О программно-технологических аспектах авторизации пользователей, процессов и данных в КС "Сайт" при формировании сводных сведений из распределенных данных

Ляхов Вячеслав Владимирович	- главный технолог ООО «Крымское аэрокосмическое агентство»
Егоров Федор Иванович	- Председатель Государственной службы специальной связи и защиты информации Украины в г. Севастополе, полковник Госспецсвязи
Прималенный Александр Алексеевич	- Председатель СО УкрЮНЕПКОМ, председатель ООО «Крымское аэрокосмическое агентство», кандидат географических наук

Рассматриваются программно-технологические аспекты авторизации пользователей, процессов и данных при формировании сведений из единой базы данных для сайтов вида АС-3 как узлов с различной политикой безопасности при взаимодействии с «открытым информационным обществом».

Ключевые слова: защита информации, авторизация, пользователи, процессы, данные,

Использование современных достижений информационно-коммуникационных технологий (ИКТ) в повседневной жизни становится привычным явлением. Как правило, степень такого использования, в основном, ограничивается финансовыми возможностями заинтересованной стороны: чем состоятельнее клиент, тем более высокие требования им предъявляются к составу приобретаемых аппаратно-программных средств и ИКТ.

Но, зачастую, даже в тех случаях, когда финансовые затраты на приобретение технических средств и информационных технологий потребителю «не кажутся обременительными», вопрос о затратах на защиту информации ставится в последнюю очередь или вообще не считается актуальным. В том числе, «ради экономии средств на другие более полезные нужды», поскольку в среде «компьютерных потребителей электронной информации» «открытого общества» бытует расхожее мнение, что защите должна подлежать информация, имеющая гриф ограничения доступа. Во всех остальных случаях панацеей от неприятностей с «открытой информацией» считается антивирусная программа.

Но разве обычным гражданам, владеющим информацией «о самих себе» в «электронном виде» безразлично, что третьи лица могут собирать эту информацию в каких-то собственных корыстных целях? Ведь это «не бумажный документ», который можно закрыть в сейфе? Или может им быть безразличным, если информация о состоянии их здоровье и собственности обращается в организациях и учреждениях без должной защиты в этих предприятиях от третьих лиц? Разве мало уже несчастий случилось с собственниками земельных участков, домов, квартир, машин, владельцев банковских счетов, получателей кредитов в банках и инвесторов? Поэтому, следуя примеру государства, для физических лиц и организаций не менее полезно владеть хотя бы базовыми знаниями о возможности исключения данной проблемы. А пример здесь весьма поучителен: государство даже для «открытой» информации, ему принадлежащей, «закрывает ее электронную версию» от несанкционированного доступа к ней с целью исключения злоумышленных действий по ее искажению, разрушению или ограничению к ней доступа. Ведь разве утрата собственной и о себе информации не влечет за собой экономических проблем? Да и только ли экономических когда через подмену документов владелец «электронных данных» может лишиться и собственности, жизни, и здоровья?

Культура же восприятия такого явления как «ограничение доступа к информации» никак не достигнет у населения и бизнеса представления «себя самих» как инициаторов данного процесса, для чего существуют вполне доступные нормативные рекомендации.

В качестве стандартной модели безопасности обычно приводят модель из трёх категорий:

- *конфиденциальность* - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

- *целостность* - избежание несанкционированной модификации информации;
- *доступность* - избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Выделяют и другие, не всегда обязательные, категории модели безопасности:

- *апеллируемость* - невозможность отказа от авторства;
- *подотчётность* - обеспечение идентификации субъекта доступа и регистрации его действий;
- *достоверность* - свойство соответствия предусмотренному поведению или результату;
- *подлинность* - свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Одним из факторов, «положительно» влияющих «в пользу решения» вопросов защиты информации, является проведение оценки ущерба от утери, огласки, модификации и т.п. информации (в целом связанное с изменением свойств информации) собственника или лица, имеющего прямое или косвенное отношение к ней. Оценка вероятности событий (рассматриваемых при оценке), наглядность величины потерь, величина наказания виновных, сумма затрат на защиту информации – все это вместе дает «реальную картину» для принятия решений по защите информации.

Другой важной стороной для пользователей «открытого общества» в принятии решения об организации защиты собственной информации, является статья 32 Конституции Украины. Суть статьи в том, что человек может собирать информацию только «о себе» как его собственности (ведь информация тоже обладает признаком собственности), поэтому «ознакомление» с ней «третьих лиц» может осуществляться только с его согласия и/или в рамках действующего законодательства.

Особенно актуальной данная проблема становится в условиях применение WEB-технологий в виде создания сайтов, где их собственники неизбежно сталкиваются с атаками на их информацию. Не касаясь, опять же, проблем пользователей «открытого общества», для государственных учреждений, например, нарушение целостности или доступности «открытой» информации на сайте является серьезной проблемой, так как это нарушает законное право граждан на ознакомление с информацией данных учреждений в установленном порядке.

Таким образом, вопрос безопасности информации при использовании современных информационно-коммуникационных технологий является очень актуальным как с позиции защиты электронно-вычислительной техники (ПЭВМ), так и в применении адаптированного к проблемной области защиты информации путем программного обеспечения.

Не касаясь вопросов защиты ПЭВМ техническими средствами, что в различных случаях может реализовываться их различной конфигурацией, есть смысл рассмотреть общий для всех ситуаций программный подход.

Таким образом, решение вопросов безопасности информации можно разделить на две группы:

- Первая - защита извне (техническими средствами, организационными мероприятиями и т.п.).
- Вторая - защита «изнутри» (структура организации хранения и применения информации является составной частью технологии работы с ней).

Как сказано выше, вторая группа представляет большой интерес, поскольку позволяет защитить информацию на более «глубоком уровне», что увеличивает гарантии безопасности. Защита изнутри основана на том, что она рассматривается как составная и неотъемлемая часть технологического процесса от момента «рождения» до момента «уничтожения».

При этом процесс защиты здесь получает возможность многоуровневой организации путем его разделения на эшелоны:

1. Декомпозиция исходных данных.
2. Назначение атрибутов объектов, субъектов и процессов и их значений.
3. Персонификация текущих процессов.
4. Синтез текущих сведений.
5. Персонификация текущих субъектов.
6. Конвертация текущих синтезированных сведений в формат, используемый субъектом.
7. Передача информации между объектом и субъектом.
8. Получение информации субъектом.

Вкратце, данная возможность эшелонирования возникает из того факта, что информация - это процесс (передачи сведений). Таким образом, и защита в данном аспекте выражается характерными особенностями. Первоначально данный процесс начинается со сбора исходных данных. Исходные данные существуют, как правило, в виде составных данных, часть которых «не представляет интерес» для формирования исходных баз данных. Например, справочники адресов проживания, телефонный справочник и т.п. содержат данные (ПОЛЯ данных) о ФАМИЛИИ в комбинации с другими ПОЛЯМИ. В этом случае формирование данных в виде отдельного списка ПОЛЕЙ возможных вариантов ФАМИЛИЙ, является декомпозицией исходных данных.

Таким образом:

Первый эшелон защиты информации – это декомпозиция исходных данных. Суть этого процесса – получить единичные значения, и реализуется это в виде формы – справочника. Например, справочники: "ФАМИЛИИ", "Названия улиц", "Названия предприятий" и т.д. Такое разделение обеспечивает накопление данных не являющихся "закрытыми", а сам процесс накопления обеспечивает формирование "уникальных" данных (не повторяющихся в пределах справочника), что позволяет иметь "эталонные значения" для дальнейшего контроля целостности информации формируемой из накопленных данных.

Второй эшелон защиты, это назначение атрибутов ПРАВА допуска, доступа, статуса для собранных данных. При этом важным фактором является то, что данные собирались с целью их дальнейшего использования, как объектов, конечными пользователями – субъектами, путем инициализации различных процессов взаимодействующих с данными. Поэтому процессы, взаимодействующие с объектами (данными), также должны иметь атрибуты, определяющие их ПРАВА допуска и доступа.

Допуск – разрешение пользователю на доступ к информации определенной в рамках законодательства категорией конфиденциальности.

Доступ - разрешение пользователю на работу с конкретной по характеристике сведений информацией согласно его допуску и полномочиям по решению собственника (руководителя) информационного объекта.

Статус - правовое положение пользователя относительно доступа к информации в связи с выражаемой им ипостаси его личности при запросе:

- *личный* - субъект, может собирать информацию только о себе, о своей собственности;
- *коммунальный* - субъект как член территориальной громады, сособственник материальной и финансовой основы местного самоуправления; может интересоваться общим ее представлением (что принадлежит громаде);
- *служебный* - субъект, может собирать информацию, в соответствии с законодательством, действуя в рамках его служебных полномочий (уставных задач, должностных обязанностей);
- *гостевой* - субъект, может собирать только открытую информацию, не попадающую под предыдущие статусы.

Третий эшелон защиты, это персонификация текущих процессов. В исходном состоянии данные и процессы, взаимодействующие с ними, – это объекты, которые могут быть использованы в процедурах, составляющих различные методы решения прикладных заданий. Поэтому комбинации взаимодействия процессов с данными могут быть различными. В том числе возможны ситуации, когда такое взаимодействие имеет ограничения. В связи с этим установление соответствия ПРАВ текущих процессов по отношению к текущим данным, с которыми они взаимодействуют, составляет процедуру персонификации текущих процессов.

Четвертый эшелон защиты, реализуемый в процессе применения выбранного метода использования имеющихся данных и процедур работы с ними. Решение конкретных задач требует использования конкретной части имеющихся данных, при этом важным аспектом является актуальность значений этих данных в их конкретной комбинации, используемой в решении задачи. Поэтому выделение необходимого и достаточного объема данных для решения текущей задачи путем синтеза текущих сведений из первичных (базовых) данных, составляет сущность защиты информации на этом этапе.

Пятый эшелон защиты - персонификация текущих субъектов. Поскольку процесс формирования сведений может быть инициализирован субъектом (процессом, пользователем (ми) и т.п.), не имеющим (их) на это право , или в более сложной ситуации, когда субъекты могут иметь разные ПРАВА, поэтому защита информации в этот момент должна базироваться на однозначном "опознании" текущего субъекта и назначение ему текущих полномочий на основании зарегистрированных ПРАВ данного субъекта по отношению к объектам, с которыми он имеет право взаимодействовать.

Шестой эшелон защиты - конвертация текущих синтезированных сведений в формат используемый субъектом (конечным пользователем). Любой результат решения задачи должен быть представлен субъекту, инициализировавшего процесс, в "приемлемом" формате. Сущность защиты информации на этом этапе заключается в процесс формирования содержания и формы представления результата решения задания. При этом формируются только те результаты, которые были запрошены при постановке исходной задачи и атрибуты ПРАВ результата соответствуют текущим "полномочиям" субъекта.

Седьмой эшелон защиты - передача информации (данных, команд управления) между пользователем и вычислительной системой. Связывающим звеном этих систем являются каналы связи. При локальном размещение всех систем в одномашинном, однопользовательском режиме эксплуатации, влияние канала связи на защиту информации не актуально. Но при использовании многопользовательских, многомашинных систем, вероятность несанкционированного использования данных пользователями велика. Поэтому важным аспектом защиты информации в данном случае становится обеспечение целенаправленной передачи информации между конкретным объектом и субъектом без возможности вмешательства (подмены) "третьей стороной".

Восьмой эшелон защиты - получение информации субъектом. Использование информации, по сути, является конечной целью процесса ее получения. Любое нарушение в этом процессе может привести к невозможности использования полученной информации. Причин этому много. Например, искаженная (недостоверная) информация, несвоевременная доставка, ее утеря в процессе передачи, потеря ее ценности при несанкционированном ознакомлении с ней и т.д. Поэтому управление и контроль процесса работы с информацией от момента ее "рождения" до "уничтожения" является важным аспектом защиты и может быть реализован в виде информационной технологии. Применение целостной информационной технологии "под ключ", когда увязаны между собой и защищены все этапы работы с информацией.

Применение всех эшелонов защиты информации в совокупности с единой информационной технологией позволяет наиболее эффективно реализовать решение прикладных задач использующих информацию. Примером такого использования может служить проект опытной автоматизированной системы класса "3" с комплексной системой защиты информации как автоматизированного рабочего места Джанкойского городского головы. Этот проект реализует информационно-аналитическую поддержку принятия решений по управлению устойчивым развитием города с использованием защищенной компьютерной системы (далее – КС) в виде информационно - технологического комплекса, использующего многоцелевую информационную технологию "Ноосфера" (далее – МИТ "Ноосфера").