Приложение №2
к приказу об организации защиты
персональных данных
от «26» 05. 2023 г. № 68/4-од

C=RU, O="ГБПОУ СО ""
Борский государственный
техникум""", CN=Беляев
Александр Анатольевич,
E=bgt-borskoe@yandex.ru
место подписания
2023.05.29 09:47:52+03'00'

ПОЛОЖЕНИЕ
о защите персональных данных в информационных системах персональных данных ГБПОУ СО «Борский государственный техникум»

Перечень использованных сокращений

АРМ – Автоматизированное рабочее место

ИС – Информационная система

ИСПДн – Информационная система персональных данных

НСД – Несанкционированный доступ

ПДн – Персональные данные

ПО – Программное обеспечение

СВТ – Средство вычислительной техники

СЗИ – Средство защиты информации

1. Общие положения

1.1. Настоящее Положение о защите персональных данных в информационных системах персональных данных Государственного бюджетного профессионального образовательного учреждения Самарской области «Борский государственный техникум» (далее – Положение) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г., методическими рекомендациями ФСТЭК России и ФСБ России.

1.2. Положение разработано в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.3. Положение определяет порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений при их обработке, порядок обучения персонала практике работы в ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения,

правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в защищаемые помещения.

2. Порядок предоставления допуска пользователей к работе в ИСПДн

2.1 Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.2 Первоначальный допуск пользователей к работе в ИСПДн осуществляется на основании матрицы доступа к обработке персональных данных, которая утверждается приказом Директора (далее Директор) Государственного бюджетного профессионального образовательного учреждения Самарской области «Борский государственный техникум» (далее – ГБПОУ СО «Борский государственный техникум»). В матрице определяется список работников, допущенных к работе с ПДн.

2.3 С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации и выполнения необходимых мероприятий по обеспечению безопасности в ИСПДн руководителем назначается ответственный за обработку ПДн.

2.4 С целью соблюдения принципа персональной ответственности за свои действия каждому работнику, допущенному к работе в ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИСПДн.

2.5 Использование несколькими работниками при работе в ИСПДн одного и того же имени пользователя ***запрещено.***

2.6 В дальнейшем процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется обращением к администратору ИСПДн.

3. Порядок работы пользователей ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн

3.1 Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

3.2 Пользователь несет ответственность за правильность включения и выключения **средств вычислительной техники** (СВТ), входа в систему и все действия при работе в ИСПДн.

3.3 Перед началом работы в ИСПДн работники учреждения, допущенные к работе с ПДн, принимают под роспись обязательство о неразглашении персональных данных.

3.4 Вход пользователя в систему должен осуществляться по выдаваемому ему электронному идентификатору и по персональному паролю.

3.5 При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

3.6 Каждый работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и **обязан**:

a. строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

b. знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;

c. хранить в тайне свой пароль (пароли). В соответствии с п. 6.4. данного Положения и с установленной периодичностью менять свой пароль (пароли);

d. хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в недоступном для посторонних месте;

e. выполнять требования Положения по организации антивирусной защиты в полном объеме;

f. немедленно известить администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

– фактов совершения попыток несанкционированного доступа (далее - НСД) к ИСПДн;

– несанкционированных изменений в конфигурации программных или аппаратных средств ИСПДн;

– отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

– некорректного функционирования установленных на компьютеры технических средств защиты;

– непредусмотренных отводов кабелей и подключенных устройств.

g. Пользователю категорически **запрещается**:

– использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

– осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

– записывать и хранить ПДн на неучтенных машинных носителях информации;

– оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД(несанкционированного доступа) (временную блокировку экрана и клавиатуры);

– оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие ПДн;

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению конфиденциальности ПДн;

– размещать средства отображения информации (монитор, принтер и т.п.) таким образом, чтобы с них существовала возможность визуального считывания информации посторонними лицами.

h. Администратор ИСПДн обязан:

– знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;

– контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;

– производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:

– реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

– вводить описания пользователей ИСПДн в информационную базу системы разграничения доступа в ИСПДн;

– своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;

– проводить инструктаж работников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;

– контролировать своевременное (не реже чем один раз в течение 360 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;

– обеспечивать постоянный контроль выполнения работниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;

– осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;

– настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;

– организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации;

– периодически тестировать функции СЗИ от НСД с использованием специальных средств анализа защищенности, особенно при изменении программной среды и полномочий исполнителей;

– восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;

– вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;

– периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования;

– проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

– обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание персональных данных на носителях информации);

– присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;

– вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

4. Порядок резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных, защищаемой информации и средств защиты информации

4.2. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

4.3. К использованию, для создания резервной копии в ИСПДн, допускаются только зарегистрированные в Журнале учета носители.

4.4. Администратор ИСПДн **обязан** осуществлять периодическое резервное копирование персональных данных.

4.5. Носители информации, предназначенные для создания резервной копии и хранения персональных данных, выдаются установленным порядком администратором ИСПДн. По окончании процедуры резервного копирования электронные носители сдаются на хранение администратору ИСПДн, или Директору.

4.6. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

4.7. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором ИСПДн в специальном хранилище.

4.8. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.

4.9. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных.

4.10. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся у администратора ИСПДн. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

4.11. Ответственность за проведение резервного копирования, мероприятий по восстановлению работоспособности технических средств, мероприятий по восстановлению средств защиты информации возлагается на администратора ИСПДн.

5. Правила антивирусной защиты

5.1. Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения, компьютерных вирусов и устанавливает ответственность Директора и работников, эксплуатирующих и сопровождающих компьютеры в составе ИСПДн, за их выполнение.

5.2. К использованию на компьютерах допускаются только лицензионные антивирусные средства.

5.3. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором ИСПДн.

5.4. Администратор ИСПДн осуществляет периодическое обновление антивирусных средств и контроль их работоспособности.

5.5. Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

5.6. Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров.

5.7. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (флеш-

накопителях, магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

5.8. Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль.

5.9. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором ИСПДн должна быть выполнена антивирусная проверка ИСПДн.

5.10.На компьютеры пользователей запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

5.11.При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором ИСПДн) должен провести внеочередной антивирусный контроль компьютера.

5.12.В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь **обязан**: приостановить обработку данных в ИСПДн;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора ИСПДн, а также смежные подразделения, использующие эти файлы в работе;

– совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;

– провести лечение или уничтожение зараженных файлов.

5.13. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора ИСПДн.

5.14. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной ИСПДн.

6. Правила парольной защиты

6.1. Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями.

6.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора ИСПДн.

6.3. При доступе пользователя в систему должна осуществляться идентификация и проверка подлинности по идентификатору и паролю, а также с использованием электронных идентификаторов.

6.4. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями самостоятельно с учетом следующих требований:

- пароль должен быть длиной не менее восьми буквенно-цифровых символов;
- символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущих;
- пользователь не имеет права сообщать личный пароль другим лицам.

6.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 360 дней.

6.6. Удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри учреждения и т.п.) должна производиться администратором ИСПДн немедленно после окончания последнего сеанса работы данного пользователя с системой, на основании указания Директора или начальника отдела кадров.

6.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри учреждения и другие обстоятельства) администратора ИСПДн.

6.8. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по изменению его пароля.

6.9. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора ИСПДн.

7. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн

7.1. Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

7.2. Право на установку, обновление и модификацию общесистемного и прикладного программного обеспечения компьютеров ИСПДн предоставляется администратору ИСПДн.

7.3. Право внесения изменений в конфигурацию аппаратно-программных средств защиты информации предоставляется администратору ИСПДн, по согласованию с администратором ГБПОУ СО «Борский государственный техникум».

7.4. Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме администратора ИСПДн **запрещено**.

7.5. Изменения в конфигурацию аппаратно-программных средств защищенных рабочих мест ИСПДн, принимает Директор, подтверждая тем самым производственную необходимость проведения изменений.

7.6. Администратор ИСПДн исполняет работы по внесению изменений в конфигурацию компьютера.

7.7. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

7.8. Установка и обновление ПО (системного, прикладного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.).

7.9. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие опасных функций.

7.10. После установки (обновления) ПО администратор ИСПДн должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки.

7.11. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, администратор ИСПДн обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.

8. Порядок контроля обеспечения защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления.

8.1. Контроль защиты информации в ИСПДн – комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

8.2. Основными задачами контроля являются:

a. проверка организации выполнения мероприятий по защите информации в учреждении, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

b. выявление демаскирующих признаков объектов ИСПДн;

c. уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

d. проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

e. проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

f. проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

g. проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;

h. оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;

i. разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

9. Порядок охраны и допуска посторонних лиц в помещения ИСПДн

9.1. В учреждении должна быть предусмотрена физическая охрана технических средств ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации.

9.2. В помещениях должна быть установлена охранная и пожарная сигнализация.

9.3. Серверное и коммутационное оборудование ИСПДн должно находиться под надежным замком, в отдельном помещении или запирающемся шкафу, ключ должен храниться у администратора ИСПДн.

9.4. Вскрытие и закрытие помещений осуществляется работниками, работающими в данных помещениях.

9.5. При закрытии помещений и сдачей их под охрану работники, ответственные за помещения проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации на которых содержатся персональные данные, убираются для хранения в запираемый ящик стола или сейф.

9.6. При обнаружении повреждения замков, дверей или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается Директору и(или) ответственному обработку информации.

9.7. При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение, или ответственному за защиту информации, или Директору, или администратору ИСПДн.

10.Заключительные положения

10.1. Требования настоящего Положения обязательны для всех работников, обрабатывающих персональные данные.

10.2. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.