УДК 681.3.069

© Меньшикова Л.В., Меньшиков В.А., Найденов М.Ю.
Menshikova L., Menshikov V., Naydenov M.

АНАЛИЗ ЗАРУБЕЖНЫХ ПОДХОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЕДИНЫХ ЦЕНТРАЛИЗОВАННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ, ПРИМЕНИМЫХ ПРИ ПОСТРОЕНИИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ МЕЖДУНАРОДНОЙ АЭРОКОСМИЧЕСКОЙ СИСТЕМЫ МОНИТОРИНГА И ПРОГНОЗИРОВАНИЯ МАКСМ

FOREIGN APPROACH ANALYSIS OF SECURITY SERVICE OF SINGLE CENTRALIZED AUTOMATIZED SYSTEM APPLICABLE TO DESIGN OF INFORMATION AND ANALYTICAL SYSTEM OF MAXM

Аннотация. *Представлена методология проектирования ЕЦАС в части информационной безопасности.*

Annotation. *Methodology of design for the single centralized automatized system in part of information security is represent.*

Ключевые слова. *Информационная безопасность, информационно-аналитическая система, проект информатизации крупномасштабного предприятия, проектирование, единая централизованная аналитическая система.*

Key words. *Security service, BI-system, IT-project of the large-scale companies, design, single centralized automatized system.*

Классификация методологий проектирования ИАС позволяет принять в ходе реинжиниринга ИАС компетентное решение о варианте организационной структуры ИТ, которая будет в ИТ – службе крупномасштабного предприятия после реинжиниринга в зависимости от адекватности бизнес-пользователей, руководства и компетенции существующего ИТ-персонала. Для информационно-аналитической системы МАКСМ лучший вариант – французский [1].

В отличие от «земных» единых централизованных автоматизированных систем (ЕЦАЗ) в МАКСМ присутствует дополнительный уровень иерархии ЕЦАС- датчики автоматизированного сбора данных мониторинга земной поверхности, что делает разработку данной системы зависимой от принятия решения по безопасности. Мировой опыт в части безопасности web-приложений, которые и планируется использовать для доступа пользователей (госорганизаций всего мира) к МАКСМ консолидирован резервным Банком Чикаго, который был представлен на международном семинаре по теме «ИТ управление для центральных банков», прошедшем в 2008 году в городе Кембридже, Великобритания.

Итак, рассмотрим политику безопасности в резервном Банке Чикаго.

В Федеральном резервном Банке Чикаго физической безопасностью занимается одно подразделение, информационной безопасностью – другое подразделение. Защита информации в нем – это дело и ответственность ИТ-подразделения.

Перед ИТ-менеджерами в резервном Банке Чика-

Меньшикова Лариса Валерьевна – кандидат физико-математических наук, доцент, экономический советник Департамента информационных систем Банка России, МИРЭА. тел.(495)753-9420;
Меньшиков Валерий Александрович – доктор технических наук, профессор, генеральный директор проекта МАКСМ;
Найденов Михаил Юрьевич – заместитель начальника научно-технического центра, «НИИ КС имени АА. Максимова» - филиал ФГУП «ГКНПЦ им. М.В. Хруничева».

Menshikova Larisa – candidate of physico-mathematical science, associate professor, economical adviser of Bank of Russia, MIREA, tel.(495)753-9420.
Menshikov Valery – doctor of technical sciences, professor, honored worker of science of the Russian Federation, company executive of nonprofit partnership international committee MAXM;
Naydenov Michael – deputy chief of scientific and technical center, «Scientific research institute of space Systems named by AAMaksimov».

го стоит задача обеспечить безопасность ИТ-систем при повсеместном использовании электронной почты, Интернета и удаленного доступа, а также определить, какие технологии и организационные меры следует использовать для обеспечения безопасности данных.

Еще одна задача, которую они решают – безопасность должна отвечать потребностям, но не быть чрезмерной, так как риск всегда есть, но он должен быть управляемым; действия по безопасности следует планировать и для этого проводить симуляции атак на системы ежегодно на основе некоторого сценария.

При этом основной проблемой является то, что при постоянном росте платежей в любом банке и требованиях проведения их без задержек каждый инцидент безопасности приводит к усложнению систем безопасности. За 10 лет количество электронных платежей станет больше чем в 2 раза в каждом регионе.

В таблице представлены тенденции роста электронных платежей с 2004 по 2009 гг. для 15 стран.

Тенденции роста электронных платежей с 2004 по 2009 гг.

Страна	Изменение в транзакциях (млн)	Средний ежегодный рост транзакций, %	Средний ежегодный рост реального GDP,%
США	52,273	12,4	3,3
Китай	17,080	31,6	8,1
Великобритания	10,994	9,8	2,5
Бразилия	9,978	13,9	3,4
Южная Корея	8,317	20,0	5,2
Германия	6,433	6,5	1,5
Франция	5,780	8,5	2,0
Канада	5,638	10,0	2,8
Россия	4,084	18,9	4,8
Мексика	3,763	17,1	3,7
Австралия	3,544	10,4	2,5
Испания	3,261	11,4	2,7
Польша	3,243	20,3	4,6
Индия	3,180	26,1	6,5
Сингапур	2,856	17,4%	4,5
Всего по вышеуказанным 15 странам	140,423	13,0	3,5
В мире	174,414	12,9	3,2

Вместе с ростом платежей растет и дополнительная угроза клиентам со стороны:

- организованной преступности;
- корпоративного шпионажа;
- компьютерного терроризма;
- подростковой преступности в варианте «старый башмак».

Объемы похищенных средств при помощи различных методов, применяемых организованной преступностью, составили:

- троянские программы, похищающие информацию по счетам $980-4900;
- использование номера кредитной карты плюс пинкода $490;
- использование информации о счете $78-294;
- использование водительского удостоверения $147;
- использование сертификата на день рождения $147;
- использование социальной карты $98;
- использование номера кредитной карты с секретным кодом и датой $6-24 ;
- использование логина и пароля счета $6.

Для обеспечения безопасности необходимо учитывать три основных фактора:

- людей;
- процессы;
- используемые технологии.

По каждому из вышеперечисленных трех факторов резервный Банк Чикаго дает следующие рекомендации:

1) по людям:

- хранить всю доступную информацию о каждом из клиентов;
- использовать знания клиентов в части средств защиты и обучать их применять новые;
- проверять работающий и нанимаемый на работу в банк персонал.

2) по процессам:

- риск всегда есть, но он должен быть управляемым;
- планировать действия по безопасности;
- проводить симуляции атак на АС ежегодно на основе сценариев взлома и т.п.

3) по используемым технологиям:

- нет единой технологии или техники, которая обеспечит безопасность в мире Интернета, поэтому рекомендуется использовать технические и технологические средства вместе;
- к ранее используемым логинам с паролями добавить физические устройства (таблетки и т.п.), а в будущем, возможно, и биометрические данные.

Таким образом, по мнению резервного банка Чикаго:

- следует минимизировать возможность «технической атаки» злоумышленников;
- логин полезен только в том случае, если он проверяется;

• не следует доверять средствам безопасности - корни секретности в организационных мерах;

• как правило, мы проверяем «неправильные» вещи;

• право аннулирования должно быть связано с назначенной ролью;

• общественный инжиниринг – это угроза;

• не следует верить тому, что читаете;

• понижение оплаты персонала может быть опасно;

• будущее без страхования неэффективно;

• атаки злоумышленников всегда мотивированы;

• измерения безопасности бесполезны, если они выключены.

Противоречивость и взаимовлияние наиболее важных параметров ИАС в части информационной безопасности и авторизованного доступа, отсутствие методов объективного определения нарушения целостности систем, их информационных ресурсов и влияния на эти факторы параметров линий связи существенно осложняют объективный выбор подходящего ПО для ИАС, КХД и транспортных уровней системы. Подобный выбор целесообразно осуществлять на основе комплексного подхода из имеющегося множества используемых для унаследованных систем ПО, зарекомендовавших себя как оптимальный вариант в части решения проблем информационной безопасности с учетом возможности использования этого ПО в новой технологической централизованной схеме. В качестве оптимизационного критерия целесообразно применять критерий обеспечения минимума затрат на реализацию новой технологической схемы на унаследованном АПК.

В рамках информационно-аналитической системы Международной аэрокосмической системы мониторинга опасных для цивилизации природных явлений и техногенных катастроф МАКСМ это означает, что в крупных промышленных структурах и государственных организациях для оптимизации бизнес-процессов и внедрения бизнес-приложений в российских компаниях и организациях должны быть выработаны единые требования к безопасности систем, которые в дальнейшем должны будут быть адаптированы в международных стандартах в части информационной безопасности web-приложений.

Таким образом, сформулируем основные подходы в части безопасности для единой централизованной системы, у которой большое число пользователей, а также большое число источников информации в части:

1.Надежности и безопасности.

Система должна быть надежной и защищенной, обеспечивать бесперебойную работу, получение достоверных результатов и защиту от несанкционированных действий.

2. Обеспечения катастрофоустойчивости системы.

Архитектура должна предусматривать возможность создания территориально распределенных комплексов (особенно центров обработки информации) – основных и резервных. Резервные комплексы должны выполнять функцию замещения основных комплексов при возникновении чрезвычайных ситуаций, ведущих к выходу последних из строя. Резервные центры должны размещаться на объектах, с заранее подготовленной инфраструктурой и информационно-телекоммуникационными ресурсами.

3. *Преемственности.*

При создании системы необходимо максимально полно использовать уже существующие технологические системы и инфраструктурные элементы. При необходимости используемые системы должны быть доработаны по требованиям, сформированным в процессе проектирования системы.

Для реализации вышеуказанных подходов требуется провести следующий комплекс мероприятий:

• спроектировать и создать единое корпоративное хранилище данных;

• централизовать процессы сбора, хранения и аналитической обработки данных с использованием каталога бизнес-терминов из различных информационных источников с учетом требований к обеспечению информационной безопасности, контроля и разграничения прав доступа к информации с различным уровнем конфиденциальности.

Литература

1. Меньшикова Л.В. , Меньшиков В.А., Найденов М.Ю. Подходы к разработке ИАС международной аэрокосмической системы мониторинга и прогнозирования МАКСМ// Технологии и средства связи. – 2012.-№6.-с.33-34.

2. Меньшикова Л.В., Найденов М.Ю. Подходы к разработке информационно-аналитической системы МАКСМ,/ Формирование современного информационного общества-проблемы, перспективы, инновационные подходы: Материалы Международного форума, Санкт- Петербург, 30 мая-3 июня 2011г./СПб.:ГУАП,СПб., 2011, с.139-144.

3. Mensbikova L.V. "Development of Informational and Analitical Systems with Asquisition of Feedback from Users in the Framework of Large-scale Projects/Abstracts of First International Specialized Symposium Space and Global Security of Humanity", Limassol-Cyprus: International Academy of Astronautics, Russian Academy of Cosmonautics, International Association "Znanie", 2009, p.57.

4. Materials of Central Banking Training Course "IT Governance for Central Banks", Autumn 2008 at King's College, Cambridge, UK.

Материал поступил в редакцию 19. 05. 2013 г.