Министерство образования Саратовской области
государственное автономное профессиональное образовательное учреждение
Саратовской области
«Энгельсский промышленно-экономический колледж»
(ГАПОУ СО «ЭПЭК»)

СОГЛАСОВАНО:
Совет учреждения
Протокол
от «14» 11 2022г. № 11
Секретарь _____ Т.А. Чернышева

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 04168B0400A5E9E42C0D2B02F4F47955
Владелец: КУКУШКИН МИХАИЛ АЛЕКСАНДРОВИЧ
Действителен: с 04.03.2022 до 04.06.2023

УТВЕРЖДАЮ:
Директор ГАПОУ СО
«ЭПЭК»
_____ М.А.Кукушкин
Приказ от «02» 12 2022г.
№ 252/1-ЛД

**Инструкция пользователя по обеспечению безопасности информационной системы персональных данных (далее – ИСПДн) в государственном автономном профессиональном образовательном учреждении Саратовской области «Энгельсский промышленно-экономический колледж».**

Энгельс 2022 г.

## 1. Общие положения

Настоящая Инструкция разработана для обеспечения защиты ПДн в ГАПОУ СО «ЭПЭК».

Пользователями информационной системы, предназначенной для обработки информации, содержащие персональные данные (далее – ИСПДн), являются работники, допущенные к работе в ИСПДн, в соответствии с приказом об утверждении списка лиц, которым необходим доступ к ПДн для выполнения служебных (трудовых) обязанностей.

Наиболее вероятными каналами утечки информации для ИСПДн являются:

-несанкционированный доступ к информации, обрабатываемой ИСПДн;

-хищение документов или технических средств с хранящейся в них информацией, а также отдельных носителей информации;

-просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;

-воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

Работа с ПДн строится на следующих принципах:

-принцип персональной ответственности - в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник.

-принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах (передача из рук в руки, снятие копий и т.п.).

## 2.Термины и определения

**Автоматизированное рабочее место (АРМ)** - персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

**Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (статья 3 Федерального закона Российской Федерации от 27.07.2006г. №152-ФЗ «О персональных данных».

**Доступ к информации** – возможность получения информации и её использования (статья 2 Федерального закона Российской Федерации от 27.07. 2006г. №149-ФЗ «Об информации, информационных технологиях и защите информации».

**Защита информации** – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на

информацию, то есть процесс, направленный на достижение информационной безопасности.

**Информация** – сведения (сообщения, данные) независимо от формы их представления (статья 2 Федерального закона Российской Федерации от 27.07.2006г. №149 «Об информации, информационных технологиях и защите информации».

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (статья 3 Федерального закона Российской Федерации от 27.07.2006г. №152 – ФЗ «О персональных данных».

**Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т.д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т.д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

**Носитель информации** – любой материальный объект или среда, используемый для хранения или передачи информации.

**Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (статья 3 Федерального закона Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных»).

**Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

**Угрозы безопасности персональных данных (УБПДн)** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**Уничтожение персональных данных** – действие, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (статья 3 Федерального закона Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных».

## 3. Обязанности работников

Работники, получившие доступ к ПДн, обязаны хранить в тайне эти сведения, ставшие им известными во время работы или иным путем, и

пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки ПДн немедленно информировать руководителя структурного подразделения, ответственного за организацию обработки ПДн.

ПДн не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению сведений ПДн.

В случае оставления занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности подразделения. В том числе: отчеты, инструкции, переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое – либо отношение к деятельности ГАПОУ СО «ЭПЭК», полученные в течение срока работы.

Работники при работе с ПДн обязаны:

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

-выполнять сведения ответственного лица по безопасности ИС, касающиеся защиты информации;

-знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах;

-хранить в тайне свой аутентификатор (пароль доступа в автоматизированную систему, либо ключевой носитель), а также информацию о системе защиты, установленной в ИСПДн;

-контролировать обновления антивирусных баз и в случае необходимости сообщать о необходимости обновления администратору безопасности;

Немедленно ставить в известность ответственного за организацию и обработку ПДн, ответственное лицо по безопасности:

-при подозрении компрометации личных ключей и паролей;

-при попытках несанкционированного доступа к защищенной ИСПДн;

-несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

-в случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ, или периферийных устройств (принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в автоматизированной системе технических средств защиты, ставить в известность администратора безопасности и (или) ответственного за организацию и обработку персональных данных.

Ставить в известность ответственное лицо по безопасности при:

-необходимости обновления антивирусных баз;

-обновления программного обеспечения;

-проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации ИСПДн;

-необходимости вскрытия системных блоков персональных компьютеров, входящих в состав ИСПДн;

-резервном копировании информации.

Вынос ПЭВМ, на которой производилась обработка ПДн, за пределы территории здания с целью их ремонта, замены и т.п. без согласования с ответственным за ПДн, запрещен. ПЭВМ, используемые для работы с ПДн, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора, не имеющими отношения к конкретно обрабатываемой информации работниками.

Запрещается:

-передавать, кому бы то ни было (в том числе родственникам) устно или письменно сведения ограниченного распространения;

-использовать сведения ограниченного распространения при подготовке открытых публикаций, докладов, научных работ и т.д.;

-выполнять работы с документами ограниченного распространения на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения директора ГАПОУ СО «ЭПЭК»;

-передавать или принимать без расписки документы ограниченного распространения;

-использовать компоненты программного и аппаратного обеспечения ИСПДн подразделения в неслужебных целях;

-самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительные любые программные и аппаратные средства.

-осуществлять обработку Пдн в присутствии посторонних (не допущенных к данной информации) лиц;

-записывать и хранить ПДн на неучтенных съемных носителях информации.

## Ответственность работников

Пользователь несет ответственность за соблюдение требований настоящей Инструкции, а также других нормативных документов в области защиты информации. За разглашение информации ограниченного распространения, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

За разглашение информации ограниченного распространения, нарушения порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.