к краже сеансов пользователя, стиранию веб-сайтов, либо перенаправлению пользователя на вредоносные сайты.

Broken Authentication and Session Management. Функции приложения, связанные с аутентификацией и управлением сеансами, часто реализуются не верно, позволяя атакующему поставить под угрозу секретные данные (пароли, ключи, маркеры сеанса), либо использовать различные дефекты реализации, чтобы украсть другие идентификационные данные пользователя. Примерами могут служить незашифрованная или не хешированная передача данных аутентификации, идентификатор сессии как часть URL, неопределенное время жизни для сессии и др.

Insecure Direct Object References. Небезопасный прямой доступ к объекту становится возможным, когда разработчик предоставляет ссылку на объект внутренней реализации, такой как файл, каталог, или ключ к базе данных. Без надлежащего контроля доступа или другой защиты атакующий может манипулировать этими ссылками, чтобы получить несанкционированный доступ к данным.

Cross-Site Request Forgery (CSRF). Данная атака вынуждает браузер зарегистрированного на сайте пользователя отправить поддельный HTTP запрос, который будет включать сеансовые cookie и любую другую аутентификационную информацию, к уязвимому веб-приложению. В результате атакующий получает возможность заставить браузер жертвы генерировать произвольные запросы, в то время как уязвимое приложение будет думать, что получает легальные запросы от жертвы.

Security Misconfiguration. Хорошая система безопасности требует определения и развертывания безопасной конфигурации для приложения, фреймворков, веб-сервера, сервера баз данных, а также самой платформы. Все эти настройки должны быть определены, реализованы и поддерживаемы, поскольку для многих из них безопасные значения не выставлены по умолчанию. Процесс конфигурации также включает в себя обновление всего программного обеспечения, включая все библиотеки, используемые приложением.

Insecure Cryptographic Storage. Множество веб-приложений должным образом не защищают уязвимые данные, такие как номера кредитных карт или учетные данные аутентификации, путем шифрования или хеширования. В результате чего атакующий может украсть, либо изменить слабо защищенные данные.

Failure to Restrict URL Access. Многие веб-приложения идентифицируют права доступа к определенной странице прежде, чем сгенерировать защищенные ссылки на нее. Однако этого не достаточно и приложения должны выполнить подобные проверки доступа каждый раз, когда

происходит обращение к таким страницам. Если же проверки не будут осуществляться, то атакующий, в конце концов, сможет подделать URL и получить доступ к таким страницам, в обход механизма аутентификации.

Insufficient Transport Layer Protection. Приложениям часто не удается аутентифицировать, зашифровать и защитить конфиденциальность и целостность чувствительного сетевого трафика. Это происходит потому, что когда они пытаются использовать механизмы защиты, то иногда поддерживают слабые алгоритмы, используют истекшие или неправильные сертификаты, либо используют то и другое некорректно.

Unvalidated Redirects and Forwards. Веб-приложения часто перенаправляют пользователей на другие страницы или веб-сайты, используя неподтвержденные данные для определения целевых страницы. Без надлежащей проверки таких данных, атакующий может перенаправить жертву на фишинговый («выуживающий» сайт-мошенник) или вредоносный сайт, а также получить несанкционированный доступ к защищенным страницам сайта.

Remote File Inclusion (RFI). Удаленное включение файла имеет место, когда расположенный на стороннем сервере файл, обычно оболочка, подключается к веб-сайту, что позволяет атакующему выполнять команды на стороне сервера как авторизованному пользователю и получить доступ к файлам. Имея доступ к серверу, злоумышленник может эксплуатировать локальные уязвимости для того, чтобы повысить свои привилегии и захватить контроль над системой. Данная уязвимость в основном характерна для сайтов, разработанных на PHP.

Http Request Smuggling (HRS). Так называемая контрабанда HTTP запросов основывается на различиях в обработке данных одного или нескольких HTTP устройств (кэш сервер, прокси-сервер, брандмауэр и т. п.) находящихся между пользователем и веб-сервером. Техника позволяет провести различные виды атак, такие как: отравление кэша, похищение сессии, межсайтовый скриптинг. Также, что особенно важно, она предоставляет возможность обойти защиту брандмауэра. Для этого посылаются специально сконструированные HTTP запросы, которые заставляют два атакованных устройства видеть различные наборы запросов, позволяя атакующему инкогнито отправить запрос одному из устройств, причем другое устройство не будет об этом ничего знать.

Приложения могут ненамеренно выдать информацию о своих внутренних механизмах работы, конфигурации или конфиденциальные данные через множество некорректно обрабатываемых ситуаций. Внутреннее состояние приложения можно вычислить, анализируя время, потраченное на обработку определенных операций, или через ответы на запросы, такие, как простое отображение сообщения или кода ошибки. Веб-приложения также часто выдают информацию о своем внутреннем состоянии через отладочные сообщения об ошибках. Часто, эта информация может усилить или даже автоматизировать более мощную атаку.

Несмотря на многообразие уязвимостей, существует ряд простых рекомендаций, позволяющих уменьшить риск проведения успешной атаки еще на этапе разработки:

- никогда не доверять и всегда проверять любые данные, приходящие от браузера;
- по возможности проверять пришли ли данные пользовательской формы от того пользователя, для которого форма была создана;
- хранить чувствительные данные в зашифрованном либо хешированном виде;
- правильно управлять сеансами пользователей;
- конфигурировать сервер наилучшим возможным способом (останавливать ненужные службы, закрывать неиспользуемые порты, правильно настраивать права доступа на файлы и папки, использовать SSH для удаленного доступа к серверу и т. д.).

Кроме того, никогда не стоит пренебрегать как обычным тестированием приложения на этапе разработки, так и тестированием на возможность проникновение для готового продукта.

Программа может функционировать как отдельный самостоятельный продукт, при этом для работы понадобится персональный компьютер, удовлетворяющий следующим минимальным требованиям:

- процессор с тактовой частотой не менее 1000 Гц;
- оперативная память RAM 256 Мбайта;
- объём внешней памяти 25 Мбайт (без учёта заполнения базы данных);
- свободное место на винчестере: 15Мб;
- манипулятор типа мышь, клавиатура;
- монитор с поддержкой качества цветопередачи в 16 тыс. цветов.

Архитектура вычислительной инфраструктуры онлайн-платформы должна обеспечивать отказоустойчивость и сохранение штатного режима работы при выходе из строя одного узла каждой подсистемы. Нагрузка вышедших из строя узлов должна автоматически распределяться между оставшимися узлами, при этом возможна деградация производительности.

Должны быть использованы основные способы повышения надежности:

– Резервирование программно-технических средств и наличие аппаратной, информационной, функциональной и алгоритмической избыточности, обеспечивающей работоспособность деградированных систем при единичных отказах без остановки оборудования.

– Защита от ложных команд и использования недостоверной информации.

– Защита данных, программного обеспечения и технических средств от несанкционированного вмешательства.

– Защита конфигурационных данных посредством резервного копирования конфигурационных файлов и базы данных конфигурации.

Вычислительная инфраструктура онлайн-платформа должна сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих внештатных ситуаций:

– при сбоях в системе электроснабжения аппаратной части, приводящих к перезагрузке операционной системы, восстановление должно происходить после перезапуска операционной системы и запуска соответствующего исполняемого файла;

– при ошибках в работе аппаратных средств (кроме носителей данных и программ) восстановление функции системы возлагается на операционную систему;

– при ошибках, связанных с программным обеспечением (операционная система и драйверы устройств), восстановление работоспособности возлагается на операционную систему.

Вычислительная инфраструктура должна поддерживать до 1000 одновременно работающих пользователей. Количественные характеристики производительности (число транзакций баз данных, скорость передачи файлов, число обращений к веб-серверу и т.д.) должны быть определены на этапе обследования и формализации архитектуры.

Платформа должна обеспечить выполнение следующих технологических функций:

– Балансировку нагрузки и распределение пользовательских запросов между веб-серверами

– Обеспечение отказоустойчивости и возможности обслуживания оборудования без простоя и без снижения функциональности

– Обеспечение управления контейнерами программного обеспечения:

- запуск контейнеризированных приложений;
- автоматическая поддержка запуска нескольких экземпляров контейнеризированных приложений;
- автоматический Перезапуск контейнеризированных приложений в случае отказа оборудования;
- автоматический процесс обновления контейнеризированных приложений без простоя.

Разрабатываемое приложение имеет понятный и удобный в использовании интерфейс, для взаимодействия между программой и пользователем.

ЛИТЕРАТУРА

1 Жуков Ю.М. Диагностика и развитие компетентности в общении, спецпрактикум по социальной психологии / Ю.М. Жуков. – М., 1990. – 256 с.

2 Жуков Ю.М. Идеология и практика тренинга. Событийная основа опыта // Методы практической социальной психологии: Диагностика. Консультирование. Тренинг: Учеб. Пособие для вузов / Ю.М. Жуков, А.К. Ерофеев, С.А. Липатов [и др.]. – М.: Аспект-пресс, 2004. – С. 97–124.

3 Лайл М. Спенсер-мл., Сайн М. Спенсер. Компетенции на работе / Лайл М. Спенсер-мл., Сайн М. Спенсер; Пер. с англ. – М: HIPPO, 2005.

4 О.Н. Образцова, О.М. Бакунова, Д.М. Кугач, А.В. Хомяков Практико-ориентированное обучение в сфере информационных технологий в БГУИР и сотрудничество вуза с ведущими компаниями IT // Проблемы современного образования: материалы VIII международной научной конференции, 10-11 сентября 2017. – Прага: Vědecko vydavatelské centrum «Sociosféra-CZ», 2017 - С.38-41

5 Бакунов А.М., Бакунова О.М., Калитеня И.Л., Образцова О.Н. Профориентация как предпосылка выбора профиля обучения // Непрерывная система образования "школа-университет". Инновации и

перспективы: сборник статей Международной научно-практической конференции (23-24 февраля 2017 г.) - Минск: БНТУ, 2017. - С. 35-37.

6 Бакунов А.М., Бакунова О.М., Калитеня И.Л., Образцова О.Н. Применение ИКТ в образовательном процессе специальности «Программное обеспечение информационных технологий» специализации «Программное обеспечение обработки экономической и деловой информации» / Подготовка специалиста-профессионала в различных видах деятельности : [электронный ресурс] : материалы Республиканской научно-практической конференции с международным участием, Гомель, 23-24 ноября 2017 г. - Гомель : Гомельский областной институт развития образования, 2017. - С. 43 - 46.

7 О. М. Бакунова, О. Н. Образцова, Силинский, Р. А. Дистанционные технологии как способ оптимизации трудовых процессов инженеров испытательной лаборатории / // Дистанционное обучение – образовательная среда XXI века: материалы X международной научно-методической конференции (Минск, 7 - 8 декабря 2017 года). – Минск: БГУИР, 2017. – С. 286.

8 Бакунова О. М., Калитеня И. Л., Бакунов А. М., Малиновская Т.И. Применение ИКТ для оказания образовательных услуг лицам с особыми потребностями на примере изучения системы 1С дистанционно // Непрерывное профессиональное образование лиц с особыми потребностями: сборник статей международной науч.- практической конференции (Минск, 14 - 15 декабря 2017 года). – Минск: БГУИР, 2017. – С. 41 – 43.

9 Бакунова О. М., Калитеня И. Л., Бакунов А. М., Антонов Е. Д., Мелешкевич Д.В. Информационные компьютерные сети и системы в сфере образования // Непрерывное профессиональное образование лиц с особыми потребностями: сборник статей международной науч.- практической конференции (Минск, 14 - 15 декабря 2017 года). – Минск: БГУИР, 2017. – С. 39 – 41.

10 Бакунова О. М., Калитеня И. Л., Бакунов А. М., Нарижный, Е. Ю., Образцова О.Н. Внедрение мобильного по в качестве методического пособия для обучения лиц с особыми потребностями // Непрерывное профессиональное образование лиц с особыми потребностями: сборник статей международной науч.- практической конференции (Минск, 14 - 15 декабря 2017 года). – Минск: БГУИР, 2017. – С. 38 – 39.

11 Бакунова О. М., Калитеня И. Л., Бакунов А. М., Палуйко А. Ф., Антонов Е. Д., Гречко И. С. Использование нейронных сетей в образовании. INTERNATIONAL ACADEMY JOURNAL Web of Scholar 1(19), Vol.1, - Warsaw, Poland, 2018 С. 8 – 11

12 Бакунова О. М., Хмелевская А.Л., Беликов А. С., Мирончик А. Н., Агапкин Л.М., Чучвал А.Ю. Использование современных подходов и нейронных сетей для качественного образования в ВУЗах // I Международный симпозиум "Гуманитарные и общественные науки в Европе: достижения и перспективы"– Вена, Австрия 2018 г