Министерство образования
Калининградской области
государственное бюджетное учреждение
Калининградской области
профессиональная образовательная организация
«Полесский техникум профессиональных технологий»
(ГБУ КО ПОО «ПТПТ»)

ИНСТРУКЦИЯ

пользователя информационных систем персональных данных государственного бюджетного учреждения Калининградской области профессиональной образовательной организации «Полесский техникум профессиональных технологий»

г. Полесск
2015 г.

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных

1. Общие положения

1.1. Настоящая Инструкция определяет задачи, функции, обязанности, права и ответственность пользователей, допущенных к работе в информационной системе персональных данных (далее – ИСПДн).

1.2. Пользователь информационных систем персональных данных (далее – Пользователь) осуществляет обработку персональных данных (далее – ПДн) в ИСПДн.

1.3. Пользователями являются сотрудники государственного бюджетного учреждения Калининградской области профессиональной образовательной организации «Полесский техникум профессиональных технологий» (далее – образовательная организация), имеющие доступ к программному обеспечению, средствам защиты и участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации, содержащей ПДн, допущенные к работе в ИСПДн в соответствии с приказом «О назначении ответственных за организацию обработки персональных данных».

1.4. Пользователь несет персональную ответственность за свои действия при обработке ПДн на средствах вычислительной техники (далее – СВТ).

1.5. Пользователь в своей работе руководствуется настоящей Инструкцией, Положением «О защите персональных данных», руководящими и нормативными документами Федеральной службы по техническому и экспортному контролю России и регламентирующими документами образовательной организации.

1.6. Методическое руководство работой пользователя осуществляется ответственным лицом за организацию обработки ПДн и выполнению мероприятий по обеспечению безопасности ПДн в образовательной организации.

2. Обязанности пользователя

2.1. При обработке ПДн пользователь обязан:

- знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите персональных данных и распоряжений, регламентирующих порядок действий по защите персональных данных;

- выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры, которые определены для него в соответствии со списком постоянных пользователей и разграничение прав доступа к обрабатываемым ПДн в ИСПДн;

- знать и соблюдать установленные требования по режиму обработки ПДн по учету и хранению съемных носителей информации. Проверять перед началом работы файлы, хранящиеся на съемных носителях информации, на наличие компьютерных вирусов.
Антивирусный контроль должен осуществляться пользователем не реже одного раза в неделю;

- соблюдать установленный режим разграничения доступа к информационным ресурсам: иметь пароль безопасности, надежно его запомнить и хранить в тайне, выполняя требования парольной политики образовательной организации;

- помнить личные пароли и идентификаторы;

- соблюдать установленную технологию обработки информации;

- соблюдать правила при обработке в сетях общего доступа и международного обмена (сеть – Интернет);

- соблюдать правила при использовании электронной почты;

- располагать экран монитора в помещении во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами;

- руководствоваться требованиями инструкций по эксплуатации установленных средств вычислительной техники и средств защиты информации;

- обо всех выявленных нарушениях, связанных с информационной безопасностью образовательной организации, необходимо обратиться к администратору информационной безопасности (далее – Администратор ИБ) или к главе администрации;

- блокировать ввод-вывод на своем рабочем месте ИСПДн в случаях кратковременного отсутствия (перерыв) или выключать СВТ ИСПДн;

- блокировать вывод информации на монитор СВТ.

2.3. Для получения консультаций по вопросу работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИБ образовательной организации.

2.4. Пользователям **запрещается**:

- разглашать защищаемую информацию третьим лицам;

- записывать и хранить информацию на неучтенных съемных носителях информации;

- оставлять во время работы съемные носители информации (или СВТ со съемными носителями информации) без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработка информации;

- производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

- самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

- несанкционированно открывать общий доступ к папкам на своей рабочей станции;

- подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

- отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами на данные СВТ;

- обрабатывать на СВТ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;

- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

- производить копирование отдельных файлов с учтенных носителей информации на неучтенные носители информации, в том числе для временного хранения информации;

- работать на СВТ при обнаружении каких-либо неисправностей;

- хранить носители информации вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;

- привлекать посторонних лиц для производства ремонта или настройки СВТ, без согласования с ответственным лицом за обеспечение защиты ПДн;

- при отсутствии визуального контроля за СВТ доступ к ним должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш CTRL-ALT-DEL и выбрать опцию БЛОКИРОВКА;

- принимать меры по реагированию, в случае возникновения внештатных и аварийных ситуаций, с целью ликвидации из последствий, в рамках, возложенных на него функций.

3. Организация парольной защиты.

3.1. Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором ИБ.

3.2. Смена паролей пользователей в ИСПДн проводится самостоятельно не реже, 1 (одного) в десять (десять) дней.

3.3. Полная плановая смена паролей в ИСПДн проводиться не реже 1 (одного) раза в 3 (три) месяца.

3.4. Правила формирования пароля:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

- пароль должен состоять не менее чем из шести буквенно-цифровых символов;

- в пароле должны присутствовать символы трех категорий из числа следующих четырех:

1) прописные буквы английского алфавита от A до Z;

2) строчные буквы английского алфавита от a до z;

3) десятичные цифры (от 0 до 9);

4) символы, не принадлежащие алфавитно-цифровому набору (например, !, %, №, ?, *).

3.5. При формировании пароля **запрещается:**

- использовать в качестве пароля имя входа в систему, простые пароли типа «012», «000» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

- использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

- использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 012345);

- выбирать пароли, которые уже использовались ранее.

3.6. Правила ввода пароля:

- ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;

- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.7. Правила хранения пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.8. Лица, использующие паролирование **обязаны:**

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

- своевременно сообщать Администратору ИБ об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Общие обязанности пользователей по обеспечению информационной безопасности при работе в ИСПДн.

4.1. Каждый пользователь образовательной организации, участвующий в рамках своих функциональных обязанностей в процессе автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным, несет персональную ответственность за свои действия и обязан:

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

- знать и строго выполнять правила работы со средствами защиты информации, установленными на объекте информатизации;

- выполнять требования по организации антивирусной защиты в части, касающейся действий пользователей;

- выполнять требования по организации парольной защиты, хранить в тайне свой пароль (пароли), с установленной периодичностью менять свой пароль (пароли);

- хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

4.2. Немедленно проверять свое рабочее место в случаях обнаружения:

- нарушений целостности пломб (наклеек, нарушении или не соответствии номеров печатей) на аппаратных средствах персонального компьютера (далее

– ПК) или иных фактов совершения в отсутствие пользователя попыток несанкционированного доступа (далее – НСД) к защищенным СВТ;

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

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

- некорректного функционирования установленных на СВТ технических средств защиты;

- непредусмотренных отводов кабелей от СВТ и подключенных к нему устройств.

5. Порядок работы с персональными данными

5.1. Пред началом работы с ПДн:

- исключить несанкционированное пребывание в помещениях образовательной организации, где обрабатываются ПДн посторонних лиц;

- ознакомиться с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации;

- изучить Инструкцию пользователя по системе защиты от несанкционированного доступа (если такое программное оборудование установлено);

- иметь необходимые учтенные документы и (или) сменные носители информации (флэш-карта, СЖД, CD-R, CD-RV).

5.2. В процессе работы с ПДн **необходимо**:

- обрабатывать информацию в соответствии с технологическим процессом обработки информации, имея права доступа к обрабатываемой в системе информации и настройкам системы в соответствии с правами доступа и настройками, установленными Администратором ИБ;

- результаты работы (готовые данные) записываются только на учтенный жесткий диск СВТ в папку пользователя. При возникновении необходимости записи учтенной информации на сменный носитель (флэш-карта, СЖД, CD-R, CD-RV) обратиться к Администратору ИБ.

5.3. Постановка на учет распечатанных конфиденциальных документов производится в установленном порядке.

6. Правила работы в сетях общего доступа и (или) международного обмена

6.1. Работа в сетях общего доступа и (или) международного обмена (далее – сеть Интернет) на элементах ИСПДн должна проводиться при служебной необходимости.

6.2. Сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности.

Образовательная организация как оператор ПДн оставляет за собой право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия.

6.3. При работе с ресурсами сети Интернет **недопустимо:**

- разглашение служебной информации образовательной организации, ставшей известной сотрудникам образовательной организации по служебной необходимости либо иным путем;

- распространение коммерческой тайны;

- публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения или ограничения функциональности любого компьютерного или телекоммуникационного оборудования, или программ для осуществления НСД, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения НСД к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

6.4. При работе в сети Интернет **запрещается:**

- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

- использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой образовательной организации;

- осуществлять работу при отключенных средствах защиты (антивирус и других);

- передавать по Сети защищаемую информацию без использования средств шифрования;

- запрещается скачивать из Сети программное обеспечение и другие файлы;

- запрещается посещение сайтов сомнительной репутации (сайты порнографического содержания, сайты, содержащие нелегально распространяемое программное обеспечение и другие);

- запрещается нецелевое использование подключения к Сети.

7. Правила работы с электронной почтой образовательной организации

7.1. При работе с корпоративной системой электронной почты сотрудникам образовательной организации **запрещается:**

- использовать адрес электронной почты для оформления подписок, без предварительного согласования с директором образовательной организации;

- публиковать свой адрес, либо адреса других сотрудников образовательной организации на общедоступных Интернет ресурсах (форумы, конференции и др.);

- отправлять сообщения с вложенными файлами, общий объем которых превышает 5 Мегабайт;

- открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;

- осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия. Данные действия квалифицируются ка СПАМ и являются незаконными;

- осуществлять массовую рассылку почтовых сообщений рекламного характера без предварительного согласования с директором образовательной организации;

- рассылка через электронную почту материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления НСД, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения НСД к платным ресурсам в сети Интернет, а также ссылки на вышеуказанную информацию;

- распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и (или) авторские и смежные с ним права третьей стороны;

- распространять информацию, содержание и направленность которой запрещены международным и Российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия;

- распространять информацию ограниченного доступа, представляющую коммерческую тайну образовательной организации;

- предоставлять пароли доступа к своему почтовому ящику, лицам, не имеющим доступа к информационным системам образовательной организации.

8. Ответственность

8.1. Пользователь несет персональную ответственность:

- за несоблюдение установленной технологии обработки информации;

- за несоблюдение режима конфиденциальности ПДн при их обработке и хранении в ИСПДн;

- за неправильность понимания и неполноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИСПДн;

- за несоблюдение требований нормативно правовых актов, приказов, распоряжений и указаний, определяющих порядок организации работ по информационной безопасности при работе с ПДн;

- за несоблюдение правил осуществления обработки персональных данных сотрудников в соответствии с положением Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

8.2. Все сотрудники образовательной организации, обрабатывающие ПДн, должны быть предупреждены об ответственности (Приложение 1).

9. Заключительные положения

9.1. Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным в образовательной организации.

9.2. Сотрудники, определенные директором образовательной организации, как пользователи, участвующие в обработке ПДн, должны ознакомиться с настоящей Инструкцией.

9.3. Обязанность ознакомления пользователей с настоящей Инструкцией лежит на ответственном лице за организацию обработки персональных данных и выполнению мероприятий по обеспечению безопасности персональных данных в образовательной организации.

Приложение 1
к Инструкции пользователя ИСПДн

Выдержки из статей Уголовного кодекса РФ.

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, - наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными

работами на срок до двух лет, либо лишением свободы на тот же срок. 2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, - наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

Статья 293. Халатность

Халатность, то есть неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе, если это повлекло существенное нарушение прав и законных интересов граждан или организаций, либо охраняемых законом интересов общества или государства, - наказывается штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо арестом на срок до трех месяцев.