ПАЛАЖЭННЕ

аб парадку забеспячэння

прыватнасці пры

апрацоўцы інфармацыі,

якая змяшчае персанальныя дадзеныя

ГЛАВА 1

АГУЛЬНЫЯ ПАЛАЖЭННІ

1. Дадзенае Палажэнне ўстанаўлівае прымяняемыя ў дзяржаўнай установе адукацыі "Станькаўская базавая школа" (далей - Установа) спосабы забеспячэння бяспекі пры апрацоўцы персанальных даных, якімі з'яўляюцца любое дзеянне або сукупнасць дзеянняў, якія ўчыняюцца з персанальнымі данымі, уключаючы збор, сістэматызацыю, захоўванне, змяненне, выкарыстанне, абязлічванне, блакіраванне, распаўсюджванне, прадастаўленне, выдаленне персанальных дадзеных.

2. Дадзенае Палажэнне распрацавана на падставе:

Канстытуцыі Рэспублікі Беларусь;

Працоўнага кодэкса Рэспублікі Беларусь,

Канвенцыі Савета Еўропы аб абароне фізічных асоб пры аўтаматызаванай апрацоўцы персанальных даных ад 28.01.1981;

Хартыі Еўрапейскага саюза аб асноўных правах ад 2007/12/12;

Закона Рэспублікі Беларусь ад 07.05.2021 № 99-З "Аб абароне персанальных даных";

Закона Рэспублікі Беларусь ад 21.07.2008 № 418-З "Аб рэгістры насельніцтва";

Закона Рэспублікі Беларусь ад 10.11.2008 № 455-З "Аб інфармацыі, інфарматызацыі і абароне інфармацыі";

Закона Рэспублікі Беларусь ад 28.05.2021 № 114-З "Аб змяненні законаў па пытаннях працоўных адносін";

іншых нарматыўных прававых актаў Рэспублікі Беларусь.

3. У адпаведнасці з заканадаўствам Рэспублікі Беларусь пад персанальнымі дадзенымі разумеецца любая інфармацыя, якая адносіцца да ідэнтыфікаванай фізічнай асобы або фізічнай асобы, якая можа быць ідэнтыфікавана, у тым ліку яе прозвішча, імя, імя па бацьку, год, месяц, дата і месца нараджэння, адрас, сямейнае, сацыяльнае, маёмаснае становішча, адукацыя, прафесія, даходы, іншая інфармацыя, неабходная Установе ў сувязі з працоўнымі адносінамі.

4. Патрабаванне забеспячэння канфідэнцыяльнасці пры апрацоўцы персанальных даных азначае абавязковае для захавання спецыялістамі Установы, дапушчанымі да апрацоўкі персанальных даных, іншымі асобамі, якія атрымалі доступ да персанальных даных асоб, патрабаванне не дапускаць іх распаўсюджвання без згоды суб'екта персанальных даных або наяўнасці іншай законнай падставы.

5. Забеспячэнне канфідэнцыйнасці персанальных даных не патрабуецца ў выпадку:

абязлічванні персанальных дадзеных (дзеянні, у выніку якіх становіцца немагчымым без выкарыстання дадатковай інфармацыі вызначыць прыналежнасць персанальных дадзеных канкрэтнаму суб'екту персанальных дадзеных);

для агульнадаступных персанальных даных (персанальныя дадзеныя, распаўсюджаныя самім суб'ектам персанальных даных або з яго згоды або распаўсюджаныя ў адпаведнасці з патрабаваннямі заканадаўчых актаў).

6. Пералікі персанальных даных і адказных за захоўванне і апрацоўку персанальных даных зацвярджаецца загадам кіраўніка Установай.

Апрацоўка і захоўванне канфідэнцыйных даных асобамі, якія не ўказаны ў загадзе, забараняецца.

7. У мэтах забеспячэння патрабаванняў захавання прыватнасці і бяспекі пры апрацоўцы персанальных даных Установа прадастаўляе спецыялістам, якія працуюць з персанальнымі данымі, неабходныя ўмовы для выканання ўказаных патрабаванняў:

знаёміць спецыяліста пад подпіс з патрабаваннямі Палітыкі аператара ў дачыненні да апрацоўкі персанальных даных Установы, з Палажэннем аб апрацоўцы і абароне персанальных даных Установы, з гэтым Палажэннем аб парадку забеспячэння канфідэнцыйнасці пры апрацоўцы інфармацыі, якая змяшчае персанальныя даныя, са службовай інструкцыяй і іншымі лакальнымі прававымі актамі Установы ў сферы забеспячэння канфідэнцыяльнасці і бяспекі персанальных даных;

уяўляе сховішчы для дакументаў, сродкі для доступу да інфармацыйных рэсурсаў (ключы, паролі і т. п.);

навучае правілам эксплуатацыі сродкаў аховы інфармацыі;

праводзіць іншыя неабходныя мерапрыемствы.

8. Спецыялістам Установы, якія працуюць з персанальнымі дадзенымі, забараняецца паведамляць іх вусна ці пісьмова каму б там ні было, калі гэта не выклікана службовай неабходнасцю. Пасля падрыхтоўкі і перадачы дакумента файлы чарнавікоў і варыянтаў дакумента пераносяцца які падрыхтаваў іх супрацоўнікам на маркіраваныя носьбіты, прызначаныя для захоўвання персанальных дадзеных.

Без узгаднення з кіраўніком структурнага падраздзялення фарміраванне і захоўванне баз даных (картатэк, файлавых архіваў і інш.), якія змяшчаюць канфідэнцыйныя даныя, забараняецца.

9. Спецыялісты Установы, якія працуюць з персанальнымі данымі, абавязаны выкарыстоўваць інфармацыю аб персанальных даных выключна для мэт, звязаных з выкананнем сваіх працоўных абавязкаў.

10. Пры спыненні выканання працоўнай функцыі, звязанай з апрацоўкай персанальных дадзеных, усе носьбіты інфармацыі, якія змяшчаюць персанальныя дадзеныя (арыгіналы і копіі дакументаў, машынныя і папяровыя носьбіты і інш.), якія знаходзіліся ў распараджэнні спецыяліста ў сувязі з выкананнем службовых абавязкаў, дадзены работнік павінен перадаць свайму непасрэднаму кіраўніку.

11. Перадача персанальных даных трэцім асобам дапускаецца толькі ў выпадках, устаноўленых заканадаўствам Рэспублікі Беларусь, Палітыкай аператара ў адносінах да апрацоўкі персанальных даных Установы, Палажэннем аб апрацоўцы і абароне персанальных даных Установы, Палажэннем аб парадку забеспячэння канфідэнцыйнасці пры апрацоўцы інфармацыі, якая змяшчае персанальныя даныя Установы, службовай. інструкцыяй і іншымі лакальнымі прававымі актамі Установы ў сферы забеспячэння канфідэнцыяльнасці і бяспекі персанальных даных

Перадача персанальных даных ажыццяўляецца адказнай за апрацоўку персанальных даных асобай Установы на падставе пісьмовага або вуснага даручэння кіраўніка структурнага падраздзялення.

12. Перадача звестак і дакументаў, якія змяшчаюць персанальныя даныя, афармляецца шляхам складання акта па ўстаноўленай форме.

13. Спецыялісты Установы, якія падалі персанальныя даныя трэцім асобам, накіроўваюць пісьмовае паведамленне суб'екту персанальных даных аб факце перадачы яго даных трэцім асобам.

14. Забараняецца перадача персанальных даных па тэлефоне, факсе, электроннай пошце, за выключэннем выпадкаў, устаноўленых заканадаўствам і дзейнымі ва Установы лакальнымі прававымі актамі.

Адказы на запыты грамадзян і арганізацый даюцца ў тым аб'ёме, які дазваляе не выдаваць у адказах персанальныя дадзеныя, за выключэннем дадзеных, якія змяшчаюцца ў матэрыялах заяўніка або апублікаваных у агульнадаступных крыніцах.

15. Спецыялісты Установы, якія працуюць з персанальнымі дадзенымі, абавязаны неадкладна паведамляць свайму непасрэднаму кіраўніку і (або) галоўнаму спецыялісту па інфармацыйнай бяспецы аб усіх вядомых фактах атрымання трэцімі асобамі несанкцыянаванага доступу або спробы атрымання доступу да персанальных даных, аб страце або нястачы носьбітаў інфармацыі. , якія змяшчаюць персанальныя дадзеныя, пасведчанняў, пропускаў, ключоў ад сейфаў (сховішчаў), асабістых пячатак, электронных ключоў і іншых фактах, якія могуць прывесці да несанкцыянаванага доступу да персанальных дадзеных, а таксама аб прычынах і ўмовах магчымай уцечкі гэтых звестак.

16. Спецыялісты, якія ажыццяўляюць апрацоўку персанальных даных, за невыкананне патрабаванняў канфідэнцыяльнасці, абароны персанальных даных нясуць дысцыплінарную, адміністрацыйную, грамадзянска-прававую або крымінальную адказнасць у адпаведнасці з заканадаўствам Рэспублікі Беларусь.

17. Адсутнасць кантролю з боку Установы за належным выкананнем работнікам сваіх абавязкаў у галіне забеспячэння канфідэнцыяльнасці і бяспекі персанальных даных не вызваляе работніка ад такіх абавязкаў і прадугледжанай заканадаўствам Рэспублікі Беларусь адказнасці.

РАЗДЗЕЛ 2

ПАРАДАК ЗАБЕСПЯЧЭННЯ БЯСПЕКІ ПРЫ АПРАЦОЎКІ ПЕРСАНАЛЬНЫХ ДАНЫХ, АБДЗЕЛЬНАЙ БЕЗ ВЫКАРЫСТАННЯ СРОДКАЎ АЎТАМАТЫЗАЦЫІ

18. Апрацоўка персанальных даных, у тым лiку якiя ўтрымлiваюцца ў iнфармацыйнай сiстэме персанальных даных або вынятых з такой сiстэмы, лiчыцца ажыццёўленай без выкарыстання сродкаў. аўтаматызацыі (неаўтаматызаванай), калі такая апрацоўка ажыццяўляецца пры непасрэдным удзеле чалавека.

19. Кіраўнік структурнага падраздзялення, якое ажыццяўляе апрацоўку персанальных даных без выкарыстання сродкаў аўтаматызацыі:

вызначае месцы захоўвання персанальных даных (матэрыяльных носьбітаў);

ажыццяўляе кантроль наяўнасці ў структурным падраздзяленні ўмоў, якія забяспечваюць захаванасць персанальных даных і выключаюць несанкцыянаваны да іх доступ;

інфармуе асоб, якія ажыццяўляюць апрацоўку персанальных даных без выкарыстання сродкаў аўтаматызацыі, аб пераліку апрацоўваных персанальных даных, а таксама аб асаблівасцях і правілах ажыццяўлення такой апрацоўкі;

арганізуе паасобнае, гэта значыць не якое дапускае змешванне, захоўванне матэрыяльных носьбітаў персанальных дадзеных (дакументаў, дыскаў, дыскет, USB флэш-назапашвальнікаў, інш.), апрацоўка якіх ажыццяўляецца ў розных мэтах.

20. Пры фіксацыі персанальных даных на матэрыяльных носьбітах не дапускаецца фіксацыя на адным матэрыяльным носьбіце персанальных даных, мэты апрацоўкі якіх заведама не сумяшчальныя. Для апрацоўкі розных катэгорый персанальных даных, што ажыццяўляецца без выкарыстання сродкаў аўтаматызацыі, для кожнай катэгорыі персанальных даных павінен выкарыстоўвацца асобны матэрыяльны носьбіт.

21. Пры несумяшчальнасці мэт апрацоўкі персанальных даных кіраўнік структурнага падраздзялення павінен забяспечыць раздзельную апрацоўку персанальных даных.

22. Знішчэнне або абязлічванне часткі персанальных даных, калі гэта дапускаецца матэрыяльным носьбітам, павінна праводзіцца спосабам, які выключае далейшую апрацоўку гэтых персанальных даных з захаваннем магчымасці апрацоўкі іншых даных, зафіксаваных на матэрыяльным носьбіце (выдаленне, вымарванне).

23. Удакладненне персанальных даных пры ажыццяўленні іх апрацоўкі без выкарыстання сродкаў аўтаматызацыі робіцца шляхам абнаўлення або змянення даных на матэрыяльным носьбіце.

ГЛАВА 3

ПАРАДАК ЗАБЕСПЯЧЭННЯ БЯСПЕКІ ПРЫ АПРАЦОЎКІ ПЕРСАНАЛЬНЫХ ДАНЫХ, АБДЗЕЛЬНАЙ З ВЫКАРЫСТАННЕМ СРОДКАЎ АЎТАМАТЫЗАЦЫІ

24. Апрацоўка персанальных даных з выкарыстаннем сродкаў аўтаматызацыі азначае ўчыненне дзеянняў (аперацый) з такімі данымі з дапамогай аб'ектаў вылічальнай тэхнікі ў камп'ютарнай сетцы Установы (далей - КСЦ).

Бяспека персанальных дадзеных пры іх апрацоўцы ў КСЦ забяспечваецца з дапамогай сістэмы абароны персанальных дадзеных, у якую ўваходзяць арганізацыйныя меры і сродкі абароны інфармацыі, а таксама выкарыстоўваныя ў КСЦ інфармацыйныя тэхналогіі.

Тэхнічныя і праграмныя сродкі абароны інфармацыі павінны задавальняць усталёўваным у адпаведнасці з заканадаўствам Рэспублікі Беларусь патрабаванням, якія забяспечваюць абарону інфармацыі. Сродкі абароны інфармацыі, якія прымяняюцца ў КСЦ, ва ўстаноўленым парадку праходзяць працэдуру ацэнкі адпаведнасці.

25. Допуск асоб да апрацоўкі персанальных даных з выкарыстаннем сродкаў аўтаматызацыі ажыццяўляецца на падставе загада кіраўніка Установы пры наяўнасці пароляў доступу.

Праца з персанальнымі дадзенымі, якія змяшчаюцца ў КСЦ, ажыццяўляецца ў адпаведнасці з "Рэгламентам дзеянняў карыстальніка", з якімі работнік, у службовыя абавязкі якога ўваходзіць апрацоўка персанальных дадзеных, знаёміцца ​​пад подпіс.

26. Праца з персанальнымі дадзенымі ў КСЦ павінна быць арганізавана такім чынам, каб забяспечвалася захаванасць носьбітаў персанальных дадзеных і сродкаў абароны інфармацыі, а таксама выключалася магчымасць некантралюемага знаходжання ў гэтых памяшканнях старонніх асоб.

27. Камп’ютары і (або) электронныя папкі, у якіх змяшчаюцца файлы з персанальнымі дадзенымі, для кожнага карыстальніка павінны быць абаронены індывідуальнымі паролямі доступу Установы.

28. Перасылка персанальных даных без выкарыстання спецыяльных сродкаў абароны па агульнадаступных сетках сувязі, у тым ліку Інтэрнэту, забараняецца.

29. Пры апрацоўцы персанальных даных у КСЦ карыстальнікамі павінна быць забяспечана:

выкарыстанне прызначаных для гэтага раздзелаў (каталогаў) носьбітаў інфармацыі, убудаваных у тэхнічныя сродкі, або здымных маркіраваных носьбітаў;

недапушчэнне фізічнага ўздзеяння на тэхнічныя сродкі аўтаматызаванай апрацоўкі персанальных даных, у выніку якога можа быць парушана іх функцыянаванне;

сталае выкарыстанне антывіруснага забеспячэння для выяўлення заражаных файлаў і неадкладнае ўзнаўленне персанальных дадзеных, мадыфікаваных ці знішчаных з прычыны несанкцыянаванага доступу да іх;

недапушчэнне несанкцыянаваных вынасу з памяшканняў, усталёўкі, падлучэнні абсталявання, а таксама выдаленні, усталёўкі або налады праграмнага забеспячэння.

30. Пры апрацоўцы персанальных даных у КСЦ распрацоўшчыкамі і адміністратарамі інфармацыйных сістэм павінны забяспечвацца:

навучанне асоб, якія выкарыстоўваюць сродкі абароны інфармацыі, якія прымяняюцца ў КСЦ, правілам работы з імі;

улік асоб, дапушчаных да працы з персанальнымі дадзенымі ў КСЦ, правоў і пароляў доступу;

улік ужывальных сродкаў абароны інфармацыі, эксплуатацыйнай і тэхнічнай дакументацыі да іх;

кантроль за выкананнем умоў выкарыстання сродкаў абароны інфармацыі, прадугледжаных эксплуатацыйнай і тэхнічнай дакументацыяй;

апісанне сістэмы аховы персанальных даных.

31. Спецыфічныя патрабаванні па абароне персанальных даных у асобных аўтаматызаваных сістэмах Установы вызначаюцца зацверджанымі ва ўстаноўленым парадку інструкцыямі па іх выкарыстанні і эксплуатацыі.

ГЛАВА 4

ПАРАДАК УЛІКУ, ЗАХОЎВАННІ І ЗВАРОТЫ са здымнымі носьбітамі персанальных дадзеных, цвёрдымі копіямі І ІХ УТЫЛІЗАЦЫІ

32. Усе якія знаходзяцца на захоўванні і ў звароце ва Установе здымныя носьбіты (дыскі, дыскеты, USB флэш-назапашвальнікі, інш.), якія змяшчаюць персанальныя дадзеныя, падлягаюць уліку. Кожны здымны носьбіт з запісанымі на ім персанальнымі дадзенымі павінен мець этыкетку, на якой паказваецца яго ўнікальны ўліковы нумар.

33. Улік і выдачу здымных носьбітаў персанальных даных ажыццяўляе інжынер-праграміст Установы або ўпаўнаважаная асоба.

Работнікі Установы атрымліваюць улічаны здымны носьбіт ад упаўнаважанага супрацоўніка для выканання работ на канкрэтны тэрмін.

Пры атрыманні робяцца адпаведныя запісы ў часопісе персанальнага ўліку здымных носьбітаў персанальных даных (далей - часопіс уліку), які вядзецца ва Установе.

Па канчатку прац карыстач здае здымны носьбіт для захоўвання ўпаўнаважанаму супрацоўніку, пра што робіцца адпаведны запіс у часопісе ўліку.

34. Пры рабоце са здымнымi носьбiтамi, якiя змяшчаюць персанальныя даныя, забараняецца:

захоўваць здымныя носьбіты з персанальнымі дадзенымі разам з носьбітамі адкрытай інфармацыі, на працоўных сталах або пакідаць іх без нагляду або перадаваць на захоўванне іншым асобам;

выносіць здымныя носьбіты з персанальнымі дадзенымі са службовых памяшканняў для працы з імі дома, у гасцініцах і г. д.

35. Пры адпраўцы або перадачы персанальных дадзеных адрасатам на здымныя носьбіты запісваюцца толькі прызначаныя адрасатам дадзеныя. Адпраўка персанальных даных адрасатам на здымных носьбітах ажыццяўляецца ў парадку, устаноўленым для дакументаў для службовага карыстання. Вынас здымных носьбітаў персанальных даных для непасрэднай перадачы адрасату ажыццяўляецца толькі з пісьмовага дазволу кіраўніка структурнага падраздзялення Установы.

36. Аб фактах страты здымных носьбітаў, якія змяшчаюць персанальныя даныя, або выдаванні змешчаных у іх звестак павінна быць неадкладна паведамлена кіраўніку Установы.

На страчаныя носьбіты складаецца акт. Адпаведныя адзнакі ўносяцца ў часопісы ўліку.

ГЛАВА 5

ЗАКЛЮЧНЫЯ ПАЛАЖЭННІ

37. З гэтым Палажэннем павінны быць азнаёмлены пад подпіс у Журнале ўліку допуску да апрацоўкі персанальных даных усе работнікі Установы і асобы, якія выконваюць работы па дагаворах і кантрактах, якія маюць дачыненне да апрацоўкі персанальных даных работнікаў Установы. Адказны за інструктаж - ўпаўнаважаная асоба.