М. Тынышбаев атындағы
ҚАЗАҚ КӨЛІК ЖӘНЕ КОММУНИКАЦИЯЛАР АКАДЕМИЯСЫ

КАЗАХСКАЯ АКАДЕМИЯ ТРАНСПОРТА И КОММУНИКАЦИЙ
имени М. Тынышпаева

«Төртінші өнеркәсіптік революция жағдайындағы дамудың жаңа мүмкіндіктері» атты ҚР Президенті Н. Назарбаевтың Жолдауын іске асыру шеңберінде «Көліктегі инновациялық технологиялар: білім, ғылым, тәжірибе» атты XLII Халықаралық ғылыми-практикалық конференцияның

МАТЕРИАЛДАРЫ

18 сәуір 2018 жыл

3 том

МАТЕРИАЛЫ

XLII Международной научно-практической конференции на тему: «Инновационные технологии на транспорте: образование, наука, практика» в рамках реализации Послания Президента РК Н. Назарбаева «Новые возможности развития в условиях четвертой промышленной революции»

18 апреля 2018 года

Том 3

Алматы, 2018

СЕКЦИЯ № 4. ИННОВАЦИИ В IT

2. Взаимодействие интегрированных приложений

Для взаимодействия приложений используются такие методы, как обмен файлами, общая база данных, удаленный вызов и асинхронный обмен сообщениями. В этом списке нет прямого обмена данными между базами данных приложений: этот метод ближе не к интеграции приложений, а к перемещению данных. С точки зрения интеграции приложений важна возможность в процессе обмена данными выполнять какую-то содержательную обработку (например, при загрузке накладных пересчитывать товарные остатки). Прямой обмен данными, который обычно выполняется средствами класса ETL (extract, transfer, load) или самодельными утилитами, обычно такой возможности не предоставляет.

Обмен файлами

Обмен файлами пожалуй, самый распространенный подход к организации взаимодействия. Это связано с относительной простотой реализации, а также существованием стандартных (или «почти» стандартных) форматов обмена. Например, большая часть корпоративных информационных систем позволяет загружать и выгружать файлы, например, в формате CSV (Comma-SeparatedValues — «поля, разделенные запятыми»). Но у этого подхода есть и недостатки: если необходимо оперировать сложными структурами, то простые форматы обмена уже не пригодны. Возникающие в таких случаях специализированные форматы файлов должны «понимать» взаимодействующие системы, что ведет к жесткой зависимости систем друг от друга. Этот недостаток обычно преодолевают всевозможными утилитами конвертации данных. Кроме того, обычно обмен файлами подразумевает участие человека — кто-то должен выгрузить файл, скопировать его на другой компьютер, загрузить. Однако, если интегрируемые методом обмена файлами системы имеют возможность автоматической загрузки/выгрузки (например, по расписанию), то данный подход позволяет построить полностью автоматизированное решение, которое вследствие своей простоты обладает высокой надежностью и пропускной способностью.

Общая база данных

Данный подход концептуально очень прост — несколько информационных систем или приложений используют одну базу данных. Главный его недостаток — связь между интегрированными приложениями настолько тесная, что иногда невозможно заметить границу между ними (обычно так интегрируются продукты одного производителя). Примером такого подхода могут служить большинство ERP-систем, где различные модули системы используют одну базу. Однако слишком тесная связь превращает конгломерат интегрированных приложений в монолит, в «суперсистему», отдельные части которой с трудом поддаются самостоятельной модернизации и замене. С этим борются, используя механизмы серверов баз данных (представления данных, промежуточные таблицы и т.п.), но далеко не всегда эффективно.

Имеются еще следующие виды коммуникации:удаленный вызов, асинхронный обмен сообщениями, топология, точка-точка, web-сервисы, ESB и SOA и т.д.

ЛИТЕРАТУРА

[1] Золотарев А.В. Коммуникативные технологии в осуществлении взаимодействия с органами государственной власти // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 8, №4 (2016) http://naukovedenie.ru/PDF/55EVN416.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

[2] Алексей Добровольский. Интеграция приложений: методы взаимодействия, топология, инструменты// Открытые системы. СУБД. 2006, № 09, по адресу:https://www.osp.ru/os/2006/09/3776464/

ӘОЖ 681.3

Л.С. Кунтунова[1,a], Н.А. Туменбаева[1,a], Т.К. Қыдырмоллаева[1,b]
[1]М.Тынышбаев атындағы Қазақ көлік және коммуникациялар академиясы, Алматы, Қазақстан,
[a]kuntunova75@mail.ru, [b]naziktumenbaeva@mail.ru

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАРДЫҢ ҚАУІПСІЗДІК САЛАСЫНДАҒЫ ОРНЫ

Аңдатпа. Бұл мақалада ақпараттық технологияның қауіпсіздік саласындағы орны мен қоғамдағы рөлі жайлы айтылған. Сонымен қатар, қауіпсіздік жүйелерінің дамуы қазіргі уақытта телекоммуникацияның қарқынды дамуымен айқындалатындығына ерекше тоқталған. Ақпаратты қорғаудың криптографиялық жүйесіне қойылатын талаптар тұжырымдалған.

Түйінді сөздер:ақпараттың көлемі, еңбекті автоматтандыру, қауіпсіздік сервистері, қауіп көзі, ақпарат технологиясы.

Аннотация. В этой статье обсуждается роль информационных технологий в области безопасности и ее роли в обществе. В то же время было указано, что развитие систем безопасности в настоящее время определяется быстрым развитием телекоммуникаций. Сформулированы требования к системе защиты криптографической информации.

Ключевые слова: объем информации, автоматизация труда, службы безопасности, угрозы, информационные технологии.

Abstract. In this article, the role of informational technologies in the security of the region and its role in the society is discussed. At any point in time, the system security is currently being determined by the rapid development of telecommunications. The system is structured into a cryptographic information system.

Key words: The volume of information, labor automation, security service, threats, information technology.

Ақпаратты қорғаудың криптографиялық жүйесі – бұл деректерді шифрлау үшін криптографиялық әдістерді пайдаланатын ақпаратты қорғау жүйесі. Қазіргі уақытта жасалынып жатқан ақпаратты қорғаудың криптографиялық жүйесіне қойылатын талаптар келесіде тұжырымдалған: шифрланған хабар тек кілт болғанда ғана оқылу керек; шифрлау алгоритмді білу қорғаудың сенімділігіне әсер етпеу керек; мүмкін болатын көптіктегі кез келген кілт ақпараттың сенімді қорғауын қамтамасыз ету керек; шифрлау алгоритмы бағдарламалық та, аппараттық та жүзеге асыруға мүмкіндік беру керек. Айтылған талаптар шифрлау алгоритмдердің бәріне толық орындалмайды. Мысалы, осал кілттердің болмау талабы (қаскүнемге шифрланған хабарды оңай ашуға мүмкіндік беретін кілттер) кейбір «ескі» блокты шифрлер үшін орындалмайды. Бірақ, жаңадан жасалынған барлық жүйелер айтылған талаптарға қанағаттандырылады.

Адамдардың өмірі мен денсаулығына қауіп төндіретін түрлі төтенше жағдайлар кенеттен пайда болады және төтенше жағдайларға қарсы әрекет ету қызметтерінен өте тез және үйлестірілген шешім қабылдауды қажет етеді. Төтенше жағдайлар бойынша қызмет көрсету уақытын барынша азайту заманауи технологиялармен және коммуникациялық жабдықпен және ақпаратты өңдеумен жабдықталған арнайы қауіпсіздік жүйелерін құрусыз мүмкін емес.

Барлық төтенше жағдайлар түрлері үшін үш жалпы ереже бар:

- жүйенің жоғары жылдамдығы, яғни көмек сигналы түскен сәттен бастап шұғыл түбіртек жіберу, бері өткен уақыт кезеңі аз болуы тиіс;
- көмек көрсету керек;

- көмек көрсетілудің жоғары сапалылығы, көп жағдайда сигналдың түсу уақытымен анықталады. Сонымен қатар берілген ақпараттың көлемі мен сенімділігіне байланысты.

Осы талаптарды қанағаттандыру үшін жақында арнайы телекоммуникациялық жүйелер пайда болды, олардың міндеті осы жағдайдың түрі мен дәрежесіне қарамастан, шұғыл көмек көрсетуді ұйымдастыру болып табылады. Бұл жүйелердің негізі қазіргі заманғы ақпараттық өңдеу құралдарымен жабдықталған диспетчерлік орталықтар, байланыс және деректерді беру. Қауіпсіздік жүйелерінің даму қарқынықазіргі уақытта телекоммуникацияның қарқынды дамуымен айтарлықтай айқындалады. Ақпараттық технологияларды енгізудің негізгі мақсаты мына ақпараттық қызметтердің көлемін арттыру:

- еңбекті автоматтандыру;
- шығарылатын ақпараттың сақтау уақытын қысқарту;
- ақпараттың толықтығы, сенімділігі мен уақтылылығы дәрежесі бойынша жұмыс көлемін қысқарту;
- есептеу және бақылау бойынша жұмыстың күрделілігін төмендету;
- ақпаратты енгізу уақытын қысқарту;
- қызметтердің жаңа түрлерін енгізу;
- ақпаратты өңдеу шығындарын азайту;
- басқару қатынастары желісін кеңейту

Ақпараттық технологияға қойылатын талаптар:

1. Ақпараттық технологияны, автоматтандыруды енгізудің арқасындабасқару жүйесінің функцияларының жалпы саны 30% дейін;

2. Басқару жүйесі мәтіндік, графикалық құжаттарды, сондай-ақ магниттік медиа туралы ақпаратты жазуға тиіс;

3. Басқару жүйесінің үш деңгейлі иерархиялық құрылымы;

4. Жасалатын құжаттар Төтенше жағдайлар министрлігінің белгіленген нормативтері мен талаптарына сәйкес келуге тиіс;

5. Есептеу және бақылау бойынша жұмыстың күрделілігін төмендетеді;

6. Кіріс және шығыс ақпаратын ұлғайту жиілігі - тәулігіне 1,5 рет (ағымдағы және есепке алу);

7. Ағымдағы құжаттарды толтыру үшін уақытша шығындарды қысқарту - бір адамға 3 минутқа дейін;

Ақпарат технологиясы— объектінің, процестің немесе құбылыстың күйі туралы жаңа ақпарат алу үшін мәліметтерді жинау, өңдеу, жеткізу тәсілдері мен құралдарының жиынтығын пайдаланатын процесс. Ақпарат технологиясы дегеніміз компьютерді және телекоммуникациялық жабдықтарды деректерді сақтау, шығару, тасымалдау және өзгертуге арналған технология. Ақпарат технологиясы ақпаратты өңдеу үшін пайдаланылатын технологиялық элементтердің, құрылғылардың немесе әдістердің жиынтығы. Ақпараттық технологияқазіргі компьютерлік технология негізінде ақпаратты жинау, сақтау, өңдеу және тасымалдау істерін қамтамасыз ететін математикалық және кибернетикалық тәсілдер мен қазіргі техникалық құралдар жиыны. Ақпараттық технологиялардың мақсаты, адамның талдау жасай отырып, нәтижесінде белгілі бір әрекетті орындау арқылы шешімдер қабылдай алатындай ақпаратты өңдіру болып табылады.

Ақпаратты қорғау - ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған шаралар кешені. Тәжірибе жүзінде ақпаратты қорғау деп деректерді енгізу, сақтау, өңдеу және тасымалдау үшін қолданылатын ақпарат пен қорлардың тұтастығын, қол жеткізулік оңтайлығын және керек болса, жасырындылығын қолдауды түсінеді. Сонымен, ақпаратты қорғау - ақпараттың сыртқа кетуінің, оны ұрлаудың, жоғалтудың, рұқсатсыз жоюдың, өзгертудің, маңызына тимей түрлендірудің, рұқсатсыз көшірмесін жасаудың, бұғаттаудың

алдын алу үшін жүргізілетін шаралар кешені. Қауіпсіздікті қамтамасыз ету кезін қойылатын шектеулерді қанағаттандыруға бағытталған ұйымдастырушылық, программалық және техникалық әдістер мен құралдардан тұрады.

Ақпаратты өңдеудің автоматтандырылған жүйес ретінде келесі объектер жиынтығын түсіну керек: есептеуіш техника құралдарын; программалық жасауды; байланыс арналарын ; түрлітасушылардағы ақпараттарды; қызметшілер мен жүйені пайдаланушыларды.

Автоматтандырылған жүйенің ақпараттық қауіпсіздігі жүйенің мына күйлерінде: жүйенің сыртқы және ішкі қауіп-қатерлердің тұрақсыздандыру әсеріне қарсы тұра алу қабілеті бар кезіндегісі; жүйенің жұмыс істеуі және жүйенің бар болуы сыртқы ортаға және оның өзінің элементтеріне қауіп келтірмеуі кезіндегісі қарастырылады.

Тәжірибе жүзінде ақпараттық қауіпсіздік қорғалатын ақпараттың келесі негізгі қасиеттерінің жиынтығы ретінде қарастырылады:конфиденциалдылық яғни, ақпаратқа тек заңды пайдаланушылар қатынайалатындығы; тұтастық - біріншіден, тек заңды және сәйкесті өкілдігі бар пайдаланушыларға өзгерте алатын ақпараттың қорғалуын, ал екінші ден ақпараттың ішкі қайшылықсыздығын және заттардың нақты жағдайын бейнелеуін қамтамасыз ететіндігі;

Желілік қауіпсіздік сервистері есептеуіш жүйелер де және желілерде өңделетін ақпараттың қорғау механизмдерін береді.

Инженерлік- техникалық әдістер өзінің мақсаты ретінде техникалық арналар арқылы ақпараттың жайылып кетуіне нақпараттың қорғалуын қамтасыз етуді қарастырады. Ақпаратты қорғауды құқықтық және ұйымдастырушылық әдістері нормалар үлгілерін жетілдіру үшін ақпараттық қауіпсіздікті қамтамасыз етуге байланысты әртүрлі қызметтерді ұйымдастырады. Ақпараттық қауіпсіздікті қамтамасыз етудің теориялық әдістері өз кезегінде екі негізгі мәселені шешеді.

Біріншіден,ақпараттық қауіпсіздікті қамтамасыз етуге байланысты әртүрлі процесстерді формализациялау. Осыдан екінші мәселе туындайды – ол, қорғалу деңгейін талдағанда ақпараттық қауіпсіздікті қамтамасыз етудегі жүйелер қызметінің қисындылығы мен адекваттығының қатаң негізделуі.

Автоматтандырылған жүйенің ақпаратық қауіпсіздігіне қауіп – бұл автоматтандырылған жүйенің өңдейтін ақпараттың конфиденциалдығы, тұтастығы мен қатынау қолайлығының бұзылуына әкеліп соғатын әсерлердің жүзеге асырылуы және де АЖ құраушыларының жоғалуына, жойылуы мен қызмет етуін тоқтатуына келтіретін мүмкіндігі. Қауіптердің жіктелуі:

Пайда болу табиғатына қарай табиғи және жасанды болып бөлінеді. Табиғи –бұл адамға байланыссыз АЖ-геофизикалық процесстер мен табиғи апаттардың әсер ету нәтижесінде пайда болған қауіп. Өз кезегінде жасанды қауіп адамның әрекетінен туындайды. Табиғи қауіптің мысалы ретінде өрт, тасқын, цунами, жер сілкінісі және т.б. айтса болады. Мұндай қауіптің жағымсыз жағы – оны болжаудың қиындығы және мүмкін еместігі.

Ниеттілік дәрежесіне сәйкес кездейсоқ және қасақана болып бөлінеді. Кездейсоқ қауіп қызметшілердің немқұрайлылығынан немесе әдейілеп жасалмаған қателіктерінен пайда болады. Қасақана қауіп әдетте бағытталып жасалған әрекет нәтижесінде пайда болады. Кездейсоқ қауіптің мысалы ретінде байқаусыз деректердің қате енгізілуін, абайсыз жабдықтың бүлдірілуін келтіруге болады. Ал қаскүнемнің физикалық қатынаудың белгіленген ережелерін бұзып қорғалатын аймаққа рұқсатсыз кіру қасақана қауіптің мысалы болып табылады.

Қауіп көзінің орналасуына байланысты былай бөлінеді:

Қауіп көзінің бақылау аумағынан тыс орналасуынан пайда болатын қауіп.Мысалы, жанама электромагнит сәулеленулерін немесе байланыс арналары мен беріліп жатқан деректерді ұстап алу; қашықтан фото және бейне түсіру; бағытталған микрофон көмегімен