

ИНСТРУКЦИЯ № И-3 от 16 май 2024 г.

за условията и реда за организиране, поддържане и достъп до електронния регистър на военнослужещите и цивилните служители – Информационна система „Автоматизирана система за управление на човешките ресурси“

Издадена от министъра на отбраната, обн., ДВ, бр. 45, от 28.5.2024 г., в сила от 28.5.2024 г.

Глава първа

ОБЩИ ПОЛОЖЕНИЯ

Раздел I

Предназначение

Чл. 1. С инструкцията се определят условията и редът за организиране, поддържане и достъп до електронния регистър по чл. 328, ал. 1, т. 1 от Закона за отбраната и въоръжените сили на Република България (ЗОВСРБ).

Чл. 2. Електронният регистър по чл. 328, ал. 1, т. 1 от ЗОВСРБ се създава като информационна система „Автоматизирана система за управление на човешките ресурси“, наричана за краткост „Информационна система“.

Чл. 3. Информационната система по чл. 2 осигурява процесите по:

1. създаване, съхраняване, обмен, защита, контрол и поддържане в актуално състояние на единен информационен ресурс за структурата на въоръжените сили, организационно-щатната структура, военнослужещите и цивилните служители в Министерството на отбраната, структурите на пряко подчинение на министъра на отбраната и Българската армия, с изключение на Служба „Военно разузнаване“;

2. създаване, поддържане в актуално състояние, обменяне, защита и съхраняване на информация за ресурсите от резерва и за комплектуването на въоръжените сили при условия и по ред, определени със Закона за резерва на въоръжените сили на Република България.

Чл. 4. Директорът на структурата по управление на човешките ресурси към министъра на отбраната координира и контролира дейностите по поддържането и развитието на Информационната система по чл. 2.

Чл. 5. Информационната система е интегрирана съвкупност от взаимнообвързани и допълващи се подсистеми и модули, използващи единна номенклатура и база данни.

Чл. 6. Информационната система функционира в средата на Комуникационна и информационна система „ЩИТ“ (КИС „ЩИТ“), предназначена за обмен на класифицирана информация.

Чл. 7. В Информационната система се обработва и съхранява информация с ниво на класификация до „Поверително“ включително.

Чл. 8. Информационната система осигурява дейностите по:

1. изграждане на структурата на въоръжените сили;
2. изготвяне на длъжностни разписания и щатове;
3. въвеждане и поддържане в актуално състояние на персонални данни на военнослужещите и цивилните служители по чл. 3, т. 1;
4. въвеждане и поддържане в актуално състояние на персоналните данни на ресурсите от резерва;
5. подготовка на документи и управление на ежедневната административна дейност по личния състав;
6. планиране и отчет на подготовката и развитието на военнослужещите, цивилните служители и резервистите;
7. подготовка на обобщена информация по нива на управление и конкретни военни формирования/структури;
8. кандидатстване за военна служба и служба в доброволния резерв.

Чл. 9. Основни правила за достъп и работа в Информационната система:

1. достъпът до системата се осъществява с персонален акаунт (потребителско име и парола) за всеки потребител;
2. по-високото йерархично звено осигурява работата и контролира въвеждането на данните на подчинените си звена;
3. на всяко ниво могат да се генерират справки върху достъпния обем от информация – съобразно правата на достъп;
4. правата на достъп на потребителите до информация в Информационната система се осигуряват чрез системни функции при спазване на принципа „необходимост да се знае“ и отчитане на нивото на класификация на информацията, достъпвана от съответния потребител.

Чл. 10. (1) Командирът на военното формирование или ръководителят на съответната структура по чл. 78 от Закона за отбраната и въоръжените сили на Република България, с изключение на Служба „Военно разузнаване“:

1. носи отговорност за поддържането на актуалността и целостта на данните в Информационната система за подчиненото военно формирование/структура;
2. със своя заповед определя потребителите на Информационната система, структурите/военните формирования, за които се дават правата, както и

конкретния достъп до съответните подсистеми и модули; заповедта се съгласува с длъжностното лице по защита на личните данни;

3. планира и заявява потребностите от функционално обучение на лицата, определени за потребители на Информационната система;

4. със своя ежегодна заповед организира и контролира процесите по въвеждане и актуализиране на данните в Информационната система, като определя сроковете и дейностите по:

а) синхронизиране на данните в подсистема „Персонални данни за служителите“ на Информационната система с азбучните служебни карти (АСК) и служебните дела – за военнослужещите, и с трудовите или служебните досиета – за цивилните служители;

б) запознаване на военнослужещите и цивилните служители с персоналните данни, които се обработват и съхраняват в Информационната система за тях, за актуализиране съгласно чл. 12, т. 1;

в) предоставяне на документи за удостоверяване на липсващата информация от военнослужещите и цивилните служители на длъжностните лица от структурите по управление на човешките ресурси (по личния състав) съгласно чл. 12, т. 2;

г) изготвяне на отчет за изпълнението на дейностите по заповедта и за степента на актуалност на въведените данни за личния състав.

(2) Директорът на структурата по управление на човешките ресурси към министъра на отбраната:

1. организира и контролира процесите по поддържането на актуалността и целостта на данните в Информационната система за личния състав от административните звена на Министерството на отбраната, като определя сроковете и дейностите по:

а) синхронизиране на данните в подсистема „Персонални данни за служителите“ на Информационната система с азбучните служебни карти (АСК) и служебните дела – за военнослужещите, и с трудовите или служебните досиета – за цивилните служители;

б) запознаване на военнослужещите и цивилните служители с персоналните данни, които се обработват и съхраняват в Информационната система за тях, за актуализиране съгласно чл. 12, т. 1;

в) предоставяне на документи за удостоверяване на липсващата информация от военнослужещите и цивилните служители на длъжностните лица от структурите по управление на човешките ресурси (по личния състав) съгласно чл. 12, т. 2;

2. предлага на министъра на отбраната или на оправомощено от него длъжностно лице определените от ръководителите на административни звена на Министерството на отбраната потребители на Информационната система, за които се дават права, както и конкретния достъп до съответните подсистеми и модули за отдаване в заповед; заповедта се съгласува с длъжностното лице по защита на личните данни;

3. заявява потребностите от функционално обучение на лицата от административните звена на Министерството на отбраната, определени за потребители на Информационната система.

Чл. 11. (1) В Информационната система се събират, обработват и съхраняват лични данни само за нуждите на Министерството на отбраната.

(2) Министърът на отбраната със свой акт прилага мерки по сигурността на обработването и защитата на личните данни в Информационната система.

Чл. 12. Актуализация на лични данни се извършва:

1. по искане на лицето, за което се отнасят личните данни, когато то е установило, че е налице грешка или непълнота в тях и удостовери това с документ;

2. по инициатива на обработващия лични данни – при наличие или изискване на документ, даващ основание за актуализация.

Раздел II

Подсистеми и модули в Информационната система

Чл. 13. Подсистема „Организационни структури“ („Указател“) осигурява дейностите по създаване и поддържане на структурата на въоръжените сили.

Чл. 14. Подсистема „Щатове и длъжностни разписания“ („Рожен“) осигурява дейностите по създаване и поддържане в нужния обем на информация за щатове, длъжностни разписания и длъжностни характеристики.

Чл. 15. Подсистема „Персонални данни за служителите“ („Витоша“) осигурява дейностите по:

1. създаване и поддържане на персонални данни на личния състав по чл. 3, т. 1 и 2;

2. подготовка и отпечатване на служебните карти на военнослужещите от Министерството на отбраната, структурите на пряко подчинение на министъра на отбраната и Българската армия, с изключение на Служба „Военно разузнаване“.

Чл. 16. Модул „Удостоверения/сертификати от военнообразователни институции (ВОИ)“ осигурява дейностите по въвеждане на данните от издадени

удостоверения/сертификати от проведено обучение в курс за придобиване и повишаване на квалификацията и преквалификацията във военнообразователните институции на личния състав по чл. 3, т. 1.

Чл. 17. Подсистема „СТАНАГ“ осигурява дейностите по планиране, въвеждане и отпечатване на резултати от проведени изпити съгласно стандартизационно споразумение на НАТО STANAG 6001 за владеење на чужд език и по въвеждане на резултати от проведените тестове ALCPT за владеење на английски език на личния състав по чл. 3, т. 1.

Чл. 18. Подсистема „Разрешения за достъп до класифицирана информация“ осигурява дейностите по въвеждане на издадени/отнети/прекратени разрешения за достъп до национална класифицирана информация и на декларации за преминато обучение по защита на класифицирана информация на НАТО и ЕС на личния състав по чл. 3, т. 1 и 2.

Чл. 19. Подсистема „Атестиране“ осигурява дейностите по въвеждане на данните от електронните атестационни формуляри на военнослужещите от Министерството на отбраната, структурите на пряко подчинение на министъра на отбраната и Българската армия, с изключение на Служба „Военно разузнаване“, както и за генериране на справки, свързани с дейностите по атестиране на военнослужещите.

Чл. 20. Модул „Квалификация“ осигурява дейностите по планиране на обучението, квалификацията и преквалификацията на личния състав по чл. 3, т. 1.

Чл. 21. Модул „Отчет на ресурсите от резерва“ осигурява дейностите по водене на отчет на ресурсите от резерва по чл. 3, т. 2, отсрочването от повикване във въоръжените сили при мобилизация и комплектуването на въоръжените сили със запасни и техника-запас, управление на мобилизационните ресурси и анализ на мобилизационната готовност.

Чл. 22. Модул „Кандидати“ осигурява дейностите по провеждане на конкурсите за военна служба и служба в доброволния резерв, анализ на кампаниите по набирането на кандидати за военна служба и служба в доброволния резерв, първоначално въвеждане на личните данни и воденето им на отчет.

Чл. 23. Модул „Безопасност и здраве при работа“ осигурява дейностите по генериране на необходимите документи и анализиране на трудовите злоупотреки в Министерството на отбраната, структурите на пряко подчинение на министъра на отбраната и Българската армия, с изключение на Служба „Военно разузнаване“.

Раздел III

Права на потребителите при работа с подсистеми и модули

Чл. 24. При работа с подсистемите и модулите на потребителите се предоставят следните права:

1. „Създаване и редактиране“;
2. „Разглеждане“;
3. „Отпечатване“;
4. „Въвеждане“;
5. „Изготвяне на служебни карти“;
6. „Въвеждане на оценка от операция/мисия“;
7. „Управление на квалификацията“;
8. „Военно формирование“;
9. „Обучаваща организация“;
10. „Управление на резерва“;
11. „Военно окръжие“;
12. „Управление на кандидатите“;
13. „Управление“.

Чл. 25. За работа в подсистема „Организационни структури“ се предоставят права за „Създаване и редактиране“ на потребителя, който може да създава и редактира структурата на въоръжените сили.

Чл. 26. За работа в подсистема „Щатове и длъжностни разписания“ на потребителя се предоставят следните права:

1. „Създаване и редактиране“ – да създава нов и да редактира съществуващ щат или длъжностно разписание;
2. „Разглеждане“ – да разглежда съществуващ щат или длъжностно разписание;
3. „Копиране“ – да копира щат или длъжностно разписание;
4. „Отпечатване“ – да отпечата щат или длъжностно разписание.

Чл. 27. За работа в подсистема „Персонални данни за служителите“ на потребителя се предоставят следните права:

1. „Въвеждане“ – да въвежда, променя или изтрива данни на личния състав по чл. 3, т. 1 и 2, достъпни от предоставените му права по организационната структура;
2. „Разглеждане“ – да разглежда данните на личния състав по чл. 3, т. 1 и 2, достъпни от предоставените му права по организационната структура;
3. „Изготвяне на служебни карти“ – да изготвя и отпечата служебни карти на военнослужещите;

4. „Въвеждане на оценка от операция/мисия“ – да въвежда данни от формуляра за оценка на изпълнението на функционалните задължения от военнослужещите при участие в операции и мисии.

Чл. 28. За работа в модул „Удостоверения/сертификати от военнообразователни институции (ВОИ)“ се предоставя право за достъп „Въвеждане“ на потребителя от структурата във военнообразователната институция, изготвяща удостоверенията/сертификатите за проведено обучение в курс за придобиване и повишаване на квалификацията и преквалификацията на личния състав по чл. 3, т. 1.

Чл. 29. За работа в подсистема „Разрешения за достъп до класифицирана информация“ на потребителя се предоставя право за достъп „Въвеждане“ да актуализира данните за издадени, отнети или прекратени разрешения за достъп до национална класифицирана информация и декларации за преминато обучение по защита на класифицирана информация на НАТО и ЕС на служителите, достъпни от предоставените му права по организационната структура.

Чл. 30. За работа в подсистема „СТАНАГ“ на потребителя се предоставят следните права:

1. „Създаване и редактиране“ – да създава изпитни сесии и протоколи в определено учебно заведение за изпитите съгласно НАТО STANAG 6001;

2. „Въвеждане“ – да въвежда в протоколи данните на явяващите се на изпит за владеење на чужд език съгласно НАТО STANAG 6001, да отразява резултатите от проведените изпити за определяне нивото за владеење на чужд език съгласно НАТО STANAG 6001 и от тест ALCPT;

3. „Отпечатване“ – да отпечата сертификати от изпита за владеење на чужд език съгласно НАТО STANAG 6001;

4. „Разглеждане“ – само да преглежда данните съгласно предоставените му права.

Чл. 31. За работа в модул „Квалификация“ на потребителя се предоставят следните права:

1. „Управление на квалификацията“ – да създава регистър на курсовете за съответната година; обобщава заявките за квалификация и подготвя годишния план за придобиване и повишаване на квалификацията, създава заповедите за провеждане на курсове;

2. „Военно формиране“ – да изготвя заявки за курсове за служителите, достъпни от предоставените му права по организационната структура;

3. „Обучаваща организация“ – да планира курсовете по дати и брой обучаеми.

Чл. 32. За работа в подсистема „Атестиране“ се предоставя право „Въвеждане“ на потребителя, който може да въвежда данни от електронните атестационни формуляри на военнослужещите, както и да генерира справки, свързани с дейностите по атестиране на военнослужещите.

Чл. 33. За работа в модул „Отчет на ресурсите от резерва“ се предоставят следните права:

1. „Управление на резерва“:

а) потребителят от Министерството на отбраната може да генерира справки за ресурсите от резерва и да извършва анализи на комплектуването на въоръжените сили;

б) потребителят от Централното военно окръжие може да: въвежда заявки от други министерства от системата за национална сигурност; определя военно окръжие за изпълнение на заявките за комплектуване на въоръжените сили; генерира справки; извършва анализи на ресурсите от резерва и на комплектуването на въоръжените сили; отсрочването от повикване във въоръжените сили при мобилизация; редакция на класификатори;

2. „Военно формирование“ – потребителят може да въвежда заявки по команди и да генерира справки и да извършва анализи за изпълнението им;

3. „Военно окръжие“ – потребителят може да: води отчет на ресурсите от резерва; въвежда заявки от други министерства от системата за национална сигурност; възлага/снима мобилизационно назначение; извършва отсрочване от повикване във въоръжените сили при мобилизация; генерира справки; извършва анализи на ресурсите от резерва и на комплектуването на въоръжените сили; отсрочва от повикване във въоръжените сили при мобилизация.

Чл. 34. За работа в модул „Кандидати“ се предоставят следните права:

1. „Управление на кандидатите“:

а) потребителят от Министерството на отбраната може да генерира справки и да извършва анализи на проведените конкурси;

б) потребителят от Централно военно окръжие може да генерира справки и да извършва анализи на проведените конкурси;

2. „Военно окръжие“ – потребителят може да въвежда данните на кандидатите и да отразява желанията им за съответния конкурс, да генерира справки и да извършва анализи на проведените конкурси;

3. „Военно формирование“ – потребителят може да въвежда длъжностите по обявен конкурс и изискванията за тях, резултатите от дейностите по провеждане

на конкурсите, да генерира справки и да извършва анализи на проведените конкурси.

Чл. 35. За работа в модул „Безопасност и здраве при работа“ се предоставят следните права:

1. „Управление“ – потребителят може да поддържа класификатори, да анализира трудовите злоупотреки и условията на труд на работните места;
2. „Военно формирование“ – потребителят може да изготвя документи при трудови злоупотреки; може да създава и редактира информация за условията на труд на работните места.

Глава втора

ПРАВА И ЗАДЪЛЖЕНИЯ НА ДЛЪЖНОСТНИТЕ ЛИЦА

Чл. 36. За функциониране на Информационната система се определят длъжностни лица, както следва:

1. системен администратор на Информационната система, определен със заповед на командира на Командването за комуникационно-информационна поддръжка и киберотбрана;
2. администратор по сигурността на Информационната система, определен със заповед на командира на Командването за комуникационно-информационна поддръжка и киберотбрана;
3. софтуерен разработчик на Информационната система, определен със заповед на министъра на отбраната или на оправомощено от него длъжностно лице;
4. потребител на Информационната система, определен със заповед на длъжностно лице по чл. 10.

Чл. 37. Права и задължения на системния администратор по чл. 36, т. 1:

1. администрира системното програмно осигуряване на сървърите на Информационната система;
2. администрира базите от данни на Информационната система;
3. администрира приложенията, като създава или модифицира обекти, правила и процеси за правилното взаимодействие с базата данни;
4. следи и анализира системните записи за възникнали грешки в работата на системата и взема мерки за отстраняването им;
5. създава и редактира еталони и форми на справки и документи;
6. следи за работоспособността на системата и дава препоръки за повишаване на ефективността.

Чл. 38. Права и задължения на администратора по сигурността по чл. 36, т. 2:

1. предоставя достъп на потребителите на Информационната система, като създава персонални акаунти и отразява в системата определения достъп до съответните подсистеми и/или модули съгласно получените заявки по чл. 44;

2. води регистър, в който поддържа актуален поименен списък на потребителите на Информационната система, персонален акаунт и права за достъп до съответните подсистеми и/или модули;

3. следи и контролира извършваните дейности от потребителите на Информационната система, като анализира записите за възникнали грешки в работата на системата за управление на базата данни и взема мерки за отстраняването им;

4. архивира базата данни на Информационната система;

5. възстановява базата данни при необходимост;

6. осъществява пряк контрол по отношение на изпълнението на мерките и процедурите за сигурност в Информационната система, като:

а) следи за спазването на мерките и процедурите за сигурност при инсталирането, конфигурирането, поддръжката и промените в Информационната система;

б) следи за правилното функциониране на механизмите за сигурност;

в) управлява, наблюдава и анализира свързаните със сигурността одитни записи на Информационната система и осигурява тяхното резервиране и съхраняване;

7. при възникване на събитие, представляващо заплаха от компрометиране, загуба на достъпност и/или цялостност на информацията в Информационната система, предприема необходимите мерки за защита на информацията.

Чл. 39. Софтуерният разработчик по чл. 36, т. 3 поддържа приложния софтуер за Информационната система и свързаните с него софтуерни средства, което включва:

1. отстраняване на проблеми и грешки;

2. адаптиране на софтуера съгласно действащата нормативна уредба, практическите изисквания и технологичното развитие по реда на чл. 59;

3. анализ на функционирането на информационните системи с оглед на подобряване на характеристиките им и набелязване на изисквания за разработване на следващи версии и издания на системите или нови системи;

4. поддържа документацията на приложния софтуер в актуално състояние в съответствие с корекциите на грешки, отстраняването на проблеми и подобренията в Информационната система; всяко коригирано издание на софтуера се придружава от коригираща документация.

Чл. 40. Задължения на потребителите по чл. 36, т. 4:

1. да са запознати с настоящата инструкция и ръководството на потребителя за съответната подсистема и/или модул;
2. да използват правата си за работа само във връзка с осъществяване на правомощия, възложени по реда на чл. 10, и във връзка с изпълнение на своите служебни задължения;
3. да осигуряват достоверността, актуалността и пълнотата на информацията, до която имат достъп за добавяне, редактиране и/или изтриване;
4. да въвеждат данните от документите, за които не са посочени конкретни срокове за въвеждане в Информационната система, до един месец от получаването им;
5. да отпечатват и съхраняват документи (сведения, справки и др.) от Информационната система съгласно действащата нормативна уредба и процедурите за сигурност;
6. да пазят от разкриване паролата си и да не предоставят за ползване акаунта си;
7. да променят паролата си в указаното време;
8. задължително да излязат от акаунта си след приключване на работа в Информационната система;
9. да докладват на системния администратор по чл. 36, т. 1 за всяка повреда на хардуера;
10. незабавно да докладват на администратора по сигурността по чл. 36, т. 2 за всички нарушения на сигурността, потенциални заплахи и съмнения за нерегламентиран достъп до класифицирана информация;
11. да въвеждат данни в Информационната система в съответствие с предоставените им права в сроковете, регламентирани в действащата нормативна уредба.

Глава трета

**УСЛОВИЯ И РЕД ЗА ДОСТЪП НА ПОТРЕБИТЕЛИ ДО
ИНФОРМАЦИОННАТА СИСТЕМА**

Раздел I

Условия за достъп до Информационната система

Чл. 41. (1) Достъп на потребител до Информационната система във връзка с изпълнение на служебни задължения или конкретно възложени задачи се разрешава след:

1. издадено разрешение за достъп до класифицирана информация до ниво не по-ниско от нивото на класификация на информацията на предоставените електронни услуги в КИС „ЩИТ“;

2. проведено обучение в областта на сигурността на КИС „ЩИТ“;

3. предоставени права за достъп до ресурсите на КИС „ЩИТ“ – потребителско име;

4. проведено първоначално обучение и получено удостоверение за преминато първоначално обучение на WEB страницата на ИС „АСУ на ЧР – HRMIS“ в КИС „ЩИТ“;

5. проведен първоначален инструктаж за защита на личните данни в Информационната система от длъжностното лице по защита на личните данни;

6. предоставен достъп за работа в Информационната система по реда на чл. 44.

(2) Потребител с предоставен достъп за работа в системата се запознава със своите права и задължения, посочени в инструкцията, и със защитата на личните данни по смисъла на Закона за защита на личните данни.

(3) Всеки потребител преминава функционално обучение в курс за допълнителна квалификация за работа в Информационната система във военнообразователните институции в страната.

(4) Всеки потребител задължително преминава ежегодно текущо обучение на WEB страницата на ИС „АСУ на ЧР – HRMIS“ в КИС „ЩИТ“ без откъсване на лицето от изпълнение на преките му служебни задължения.

Чл. 42. (1) След три последователни неуспешни опита за влизане в акаунта си в Информационната система достъпът на потребителя автоматично се заключва.

(2) Възстановяване на достъпа до Информационната система се извършва от администратора по сигурността по чл. 36, т. 2.

Чл. 43. (1) Достъпът до акаунт на потребител, който не е ползван повече от три месеца, се заключва с изключение на акаунтите на потребителите в модули „Отчет на ресурсите от резерва“ и „Кандидати“.

(2) Възстановяване на достъпа може да се извърши единствено от администратора по сигурността по чл. 36, т. 2.

(3) Акаунтът на потребител, който не е ползван повече от една година или в случаите на чл. 45, се деактивира и се архивира.

Раздел II

Ред за предоставяне на достъп до Информационната система

Чл. 44. (1) Предоставянето на достъп до Информационната система се осъществява след изготвяне на електронна заявка за „АСУ на ЧР“, която се достъпва чрез електронната платформа на „Център за електронни заявки в КИС „ЩИТ“, в съответствие с указанията на главния информационен мениджър относно създаване на организация за използване на електронни заявки за включване/изключване и предоставяне/снемане на електронни услуги в КИС „ЩИТ“ и интернет (домейн armf.bg).

(2) Заявката по ал. 1 включва:

1. звание, име, презиме, фамилия, длъжност на потребителя;
2. структура/военно формирование, адрес, стая, телефон;
3. потребителско име в КИС „ЩИТ“;
4. желано ниво за достъп до класифицирана информация в Информационната система;
5. права за достъп до структури/военни формирования;
6. права на потребителите при работа с подсистеми и модули в Информационната система.

(3) Заявките за достъп се изготвят от определено от ръководителите на съответните структури или командири/началниците на военни формирования лице.

(4) Заявките за достъп се утвърждават от командира (началника) на военното формирование или от ръководителя на съответната структура, издала заповедта по чл. 10, или от оправомощено от него длъжностно лице.

(5) Към заявката по ал. 1 се прикачват копие на заповедта по чл. 10 и копие на удостоверението за успешно преминато първоначално обучение.

(6) При получаване на електронна заявка за предоставяне на достъп до Информационната система администраторът по сигурността я приема за изпълнение и в едноседмичен срок създава необходимия акаунт на потребителя.

(7) Потребителят получава нужната информация за новосъздадения акаунт в Информационната система на своята електронна поща в КИС „ЩИТ“.

(8) Администраторът по сигурността на Информационната система може да откаже изпълнението на заявката по ал. 1 при следните случаи:

1. некоректно подадени данни;
2. непълно подадени данни;
3. липса на прикачена към заявката заповед по чл. 10;

4. липса на прикачено към заявката удостоверение за успешно преминато първоначално обучение;

5. несъответствие между заявката и прикачената към нея заповед по чл. 10 относно желаня достъп на потребителя до дадена подсистема или модул.

(9) Администраторът по сигурността на Информационната система отразява в заявката на електронната платформа на „Център за електронни заявки в КИС „ЩИТ“ отказ за изпълнението ѝ.

Чл. 45. В десетдневен срок от промяна във функционалните задължения, преназначаване или освобождаване от длъжност на потребител на Информационната система ръководителят на съответната структура или командирът/началникът на военно формирование, или оправомощено от тях длъжностно лице изпраща електронна заявка за прекратяване на правата за достъп за работа до съответната подсистема или модул чрез електронната платформа на „Център за електронни заявки в КИС „ЩИТ“.

Раздел III

Ред за ползване на автоматизирани работни места за работа с Информационната система

Чл. 46. Потребителите от структурите или военните формирования, в които няма разкрити автоматизирани работни места (АРМ) за въвеждане и актуализиране на данните в Информационната система, могат да ползват АРМ от други военни формирования/структури или административни звена в МО, определени с акт на министъра на отбраната или оправомощено от него длъжностно лице.

Чл. 47. Като резервни АРМ за въвеждане и актуализиране на данните в Информационната система се ползват АРМ на военните окръжия в тяхната зона на отговорност, на старшите щабовете/командвания/управления или на военно формирование 26340 – София.

Чл. 48. Ръководителят на съответната структура или командирът/началникът на военно формирование, или оправомощено от тях длъжностно лице, от чиито АРМ се въвеждат данните в Информационната система, със своя заповед организира използването на автоматизираните работни места.

Чл. 49. На предоставените АРМ по чл. 46 се води дневник за отразяване използването им от други структури/военни формирования.

Чл. 50. (1) Достъпът до АРМ на потребител на Информационната система от структурите или военните формирования, в които няма разкрити

автоматизирани работни места, се разрешава само при наличие на права за достъп до ресурсите на КИС „ЩИТ“ и до Информационната система.

(2) Организирането на достъпа на лицата по ал. 1 се извършва съвместно между техните командири/началници/ръководители и командирите/началниците/ръководителите по чл. 48.

Глава четвърта

ПОДДЪРЖАНЕ И СИГУРНОСТ НА ИНФОРМАЦИОННАТА СИСТЕМА

Раздел I

Поддържане на данните

Чл. 51. В Информационната система се поддържат актуални и цялостни данни, необходими за предоставяне на справки.

Чл. 52. Въвеждането и промяната на данни в Информационната система се извършва при следните обстоятелства:

1. въвеждане на данни при първоначално създаване на базата данни;
2. въвеждане на данни при текущо актуализиране на съдържанието на базата данни;
3. обработващи дейности върху въведените данни за установяване и осигуряване на тяхната актуалност и цялостност.

Чл. 53. В Информационната система не може да се въвежда свободен текст за данни, които представляват номенклатура.

Раздел II

Поддържане на Информационната система и нейните компоненти (техническо поддържане)

Чл. 54. Поддържането на Информационната система обхваща най-малко:

1. поддържане на експлоатационните характеристики, безотказност на подсистемите и модулите и на включените в тях компоненти;
2. поддържане на сигурността на системата и данните съгласно изискванията на нормативната уредба;
3. управление на работния цикъл на системата, нейното надграждане и усъвършенстване;
4. възстановяване на работоспособността на Информационната система след отказ и/или замяна на хардуерен компонент (сървър);
5. осигуряване на помощ и съдействие на потребителите, участващи в работните процеси, свързани със системата, и на ползващите информация от нея.

Чл. 55. (1) В периода на експлоатация Информационната система се поддържа в работоспособно състояние с характеристики не по-ниски от предвидените при създаването ѝ.

(2) Експлоатационното поддържане на Информационната система включва нейното актуализиране в съответствие с променящите се нормативни, технологични и произлизащи от практиката изисквания.

Чл. 56. (1) Поддържането на приложния софтуер за Информационната система и на свързаните с него софтуерни средства включва:

1. отстраняване на проблеми и грешки;
2. адаптиране на софтуера съобразно промени в нормативната уредба, практическите изисквания и технологичното развитие;
3. анализ на функционирането на Информационната система с оглед на подобряване на характеристиките ѝ и набелязване на изисквания за разработване на следващи версии на системата или нова система.

(2) Инсталирането на нова версия на Информационната система се извършва, без тя да спира работа.

(3) Документацията на приложния софтуер се поддържа в актуално състояние в съответствие с корекциите на грешки, отстраняването на проблеми и подобренията в Информационната система. Всяко коригирано издание на софтуера се придружава от коригираща документация.

Чл. 57. Ежегодно структурата по чл. 4 актуализира Ръководството на потребителя за работа с Информационната система (в случай на извършени промени).

Чл. 58. За осигуряване на дейностите по поддържане и развитие на Информационната система, свързани с приемане на доклади за състоянието на системата при възникнал проблем, заявки за услуги и друга кореспонденция, за длъжностните лица по чл. 36 и за представителите на структурата по чл. 4 се създава точка за контакт.

Раздел III

Ред за извършване на промени в работните процеси и за усъвършенстване на Информационната система

Чл. 59. След извършени законодателни, административни, структурни или организационни промени и получена информация на точката за контакт по чл. 58 структурата по чл. 4 изпраща до софтуерния разработчик на Информационната система заявка с изискванията за извършване на промени в работните процеси на системата.

Чл. 60. Началникът на административното звено, инициращо промяна в Информационната система, изпраща заявка по електронен път до началника на административното звено с функции и задачи по развитието и поддръжката на Информационната система в структурата по управление на човешките ресурси към министъра на отбраната.

Чл. 61. Командирът (началникът) на военното формирование или ръководителят на съответната структура при възникнала необходимост изпраща заявка по електронен път до структурата по управление на човешките ресурси към министъра на отбраната за извършване на промени в работните процеси на системата.

Чл. 62. Всяка промяна за усъвършенстване на програмното осигуряване да бъде представяна за разглеждане на заседание на Органа по развитие и експлоатация на КИС „ЩИТ“ след тестване на функционалните възможности за съответствие със заложените технически и функционални изисквания.

Чл. 63. Промените по чл. 62 се въвеждат в експлоатация с решение на Органа по развитие и експлоатация на КИС „ЩИТ“.

Раздел IV

Сигурност на личните данни в Информационната система

Чл. 64. (1) В Информационната система, в която се обработват лични данни, се водят системни дневници (логове) за следните дейности: въвеждане, промяна и изтриване.

(2) Логовете по ал. 1 са за установяване на дата, час и идентификация на потребителя, който е извършил дейностите с данните.

(3) Логовете по ал. 1 се използват единствено за целостта и сигурността на личните данни.

(4) Срокът за съхранение на логовете по ал. 1 е 5 години. След изтичане на срока логовете се архивират и се съхраняват до края на използването на Информационната система.

ДОПЪЛНИТЕЛНА РАЗПОРЕДБА

§ 1. По смисъла на тази инструкция:

1. „Автоматизирано работно място“ (АРМ) за работа с Автоматизираната система за управление на човешките ресурси е работна станция от КИС „ЩИТ“, на която има инсталиран софтуер за работа с Автоматизираната система за управление на човешките ресурси.

2. „Ръководител на структура“ са министърът на отбраната и ръководителите на структурите по чл. 78 от Закона за отбраната и въоръжените сили на

Република България, с изключение на Служба „Военно разузнаване“, или оправомощени от тях длъжностни лица.

3. „Актуалност на данните“ е съответствието им с юридическите факти към определен момент като следствие на честотата на обновяването им.

4. „Цялост на данните“ означава, че личните данни са точни и подходящи за целта, за която се обработват през целия им жизнен цикъл.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 2. Инструкцията се издава на основание чл. 328а, ал. 2 от Закона за отбраната и въоръжените сили на Република България и отменя Инструкция № И-1 от 8.06.2022 г. за условията и реда за организиране, поддържане и достъп до електронния регистър на военнослужещите и цивилните служители – „Автоматизирана система за управление на човешките ресурси“ (ДВ, бр. 45 от 2022 г.).

§ 3. Инструкцията влиза в сила от деня на обнародването ѝ в „Държавен вестник“.

Министър: Атанас Запрянов