



РЕПУБЛИКА БЪЛГАРИЯ

Министерство на земеделието, храните и горите
Изпълнителна агенция по селекция и
репродукция в животновъдството



ЗАПОВЕД

№ ЦУ-РД 9-148/14.09.2021г.

На основание чл. 8, от Устройствения правилник на Изпълнителна агенция по селекция и репродукция в животновъдството и във връзка с чл. 4 от Закона за киберсигурността и чл. 1, ал. 1., т. 5, ал. 2 и чл. 4 от Наредбата за минималните изисквания за мрежова и информационно сигурност

УТВЪРЖДАВАМ:

1. Вътрешни правила за информационна и мрежова сигурност на изпълнителна агенция по селекция и репродукция в животновъдството.
2. Всички служители да бъдат запознати с Вътрешни правила за информационна и мрежова сигурност на изпълнителна агенция по селекция и репродукция в животновъдството.

Контрол по изпълнението на заповедта възлагам на Бонка Чолакова, главен секретар.

зооинж. ГЕОРГИ ЙОРДАНОВ
Изпълнителен директор

БЧ/IASРЖ



РЕПУБЛИКА БЪЛГАРИЯ

Министерство на земеделието, храните и горите

Изпълнителна агенция по селекция и
репродукция в животновъдството

утвърди
ЗООИНЖ. ГЕОРГИ МЕДАНОВ
изпълнителен ДИРЕКТОР
СОС



ВЪТРЕШНИ ПРАВИЛА

ЗА ИНФОРМАЦИОННА И МРЕЖОВА СИГУРНОСТ НА ИЗПЪЛНИТЕЛНА АГЕНЦИЯ ПО СЕЛЕКЦИЯ И РЕПРОДУКЦИЯ В ЖИВОТНОВЪДСТВОТО

РАЗДЕЛ I ОБЩИ ПОЛОЖЕНИЯ

Чл. 1.(1) С настоящите Вътрешни правила за мрежова и информационна сигурност, наричани по-долу „Правилата”, се определят необходимите технически и организационни мерки за защитата на информационните мрежи и системи, както и информационния обмен между териториалните звена на дирекциите в Изпълнителна агенция по селекция и репродукция в животновъдството (IASРЖ, Агенцията).

(2) Правилата са разработени в съответствие със Закона за киберсигурност, Закона за електронното управление и Наредбата за минималните изисквания за мрежова сигурност (приета с ПМС № 186 от 26.07.2019 г. и имат за цел осигуряването на контрол и управление на работата на информационните системи в Агенцията. В този смисъл понятието информационна система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни и обслужващ персонал, като компютрите могат да бъдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез съответните устройства и програми.

Чл.2. (1) Правилата са част от политиката за мрежова и информационна сигурност на Агенцията и целят защитата на информационните мрежи и системи срещу неправомерен

или случаен достъп, използване, правене достояние на трети лица, промяна или унищожаване, доколкото такива събития или действия могат да нарушият достъпността, автентичността, целостта, интегритета и конфиденциалността на съхраняваните или предаваните данни, а също така на предоставяните електронни услуги, свързани с тези мрежи и системи.

(2) Информационните активи на ИАСРЖ са:

1. хардуерните устройства;
2. софтуерните продукти;
3. информационните системи;
4. комуникационната инфраструктура

(3) Потребителите на информационни активи в Агенцията са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 3. Проектирането и изграждането на информационни и комуникационни системи се извършва така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда и при спазване на Наредбата за минималните изисквания за мрежова сигурност (Приета с ПМС № 186 от 26.07.2019 г.).

РАЗДЕЛ II

ОРГАНИЗАЦИЯ НА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ

Чл.4.(1) Изпълнителният директор взема необходимите документирани решения, чрез утвърждаването на политики, правила и процедури за осигуряване на необходимата инфраструктура за гарантиране на мрежовата и информационна сигурност на използваните информационни мрежи и системи.

(2) Отговорностите на служителите по информационни технологии за гарантиране на мрежовата информационна сигурност на използваните информационни мрежи и системи се определят в длъжностните им характеристики или работни планове, както и на друго документирано основание.

(3) Изпълнителният директор със заповед определя служител по информационни технологии от общата администрация, който да отговаря за мрежовата и информационна сигурност.

(4) Изпълнителният директор възлага на Главния секретар контрола по изпълнението на взетите документирани решения за гарантиране на мрежовата и информационна сигурност на използваните информационни мрежи и системи.

Чл.5.(1) Служителят отговарящ за мрежовата и информационна сигурност създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща на служителите в администрацията и специализираните дирекции на Агенцията.

(2) Ползването на компютърната мрежа и електронна поща от служителите става, чрез получаване на потребителско име и парола.

РАЗДЕЛ III

ПРАВА И КОНТРОЛ НА ДОСТЪП И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл. 6. (1) При назначаване на нов служител или служител по заместване на длъжност, при която в длъжностната му характеристика са отразени задължения и отговорности с право на въвеждане, обработка и съхранение на електронна информация, служителят по Човешки ресурси не по късно от 3 работни дни преди назначаване, уведомява директора на дирекция АПФСИО за служител в общата администрация или Главните директори на ГД ККРД и ГД УГРРП за служител в специализираната администрация.

(2) При прекратяване на служебното (трудово) правоотношение между ИАСРЖ и определен служител, служителят по Човешки ресурси не по късно от 3 работни дни преди датата на прекратяване, уведомява директора на дирекция АПФСИО.

(3) Информация за възникване, изменение и прекратяване на потребителските акаунти се предоставя посредством одобрена от Главния секретар докладна на:

1. Главните директори на ГД ККРД и ГД УГРРП за служителите в специализираната администрация;

2. Директора на дирекция „АПФСИО“ за служителите от общата администрация.

(4) Докладната съдържа имената на служителя, длъжността и мястото в йерархията на дирекцията, както и специализираните информационни системи, до които следва да бъде предоставен, изменен или прекратен достъпа.

(5) На база одобрена докладна по ал.4, служителят отговарящ за мрежовата и информационна сигурност по чл.4, ал.3 създава потребителско име и парола за работа с компютърната мрежа на служителя, съгласно правата му на достъп до определени ресурси, или с изтичане на работния ден предхождащ прекратяване на правоотношенията, прекратява правата на достъп до мрежовите ресурси на Агенцията и електронната поща. При необходимост се пристъпва до преинсталация на компютъра.

Чл. 7. (1) Всеки служител има точно определени права на достъп и използва уникален потребителски профил за вход в системата и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили.

(2) Предоставянето на достъп става по дефиниран вътрешен ред, като се задават определени права на достъп до конкретни информационни ресурси, според заемната длъжност и функция. Не се задава и не се осигурява достъп на неоторизирани лица.

(3) Новите служители се инструктират относно спазването на политиката за мрежова и информационна сигурност на Агенцията, както и относно настоящите Правила от служителя отговарящ за мрежовата и информационна сигурност.

Чл.8. Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:

1. Разделяне на потребителски от администраторски функции;
2. Установяване на нива на достъп до информация;
3. Регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;
4. Техниката да се използва изключително и само за служебни цели;

5. Не се позволява инсталирането на какъвто и да е нов и реконфигурирането от потребителите на вече инсталиран софтуер и хардуер, както и самостоятелни опити за поправка или подобрения на горепосочените. При съмнение за възникнал проблем незабавно се уведомява експерт информационни технологии, който от своя страна уведомява директора на дирекция АПФСИО;

6. Използването на внесени отвън информационни носители (оптични дискове, флаш памети и др.) става при условие, че първо те се сканират за наличието на вируси. Ако антивирусният софтуер намери такива, носителите не се използват;

7. Не се допускат външни лица до комуникационните отделения и техниката за интернет връзка, с изключение на техници от оторизирани фирми и то само придружени от експерт информационни технологии;

8. Не се допуска достъпа на външни лица до компютърната техника в кабинетите в сградата на ИАСРЖ;

9. Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели;

10. Паролите за достъп на служителите, описани по видове и приложения се съхраняват при лицето отговарящо за мрежовата и информационна сигурност.

11. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 9. (1) Лицата, които обработват лични данни, използват уникални пароли с достатъчна сложност, които не се записват или съхраняват онлайн.

(2) Всички пароли за достъп на системно ниво се променят периодично.

(3) Всички носители на лични данни се съхраняват в безопасна и сигурна среда с ограничен и контролиран достъп.

Чл. 10. На служителите на Агенцията, които използват електронни бази данни и техни производни се забранява:

1. да ги изнасят под каквато и да е форма извън служебните помещения преди извеждане от деловодството (извършване на услуга);

2. да ги използват извън рамките на служебните си задължения;

3. да ги предоставят на външни лица без да е заявлена услуга.

Чл. 11. За нарушение целостта на данните се считат следните действия:

1. унищожаване на бази данни или части от тях;

2. повреждане на бази данни или части от тях;

3. вписване на невярна информация в бази данни или части от тях.

Чл. 12. При изнасяне на носители извън физическите граници на Агенцията, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 13. На служителите е строго забранено да използват служебни мобилни/компютърни средства на места, където може да възникне риск за средството и информацията в него.

Чл. 14. Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Чл. 15. След като повече не са необходими, носителите се унищожават сигурно и безопасно с цел намаляване на риска от изтичане на чувствителна информация към неупълномощени лица. Предварително се проверят, за да е сигурно, че необходимата информация е копирана и след това цялата информация е изтрита от тях преди унищожаване.

РАЗДЕЛ IV

РАБОТНО МЯСТО

Чл. 16. (1) Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

(2) Работното място се оборудва при спазване изискванията на Наредба №7 от 15.08.2015 г. за минималните изисквания за осигуряване на безопасни условия на труд при работа с видеодисплеи.

(3) Сървъра на локални компютърни мрежи се разполага в самостоятелно помещение.

Чл. 17. Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталиирани на компютъра на неговото работно място, съобразно дадените му права.

Чл. 18. Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни се осъществява от него с въвеждането на потребителско име и парола.

Чл. 19. Забранява се на външни лица да работят с персоналните компютри на Агенцията, освен в следните случаи:

1. упълномощени фирмени специалисти да извършват първоначална инсталация на компютърна и периферна техника, програми, активни и пасивни компоненти на локални компютърни мрежи, комуникационни устройства и сервизна намеса на място, но задължително в присъствие на служител по информационни технологии;

2. провеждане на обучения от външни специалисти след разрешението на изпълнителния директор на ИАСРЖ и задължително в присъствието на експерт информационни технологии.

Чл. 20. След края на работния ден всеки служител задължително изключва компютъра, на който работи.

Чл. 21. При загуба на данни или информация от служебния компютър служителят незабавно уведомява експерт информационни технологии, който незабавно оказва съответната техническа помощ.

Чл. 22. Забраняват се опити за достъп до компютърна информация и бази данни, до които не са предоставени права, съобразно заеманата от служителя длъжност, както и извършването на каквито и да е действия, които улесняват трети лица за несанкциониран достъп.

Чл. 23. Инсталиране и разместяване на компютърни конфигурации и части от тях, на периферна техника, на активни и пасивни компоненти на локални компютърни мрежи,

на комуникационни устройства се извършва само след съгласуване с директора на дирекция АПФСИО и главния секретар.

Чл. 24. Забранява се използването на преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на ИАСРЖ.

Чл. 25. Служителите имат право да обменят компютърна информация посредством вътрешна компютърна мрежа само във връзка с изпълнение на служебните си задължения и само със служителите, с които имат преки служебни взаимоотношения.

Чл. 26. Архивирана компютърна информация се предоставя само на служителите, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача.

Чл. 27. Достъпът до компютърна информация, бази данни и софтуер се ограничава посредством технически методи – идентификация на потребител, пароли, отчитане на времето на достъп, забрани за копиране, проследяване на несанкциониран достъп.

Чл. 28. (1) Достъпът до помещението с комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

(2) Всички комуникационни шкафове се заключват, като ключовете от тях се съхраняват при директор АПФСИО.

(3) В помещение, където се съхраняват електронни база данни и програмни продукти на магнитни и магнитно-оптични носители, оставането на служителите в извън работно време става само при възложена конкретна задача, за чието изпълнение оставането е наложително, при спазване разпоредбите за достъп в сградата на Агенцията.

РАЗДЕЛ V

ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 29. (1) За общо ползване от администрацията на Агенцията и от териториалните звена е предвидена деловодна система с права на достъп съгласно длъжностните характеристики на служителите и вменените им със заповед на изпълнителния директор задължения.

(2) Публикуване на интернет страницата на Агенцията на информация относяща се до дейността на Агенцията и на Развъдните организации се извършва от служител по информационни технологии или определен друг служител определен със заповед на изпълнителния директор.

Чл. 30. Ползването на компютърната мрежа и електронни платформи АКСТЪР, ИАСРЖ КОНТРОЛ, СЕБРА, WORKFLOW, ОМЕКС, АЖУР и други счетоводни програми от служителите става чрез получени потребителско име и парола.

Чл. 31. Ползването на интернет и служебна електронна поща се ограничават съобразно скоростта на ползвания достъп до интернет, броя на откритите работни места и необходимостта от ползване на тези услуги съобразно служебните задължения на служителите.

Чл. 32. Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронните платформи при използване на предоставените им потребителски имена и пароли.

Чл. 33. Забранява се свързването на компютри едновременно в мрежата на Агенцията и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на ИАСРЖ и/или е в противоречие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност.

Чл. 34. (1) Компютрите, свързани в мрежата на ИАСРЖ, използват интернет само от доставчик, с когото Агенцията има сключен договор за доставка на интернет.

(2) Фирмата, доставчик на интернет услугата може да предостави, в случай на нужда от страна на Агенцията, необходимите мрежови комутатори, VLAN, рутери, защитни стени, VPN.

(3) Експерт информационни технологии на ИАСРЖ и фирмата доставчик на интернет услугата съвместно избират техническите устройства, извършват необходимите настройки за достъп до интернет, разделят логически локалната мрежа.

Чл. 35. Използването на комуникатори (skype, facebook, messenger, viber, zoom и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на Агенцията и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите, свързани в компютърната мрежа на ИАСРЖ, да е ограничено и единствено и само за служебна цел.

Чл. 36. Забранява се съхраняването на компютрите на ИАСРЖ на лични файлове с текст, изображения, видео и аудио.

Чл. 37. Забранява се отварянето без контрол от страна на експерт информационни технологии на:

1. получени по електронна поща или на преносими носители изпълними файлове, файлове с мобилен код и файлове, които могат да предизвикат промени в системната конфигурация, напр. файлове с разширения .exe, .vbs, .reg и архивни файлове;

2. получени по електронна поща съобщения, които съдържат неразбираеми знаци.

Чл. 38. Не се толерира влизането в интернет сайтове с неизвестно съдържание.

РАЗДЕЛ VI

ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 39. С цел антивирусна защита се прилагат следните мерки:

1. всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява.

2. експерт информационни технологии извършва следните дейности:

а/ активира защитата на съответните ресурси – файлова система, електронна поща и извършва първоначално пълно сканиране на системата;

б/ настройва антивирусния софтуер за периодични сканирания през определен период;

в/ активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на системата;

г/ проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер.

3. при поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително и незабавно информира експерт информационни технологии, който от своя страна уведомява директора на дирекция АПФСИО.

РАЗДЕЛ VII

НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл. 40. Следните мерки се прилагат с цел антивирусна защита:

1. всички устройства за съхранение на данни да са свързани към устройство за непрекъсваемост на ел. снабдяването.

2. при липса на ел. захранване за повече от 10 (десет) минути, експерт информационни технологии започва процедура по поетапно спиране на устройствата за съхранение на данни.

3. при срив в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация.

РАЗДЕЛ VIII

СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

ЧЛ. 41. (1) Всеки служител, който работи с класифицирана информация, осигурява автоматично създаване на архивни копия всекидневно.

(2) Информацията, включително тази, съдържаща лични данни, се резервира по следните начини:

1. автоматизирано и планово се извършва архивиране на цялата работна информация на запаметяващите устройства и дисковите масиви.

2. архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг компютър и да се продължи работният процес без чувствителна загуба на данни.

(3) определеният по чл.4, ал.3 служител се грижи за изготвяне на резервни копия от важна информация за дейността на Агенцията, а в определени случаи за възстановяване на основни данни при хардуерен, софтуерен или потребителски срив.

РАЗДЕЛ IX

ОЦЕНКА И УПРАВЛЕНИЕ НА РИСКА

Чл. 42. (1) С настоящите Правила се определят основните действия по управление на риска за мрежовата и информационна сигурност в Агенцията, както и идентифициране на потенциалните рискови фактори във връзка с нея.

(2) Рискът за сигурността се определя като фактическо състояние, създаващо заплахи за уязвяване на един или няколко информационни актива, което предизвика тяхното повреждане или унищожаване.

Чл. 43. Оценката на риска се дефинира, чрез определяне на вероятността за уязвяване въз основа на ефективността на съществуващите или планирани мерки за сигурност.

Чл. 44. Заплахите за мрежовата и информационна сигурност се класифицират по следните критерии:

1. по елементите на мрежовата и информационната сигурност (достъпност, автентичност, цялостност и конфиденциалност), към които са насочени;
2. по компонентите на информационната система (апаратура, софтуер, данни, поддържаща инфраструктура), към които са насочени;
3. по начина на осъществяване (случайни или преднамерени действия, от природен или технологичен характер, човешки грешки и други);
4. по разположението на източника — вътре или извън информационната система.

Чл. 45. Действията по управление на риска обхващат оценка на неговия размер, изработване на ефективни и икономични мерки за неговото снижаване и оценка дали резултативният риск е в приемливи граници. Управлението на риска се извършва, чрез последователно прилагане на два типа циклично повтарящи се действия:

1. оценка (преоценка) на риска;
2. избор на ефективни и икономични средства за неговата неутрализация.

Чл. 46. При идентифициране на риска се предприема едно от следните действия:

1. ликвидиране на риска, чрез отстраняване на причиняващите го обстоятелства;
2. намаляване на риска, чрез използване на допълнителни защитни средства;
3. приемане на риска и разработване на план за действия в обстановка на риск.

Чл. 47. Процесът на управление на риска включва следните етапи:

1. идентификация на информационните активи;
2. анализ на заплахите и последствията от тях, откриване на уязвимите места в защитата;
3. оценка на рисковете и избор на защитни мерки;
5. реализация и проверка на избраните мерки;
6. постоянен контрол, мониторинг и адаптиране на системите към новите уязвимости и заплахи.
7. оценка на остатъчния риск, в случаите когато той не удоволетворява ръководството на Агенцията. Остатъчния риск се провежда минимум веднъж годишно.

Чл. 48. Потенциалните рискови фактори за мрежовата и информационната сигурност, които могат да застрашат достъпността, автентичността, целостта и конфиденциалността, са както следва:

1. подслушване, изразяващо се в достъп до служебна информация, чрез прихващане на електронни съобщения;
2. нежелан код, който може да доведе до загуба на конфиденциалността чрез записване и разкриване на пароли;
3. маскиране на потребителската идентичност може да доведе до заобикаляне на проверка за достоверност и всички услуги свързани с нея;
4. погрешно насочване или пренасочване на съобщенията може да доведе загуба на конфиденциалност, ако се осъществи нерегламентиран достъп до трети лица;
5. софтуерни грешки могат да застрашат конфиденциалността, ако софтуерът е създаден с контрол на достъпа или ако той осигури нежелан достъп до информационната система на Агенцията.
6. допуснати грешки при поддръжката на системата;
5. нерегламентиран достъп до информационните активи, повреждане, кражба и злоупотреба с тях;
7. грешки при предаването на информация;
8. употреба на нерегламентирани програми и информация;
9. потребителски грешки могат да наручат достъпността, чрез неумишлено или умишлено действие;
10. претоварване на комуникационния трафик може да доведе до нарушаване достъпността до обмен или въвеждане на данни;
11. природни бедствия, технически аварии и аварии в комуникационното оборудване, аварии в електрозахранването и климатичните инсталации, и външни въздействия с огън, вода, химикали и други могат да доведат до унищожаване на данни в информационната система.

Чл.49. (1) Идентифицирането, оценката и управлението на рисковете за мрежовата и информационна сигурност се извършва както следва в следната последователност:

1. определеният по чл.4, ал.3 служител съвместно със специалистите информационно обслужване идентифицират риска и отстраняват причиняващите го обстоятелства;
2. при идентифициран риск, определеният по чл.4, ал.3 служител съвместно със специалистите информационно обслужване и началник отделите/в случаите на риск в териториалните звена/, анализират и оценяват общото състояние на информационната структора и изготвят предложение до изпълнителният директор за възможните за предприемане конкретни защитни мерки;
3. при идентифициран, анализиран и оценен риск, определеният по чл.4, ал.3 служител разработва план за действие в обстановка на риск на база конкретни предложения, който се представя пред изпълнителния директор за одобрение;

4. изпълнителният директор приема действия за изпълнение и контрол на плана за работа при условията на рисък или за предотвратаване конкретни рискове за мрежовата и информационна сигурност.
- (2) Определеният по чл.4, ал.3 служител, създава и поддържа Регистър с рисковете приложими за информационните активи описани в Агенцията.

РАЗДЕЛ X

МЕРКИ ЗА НАЛАГАНЕ НА ИНФОРМАЦИОННА СИГУРНОСТ И ДИСЦИПЛИНАРНА ОТГОВОРНОСТ

Чл.50. Административни (организационни, процедурни) мерки. Тези мерки включват:

1. одобрени правила, процедури и указания. Те информират персонала, какво трябва и какво не трябва да прави при всекидневната си работа.
2. забрана за инсталлиране на програмни продукти и изнасяне на файлове с документи и други данни без разрешението на изпълнителният директор.
3. съгласие и информираност за работа с конфиденциална информация.
4. подбор на персонала - при назначаване на нови служители да се взима под внимание и риска от злонамерени действия.

Чл.51. Технически (логически) мерки. Те включват:

1. използване на надежден софтуер.
2. мониторинг, контрол и управление на достъпите до информацията в компютърните системи.
3. сигурност на паролите, която включва:
 - а) да не се използват рождения дати, имена, смислени думи;
 - б) паролата да е комбинация от букви и цифри, малки и главни букви и да е дълга поне 8 символа;
 - в) паролата да е лесна за запомняне от потребителя, да не се записва на хартия;
 - г) служителите периодично да сменят паролите си.
5. използване на електронен подпис.
6. криптиране на файловете.
7. архивиране и възстановяване.
8. предприемане на адекватна защита от вреден софтуер.
9. при установяване на смущения в информационните системи да се предприемат следните стъпки:
 - а) установяване на причината;
 - б) установяване на връзка с определеният служител по чл.4, ал.3 и при необходимост с доставчика на Интернет услугата и Националния екип за реагиране при инциденти с компютърната сигурност към ДАЕУ.

Чл.52. Физически мерки. Тези мерки включват контрол над работната среда, чрез осигуряване на:

1. сигурни зони - зони с контролиран достъп. Не се допускат външни лица без придружител в кабинетите на изпълнителния директор, главния счетоводител и помещението, където се съхраняват електронни база данни и програмните продукти.
2. физическа сигурност - заключване на кабинетите.
3. механизъм за контрол и физическа защита на кабелната система, комуникационното оборудване, сървърите от неоторизиран достъп се извършва чрез осигуряване на пропускателен режим или видеонаблюдение..
4. защита от повреда или срив в електрозахранването с осигурени UPS устройства.

Чл. 53. Дисциплинарна отговорност носят служителите на Агенцията при:

1. умышлено въведени неверни данни;
2. създадени условия за разпространение на невярна информация;
3. умышлено унищожена служебна информация;
4. неизпълнение на настоящите правила.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Настоящите правила са разработени съгласно Наредбата за минималните изисквания за мрежова сигурност (приета с ПМС № 186 от 26.07.2019 г.).

Ръководителите и служителите в Изпълнителна агенция по селекция и репродукция в животновъдството са длъжни да познават и спазват разпоредбите на тези правила.

§2. За неуредени в тези правила въпроси по отношение на мрежовата и информационна сигурност в Агенцията, се изпълняват разпоредбите на действащото законодателство в Република България.

§3. Правилата се разглеждат и оценяват периодично с оглед тяхната ефективност като могат да се допълват и изменят с цел прилагане на допълнителни целесъобразни мерки и процедури за защита на информацията. Допълненията и измененията се извършват само със заповед на изпълнителния директор на ИАСРЖ.

§4. Указания и текущ контрол по приложението и изпълнението на настоящите вътрешни правила се осъществява от директора на дирекция АПФСИО и главния секретар на ИАСРЖ

§5. Настоящите правила влизат в сила от деня на утвърждаването им със Заповед № ЦУ-РД 9-148/14.09.2021г. на изпълнителния директор на ИАСРЖ.