РЕПУБЛИКА БЪЛГАРИЯ
Министерство на земеделието, храните и горите
Областна дирекция "Земеделие" гр. Ловеч

З А П О В Е Д
№ РД-04-39
гр. Ловеч, 01.04.2019 г.

На основание чл.3, ал.3, т.24 и ал.4 и чл.26 от Устройствения правилник на Областните дирекции „Земеделие"

УТВЪРЖДАВАМ:

Вътрешни правила за повишаване нивото на мрежова и информационна сигурност в Областна дирекция „Земеделие" Ловеч.

Правилата са задължителни за прилагане от служителите на Областна дирекция „Земеделие" Ловеч и служителите на Общинските служби по земеделие на територията на област Ловеч като териториални звена.

Възлагам изпълнението на настоящата заповед на директорите на дирекции в Областна дирекция „Земеделие" Ловеч и началниците на ОСЗ.

Контролът по изпълнението на заповедта ще упражнявам лично.

Настоящата заповед да се връчи на главния секретар, директора на дирекция „АПФСДЧР" , Главна дирекция „Аграрно развитие" и началниците на Общинските служби по земеделие .

ДИЯНА РУСКОВА / П /
Директор на ОД"Земеделие" Ловеч

УТВЪРЖДАВАМ: /П/ Приложение към Заповед №РД-04-39/01.04.2019г.

ДАТА: 01.04.2019г.

ДИЯНА РУСКОВА

ДИРЕКТОР НА

ОБЛАСТНА ДИРЕКЦИЯ „ЗЕМЕДЕЛИЕ” –

ГР. ЛОВЕЧ

ВЪТРЕШНИ ПРАВИЛА

ЗА ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОБЛАСТНА ДИРЕКЦИЯ „ЗЕМЕДЕЛИЕ“ – ЛОВЕЧ

гр. ЛОВЕЧ
2019 година

РАЗДЕЛ I
ОБЩИ ПОЛОЖЕНИЯ

Чл.1. Настоящите правила имат за цел осигуряването на контрол и управление на работата на информационните системи в ОД „Земеделие“ – Ловеч (ОДЗ Ловеч). 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. Програмните продукти и БД са специфични за всяко звено от дирекцията и с общо предназначение.

Чл.2. Потребителите на информационните системи в ОДЗ Ловеч 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 възможности за интеграция в единна потребителска среда и при спазване на Наредбата за общите изисквания за мрежова и информационна сигурност (ЗАГЛ. ИЗМ. – ДВ БР. 5 от 2017г., в сила от 01.03.2017г.).

ЦЕЛ

Чл.4. Целта на тези правила е да се осигури необходимото ниво на защита на базите с данни (БД) от съответните заплахи към тях, без оглед на тяхната природа, дали са породени от вътрешни или външни за организацията източници, умишлени или случайни.
Чрез прилагането на описаните правила се цели да се постигне:

1. Предпазване от нерегламентиран вътрешен или външен достът до БД с цел повреждане, модифициране или унищожаване на данни;
2. Недопускане на кражба или източване на информация от БД, както и използването й за лични облаги;
3. Предпазване от случайна, преднамерена и/или по непредпазливост промяна или загуба на данни;
4. Предпазване от увреждане или унищожаване на информация при експлоатационните процеси в организацията;
5. Предотвратяване на загуби на информация при съхранението и преноса на БД на външни устройства;
6. Постигане и поддържане на оторизирания достъп до наличност на информацията в БД за упълномощени потребители, процеси и/или приложения, без прекъсване на работните процеси;
7. Спазване на националните законови и подзаконови изисквания за защита на различните типове информация;
8. Непрекъснатост на дейностите по оценка и анализ на заплахите, уязвимостта и свързаните с тях рискове към сигурността на БД;
9. Предотвратяване на загуба на данни, в следствие на други въздействия като пожар, наводнения, стихийни бедствия, аварии и други.

РАЗДЕЛ II
КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл.5. 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. Осъществяването на контрол от служители на ОДЗ Ловеч.

Чл.6. 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 ползването на групови профили.

Чл.7. Предоставянето на достъп става по дефиниран вътрешен ред, като се задават определени права за достъп до конкретни информационни ресурси, според заеманата длъжност и функция. Не се задава и не се осигурява достъп на неоторизирани лица.

Чл.8. Лицата, които обработват лични данни, използват уникални пароли с достатъчна сложност, които не се записват или съхраняват онлайн. Всички пароли за достъп на системно ниво се променят периодично.

Чл.9. Всички носители на лични данни се съхраняват в безопасна и сигурна среда – в заключени шкафове, с ограничен и контролиран достъп.

Чл.10. На служителите на ОДЗ Ловеч, които използват електронни БД и техните производни (текстове, разпечатки, карти и скици) се забранява:

1. Да ги изнасят под каквато и да е форма извън служебните помещения преди извеждането от деловодството (извършване на услугата);
2. Да ги използват извън рамките на служебните си задължения;
3. Да ги предоставят на външни лица, без да я заявена услуга.

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

1. Унищожаване на БД или части от тях;
2. Повреждане на БД или части от тях;
3. Записване на невярна информация в БД или части от тях.

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

Чл.13. На служителите е строго забранено да използват мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него. Потребителите на мобилни компютърни средства и мобилни телефони отговарят за защитата им от кражба и не ги оставят без наблюдение.

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

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

Чл.16. Събирането, подготовката и въвеждането на данни на интернет страницата на ОДЗ Ловеч се извършва от служители, определени със заповед на директора. На горепосочените

длъжности лица се изготвя заявка до МЗХГ за създаване на потребителски имена и пароли за извършване на актуализациите.

Чл.17. Събирането и подготовката на данните се извършва от служители в техния ресор, след което данните се изпращат в електронен вид на служителя, отговорни за качването им в интернет страницата на ОДЗ Ловеч.

РАЗДЕЛ III
РАБОТНО МЯСТО

Чл.18. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника и комуникационни средства.

Чл.19. Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място.

Чл.20. Служителят има право да работи на служебен компютър, като достъп до съхраняваните данни в програмен продукт ФЕРМА се осъществява с въвеждането на потребителско име и парола.

Чл.21. Забранява се на външни лица работа с персоналните компютри на ОДЗ Ловеч, освен на упълномощени фирмени специалисти в случаите на първоначална инсталация на компютърна и периферна техника, програмни активни и пасивни компоненти на локални компютърни мрежи, комуникационни устройства и сервизна намеса на място, но задължително в присъствието на системния администратор или служител от дирекция „АПФСДЧР“.

Чл.22. В края на работния ден всеки служител задължително изключва компютъра, на който работи.

Чл.23. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява системния администратор, който му оказва съответната техническа помощ.

Чл.24. Забраняват се опити за достъп до компютърна информация и БД, 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.25. Инсталиране и разместване 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 от системния администратор.

Чл.26. Служителите имат право да обменят компютърна информация посредством вътрешната компютърна мрежа само във връзка с изпълнение на служебните си задължения и само със служителите, с които имат преки служебни взаимоотношения.

Чл.27. Архивираната компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача.

Чл.28. Достъп до компютърна информация, БД и софтуер се ограничава посредством технически методи – идентификация на потребител чрез пароли.

РАЗДЕЛ IV
ОТГОВОРНОСТИ НА СЛУЖИТЕЛИТЕ ПО ПОДДРЪЖКАТА НА БАЗА ДАННИ

Чл.29. Отговорности на служителите по поддръжката на база данни са:

1. Да прилагат правилата за информационна сигурност на БД и свързаните с тях специфични изисквания.
2. Да изготвят специфични изисквания за сигурност на БД, вкл. процедури, инструкции и др.
3. Да инсталират, конфигурират и управляват системите за управление на БД (СУБД). Да следят за актуалността и допълнения на СУБД, като създават организация за прилагането им;
4. Да създават, администрират и поддържат база данни, според конкретните нужди на информационната система и при спазване на правилата за сигурност на БД;
5. Да резервират и архивират БД;
6. Да упражняват ежедневен контрол на БД относно нарастване, консистентност, повреди и др.;
7. Да предприемат необходимите действия при възникване на инциденти или при установяване на уязвимост, свързани със сигурността на базите;
8. Да участват в разрешаването на извънредни ситуации във връзка с нормалното функциониране на БД;
9. Да контролират и извършват периодичен преглед на правата на достъп до БД;
10. Да осъществяват контрол по спазването на изискванията за сигурност на БД;

Чл.30. При реализацията на проекти по разработване и внедряване на програмни продукти и модули, съдържащи БД, екипът по проекта:

1. Определя изискванията към сигурността на БД в съответствие с правилата за сигурност за БД;
2. Подпомага избора и прилагането на подходящи решения за сигурност на БД;
3. Дефинира при какви условия ще бъде осигуряван достъпа на потребителите до БД, спазвайки съответните правила.

Чл.31. Инсталирането, конфигурирането и актуализирането на СУБД се извършва при следните условия:

1. Инсталирането и конфигурирането на СУБД се извършва от оторизирани служители при спазване на лицензионната.
2. Не се допускат промени по СУБД от други служители, освен ако изрично не са упълномощени за това;
3. Актуализирането на СУБД се извършва само след предварително проведени тестове и подготвен подробен план за актуализация;

Чл.32. БД се създават и разполагат на отделни работни станции. При определени изисквания и условия може да се използва споделено ползване на данни като една работна станция се определя с права на сървър и потребителски работни станции с определени права на достъп.

Чл. 33. Резервиране и архивиране на БД. На определената работна станция за сървърна по определен график се извършва архивиране на данните въведени в отделните БД.

РАЗДЕЛ V
ПОЛЗВАНЕ НА КОМПЮТЪРНА МРЕЖА И ИНТЕРНЕТ

Чл.34. Упълномощени служители от дирекцията извършват необходимите настройки за достъп до интернет, създават потребителски имена и пароли за работа в Система за управление на документооборота и работния поток – Eventis и електронната поща на ОДЗ Ловеч и ОСЗ на областта.

Чл.35. Ползването на компютърната мрежа и електронната поща от служителите става чрез получените потребителско име и парола, а за определени приложения електронен подпис (Docx / Doc Pro).

Чл.36. Служителите от ОДЗ Ловеч 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, достъп до интернет или електронна поща при използването на предоставените им потребителски имена и пароли.

Чл.37. Компютрите, свързани в мрежата на ОДЗ Ловеч използват интернет само от доставчици, с които дирекцията има сключен договор.

Чл.38. Забравяна се свързването на компютри едновременно в мрежата на ОДЗ Ловеч и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на дирекцията и/или е в противоречие с изискванията в Закона за електронно управление (ЗЕУ) и Наредба за общите изисквания за мрежова и информационна сигурност (Загл. Изм. – ДВ, бр.5, 2017г., в сила от 01.03.2017г.).

Чл.39. Забравяна се инсталирането и използването на комуникатори и месенджери, осигуряващи достъп извън рамките на компютърната мрежа на ОДЗ Ловеч 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 дирекцията.

Чл.40. Забранява се съхраняването на работните станции на ОДЗ Ловеч лични файлове с текст, изображение, видео и аудио.

Чл.41. Забранява се отварянето без контрол от страна на системния администратор 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, например файлове с разширения .exe, .vbs, .reg и архивни файлове;
2. Получени по електронна поща съобщения, които съдържат неразбираеми знаци.

РАЗДЕЛ VI
ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл.42. За антивирусна защита в ОДЗ Ловеч се прилагат следните мерки:
1. Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.
2. Системният администратор извършва следните дейности:
   2.1. Активира защитата на съответните ресурси – файлова система, електронна поща и извършва първоначално пълно сканиране на системата;
   2.2. Настройва антивирусния софтуер за периодично сканиране през определен период, но поне веднъж седмично;
   2.3. 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 в дирекцията или от общинската служба задължително информира системния администратор.

Чл.43. Организационни мерки за защита:
1. Превенция за възникнали уязвимости и осъществени атаки – със заповед на директора на ОДЗ Ловеч се определя служител, отговарящ за провеждане на дейности свързани с прилагане на политиките за мрежовата и информационна сигурност.
2. Регламентиране на права и задължения на потребителите на комуникационно информационната среда.

Чл.44. Мерки за защита на хост – работна станция;
1. Подобряване сигурността на хостовете (security hardening):
   1.1. Прилагане на Политики, които ограничават портове, услуги и забраняват уязвими протоколи;
   1.2. Прилагане на политики: политика за пароли (комбинация от цифри, букви, специални символи), управление на акаунти и достъпи до различни системи, изпълнение на политики за използване на минимални привилегии (least privilege). Ограничаване на софтуера, който може да бъде инсталиран и изпълняван.
   1.3. Управление на оборудването – сигурно изтриване на информацията преди дадено устройство да бъде изведено от употреба.

Чл.45. Мерки за мрежова сигурност.
Във връзка с повишения риск от кибератаки и инциденти, както и увеличаване на злонамерените действия и щетите, които нанасят с цел запазване на целостта, автентичността, наличността и достъпността на информацията, и системите и регистрите, в които тя се събера, обработва, използва и съхранява се предприемат следните мерки:
1. Мониторинг на комуникационните канали, осигуряващи свързаността на ОДЗ Ловеч;
2. Наблюдение на параметри за нормално функциониране на ИКТ инфраструктурата в ОДЗ Ловеч;
3. Електронна поща, БД, приложения и др.;
4. Своевременно уведомяване на администраторите при настъпили отклонения в наблюдаваните параметри, за да бъдат предприети адекватни мерки за отстраняване на проблема.

Чл.46. Мерки за защита на приложения и данни:
1. При използване на приложения и данни от вътрешната мрежова инфраструктура, мерките за защита се отнасят за решения свързани със съвместната работа на различни приложения и услуги – електронна поща, вътрешни портали, файлови услуги, комуникация в реално време и др.
2. За защита на услугата електронна поща да се извършва сканиране на входящ и изходящ трафик;
3. За преносимите носители на информация се прилагат добри практики за ограничаване автоматичното стартиране на преносим код при включването им и дейности свързани с защита на преносимите медии, заличаване на информация при изваждане от употреба, обозначаване, съхранение и транспортиране.
4. Достъп на служителите до работните им станции и общите информационни системи да се осъществява със служебни потребителско име и парола.
5. При прекратяване на служебното/трудово правоотношение, с изтичане на работния ден предхождащ прекратяването, системния администратор прекратява правата на достъп до мрежови ресурси, електронна поща и компютър. При необходимост се извършва преинсталация на компютъра.

Чл.47. Мерки за непрекъснатост на работа: Всички важни компютърни конфигурации със споделени ресурси /ползвани като сървър / са със непрекъсваемо захранване, като при отпадане на основното захранване операторът е длъжен да я изключи по нормален начин до 10 мин..

РАЗДЕЛ VII
КОНТРОЛ

Чл.48. Ръководителите на звена от администрацията (Директорите на дирекции и началниците на общинските служби по земеделие) контролират използването на компютърната и периферната техника, като при необходимост изясняват причините за неизползването на техниката и програмите или използването им не по предназначение, като уведомяват Главния секретар на ОДЗ Ловеч, с цел прилагане на съответните административни действия.

Чл.49. Системният администратор контролира изпълнението на дейности, които засягат работата с електронни БД, достъп до отдалечени ресурси и които не се контролират от други инстанции. При установяване на неизпълнение или лошо изпълнение на някоя от точките, касаещи работата с електронни данни предприема действия за възстановяване на изправността и уведомява Главния секретар с цел прилагане на съответните административни действия.

Чл.50. На периодична проверка от системния администратор подлежат веднъж годишно:
Компютрите относно: промени в хардуерната конфигурация, инсталирания софтуер, допълнително инсталиран софтуер, неразрешени промени в операционната система на компютъра;

РАЗДЕЛ VIII
ЗАЩИТА СРЕЩУ НЕЖЕЛАН СОФТУЕР

Чл.51.Защитата срещу нежелан софтуер в информационните системи на ОДЗ Ловеч се организира от служители, отговарящи за мрежовата и информационната сигурност на дирекцията. Защитата и мерките са описани в приложение 1.

Чл.52. Съгласно чл.41 от Наредбата за общите изисквания за мрежова и информационна сигурност Директорът на ОДЗ Ловеч осигурява мерки за физическа защита на информационните системи в дирекцията и общинските служби по земеделие.

Чл.53. Съгласно чл.41 от Наредбата за общите изисквания за мрежова и информационна сигурност Директорът на ОДЗ Ловеч осигурява мерки за защита срещу нежелан софтуер.

Чл.54. Националният център за действие при инциденти по отношение на мрежовата и информационната сигурност поддържа актуална информация за всички опити за проникване на нежелан софтуер в информационните системи на административните органи, както и за предприетите действия за защита от тях.

Чл.55. Директорът на ОДЗ Ловеч предприема превантивни действия за защита на информационните системи от природни бедствия като застрахова риска „Щети от природни бедствия“ в рамките на задължителните годишни застраховки.

Чл.56. Директорът на ОДЗ Ловеч осигурява условия, при които неовластени лица не могат да получат физически достъп до работните станции, използвани от администрацията.

Чл.57. Директорът на ОДЗ Ловеч утвърждава план за действие при инциденти, свързани с мрежовата и информационната сигурност на използваните от тях информационни системи, с цел осигуряване непрекъсваемост на дейността на съответната общинска служба по земеделие. Планът трябва да съответства на изискванията на приложение № 2.

Чл.58. Служителят по мрежова и информационна сигурност в ОДЗ Ловеч е длъжен да уведоми незабавно Националния център за действие при инциденти по отношение на мрежовата и информационната сигурност за всеки инцидент в информационните системи на дирекцията.

РАЗДЕЛ IX
ДИСЦИПЛИНАРНА ОТГОВОРНОСТ

Чл.59. Служители, които не поддържат актуални данните, с които работят, въведат умишлено неверни данни и създават условия за разпространяване на невярна електронна информация, се наказват с дисциплинарно наказание за нарушаване на трудовата дисциплина в съответствие с чл.187, ал. 1, т.3, 4, 7, 8 и 10 от КТ или чл.89, ал.2 от ЗДСл и се задължават да възстановят данните в актуално състояние.

Чл.60. Служители на ОДЗ Ловеч, които с умишлени и неумишлени действия / посещения на не регламентирани сайтове или торент сайтове / създават предпоставки за заразяване на програми и БД с компютърни вируси се наказват с дисциплинарно наказание за нарушаване на трудовата дисциплина в съответствие с чл.187, ал.1, т.9 от КТ или чл.89, ал.2 от ЗДСл, със заплащане на стойността на повредените програми и на разходите за възстановяване на данните.

Чл.61. Служители на ОДЗ Ловеч, които деинсталират, инсталират или разместват компютърни конфигурации, части от тях, периферна техника, активни и пасивни компоненти на локални компютърни мрежи, както и комуникационни устройства, се наказват с дисциплинарно наказание за нарушаване на трудовата дисциплина в съответствие с т.187, ал.1, т. 3 и 9 от КТ и чл. 89, ал.2 от ЗДСл, а при повреда на техниката – и със заплащане на стойността на повредената такава.

Чл.62. При установяване на използване на компютърната периферна техника от външни лица служителите на ОДЗ Ловеч допуснали това се наказват с дисциплинарно наказание за нарушаване на трудовата дисциплина в съответствие с т.187, ал.1, т. 3, 8 и 9 от КТ и чл. 89, ал.2 от ЗДСл, а при установяване на повреди на техника, данни и програми и със заплащане стойността на повредените техника, програми, както и на разходите за възстановяване на данни.

Чл.63. При установяване на не регламентирани действия на служителите на ОДЗ Ловеч, които са довели до унищожаване на служебна информация, разположена на ползваните от тях компютри, служителите се наказват с дисциплинарно наказание за нарушаване на трудовата дисциплина в съответствие с т.187, ал.1, т. 3, 8 и 9 от КТ и чл. 89, ал.2 от ЗДСл.

Чл.64. Служителите на ОДЗ Ловеч, които в установеното работно време при изпълнение на служебните си задължения и поставените им задачи, използват компютрите за игри или друг вид дейност, която не е свързана с изпълнение на служебните им задължения, наказват с дисциплинарно наказание за нарушаване на трудовата дисциплина в съответствие с т.187, ал.1, т.2 и 3 от КТ и чл. 89, ал.2 от ЗДСл.

Чл.65. При следващи нарушения, на провинилият се служител се налагат следващите по степен дисциплинарни наказания съгласно чл.188 от КТ и чл. 90 от ЗДСл.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

- § 1. Настоящите правила са неразделна част към Системите за финансово управление и контрол в ОДЗ Ловеч и подлежи на периодичен преглед и актуализиране при възникнала необходимост.
- § 2. Правилата и процедурите могат да се допълват и изменят със заповед на директора на ОДЗ Ловеч.
- § 3. Указания по прилагането на настоящите правила дава директор Дирекция „АПФСДЧР“.
- § 4. Контрола по прилагане на настоящите правила се осъществява от Главния секретар на ОДЗ Ловеч.

Приложение 1

Защита срещу нежелан софтуер

1. Нежеланият софтуер, който може да експлоатира уязвимостта на един или няколко информационни актива и да предизвиква смущаване на нормалната им работа, увреждане или унищожаване, включва следните основни програми:
   а) компютърни вируси;
   б) мрежови червеи;
   в) троянски коне
   г) логически бомби
2. Защитата срещу нежелан софтуер в информационните системи на ОДЗ Ловеч трябва да бъде ориентирана в две основни направления:
   а) чрез забрана за използване на нерегламентиран софтуер;
   б) чрез задължително използване на утвърден за цялата администрация антивирусен софтуер и софтуер за откриване на нерегламентирани промени на информационните активи.
3. Администраторът на единната национална мрежа (ЕНМ) трябва да прилага средства за откриване на опити за проникване на различни нива и периметри на мрежата.
4. Програмните продукти, предназначени за откриване на опити за проникване, трябва да разпознават следните подозрителни действия в мрежата:
   а) опити да се използват услуги, блокирани от защитни стени;
   б) неочаквани заявки, особено от непознати адреси;
   в) неочаквани шифровани съобщения;
   г) извънредно активен трафик от непознати сървъри и устройства;
   д) значителни изменения на предишни действия на мрежата;
   е) опити за използване на известни системни грешки или уязвимости;
   ж) опити за вход от непознати потребители от неочаквани адреси;
   з) несанкционирано или подозрително използване на администраторски функции;
   и) значителни изменения в обичайните действия на потребител и пр.
5. При установяване на открити опити за проникване трябва незабавно:
   а) да се уведомява системния администратор за предприемане на адекватни мерки;
   б) да се изключват или ограничават мрежовите услуги, свързани с информационния актив – обект на проникване.
6. Всяко устройство, което се включва в мрежата на съответната администрация, автоматично да се проверява за вируси и нежелан софтуер, преди да получи достъп до ресурсите на мрежата.

Приложение 2

Управление на инциденти, свързани с мрежовата и информационната сигурност

1. Планирането на дейността по управление на инциденти, свързани и с мрежовата, и с информационната сигурност, включва следните етапи:
   а) определяне на критично важните функции на системата и установяване на приоритетите за възстановителни работи;
   б) идентификация на ресурсите, необходими за изпълнение на критично важните функции;
   в) определяне списък на възможните инциденти с вероятности за появяването им, изхождайки от оценките на риска;
   г) разработка на стратегии за възстановителни работи;
   д) подготовка на мероприятия за реализация на стратегиите.
2. Цикълът на управлението на инциденти включва следните основни етапи:
   а) подготовка;
   б) откриване и анализ;
   в) ограничаване на влиянието, премахване на причината, възстановяване;
   г) дейности след инцидента.
3. Критичен елемент от управлението на инциденти е незабавното възстановяване на дейността на системата.
4. Политиката за защита от инциденти и възстановителни работи на ОДЗ Ловеч, която произтича от оценката на риска по глава трета, раздел трети от Наредбата за общите изисквания за мрежова и информационна сигурност, идентифицира средствата за резервиране и възстановяване с оглед покриване ниво на резервиране над пето по класацията на Асоциация Share.
5. Средствата по т.4 могат да бъдат:
   а) Резервиране на важни данни на външни носители / CD, HDD и Flash памети /
6. Планът за действия при инциденти на ОДЗ Ловеч, включва мерки, които да се проведат след възстановяването и които да целят избягване на инциденти, а именно:
   а) повишаване нивото на контрол на достъпа;
   б) промяна на конфигурациите на зоните за сигурност;
   в) изменение на режима на физически достъп;
   г) инсталиране на допълнителни модули за защита на софтуера на системата;
   д) сканиране и декласификация на носителите.

ДИЯНА РУСКОВА
Директор на ОД „Земеделие” Ловеч

Съгласувал:
Инж.Д.Николов
Директор „АПФСДЧР“

Изготвил:
Инж. В. Вълков
Главен експерт