МОДУЛ 5: *ОРГАНИЗИРАНЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ*

ТЕМА: ОРГАНИЗИРАНЕ СИГУРНОСТТА НА ДАННИТЕ

Защита от случайно, неразрешено или умишлено разкриване на данни

ТЕМА: ОРГАНИЗИРАНЕ СИГУРНОСТТА НА СОФТУЕР

Технически и организационни средства за защита сигурността на софтуера

Организиране сигурността на данните

Защита от случайно, неразрешено или умишлено разкриване на данни

Понастоящем известните общи методи за осигуряване на информационна сигурност се състоят от организационни, технически, икономически и правни.

Наборът от мерки за гарантиране на технологичната и експлоатационна безопасност на софтуерните компоненти трябва да бъде поверителен. Необходимо е да се осигури постоянен, всеобхватен и ефективен контрол върху дейността на програмистите и потребителите. В допълнение към общите принципи обикновено е необходимо да се конкретизират принципите на софтуерната сигурност на всеки етап от жизнения й цикъл.

Организационните и техническите методи за информационна сигурност (ИС) включват:

- система за информационна сигурност (под която се разбира набор от мерки (вътрешни правила за работа с данни, разпоредби за пренос на информация, достъп до тях и т.н.) и технически средства (използване на програми и устройства за поддържане на поверителност на данните));
- разработване (създаване на нови), експлоатация и усъвършенстване на съществуващи средства за защита на информацията;
- постоянен контрол върху ефективността на мерките, предприети в областта на осигуряване на информационна сигурност.

Организиране сигурността на данните

Защита от случайно, неразрешено или умишлено разкриване на данни

- Последната точка е особено важна. Без методология за оценка е много трудно да се определи ефективността на информационната сигурност. Ако ефективността спадне, трябва да се направят спешни корекции (за това е необходимо постоянно наблюдение).

- Те са тясно свързани с правните методи за информационна сигурност на България

- Факторът на правната сигурност на България се състои от:
  - лицензиране на дейности по отношение на осигуряване на информационна сигурност;
  - сертифициране на технически средства за защита на информацията;
  - сертифициране на обекти на информатизация в съответствие със стандартите за информационна сигурност на Бултария.

- Третият компонент, икономически, включва:
  - изготвяне на програми за осигуряване на информационна сигурност на България;
  - определяне на източниците на тяхната финансова подкрепа;
  - разработване на механизми за финансиране;
  - създаване на механизъм за осигуряване на информационен риск.

Организиране сигурността на данните

Защита от случайно, неразрешено или умишлено разкриване на данни

Информационната сигурност винаги е комплексна система, която е предназначена да предотврати изтичането на поверителна информация по технически канали, както и да предотврати достъпа на трети страни до носители на информация. Всичко това, съответно, гарантира целостта на данните при работа с тях: обработка, предаване и съхранение, което трябва да се извърши в правната област. Правилно организираните технически събития позволяват да се определи използването на специални електронни устройства за неразрешено изтегляне на информация, разположени както в помещение, така и в средствата за връзка (комуникациите).

Организационният метод за осигуряване на информационна сигурност има следните компоненти:

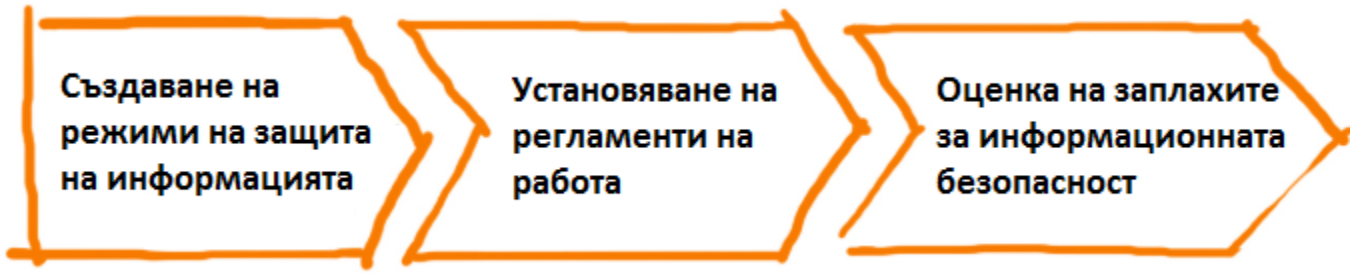
- създаването на режим на защита на информацията
- разработване на правила за взаимоотношенията между служителите;
- регулиране на работата с документи;
- правила за използване на технически средства в рамките на съществуващото правно поле на България;
- аналитична работа за оценка на заплахите за информационната сигурност.

Организиране сигурността на данните

Защита от случайно, неразрешено или умишлено разкриване на данни

Защитата на информационната инфраструктура от неоторизиран достъп се осигурява чрез регулиране на достъпа на субектите (работниците) до обекти (носители на данни и канали за предаване). Организационният метод за осигуряване на информационна сигурност не предполага използването на технически средства.

Използването на техническо оборудване и различни програми за осигуряване на информационна сигурност, включително системи за управление на бази данни, приложен софтуер, различни шифри, DLP системи и SIEM системи, които предотвратяват изтичане на данни през компютърна мрежа, се отнася до техническия метод за осигуряване на информационна сигурност.



Етапи на осигуряване на информационна сигурност във фирма

Организиране сигурността на данните

Защита на данните в ЕС

В Хартата на основните права на ЕС се посочва, че гражданите на ЕС имат право на защита на личните си данни. https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_bg

Нов пакет за защита на данните (Общ регламент относно защитата на данните - ОРЗД) се прилага от 25 май 2018 г., с цел трансформиране на Европа към цифровата ера.
Регламент (ЕС) 2016/679 се отнася за защита на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни

Държавите от ЕС са създали национални органи (http://www.cpdp.bg/) , които отговарят за защитата на личните данни в съответствие с член 8, параграф 3 от Хартата на основните права на ЕС.

Контрол на личните данни в Интернет и свързаните в мрежа устройства

Хората трябва да могат да избират как се използват данните за тях и създадени от тях. Те следва да бъдат осведомени за последиците от това как техните данни могат да бъдат използвани в дигиталната икономика и да бъдат дадени прости и ефективни начини за упражняване на контрол или намаляване на рисковете.
Най-добрата практика е автоматично изтриване на данните на всеки посетител в рамките на 24 часа след достъпа му до даден уебсайт, лесна за четене политика за поверителност и система, проектирана така, че компанията да не знае нищо за това кой я използва.

Организиране сигурността на данните

Защита на данните

Система и мерки за организиране на защита на данните в една организация

Мерките за защита на личните данни в една организация включват организиране на:

- автоматичен тайм-аут потребителски терминал. Ако не се използва, за повторно отваряне се изискват идентификация и парола;
- автоматично изключване на идентификатора на потребителя при въвеждане на няколко неправилни пароли, файл на дневник на събитията (наблюдение на опитите за хакване);
- системите за защита на данните в организацията изискват определяне правата на всеки служител за достъп до лични данни;
- информиране на персонала за отговорностите и последствията от всякакво техно нарушаване. Осигуряване на достъп на служителите до лични данни и ресурси като част от изпълнението на служебните задължения;
- контролирате достъпа за използване на определени области на системата за обработка на данни.

Разработването на регламент за обработка и защита на личните данни в дадена организация включва следните стъпки:
определяне какви данни се използват;
методи за събиране;
методи за обработка;
правила за съхранение.

Организиране сигурността на данните

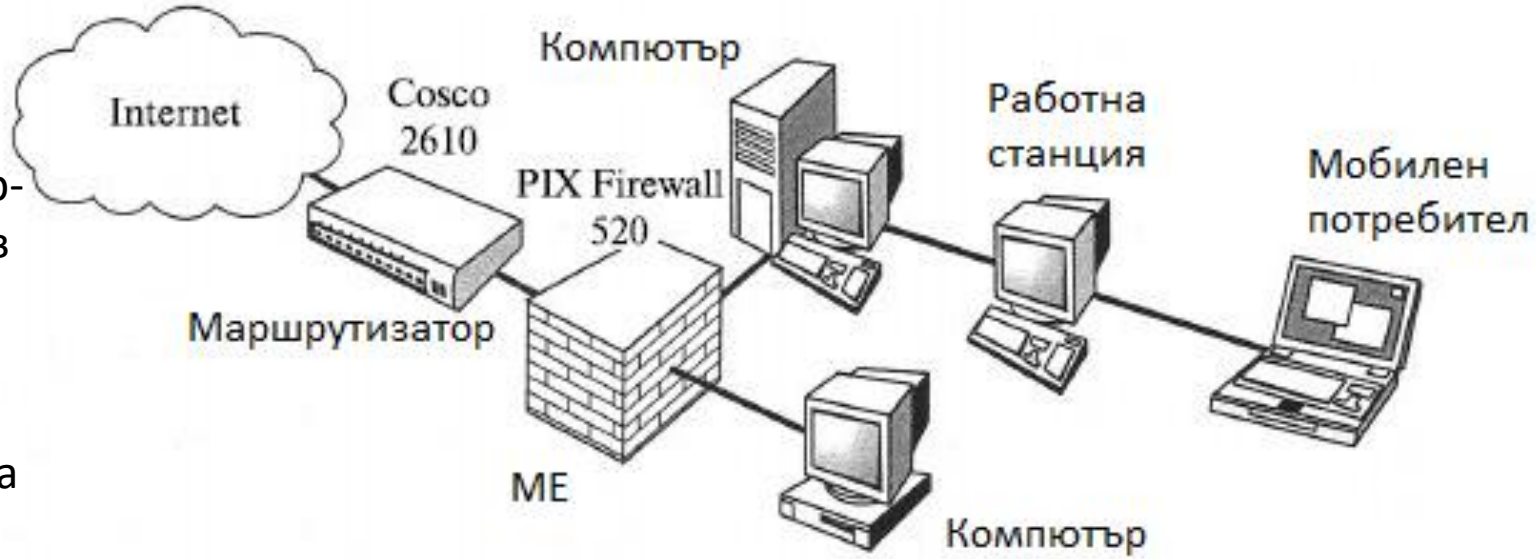
Организационна защита на данните

Система и мерки за организиране на защита на данните в една организация

Разработването на регламент за обработка и защита на личните данни в дадена организация включва следните стъпки:

- определяне какви данни се използват;
- методи за събиране;
- методи за обработка;
- правила за съхранение.

Използване на комплекса «рутер-защитна стена» в системите за защита на информацията, когато има връзка към Интернет



Организиране сигурността на данните

Организационна защита на данните

Организационните дейности включват:

- дейности, извършвани в проектирането, строителството и оборудването на офис и промишлени сгради и помещения;
- дейности, извършвани по подбор на персонал;
- организация и поддържане на надежден контрол на достъпа, сигурност на помещенията и територията, контрол върху посетителите;
- организация на съхранението и използването на документи и носители на поверителна информация;
- организация на информационната сигурност;
- организиране на редовно обучение на служителите.

Организиране сигурността на данните

Организационна защита на данните

НАЧИНИ ЗА НАНАСЯНЕ НА ЩЕТИ	ОБЕКТИ НА ВЪЗДЕЙСТВИЕ			
	ОБОРУДВАНЕ	ПРОГРАМИ	ДАННИ	ПЕРСОНАЛ
Разкриване (изтичане) на информация	Кражба на носители на информация, включване към комуникационна линия, неразрешено използване на ресурси	Неоторизирано прихващане на копие	Кражба, копиране, прихващане	Предаване на информация за защита, разкриване, небрежност
Загуба на цялостност на информацията	Свързване, модификация, специални инвестиции, промяна на режимите на работа, неразрешено използване на ресурси	Внедряване на троянски коне и бъгове	Изкривяване, модификация	Вербуване на персонал, „маскарад“
Нарушаване работоспособността на автоматизираната система	Промяна на режимите на работа, повреда, кражба, унищожаване	Изкривяване, изтриване, заместване	Изкривяване, изтриване, налагане на неверни данни	Грижи, физическа елиминация
Незаконно тиражиране на информация	Производство на аналози без лицензи	Използване на незаконни копия	Публикация без знанието на авторите	

Класификацията на видовете неизправности в системата и неоторизиран достъп до информация за обекти на въздействие и методи за причиняване на щети на сигурността

Организиране сигурността на данните

Организационни мерки за защита на информацията

Очевидно е, че в организационните структури с ниско ниво на законност и ред, дисциплина и етика, повдигането на въпроса за защитата на информацията е просто безсмислено. На първо място е необходимо да се решат правни и организационни въпроси.
Организационните мерки играят важна роля за осигуряване на сигурността на компютърните системи и данните. Организационни мерки - това е единственото, което остава, когато други методи и средства за защита отсъстват или не могат да осигурят необходимото ниво на сигурност. Това обаче изобщо не означава, че системата за защита трябва да се изгражда единствено на тяхна основа, както често се опитват да правят служители, които са далеч от технологичния прогрес.

Недостатъци на организационните мерки:
• ниска надеждност без подходяща поддръжка от физически, технически и софтуерни средства (хората са склонни да нарушават установените допълнителни ограничения и правила, ако същите могат да бъдат нарушени);
• допълнителни неудобства, свързани с голямо количество рутинни и официални дейности.

Организационни мерки са необходими, за да се гарантира ефективното прилагане на други мерки и средства за защита по отношение на регулирането на човешките действия. В същото време организационните мерки трябва да бъдат подкрепени с по-надеждни физически и технически средства.

Организиране сигурността на софтуер

Термини за сигурност на софтуера

Софтуерната сигурност в широк смисъл е свойството на софтуера да функционира, без да проявява различни отрицателни последици за определена компютърна система. Под ниво на софтуерна сигурност се разбира вероятността при определени условя да се получи функционално подходящ резултат по време на неговото изпълнение.

Причините, водещи до функционално неподходящ резултат, могат да бъдат различни:

- неизправности в компютърните системи
- грешки на програмисти и оператори
- дефекти в софтуера

Дефектите се считат за два вида:

- умишлени - резултат от злонамерени действия
- непреднамерени - погрешни човешки действия

Организиране сигурността на софтуер

Термини за сигурност на софтуера

- Неволен дефект - обективно и (или) субективно образуван дефект, водещ до получаване на неверни решения (резултати) или нарушаване на функционалността на КС.
- Умишлен дефект – криминален дефект, внесен от субекта за целенасочено нарушение и (или) разрушаване на информационния ресурс.
- Разрушаващ софтуер – съвкупност от програмни и/или технически средства, предназначен за нарушаване (изменение) на зададената технология за обработка на информация и/или целенасочено разрушаване извън вътрешното състояние на информационно-изчислителния процес в КС.
- Средства на активно противодействие - средства за защита на информационния ресурс на КС, позволяващи блокиране на канала на изтичане на информация, разрушаване на действията на противника, минимизиране на нанесената щета и предотвратяване на последващо деструктивно действие на противника, посредством ответно въздействие на информационния ресурс.
- Несанкциониран достъп – действия, водещи до нарушаване на безопасността на информационния ресурс и получаване на секретни сведения.

Организиране сигурността на софтуер

Термини за сигурност на софтуера

- Нарушител (нарушители) - субект (субекти), извършващи неоторизиран достъп до информационния ресурс.
- Модел на заплахите - вербален, математически, имитационнен или натурен модел, формализиращи параметрите на вътрешните и външните заплахи за сигурността на софтуера.
- Оценка на сигурността на софтуера – процес на получаване на количествени или качествени показатели на информационна сигурност при отчитане на преднамерени и непреднамерени дефекти в системата.
- Система за осигуряване на информационна сигурност – обединена съвкупност от мероприятия, методи и средства, създавани и поддържани за осигуряване на необходимото ниво на сигурност на информационния ресурс.
- Информационна технология – подредена съвкупност на организационни, технически и технологични процеси на създаване на софтуера и обработка, съхраняване и предаване на информация.
- Технологична сигурност – свойство на софтуера и информацията да не бъдат умишлено изкривени и (или) резервни модули (структури) с диверсионно предназначение на етапа на създаване на КС.
- Експлоатационна сигурност – свойство на софтуера и информацията да не бъдат умишлено изкривени (изменени) на етап на експлоатация на КС.

Организиране сигурността на софтуер

Технически и организационни средства за защита сигурността на софтуера

Софтуерната сигурност в широк смисъл е свойството на софтуера да функционира, без да проявява различни отрицателни последици за определена компютърна система. Под ниво на софтуерна сигурност се разбира вероятността при определени условя да се получи функционално подходящ резултат по време на неговото изпълнение.

Причините, водещи до функционално неподходящ резултат, могат да бъдат различни:

- неизправности в компютърните системи
- грешки на програмисти и оператори
- дефекти в софтуера

Дефектите се считат за два вида:

- умишлени - резултат от злонамерени действия
- непреднамерени - погрешни човешки действия

Организиране сигурността на софтуер

Технически и организационни средства за защита сигурността на софтуера

Безопасност (сигурност) на софтуера в широк смисъл е свойството му да функционира без проявления на различни негативни последствия за конкретната компютърна система или оборудване.

Ниво на безопасност на софтуера – вероятността при зададени условия в процеса на експлоатация в процеса му на експлоатация да се получат функционално годен резултат.

Причините за получаване на функционално непригоден резултат могат да са различини:

- срив на компютърната система
- грешка на програмистите и операторите
- дефекти в програмата

Видове дефекти:

- Преднамерени
- Непреднамерени

При изследване на проблемите за защита на софтуера от преднамерени дефекти е неизбежна постановката на следните въпроси:

- Кой потенциално може да осъщест практическо внедряване на програмни дефекти с разрушителното въздействие в изпълнимия програмен код?
- Какви са възможните мотиви за действието на субекта, осъществяващо разработката на такива дефекти?
- Как може да се идентифицира наличието на програмен дефект?
- Как може да се различи преднамерения програмен дефект от програмната грешка?
- Какви са най-вероятните последствия от активирането на деструктивните програмни средства при експлоатация на компютърните системи и техническите системи?

Организиране сигурността на софтуер

Технически и организационни средства за защита сигурността на софтуера

При решаването на проблема за повишаване на нивото на сигурност на информационните ресурси на КС е необходимо да се изхожда от факта, че най-вероятният информационен обект на който се въздейства е софтуера, представляващ основата на комплекса от средства за получаване, семантична обработка, разпространение и съхранение на данни, използвани в експлоатацията на критични системи.

В момента едно от най-опасните средства за въздействие на информацията върху компютърните системи са програми - вируси или компютърни вируси.

Наред с други средства за информационно влияние е необходимо да се разгледат алгоритмичните и софтуерните отметки като основно средство за вредно (разрушително) въздействие върху КС.

Действията на алгоритмичните и програмните отметки могат условно да се разделят на три класа: промяна на функционирането на компютърната система (мрежа), неразрешено четене на информация и неразрешено изменение на информацията, до нейното унищожаване. В последния случай под информация се разбира както данните, така и кодовете на програмите. Трябва да се отбележи, че тези класове въздействия могат да се припокриват.

Действията на алгоритмичните и програмните отметки могат условно да се разделят на три класа:

- промяна на функционирането на компютърна система (мрежа)
- неразрешено четене на информация
- неразрешено изменение на информацията, до нейното унищожаване. В последния случай слячай под информацията се се разбират както данните, така и програмните кодове. Тези класове въздействия могат да се пресичат.

Организиране сигурността на софтуер

Технически и организационни средства за защита сигурността на софтуера

- Въздействия от промяна на функционирането на компютърна система (мрежа):

▪намаляване на скоростта на изчислителната система (мрежа);
▪частично или пълно блокиране на системата (мрежата);
▪имитация на физически (хардуерни) неизправности на изчислителните съоръжения и периферни устройства;
▪препращане на съобщения;
▪заобикаляне на софтуер и хардуер за преобразуване на криптографска информация;
▪осигуряване на достъп до системата от непредвидени периферни устройства.

- Въздействия от неразрешено четене на информация

▪ четене на пароли и идентифицирането им с конкретни потребители;
▪ получаване на класифицирана информация;
▪идентификация на исканата от потребителите информация;
▪подмяна на пароли с цел достъп до информация;
▪ мониторинг на активността на абонатите на мрежата за получаване на косвена информация за взаимодействията на потребителите и естеството на информацията, обменяна от мрежови абонати.

- Неправомерното модифициране на информация е най-опасната форма на програмни отметки, тъй като води до най-опасните последици:

▪унищожаване на данни и кодове на изпълними програми;
▪правене на фини, трудни за откриване промени в информационните масиви;
▪внедряване на програмни маркери в други програми и подпрограми (вирусен механизъм на действие);
▪изкривяване или унищожаване на собствената информация на сървъра и по този начин прекъсване на мрежата;
▪модификация на пакетите за съобщения.

Организиране сигурността на софтуер

Технически и организационни средства за защита сигурността на софтуера

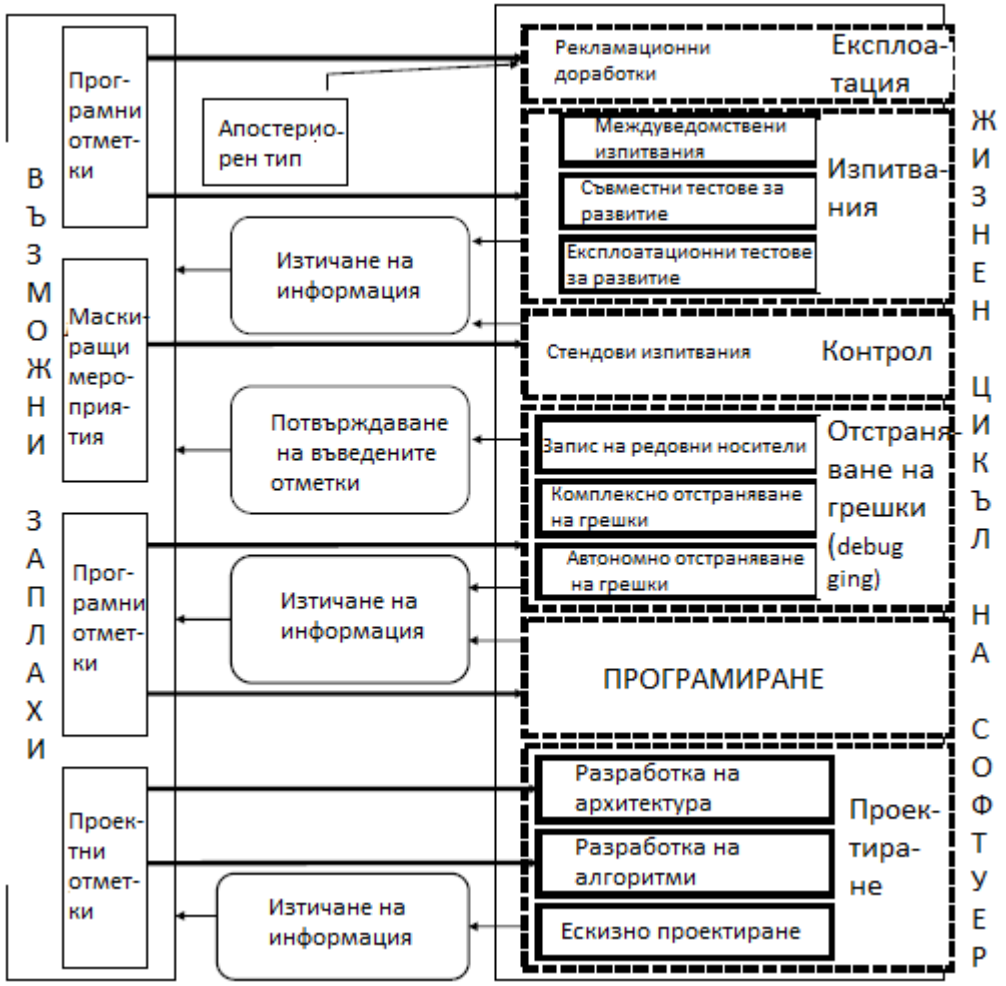


Схема на заплахите за технологична сигурност на софтуера

Организиране сигурността на софтуер

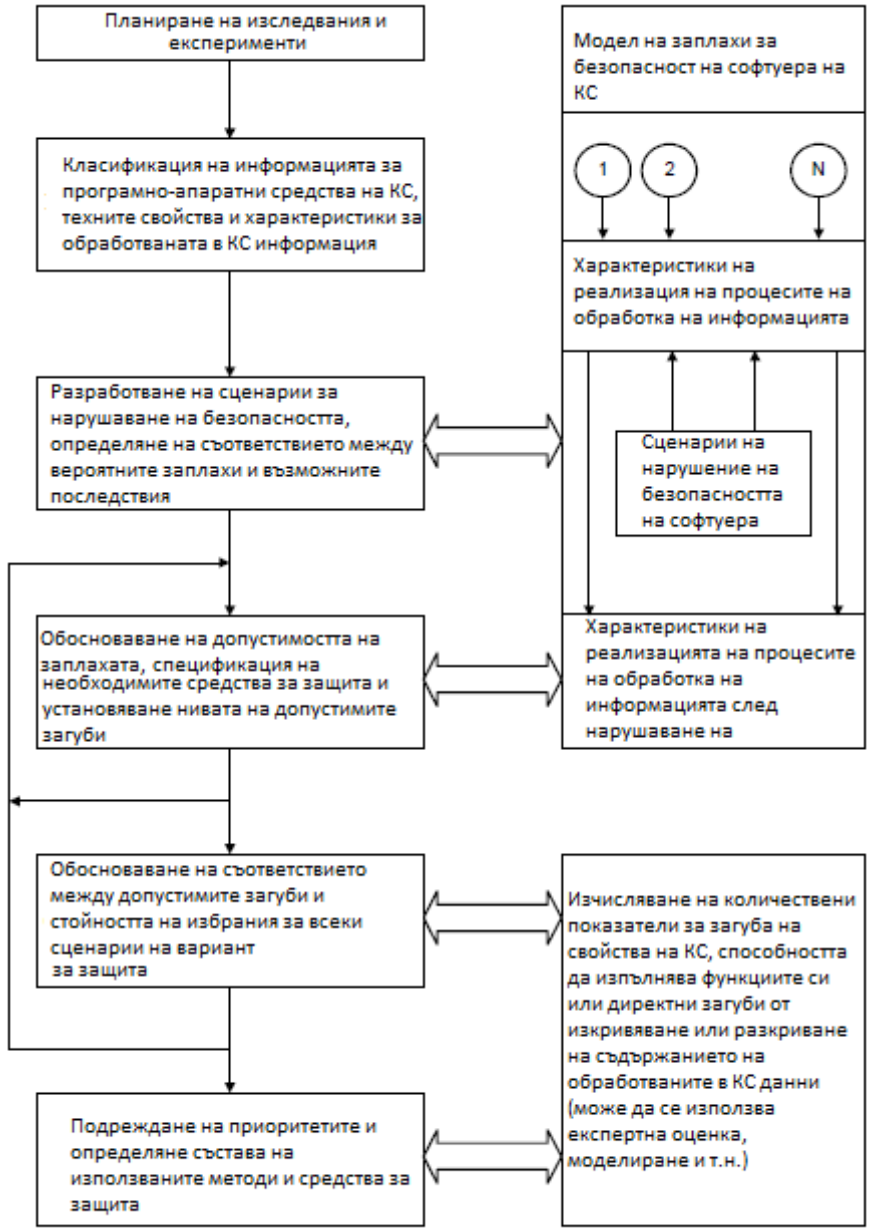
обща структура на набора от потенциални заплахи за сигурността на информацията и софтуера на етапа на експлоатация на КС

Заплахи за нарушаване безопасността на софтуера	Неоторизирани действия		
	Случайни	Преднамерени	
		Пасивни	Активни
Преки	неуспехи и грешки на техническото оборудване на КС; грешки на оператора; отказ на инструменти за криптиране; пренапрежения на електрозахранването на технически средства; стареене на носителите на информация; унищожаване на информация под влияние на физически фактори (авария и др.). неоткрити грешки в софтуера на КС	маскиране на неоторизирани заявки за заявка на ОС; байпас програми за контрол на достъпа; четене на поверителни данни от източници на информация; връзка с каналите за комуникация с цел получаване на информация („подслушване“ и / или „препредаване“); при анализ на трафика; използване на терминали и компютри на други оператори; умишлено предизвикаване на случайни фактори	включване в софтуера на разрушаваща програма, която изпълнява функция за нарушаване на целостта и поверителността на информацията и софтуера; въвеждане на нови програми, които изпълняват функции за нарушаване на софтуерната сигурност; незаконно използване на ключове за контрол на достъпа; байпас програми за контрол на достъпа; отказ на подсистемата за регистрация; унищожаване на криптиращи ключове и пароли; връзка с каналите за комуникация с цел промяна, унищожаване, забавяне и пренареждане на данни; неизправност на подсистемата за регистрация; отказ на елементите на физическите средства за защита на информацията в КС; умишлено предизвикване на случайни фактори.
Косвени	нарушение на контрола на достъпа и поверителността; естествени потенциални полета; шумове и т.н.	прихващане на електромагнитно излъчване от технически средства; кражба на промишлени отпадъци (разпечатки); визуален канал; устройства за слушане; дистанционна фотографиране и т.н.	смущения; прекъсване на захранването; умишлено предизвикване на случайни фактори.

Организиране сигурността на софтуер

Технически и организационни средства за защита сигурността на софтуера

Неформално описание на модела на заплахи за сигурността на софтуера на етап изследване на опити за нерегламентирани действия във връзка с информационните ресурси на КС



Организиране сигурността на софтуер

Технически и организационни средства за защита сигурността на софтуера

- Принципите за технологична безопасност при обосновката, планирането на работа и проектния анализ на софтуера:

- **Комплексност на осигуряването на безопасността на софтуера** - свързана с разглеждането на проблема със сигурността на информационните и изчислителни процеси, като се вземат предвид всички структури на компютърните системи, възможните канали за изтичане на информация и неправомерен достъп до нея, времето и условията на тяхното възникване, интегрираното използване на организационни и технически мерки.
- **Планирането на използването на средствата за безопасност на софтуера** , предполагащи прехвърляне на акцента върху съвместното системно проектиране на софтуера и средствата за неговата безопасност, планиране на тяхното използване в предполаганите условия на работа.
- **Валидиране на средствата за осигуряване на безопасност на софтуера**, която се състои в дълбок, научно-обоснован подход за вземане на проектни решения за оценка на степента на сигурност, прогнозиране на заплахите за сигурността и всестранна априорна оценка на показателите на средствата за защитата.
- **Достатъчност на софтуерната сигурност**, отразяваща необходимостта от търсене на най-ефективните и надеждни мерки за сигурност, като в същото време се намаляват разходите за тях.

Схема на заплахите за технологична сигурност на софтуера

Организиране сигурността на софтуер

Технически и организационни средства за защита сигурността на софтуера

- Принципите за технологична безопасност при обосновката, планирането на работа и проектния анализ на софтуера:

- **Гъвкавост на управлението на защитната програма,** която изисква от контролиращата и управляващата система осигуряваща информационна безопасност на софтуера, способност за диагностициране, изпреварващо неутрализацията, оперативното и ефективното отстраняване на възникващите заплахи в условията на резки изменения в обстановката на информационната борба.
- **Напредък на разработването на средства за осигуряване на сигурност** и контрол на производството на софтуер, състоящ се в превантивния характер на мерките за осигуряване на технологична безопасност на работа в интерес на недопускане на намаляване на ефективността на системата за сигурност на процеса на създаване на софтуера.
- **Документируемост** на технологията за създаване на програми, която предполага разработването на пакет от нормативно-технически документи за контрола на софтуера за наличие на умишлени дефекти.

Схема на заплахите за технологична сигурност на софтуера

Организиране сигурността на софтуер

Технически и организационни средства за защита сигурността на софтуера

❑ Принципи за достигане на технологична сигурност на софтуера в процеса на разработка:

- **Регламентиране на технологичните етапи на разработване на софтуер**, включващо подредени фази на междинен контрол, спецификация на програмни модули и стандартизация на функциите и формата за представяне на данни.
- **Автоматизация на средствата за контрол на управляващите и изчислителните програми** за наличие на дефекти, създаване на типова обща информационна база от алгоритми, изходни текстове и програмни средства, които позволяват да се идентифицират умишлени софтуерни дефекти.
- **Последователно многостепенно филтриране на софтуерни модули** в процеса на тяхното създаване, използвайки функционално дублиране на разработките и поетапен контрол.
- **Типизиране на алгоритми, програми и средства за информационна сигурност**, осигуряващо информационна, технологична и софтуерна съвместимост въз основа на тяхното максимално унифициране по всички компоненти и интерфейси.

Схема на заплахите за технологична сигурност на софтуера

Организиране сигурността на софтуер

Технически и организационни средства за защита сигурността на софтуера

- Принципи за осигуряване на технологична безопасност на етапите на стендови и приемо-предавателни изпитвания:

- **Тестване на софтуер,** основаващо се на разработването на тестови комплекси, които могат да бъдат параметризирани на конкретни класове програми с възможност за функционален и статистически контрол в широк диапазон на изменение на входни и изходни данни.
- **Провеждане на натурни изпитвания на програми** при екстремални натоварвания със симулирано въздействие на активни дефекти.
- **Осъществяване на „филтрация“ на софтуерни комплекси** с цел идентифициране на възможни умишлени дефекти с определено предназначение въз основа на създаването на модели на заплахи и съответни сканиращи софтуери.
- **Разработка и експериментално тестване** на средствата за верификация на програмни изделия.

Схема на заплахите за технологична сигурност на софтуера

Организиране сигурността на софтуер

Технически и организационни средства за защита сигурността на софтуера

❑ Принципи за осигуряване на безопасността при експлоатация на софтуера:

- **Съхраняване и ограничаване на достъпа до еталони на софтуера**, недопускане на внасяне на изменения в тях.
- **Профилактично извадково изпитване и пълно сканиране на софтуера** за наличие на преднамерени дефекти.
- **Идентификация на софтуера в момента на въвеждането му в експлоатация,** в съответствие с предполагаеми заплахи за сигурността на софтуера и неговия контрол.
- **Осигуряване на модификация на програмните изделия** по време на тяхната експлоатация , посредством замяна на отделни модули без изменение на общата структура и връзка с други модули.
- **Строго отчитане и каталогизиране** на всички съпровождащи софтуери, също и събираната, обработваната и съхраняваната информация.
- **Статистически анализ на информацията за всички процеси**, работни операции, отстъпления от режимите на редовното функциониране на софтуера.
- **Гъвкаво използване на допълнителни средства** за защита на софтуер, в случая на откриване на нови, непрогнозирани заплахи за информационната безопасност.

Схема на заплахите за технологична сигурност на софтуера