ПРОКУРАТУРА НА РЕПУБЛИКА БЪЛГАРИЯ

ГЛАВЕН ПРОКУРОР

ЗАПОВЕД
№ РД-02-16
гр. София, 30.06. 2016 г.

ОТНОСНО: Утвърждаване на вътрешни правила за информационна сигурност на автоматизираните информационни системи или мрежи в Прокуратурата на Република България

С цел осигуряване на информационната сигурност на автоматизираните информационни системи или мрежи в Прокуратурата на Република България и на основание чл. 138, т. 1 от Закона за съдебната власт

ЗАПОВЯДВАМ:

1. Утвърждавам Вътрешни правила за информационна сигурност на автоматизираните информационни системи или мрежи в Прокуратурата на Република България
2. Заповедта да се публикува на ведомствения информационен сайт на Прокуратура на Република България.

ГЛАВЕН ПРОКУРОР

СОТИР ЦАЦАРОВ

ПРОКУРАТУРА НА РЕПУБЛИКА БЪЛГАРИЯ

ГЛАВЕН ПРОКУРОР

ВЪТРЕШНИ ПРАВИЛА
за информационна сигурност
на автоматизираните информационни системи или мрежи
в Прокуратурата на Република България

Раздел I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Вътрешните правила определят правата, задълженията и отговорностите на административните ръководители, администраторите по информационната сигурност и потребителите на автоматизирани информационни системи или мрежи (АИС/М) в Прокуратурата на РБ във връзка със сигурността на информацията, с изключение на АИС/М, в които се създава, пренася и обработва класифицирана информация.

(2) Потребители на АИС/М в ПРБ са всички магистрати и служители по служебно или трудово правоотношение.

(3) Потребители на АИС/М в ПРБ са и лицата, извън посочените в ал. 2, ползващи компютърни и мрежови ресурси на ПРБ. Последните подписват декларация, че са запознати с тези правила.

Чл. 2. Административните ръководители на прокуратурите:

1. отговарят за мрежовата и информационната сигурност на ръководената от тях структура;
2. със заповед възлагат функции на администратор по информационната сигурност на АИС/М на служител от съответната прокуратура или на служител от друга прокуратура със съгласието на административния ръководител на служителя;
3. организират комплексни проверки за оценяване степента на постигнатата мрежова и информационна сигурност;
4. осигуряват необходимата техническа обезпеченост за гарантиране на информационната сигурност на използваните информационни системи съгласно тези правила.

Чл. 3. Дирекция „Информационно обслужване и технологии“ при Администрацията на главния прокурор:

1. отговаря за прилагането на съгласувани технологични решения и обезпечаване на информационната сигурност на ПРБ;
2. периодично обсъжда и предлага на Главния прокурор за утвърждаване управленски мерки за предотвратяване на инциденти в информационната сигурност;
3. периодично, но не по-малко от веднъж в годината изготвя доклад за състоянието на информационната сигурност;
4. извършва одити за спазването на тези правила от прокуратурите при необходимост;

5. изготвя списък на минимално задължителните процедури за сигурност, които трябва да разработи всяка прокуратура.

Чл. 4. (1) Всички АИС (компютърни конфигурации, мобилни компютри, сървъри и др. компютърно оборудване, вкл. базов и специализиран софтуер) и автоматизирани информационни мрежи (или само "мрежи") формират компютърната среда на ПРБ.

(2) С цел защита на системния и приложния софтуер и служебната информация се налагат ограничения върху потребителски права в компютърната среда съгласно определеното ниво на сигурност.

(3) На персоналните компютри се извършват типови инсталации на програмни продукти в зависимост от профила на потребителя и съобразно притежаваните лицензи.

(4) Разрешеният за инсталиране и използване софтуер в ПРБ е посочен в Приложение 1 към настоящите правила. Списъкът може да се допълва със заповед на административния ръководител на съответната прокуратура в зависимост от спецификите. Ползването на нелицензирани или неодобрени софтуерни продукти е забранено.

Чл. 5. (1) За АИС/М в ПРБ, се определят следните нива на сигурност:

- ВИСОКО – това ниво на сигурност е предвидено за потребители, които боравят с чувствителна информация.
- СТАНДАРТНО - това ниво на сигурност е предвидено за общ режим на работа в ПРБ.
- НИСКО – това ниво на сигурност е предвидено като изключение, за потребители, които имат необходимата компютърна грамотност и служебна необходимост, след разрешение от административния ръководител.

(2) Администраторът по информационната сигурност конфигурира АИС/М, съгласно посочените в Раздел IV от тези правила минимални задължителни мерки за сигурност.

(3) По подразбиране нивото на сигурност на всички АИС/М в ПРБ е „СТАНДАРТНО", ако изрично не е определено друго.

(4) Нивото на сигурност на АИС/М се променя от администратора по информационна сигурност по искане на потребителя съгласувано от неговия пряк ръководител, съобразно обработваната информация чрез писмено заявление по образец, копие на което се съхранява от администратора по информационната сигурност.

(5) АИС/М с различни нива на сигурност не следва да имат директна IP връзка помежду си.

Раздел II
АДМИНИСТРАТОР ПО ИНФОРМАЦИОННАТА СИГУРНОСТ НА АИС И МРЕЖИ

Чл. 6. (1) Администраторът по информационната сигурност на АИС/М е служител, който реализира дейностите, свързани с постигане на информационна сигурност в съответната прокуратура, в съответствие с нормативната уредба и политиките и целите за информационна сигурност на организацията.

(2) При необходимост могат да се определят повече от един администратор по информационната сигурност на АИС/М, отговарящи за обособени нейни части, като един от тях се определя за администратор по информационната сигурност на цялата АИС/М.

(3) Когато автоматизираната мрежа обхваща няколко прокуратури, всяка от тях определя администратор по информационната сигурност за нейната част от мрежата.

Администраторът по информационната сигурност на цялата мрежа се определя от организатора на мрежата.

Чл. 7. (1) Администраторът по информационната сигурност на АИС/М:

1. изготвя и актуализира процедурите по информационната сигурност на АИС/М;

2. изготвя експлоатационни документи по информационната сигурност на АИС/М на базата на утвърдените процедури за сигурност;

3. изпълнява възложените му процедури за сигурност в АИС/М;

4. периодично консултира административния ръководител и потребителите по въпросите на сигурността на АИС/М;

5. осигурява на потребителите достъп до ресурсите на АИС/Ма в съответствие с предоставените им права;

6. осъществява пряк контрол по отношение на изпълнението на мерките и процедурите за сигурност в АИС/М, като:

а) следи за спазването на мерките и процедурите за сигурност на АИС/М;

б) следи за спазването на мерките и процедурите за сигурност при инсталирането, конфигурирането, поддръжката и промените в АИС/М;

в) следи за правилното функциониране на механизмите за сигурност;

г) управлява, наблюдава и анализира свързаните със сигурността одитни записи на системата и при констатиране или при съмнения за компрометиране на сигурността докладва на административния ръководител;

д) осигурява резервиране и съхраняване на одитните записи в определените срокове;

7. участва в установяването на обстоятелствата, свързани с компрометиране на сигурността на АИС/М;

8. изпълнява функциите на администратор по криптографска защита на информацията, ако в АИС/М се прилагат криптографски методи и средства.

9. изготвя списък от заплахи и потенциални рискове за съответната администрация и ги актуализира ежегодно.

10. изготвя доклади и анализи за настъпили инциденти, засягащи мрежовата и информационната сигурност, и предлага действия за компенсиране на последствията и предотвратяване на други подобни инциденти.

(2) Функциите по ал. 1 могат да бъдат разпределени между няколко специално определени администратори по информационната сигурност на АИС/М.

(3) Носи пълна отговорност за ежедневното архивиране на данните, съхранявани върху файловете сървъри.

(4) Носи пълна отговорност за защитата и опазването на информацията, съхранена върху файловете сървъри от повреда или случайна загуба.

(5) Поддържа база от данни с актуална информация за наличните информационни и хардуерни активи.

(6) Предоставя за съхранение запечатан списък на паролите за достъп до информационните системи, сървърното и мрежовото оборудване в регистратурата за класифицирана информация първоначално и при промяна, но не по-рядко от веднъж на 3 месеца.

Раздел III
ПОТРЕБИТЕЛИ НА АИС И МРЕЖИ

Чл. 8. Всеки потребител има право да ползва компютърното оборудване и информационните ресурси в ПРБ, доколкото същите им са необходими за изпълнение на служебните задължения, съгласно длъжностната им характеристика или вътрешноведомствени актове.

Чл. 9. (1) За всеки потребител се създава "акаунт" (валидно потребителско име и парола), осигуряващ му идентификация и достъп до персоналния компютър и мрежовите ресурси, съобразно служебната необходимост.

(2) Потребителското име и паролата (акаунтът) се създава от администратора по информационната сигурност, съгласно одобрена процедура и/или писмена резолюция на административния ръководител и се предоставят лично на потребителя.

(3) Паролата се състои от не по-малко от 8 (осем) знака, съдържащи букви, цифри и символи. Паролата трябва да се сменя не по-рядко от веднъж на 6 месеца, което се изисква от потребителя автоматично.

(4) Всеки потребител използва само и единствено предоставеното му потребителско име и лична парола. Парола, станала известна на неоторизирано лице, трябва да се смени незабавно. Отговорност за смяната на паролата носи изцяло потребителят.

(5) Всеки потребител е отговорен за действията, извършени в компютърната и информационна среда на ПРБ с неговото потребителско име и парола, когато това се дължи на виновното му поведение.

Чл. 10. Съхраняване и защита на служебната информация

(1) На всеки потребител (или група потребители) се предоставя възможност за достъп до дисково пространство, намиращо се на файлов сървър, с оглед съхраняването и споделянето на служебни файлове.

(2) Съхраняването на служебна информация върху локалния диск на персоналния компютър крие рискове и не е препоръчително. Всеки потребител носи лична отговорност за съхранението и защитата от повреда и загуба на файловете и информацията, които се съхраняват на локалния твърд диск на персоналния компютър, предоставен за служебно ползване, чрез архивиране, поддържане на резервни копия и др.

(3) Преди бракуването на информационен актив/носител на информация или преди предаването му на друг орган/ ведомство наличната информация се изтрива с инструмент за необратимо изтриване на информацията.

Чл. 11. Всеки потребител има право на достъп до интернет и електронна поща при спазване на следните правила:

(1) За изпълнение на присъщите му служебни задължения или за други цели, в интерес на ПРБ. В случай на злоупотреба, правата за достъп до интернет на съответния потребител могат да бъдат ограничени или отнети.

(2) Забранен е достъпът (съответно действия с файлове) до сайтове с нецензурно и/или със съдържание, противоречащо на законодателството на Р България и Европейската общност. Това се отнася и до действия, чиито резултат представлява нарушение на споменатите законодателства. Забранено е ползването от служебните компютри на интернет радио, интернет телевизия, интернет видео, торент клиенти, P2P мрежи, софтуер за размяна на файлове по интернет, download (сваляне) на музика, филми, софтуер, освен при служебна необходимост.

(3) Администраторът по информационната сигурност има право да налага временни ограничения за достъп до сайтове, изтегляне (download) на файлове и други услуги, които могат да доведат до проблеми със сигурността или работоспособността на мрежата и/или предоставяните електронни услуги.

(4) Забранени са действия, които могат да доведат до проблеми със сигурността или работоспособността на външни мрежи, като например: действия, свързани със сканиране на портове на сървъри и/или мрежи, изпращане на множество заявки към сървър, с цел претоварването му, опити за преодоляване на защитни механизми на сървъри и/или мрежи и др.

(5) Разрешено е използването само на служебен e-mail на оторизирания сървър на ПРБ за служебна кореспонденция. Служебната електронна поща е сигурно и защитено средства за обмен на информация в рамките на ПРБ. При изпращане на чувствителна информация към адресати извън ПРБ, тя следва да се защити допълнително чрез криптиране. Забранено е пренасочването на служебната електронна поща към сървъри извън мрежата на ПРБ. Това важи и за пренасочването към публични сървъри за електронна поща със свободен режим на регистрация (например: hotmail.com, yahoo.com, gmail.com, abv.bg и други, независимо дали са в България, или не).

(6) Не трябва да се отварят електронни съобщения от неизвестен или съмнителен подател. При получаване на съмнителни електронни съобщения, да не се стартират посочените в тях линкове и да не се отварят прикачените към тях файлове. Препоръчително е такива съобщения незабавно да се изтриват.

Чл. 12. Работа с чувствителна служебна информация

(1) Външни носители (дискети, CD, DVD, Flash памети и др.), на които е записана чувствителна служебна информация в електронен вид, трябва да се съхраняват в заключващи се канцеларски шкафове или каси.

(2) Когато е необходима повишена сигурност, следва да се използва софтуер за криптиране и за изтриване на данните, съгласно препоръките на администратора по информационната сигурност.

(3) При необходимост, следва да се използват вградените функции на Microsoft Office за въвеждане на пароли за достъп до документи. В този случай потребителят сам носи отговорността за опазването на паролата като възстановяването на информацията при загуба на паролата е невъзможно.

Чл. 13. (1) За електронно подписване на служебни документи и достъп до електронни услуги, за които е необходима идентификация на потребителя, следва да се използва квалифициран електронен подпис, издаден по служебен път от ПРБ чрез лицензираните за тази дейност фирми в България.

(2) Персоналните удостоверения за електронен подпис са поименни и не се преотстъпват за ползване на други лица.

(3) Издаването на удостоверения за квалифициран електронен подпис (КЕП) става въз основа на заповед на административния ръководител, с която съответния служител се упълномощава да прави електронни изявления и да представлява Прокуратурата на РБ, в рамките на своите правомощия или за изпълнението на конкретна задача.

(4) Лицата, получили удостоверения за електронен подпис, са длъжни да ги съхраняват по подходящ начин, недопускащ кражби, изгубване или унищожаване на физическия носител (смарт/SIM карта), унищожаване или опити за унищожаване на данните, съдържащи се в сертификата, както и разкриване на информация (PIN/PUK код), осигуряващи достъп до частния ключ. При настъпване на някое от посочените събития

съответният служител е длъжен незабавно да уведоми в писмена форма прекия си ръководител и администратора по информационната сигурност.

(5) При прекратяване на трудовото или служебно правоотношение с лице, на което е било издадено КЕП, е длъжно да го предаде на материално отговорното лице.

Чл. 14. Всеки потребител е длъжен да ползва повереното му компютърно оборудване с грижата на добър стопанин и да спазва следните правила за експлоатация:

1. да не премества устройствата от определените им места;

2. да не поставя книги, хартия, дрехи, хранителни продукти, напитки и други предмети в близост до устройствата и върху тях, с оглед нормалното охлаждане на устройствата;

3. да не допуска попадане на чужди тела и течности в устройствата; при възникване на инцидент или повреда, потребителят веднага трябва да изключи устройството от електрическото захранване и да уведоми незабавно администратора по информационната сигурност и своя ръководител;

4. да не допуска прегъване, опъване, притискане и стъпване върху свързващите кабели;

5. да оказва съдействие на администратора по информационна сигурност за отстраняване на възникнали проблеми, диагностика и поддръжка на системите, включително с осигуряване на физически и отдалечен достъп до компютъра с всички необходими пароли (с изключение на случаите, когато това са пароли на директории с ограничен достъп);

6. да не ограничава по никакъв начин работата на софтуера за управление на работната станция и антивирусната защита;

7. да върне изцяло и в пълна изправност предоставената му техника и софтуер при прекратяване на служебното или трудовото правоотношение с ПРБ; след това потребителят получава подпис в обходния си лист от домакина на съответната прокуратура; административният ръководител, с подписването на обходния лист, удостоверява, че е приета цялата служебна информация в електронен вид.

Чл. 15. Потребителят няма право:

1. да отваря и променя конфигурациите на компютъра, монитора и другите устройства;

2. да променя настройките в хардуерния SETUP на компютъра (BIOS), системните настройки на операционната система, потребителския интерфейс и конфигурацията на компютъра, без съгласието на системния администратор. Това се отнася и за слагането на пароли в хардуерния SETUP (BIOS) на компютъра, както и всичко друго, което би могло да ограничи действията на администратора, в случай на отсъствие на потребителя;

3. да инсталира или позволява на друго лице инсталирането на софтуер и хардуер на компютъра, без съгласието на администратора по сигурността;

4. да използва компютър на друг служител, без изричното съгласие на титуляра или негов ръководител;

5. да включва външно оборудване към мрежата на прокуратурата без разрешение на администратора по сигурността;

6. при съвместно използване на принтери или други общи компютърни и мрежови ресурси, да заема изцяло или да ограничава използването им от други потребители;

7. да прави опити, или да подпомага такива, за неоторизиран достъп до мрежови ресурси, информация и база данни, компютри и други устройства (използване на чуждо потребителско име/парола; физически достъп до компютър, на който в момента е оторизиран друг потребител;

8. потребителят е длъжен да уведоми веднага администратора по информационната сигурност при съмнения за неоторизиран достъп.

Раздел IV
МЕРКИ ЗА ЗАЩИТА НА АИС И МРЕЖИ

Чл. 16. За осигуряване на компютърната защита на АИС/М, администраторът по сигурността предприема следните минимални задължителни мерки:

(1) НИВО „СТАНДАРТНО“

1. На потребителските компютри се инсталира операционна система MS Windows 7 или по-нова, която е в цикъл на поддръжка от производителя с инсталирани всички приложими обновявания, свързани със сигурността.
2. Конфигурира се ниво на достъп до ОС: потребител с ограничени права.
3. Конфигурира се автоматично заключване на персоналния компютър с парола след определен период на неактивност.
4. Системно се забранява стартирането от потребителя на изпълними файлове/скриптове извън разрешените.
5. Инсталира се антивирусна програма с централизирана поддръжка, обновена до най-новата версия.
6. За достъп до интернет се инсталира браузър MS Internet Explorer или алтернативен, обновен до най-новата поддържана версия.
7. Инсталира се офис пакет MS Office 2010 или по-нов или алтернативен пакет, който е в цикъл на поддръжка от производителя с инсталирани всички приложими обновявания, свързани със сигурността..
8. Инсталира се MS Outlook 2010 или по-нов или алтернативен клиент в цикъл на поддръжка от производителя с инсталирани всички приложими обновявания, свързани със сигурността, който достъпва пощенска кутия на сървър, поддържан от ПРБ.
9. Конфигурира се пълна забрана за инсталиране на добавки и разширения на браузърите и приложенията от потребител.
10. Системно се ограничава достъпа до интернет сайтове с нецензурно/нелегално/опасно съдържание според техническите възможности.
11. Осигурява се централизиран мениджмънт и контрол на обновяването на всички компоненти на ОС и приложенията, за които производителят им предлага такива, свързани със сигурността.
12. Конфигурира се софтуерна защитна стена на всеки компютър.
13. Ограничава се чрез парола достъпа до BIOS.

(2) НИВО „ВИСОКО“

1. Предприемат се всички мерки от ниво „СТАНДАРТНО“, както и:
2. Осигурява се криптиращ софтуер, който е одобрен за служебно ползване.
3. Осигурява се софтуер за сигурно изтриване на документи;
4. Системно се ограничава достъпа до USB устройства за съхранение на данни;
5. Браузърът се конфигурира в режим „Максимална защита“, вкл. забрана за изпълняване на код върху клиента и сваляне на файлове, с изключение на списък с разрешени сайтове, който се актуализира от администратора по информационната сигурност.

6. Системно се забранява се изпълнение на макроси и ActiveX контроли.
7. Системно се ограничава инсталирането на Flash Player.

(3) НИВО „НИСКО“

1. Операционна система и права за достъп до ОС: според нуждите.
2. Осигурява се актуална антивирусна програма,
3. Ограничават се правата само до „четене“ при достъп до папки, споделени с потребители с по-високи нива на сигурност („СТАНДАРТНО“ и „ВИСКО“).

(4) Информацията, съхранявана на мобилни компютри с ниво на сигурност „Стандартно“ или „Високо“, задължително се криптира.

Чл. 17. (1) За осигуряване на физическата защита на информационните ресурси и системи, ръководството на всяка прокуратура предприема следните минимални задължителни мерки:

1. Изготвяне на списък на помещенията, в които е инсталирана компютърна техника.
2. Регламентиране и контролиране на достъпа на магистрати и служители до помещенията по т.1.
3. Определяне на служители, които имат право на достъп до сървърните помещения и/или комуникационни/сървърни шкафове;
4. Регламентиране на достъпа на външни лица до работните помещения, сървърните помещения и комуникационните/сървърните шкафове;
5. Включване на помещенията с контролиран достъп в общата система за охрана;
6. Организиране на системата за контрол на физическия достъп по възможност да включва използването на пропускателен режим, сигналноохранителна техника, визуално наблюдение на сградния фонд, сървърните и работните помещения;
7. Изграждане на комуникационната инфраструктура и мрежите така, че лицата намиращи се в сградата да нямат пряк достъп и да не могат да извършват незабелязани манипулации по тях;
8. Предприемане на действия относно пожарната безопасност на хардуерните ресурси, чрез изграждане на пожароизвестителна система;
9. Гарантиране на нормална работна температура на хардуерните ресурси, като при необходимост се изгражда климатизация на помещението/ята.
10. Гарантиране на непрекъсваемостта на електрическото захранване на сървърните и комуникационните устройства;
11. Създаване на ред за действие на служителите при възникване на извънредна ситуация (пожар, наводнение и др.).

Чл. 18. Техническо обслужване на информационните активи:

(1) Инсталирането на компютърните конфигурации, системните и приложните програми, както и следващите промени в тях се прави само от определения служител или упълномощените за това фирми - доставчици на компютърна, периферна техника и програмни продукти, но задължително в присъствие на администратора по сигурността.

(2) Гаранционното обслужване на техниката се извършва само от упълномощените за това фирмени сервизи.

(3) Внасянето и изнасянето на компютърна и периферна техника от сградата на прокуратурата става в присъствието на определен служител, отговорен за материалните активи, а ако те са в експлоатационен режим и уведомяване на администратора по информационната сигурност.

ДОПЪЛНИТЕЛНА РАЗПОРЕДБА

§ 1. По смисъла на тези правила:

1. "Автоматизирана информационна система" (АИС) е съвкупност от технически и програмни средства, методи, процедури и персонал, организирани за осъществяване на функции по създаването, съхраняването, обработването, ползването и обмена на електронна информация в границите на системата.
2. „Автоматизирана информационна мрежа" (или само „мрежа") е съвкупност от технически и програмни средства, методи и ако е необходимо, персонал и процедури, организирани за осъществяване обмен на данни (информация) между две или повече АИС или в рамките на една АИС.
3. „Антивирусен софтуер" е компютърна програма за защита от вируси, извършва сканиране за наличие на вируси в реално време на всички потенциално опасни файлове и приложения .
4. „Интранет" е вътрешноведомствена интернет-базирана информационна мрежа.
5. „Непрекъсваеми токозахранващи устройства" (UPS) са устройства, осигуряващи нормално изключване на персоналния компютър при спиране на електрозахранването.
6. „Операционна система" е системно програмно осигуряване, осигуряващо взаимодействието между хардуера на компютъра и приложното програмно осигуряване
7. „Персонална електронна поща" е уникален e-mail адрес от вида username@subdomain.dom, съвместим с използвания в интернет Simple Mail Transfer Protocol (SMTP).
8. „Персонален компютър" или „Работна станция" е съвкупност от хардуер и софтуер предназначени за обработка на информация от един потребител, може да бъде свързан в локална мрежа и да ползва мрежови ресурси.
9. „Сървър" е устройство, предоставящо мрежови услуги на други членове на локалната и/или глобалната мрежа; според ролята, която изпълнява, той може да бъде мрежови, файлов, принт, пощенски сървър.
10. „Хардуер" са всички електронни и електрически компоненти, съставляващи един персонален компютър.
11. „Информационен актив" по смисъла на НАРЕДБА ЗА ОБЩИТЕ ИЗИСКВАНИЯ ЗА ОПЕРАТИВНА СЪВМЕСТИМОСТ И ИНФОРМАЦИОННА СИГУРНОСТ /НОИОСИС/ са материалните и нематериалните активи и информационни обекти, свързани с информационните системи, които имат полезна стойност за определена администрация
12. „Информационен ресурс" са тази част от информационните активи, които оказват критично въздействие върху функционирането на информационната инфраструктура
13. „Информационна услуга" са всички услуги, които се прпедоставят чрез информационните ресурси и които са предназначени за достъп, обраотка и съхраняване на информация, достъп до вътрешни и външни информационни ресурси, достъп и оперирane с електронни форми, документи, електронна поща и интернет, достъп до външни информационни услуги
14. „Информационна инфраструктура" - съвкупност от информационен актив, ресурс и услуга

15. „Комуникационна инфраструктура“ - съвкупност от пасивно /розетки, свързващи кабели, комутационни панели и др./ и активно оборудване /комутатори, маршрутизатори, концентратори, модеми и др./, чрез които се осъществява контролируем, защитен и надежден обмен на данни, както в структурата, така и между ПРБ и външни структури и интернет пространство
16. „Хардуерни ресурси“- сървъри, работни станции, мрежово оборудване, периферни устройства - принтери и скенери

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. В срок до 3 месеца от одобрението на тези правила, прокуратурите са задължени да изпълнят мерките за защита.

Приложение № 1

Софтуер, стандартно инсталиран на всеки персонален компютър, включен в компютърната мрежа на ПРБ

1. Операционна система: MS Windows 7 или по-нова.

2. Офис пакет MS Office 2010 или алтернативен.

3. Програма за антивирусна защита

4. Софтуер за визуализиране на документи във формат "pdf"

5. Интернет браузър: Internet Explorer и/или алтернативни

6. Програма за възпроизвеждане на звук и видео: Windows Media Player, VLC

7. Софтуер за записване върху DVD/CD – за компютри, на които има записващо устройство

8. Специализиран приложен софтуер, в съответствие с конкретни служебни задължения (напр. счетоводен софтуер)

9. Препратки към програмни продукти за общо ползване с мрежови инсталации (напр. правноинформационни системи "Апис", "Сиела")