Защита на информацията в мрежова среда

Удебеленият текст в тази страница е планът за записване в тетрадките

1. Рискове, свързани с работата в мрежова среда

Компютърните мрежи са бъдещето за обмен на информация. Те непрекъснато се развиват и усъвършенстват. Този факт налага необходимостта от сигурна защита на данните от загуба или злоупотреба. Възникват два основни приоритета:

- **защита от отказ и възстановяване;**
- **мрежова сигурност.**

2. Защита от отказ и възстановяване

Хардуерните повреди могат да бъдат сериозна причина за загуба на информация, затова е необходимо вземането на определени мерки за защита и възстановяване на данните от сривове. Могат да се предприемат някои препоръчителни действия в тази насока:

а) **Използване на аварийно захранване** за избягване на проблеми с електрозахранването. Често срещан вариант е включването на UPS устройства, които притежават батерии, съхраняващи определено количество заряд. Така се осигурява време за работа на системата след прекъсване на основното захранване.

б) **Архивиране на данните** с помощта на програма за архивиране в случай на повреда на твърд диск или вирусен проблем. Необходимо е осигуряване на допълнително устройство, на което да се съхраняват архивираните данни.

3. Мрежова сигурност

Осигуряването на мрежовата сигурност е много важна дейност при използването на мрежова среда. Известни са много случаи на проникване в компютърните мрежи на правителствени и бизнес организации, както и сериозни атаки от компютърни вируси, които засягат компютърните системи на много потребители. Терминът сигурност се свързва с необходимите действия, които трябва да се предприемат за защита на един компютър и съдържащата се в него информация. Заплахите могат да бъдат външни и вътрешни.

а) Външни заплахи

- Неоторизирано използване на чужди потребителски имена и пароли
- Компютърни вируси и червеи
- Троянски коне

б) Вътрешни заплахи

Вътрешните заплахи са тези, които могат да се извършат директно върху избрана система или през локалната мрежа.

в) Мерки за сигурност

Външните и вътрешните заплахи могат да бъдат избегнати при прилагане на определени мерки за сигурност като:

1. **Използване на операционни системи с висока степен на сигурност.** Съвременните операционни системи удовлетворяват това изискване. Например разновидностите на Windows или Linux очакват въвеждането на валидно потребителско име и парола, за да позволят зареждане и работа със системата. Съхранението на паролите е във вид, неудобен за осъществяване на лесен достъп до тях.
2. **Автентикация и идентификация.** Автентикацията е процес на удостоверяване на правилния потребител. В качеството на синоним на термина автентикация понякога се използва терминът проверка на идентичност. Например правилността на паролата за определено потребителско име гарантира, че потребителят е автентичен.
3. **Криптиране на данните.** Криптирането на данните е технология, базирана на науката криптография. Криптирането използва код или ключ за разбъркване (шифриране) и след това за подреждане (дешифриране) на данните с цел представянето им в първоначалната им форма.
4. Използване на **защитна стена** (Firewalls) и прокси сървър. Защитната стена филтрира входящите и изходящите пакети и определя дали да разреши преминаването на даден пакет. Тя се настройва от администратора на мрежата и обикновено се разполага на шлюза (gateway) на мрежата.

5. Използване на **антивирусен софтуер**. В днешно време е задължително използването на антивирусни програми за защита на системата от вируси. Антивирусният софтуер открива вирусни инфекции, сигнализира за тях и се опитва да предотврати евентуални техни поражения.

4. Нормативни документи за защита на лични данни

а) Закон за защита на личните данни

На 23 май 2018 г. представители на Съвета на Европейския съюз и Европейския парламент се споразумяха за нов регламент относно боравенето с лични данни. Новите правила са съобразени с **Общия регламент за защита на данните** (**GDPR**), който влезе в сила на 25 май 2018 г.

Обработването на вашите лични данни е разрешено:

- когато сте дали своето съгласие;
- ако сте страна при изпълнение на задължения по договор;
- при защита на вашия живот и здраве;
- при изпълнението на задачи, които са в обществен интерес.

Забранено е използването на ваши лични данни, които:

- разкриват вашия расов или етнически произход;
- разкриват вашите политически или религиозни убеждения;
- се отнасят до вашето здраве.

Вие имате право на достъп до отнасящите се за вас лични данни.

Защитата при обработване на личните ви данни и при осъществяването на достъпа до тези данни се контролира от **Комисията за защита на личните данни**.

б) Закон за авторското право и сродните му права

Според него обект на авторско право е всяко произведение на литературата, изкуството и науката, което е резултат на творческа дейност. Защитени са литературни, музикални произведения, компютърни програми, филми, база данни, печатни издания и др.

5. Електронен подпис

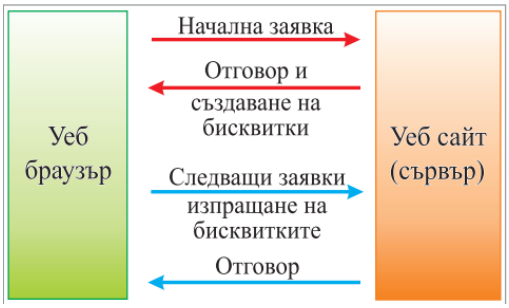
Електронният подпис **изпълнява ролята на саморъчен подпис, с който се идентифицирате онлайн и подписвате документи**. Неговата правна сила е равностойна на тази на саморъчния подпис. Основава се на уникална **комбинация от частен и публичен ключ**.

Електронният подпис се издава от сертифициращ орган и съдържа името на титуляра, сериен номер, дата на валидност и копие от публичния ключ. Съхранява се на флаш памет или смарт карта. Подписаният документ остава подписан без значение дали го съхранявате върху магнитен, оптичен или друг носител, дали го изпращате по електронна поща или го правите достъпен през интернет. Подписването на електронен подпис означава, че:

- се идентифицирате като автор на електронния документ;
- се съгласявате със съдържанието на документа;
- защитавате документа от последващи промени.

С помощта на електронен подпис можете да използвате електронните услуги на държавната и общинската администрация – да подавате данъчни декларации, молби, жалби и други документи през интернет.

6. Бисквитки (cookies)



Когато уеб сайт, който посещавате, изисква попълване на някаква информация (напр. име и парола), той може **да запомни тази информация, за да не се налага да я попълвате пак**. Това става чрез така наречената **HTTP бисквитка** (англ. HTTP cookie). Това е съвсем малък по размер файл, който се създава и изпраща от уеб сайта (сървър) и се записва от уеб браузъра на потребителя в системното му пространство. При всяка следваща заявка, направена от браузъра към същия уеб сайт, информацията от бисквитката се изпраща към сървъра.

Бисквитките се използват от уеб сайтовете, за да „различават" и „запомнят" своите посетители, регистрирани или гости, да запомнят предпочитанията на потребителите и състоянието на дадена функционалност, услуга или особеност в сайта.

Потребителят може да изтрие по всяко време, да позволи или забрани използването на бисквитки. За да направи това, трябва да промени настройките за поверителност на своя браузър.

Всички уеб сайтове, които използват бисквитки, трябва да търсят съгласието на потребителите си.

Въпроси и задачи

1. *Какви рискове съществуват при работа в мрежова среда?*
2. *Кои са основните приоритети, свързани с опазване на данните при работа в мрежова среда?*
3. *Избройте някои външни заплахи за сигурността в мрежова среда?*
4. *Какви мерки за сигурност могат да се предприемат за предотвратяване на вътрешна заплаха срещу индивидуална система?*
5. *Какво означава криптиране на данните?*
6. *Каква е ролята на защитните стени?*
7. *Какво забранява европейския регламент GDPR?*
8. *За какво служи електронният подпис?*
9. *За какво служи бисквитката? За или против?*