Електронното подписване – метод за реализация на Информационна система обслужваща организации от типа на „СВОБОДНОТО ЗИДАРСТВО“

...Да пазя мълчание относно обичаите и вътрешните дела на Масонството и да не разговарям по такива въпроси с хора, за които не съм се напълно убедил, че са Свободни Зидари... (Клетва на Чирак)

...Системата Регистрация – Вписване ще прилага механизъм за идентифициране, който се основава на принципа „докажи, че си този, който твърдиш, че си!“, когато потребителите се регистрират, за да използват дадена услуга... (Електронен портал на Правителството на Р. България)

Информационната сигурност в перспектива при създаването на Информационна система за Великата Ложа и Върховен Съвет, 33 Степен

Организациите имат формулирани цели. Действащите процеси и процедури са случаите в организацията, в които се реализират тези цели. При изпълнението на тези процеси и процедури организацията става все по-зависима от доброто функциониране на доставянето на информация. От друга страна, се повишава зависимостта от информационната сигурност при обслужването, за да посрещне изискванията на организацията.

Начинът, по който се доставя информацията, е организиран в зависимост от типа на организацията и вида на продуктите или услугите, които тя доставя в своето развитие (процеси). Организацията събира данни, за да доставя продукти или услуги. Данните се пазят, преработват и са налични винаги когато потрябват. Хората, за които е необходима тази информация, трябва винаги да разчитат на нейната цялост. Важно е да се осигури достъпът до информация само за тези, които са оторизирани за това. Необходимо е поверителността, интегритетът и наличността да не бъдат отворени за обсъждане. Затова организацията трябва да организира събирането, съхранението, преработването и предоставянето на данни по начин, задоволяващ тези условия.

Информационната сигурност съществува, за да служи на интересите на организациите. Не цялата информация и не цялото информационно обслужване са еднакво важни за организацията. Нивото на информационната сигурност трябва да съответства на важността на информацията. Тази „приспособена сигурност“ се постига чрез намиране на баланс между мерките за сигурност, тяхната стойност, от една >>>

Продължава на 30 стр.

>>>

Продължава от 27 стр.

страна, и от друга, стойността на информацията и риска от развитието на околната среда.

Сигурността има важно значение за информационните системи. И най-накрая, сигурността за информационните системи означава, че повечето задачи могат да бъдат изпълнявани по отговорен и надежден начин.

Ползата от информацията

Информационната сигурност е планирана (създадена), за да защитава информацията.

Сигурността е средство за достигането на приемливо ниво на остатъчния риск.

Стойността трябва да бъде защитена. Тази стойност се определя от поверителността, целостта и наличността.

Поверителността (конфиденциалността): Защита на информацията от неоторизиран достъп или прихващане (пресичане).

Целостта (integrity): Съхранението на точността, прецизността и завършеността на информацията и съответните програмни системи.

Наличността (availability): Подсигуряването, че информацията и жизненоважните информационни услуги са налични, когато се изискват.

Някои аспекти, произтичащи от горните, са:

privacy (строго поверителни, интимни – поверителността и целостта на информацията, проследени за отделна личност),

anonymity (анонимни – конфиденциалността на самоличността на потребителя),

verifiability (възможността за потвърждение и доказване – информацията е използвана правилно (по предназначение) и мерките за сигурност работят, както трябва).

Важността за предоставянето на точна информация, както и на подходящата информационна сигурност се удвоява за организацията.

Вътрешна сигурност: Организацията може да работи правилно единствено ако има достъп до поверителната точна информация в необходимия момент (in good time). Информационната сигурност е и гарантиране на това, че поверителността, целостта и наличността на информацията и информационното обслужване са поддържани.

Външна сигурност: Организационните процеси снабдяват с услуги, които са налични за дадена общност. Доставянето на недостатъчна, неточна и неподходяща информация води до незавършени, непълни и дефектни услуги. Подходящата информационна сигурност е важна предпоставка за доставянето на адекватна информация.

Освен от потока от услуги безбройната информация се движи от външната среда към организациите, вътрешно през организацията и от нея към околната среда. Ако тези потоци изведнъж пресъхнат, организацията вече няма да бъде способна да работи правилно. Информацията е средство на реализацията, от което организациите стават все по-зависими през годините.

Степента, в която >>>

>>>

развитието на бизнеса зависи от запаса от информация, може да бъде специфицирана в качествени изисквания за предоставянето на информация. В този смисъл сигурността трябва да оформя цялостна част на качественото управление, осигуряването на качествен процедури и действия в цялата организация. Целта на използваната информацията в организацията зависи в голяма степен от процесите, в които тя се използва. Поради тази причина изискванията за доставянето на информацията като цяло трябва да се определят от хората, които управляват процесите.

Мерки за сигурност

Информационна сигурност е защитата на информационните системи и данни от неправомерен (случаен или преднамерен) достъп, модифициране или унищожаване. В тази защита се включват още поверителност, непокътнатост и наличност на тези системи и данни.

Според изискванията за информационна сигурност всички промени в системите и данните трябва да могат да бъдат проверени и ако е необходимо, проследени до отделна личност или структура в определено време и дата. Сигурността на данните може да бъде постигната чрез комбинация от служители, политика, ръководни принципи и критерии, процедурни, софтуерни, хардуерни и физически мерки за сигурност. Програма за информационна сигурност може да бъде въведена от различни ключови позиции в дадена организация. Тъй като всяка организация се изправя срещу различни проблеми в сигурността, една ефективна система за сигурност може да се окаже напълно неотговаряща на нуждите на друга структура. По тази причина честата оценка на рисковете е ключ към всяка система за сигурност.

Поверителността, като неделима част от информационната сигурност, има две основни измерения – проверка на непокътнатостта на предадено съобщение и проверка на идентичността на потребител, който се свързва към дадена мрежа.

Информационната сигурност може да бъде разделена на 5 основни компонента:

Политики по информационна сигурност

Сигурността на информацията и нейното управление трябва да започне от най-високо управленско равнище. Този компонент на сигурността включва създаване на политики за сигурност, постигане на убеденост в потребителите за спазване на тези политики, контрол на спазването на политиките, както и обучението на потребителите като основна предпоставка за постигане на информационна сигурност.

Управление на сигурността на критични процедурни приложения

Във всяка организация и особено в затворените структури съществуват така наречените критични приложения. Това са информационни системи, от които зависи дейността на организацията. >>>

>>>

Осигуряването на тяхното функциониране е особено важно, тъй като те са най-често атакувани и представляват най-голям риск за функционирането на организацията. Определянето на едно приложение като критично се обуславя от важността на информацията, която то съхранява и управлява.

Управление на сигурността на компютърните инсталации

Сигурността на информацията на отделния компютър е особено важна, тъй като той е основна градивна единица във всяка информационна инфраструктура. Постигането на тази сигурност включва използването на надежден хардуер и софтуер (използване на компютърни конфигурации и системен софтуер от световно утвърдени и признати производители).

Контролът и мониторингът на достъпа, както и антивирусната защита и редовното обновяване на софтуера са подкомпоненти на сигурността на компютърните инсталации.

Управление на сигурността на комуникационната инфраструктура

Управлението на комуникационната инфраструктура заедно със сигурността на компютърните инсталации осигуряват информационния скелет, върху който работят критичните приложения. Този компонент включва както локалните мрежи, така и сигурността на комуникацията по Интернет, безжичните устройства и гласовите комуникации. Това са основните канали за пренос на значима информация и за това са особено уязвими за различни видове атаки. Осигуряването на физическа защитеност на тези комуникационни канали, както и защитата на информацията, пренасяна по тях, са основните аспекти на този вид сигурност.

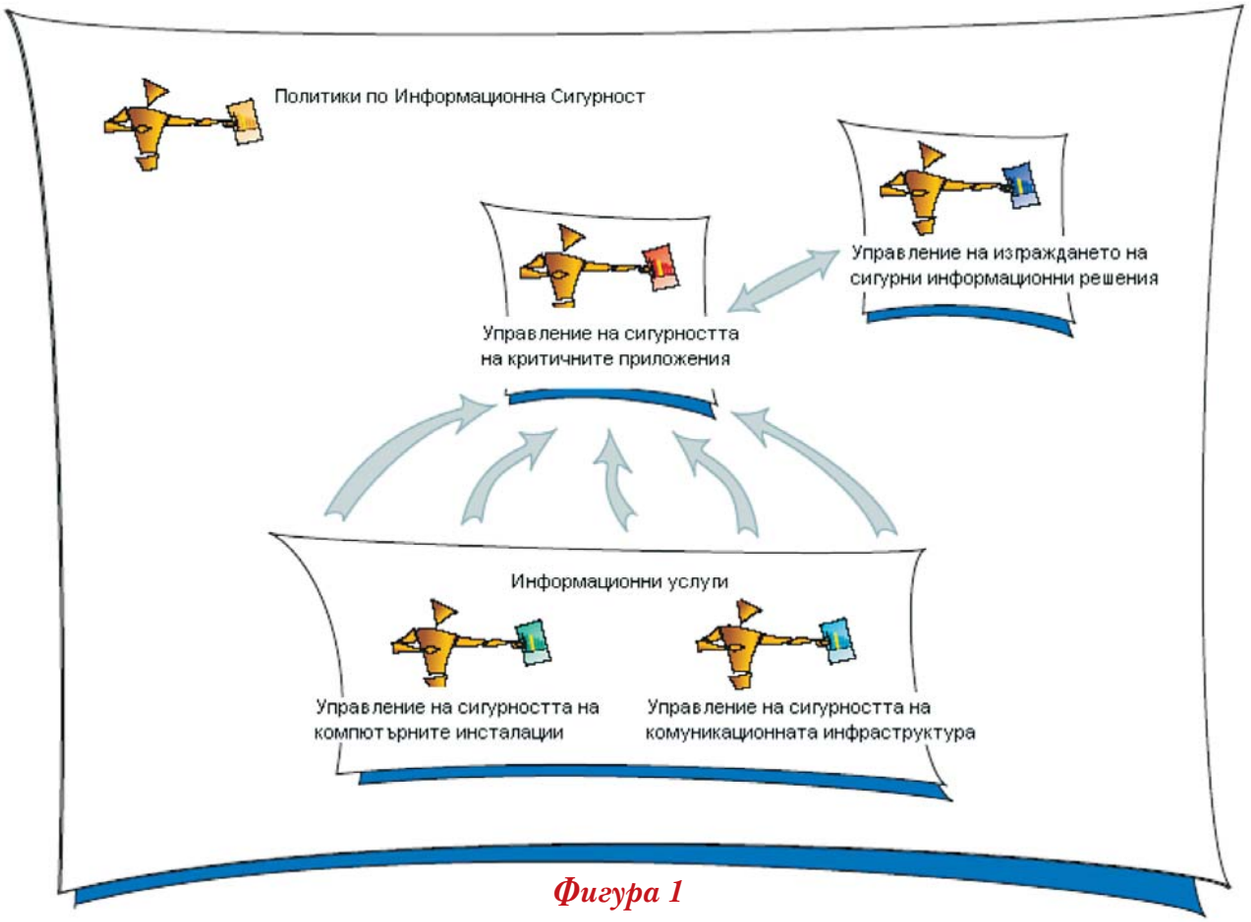
Комуникациите вътре в организацията, отдалечените комуникации, както и тези между регионалните и централните звена на управлението трябва да бъдат надеждни, като същевременно е важно да се използват отворени стандарти. Използването на изолирана мрежа е добър вариант за постигане на висока сигурност, но този подход може да доведе до затруднена комуникация с различни приложения в тази затворена среда. Друг подход е да се използва Интернет като преносител, като се осигурят сигурни криптирани (128 bit SSL) канали за комуникация между различните участници.

Управление на изграждането на сигурни информационни решения

Сигурността на критичните приложения трябва да бъде осигурена още при тяхната разработка. Вграждането на сигурност по време на разработката е по-ефективно и надеждно от опитите за постигане на защитеност впоследствие.

В този компонент са включени организацията на служителите, отговорни за разработването на приложения, методологията, използвана при изграждането им, както и подсигуряването на надежден контрол по качеството.

Обхватът на >>>



Фигура 1

>>>

дейността и връзките между различните компоненти на управлението на информационната сигурност са показани на ***Фигура 1***.

Бизнес перспектива: как можем да постигнем сигурност на информацията?

Начална точка е правилната организация за сигурност на информацията, т.е. отговорности, способности и задължения, които трябва да бъдат класифицирани:

– Политика и/или принципи на ръководене;

– Процеси;

– Процедури;

– Инструкции за работа.

Поддържането на информационната сигурност е итеративен процес. Всички фактори, които въздействат върху резултатите, са разглеждани като входящи. Съществуват вътрешни и външни въздействия, които имат ефект върху информационната сигурност. Вътрешните са свързани с решенията в организацията, външните са въздействията на околната среда, свързана с процесите.

Примери за промени във входящата информация, които изискват адаптация на промените, са:

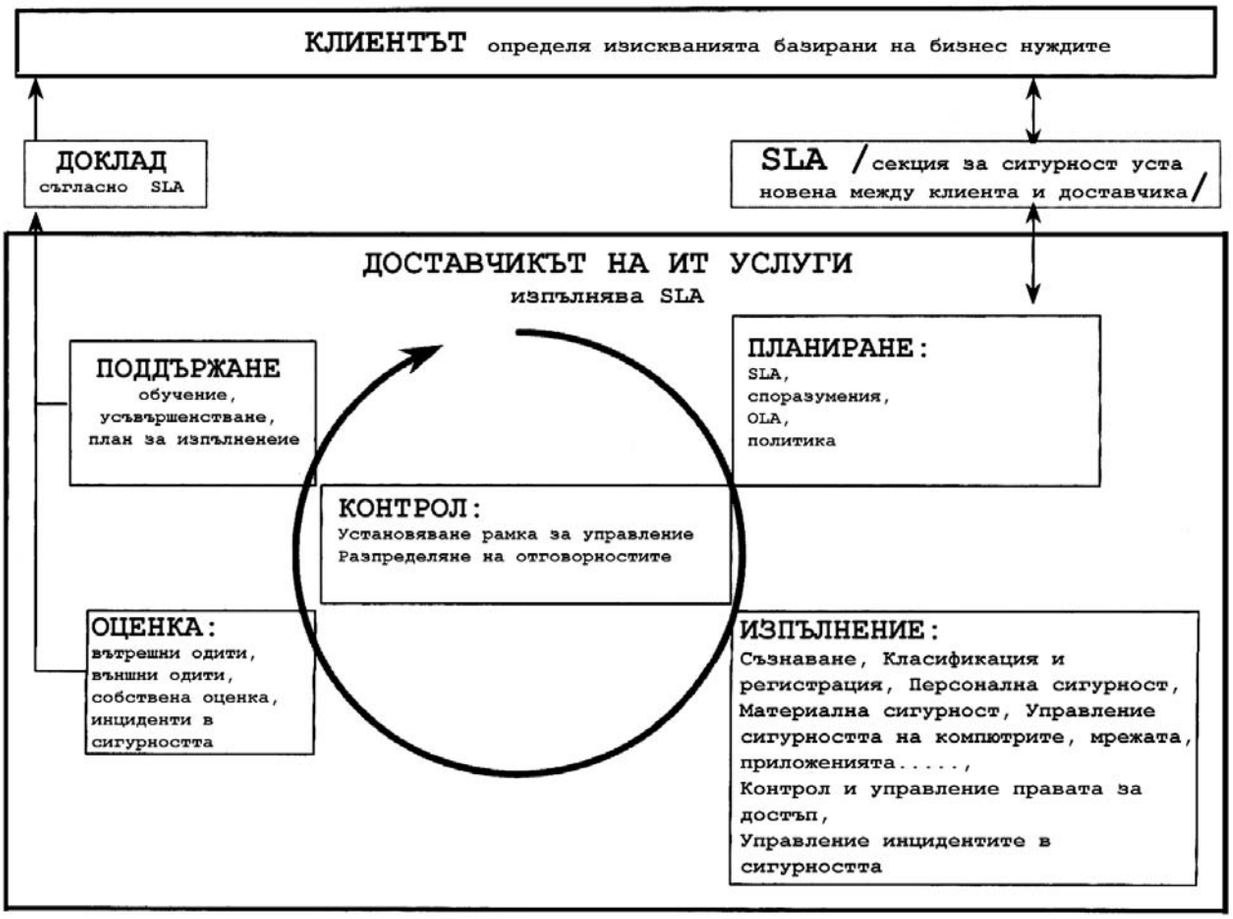
– Промени в задачите или важността на задачите;

– Материални промени, т.е. промяна в условията;

– Промени в средата;

– Промяна в оценката на използваните ИТ;

– Промени в процесите на търсенето; >>>



Фигура 2

>>>

– Промени в легалните изисквания – „legal demands“;

– Промени в софтуера и хардуера;

– Промени в процедурните изисквания;

– Промени в законовите изисквания;

– Представяне на нови технологии.

Резултатът трябва да бъде такъв, че от бизнес гледна точка процесите на управление на сигурност да осигуряват голяма степен на поверителност, постигната с високи нива на конфиденциалност, интегритет и наличност, което е достатъчно за целите и партньорите на организацията. ***(Фигура 2)***

Потребителите ще се идентифицират към приложенията, използвайки цифров сертификат. Още преди потребителите да получат достъп до входа на системата, те ще трябва да се регистрират в базата данни на системата. В рамките на влизането процесът по регистрация ще има различни раздели за различните видове потребители: физически лица, организации (или лица, които действат от името на дадена организация), агенти или представители (които действат от името на други индивиди). Всеки един раздел ще предполага към отделен процес на регистрация, който ще се различава от този на останалите видове потребители. >>>

>>>

За по-специфични правителствени услуги достъпът ще се осъществява чрез използването на цифрови сертификати. Цифровите сертификати ще трябва да се заявят и получат предварително от одобрена Институция за издаване на цифрови сертификати – CA (Certification Authority). По време на регистрационния процес ще се събира информация за потребителите, като парола, име и електронен адрес (опционално). Регистрацията и идентификаторите на даден потребител ще се прибавят в базата данни, осигурявайки достъпа на потребителя до съответната back-end услуга, както и това, че той може да бъде идентифициран от back-end системата (системата на съответната институция). Услугата back-end също ще приема съобщение, което съдържа пакета от идентификационните данни на новия потребител, така че back-end системата да може да извършва допълнителна обработка, за да приема съобщенията, изпращани от този потребител. Когато един потребител се регистрира в системата Регистрация – Вписване, той ще трябва да представи одобрен сертификат и да докаже, че има ключ за активиране на сертификата. За да бъде улеснен този процес, Р – В системата ще предлага на потребителя една страница, която съдържа XML за подпис. Това ще е протокол, използван в процеса на включване. След като приключи първата фаза по регистрацията, потребителят впоследствие ще бъде връщан към същия сайт с помощта на един token символ за активиране. Преди обаче да използва token символа за активиране, потребителят трябва да се свърже със системата за регистрация и вписване, за да докаже по този начин отново, че е притежателят на представения сертификат.

Данните за един успешно регистриран потребител ще се съхраняват в базата данни Регистрация – Вписване. Ако потребителят използва цифров сертификат, то тогава органът, който го е издал, и серийният номер на сертификата ще се съхраняват и използват за осъществяване на последващите включвания/транзакции.

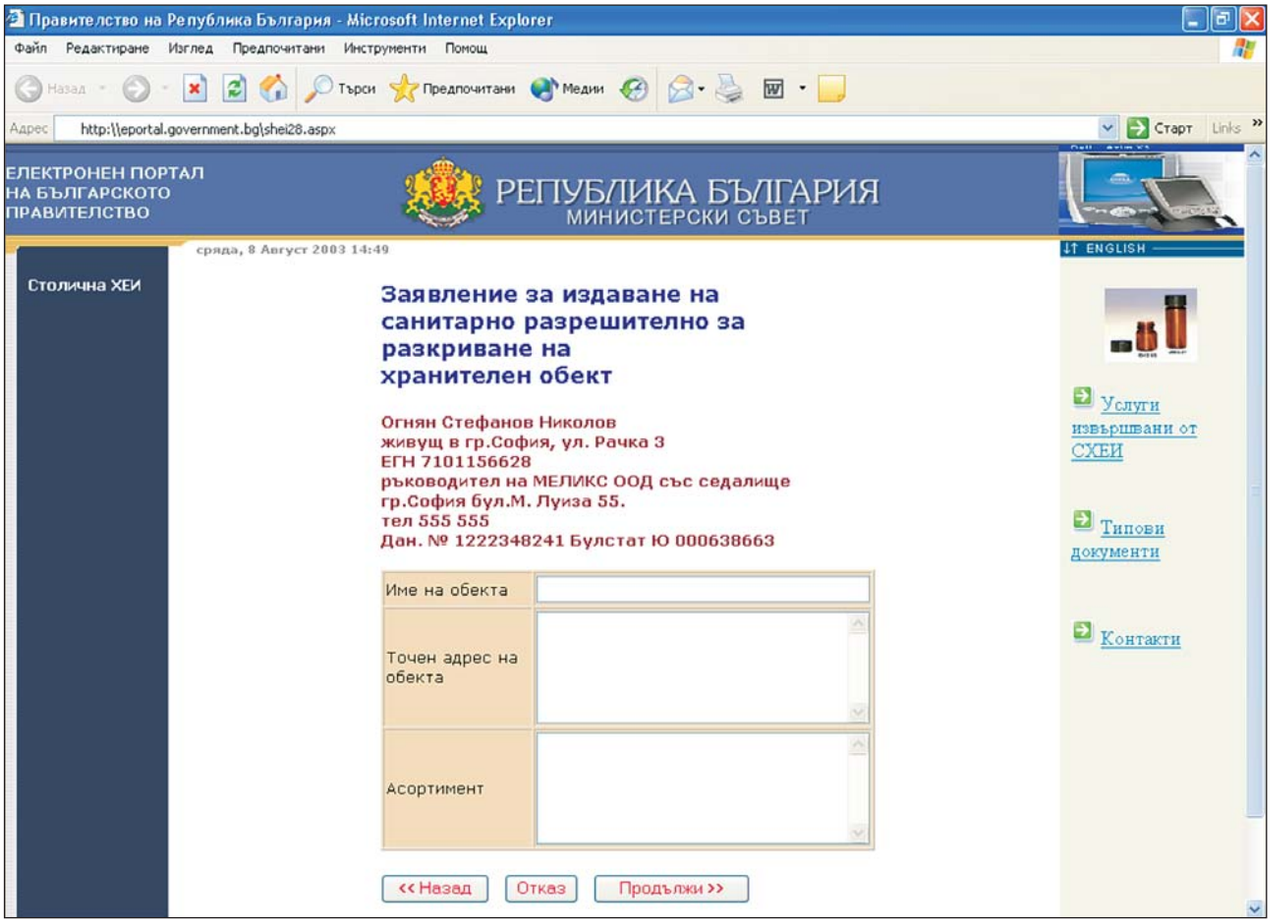
На ***фигура 3*** е показана примерна форма за заявление за издаване на разрешително за разкриване на хранителен обект. Разрешителното се издава от ХЕИ. Личните данни се взимат от подадената информация при регистрацията на лицето (физическо или юридическо) в електронното правителство. Необходимите документи (декларации, данъчна регистрация и т.н.), които съпътстват заявлението, могат да се прикачат в електронен вид, тъй като след тяхното издаване се съхраняват в сървърите на системата. Оригиналността им е гарантирана от електронен сертификат за автентичност.

До влизането на Република България в Европейския съюз цифровите сертификати ще се използват, както следва:

Административни услуги за граждани:

1. Подоходни данъци: декларации, уведомяване.
2. Услуги по търсене на работа при бюрата на труда.

>>>



Фигура 3. *Примерна форма на заявление за издаване на разрешително за разкриване на хранителен обект от ХЕИ.*

>>>

3. Социални осигуровки, помощи за безработни, добавки за деца, медицински разходи, стипендии.

4. Лични документи (паспорти, свидетелства за управление на МПС).

5. Регистрации на МПС (нови, използвани, внесени МПС).

6. Документи за строителни разрешения.

7. Декларации към полицията (напр. при кражба).

8. Публични библиотеки (каталози, машини за търсене).

9. Свидетелства (за раждане, брачни и др.).

10. Дипломи за средно и висше образование.

11. Смяна на адресна регистрация.

12. Услуги, свързани със здравеопазването.

Административни услуги за бизнеса:

13. Социални осигуровки за заетите.

14. Корпоративни данъци: декларации, уведомяване.

15. Данък върху добавената стойност: декларации, уведомяване.

16. Регистрация на нова фирма.

17. Изпращане на данни до Националния статистически институт.

18. Митнически декларации.

19. Разрешения, свързани с екологични изисквания (включително докладване).

20. Обществени поръчки.

Легенда:

Зелено – Разработено в пилотен проект.

Жълто – Предстояща разработка в пилотен проект

Бр. Пламен Матеев, 18°
Трижде Почитаем Майстор