Автономная некоммерческая организация
дополнительного профессионального образования
«Учебно-курсовой комбинат»

УТВЕРЖДАЮ
Директор
АНО ДПО «Учебно-курсовой комбинат»
_____ Н.М. Плотникова
20 мая 2019 г.

ИНСТРУКЦИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ В АНО ДПО «Учебно-курсовой комбинат»

20 мая 2019 г.

г. Коркино

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция определяет основные обязанности и права администратора безопасности информационных систем персональных данных АНО ДПО «Учебно-курсовой комбинат» (далее по тексту – Организация).

1.2. Администратор безопасности информационных систем персональных данных (далее – ИСПДн) назначается приказом руководителя.

1.3. Решение вопросов обеспечения информационной безопасности входит в прямые служебные обязанности администратора безопасности ИСПДн.

1.4. Администратор безопасности ИСПДн обладает правами доступа к любым программным и аппаратным ресурсам ИСПДн Организации.

1.5. Целью защиты информации является:

1.5.1. Предотвращение утечки, хищения, утраты, подделки информации, а также неправомерных действий по уничтожению, модификации, искажению, несанкционированному копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы обеспечения правового режима документированной информации как объекта собственности.

1.5.2. Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в ИСПДн Организации.

1.5.3. Сохранение конфиденциальности информации в соответствии с законодательством Российской Федерации.

1.5.4. Обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

1.6. Основными видами угроз безопасности информационных систем являются:

1.6.1. Противоправные действия третьих лиц.

1.6.2. Ошибочные действия пользователей ИСПДн.

1.6.3. Отказы и сбои технических средств ИСПДн, приводящие к её модификации, блокированию, уничтожению или несанкционированному

копированию, а также нарушению правил эксплуатации ЭВМ и сетевого оборудования.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

2.2.Антивирусная защита – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного ПО при помощи антивирусных программных продуктов.

2.3.Антивирусный программный продукт – программный пакет, предназначенный для эффективной защиты, перехвата и удаления из операционной системы компьютера максимального количества вредоносных (или потенциально вредоносных) программ.

2.4. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)*(ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).*

2.5.Доступ к информации – возможность получения информации и её использования *(ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).*

2.6.Защита информации – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.7.Информация – сведения (сообщения, данные) независимо от формы их представления *(ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).*

2.8.Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств *(ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).*

2.9.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 путём изменения (повышения, фальсификации) своих прав доступа.

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

2.11.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 (*ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).*

2.12.Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (*ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).*

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

2.14. 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, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных (*ст. 19 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»*)

2.15.Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (*ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).*

3. ОБЩИЕ ОБЯЗАННОСТИ

Администратор безопасности ИСПДн обязан:

3.1.Знать перечень сведений, составляющих персональные данные и условия обработки персональных данных в Организации.

3.2.Знать перечень установленных в организации технических средств, в том числе съёмных носителей, конфигурацию ИСПДн и перечень задач, решаемых с её использованием.

3.3.Определять полномочия пользователей ИСПДн (оформление разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей.

3.4.Осуществлять учёт съёмных машинных носителей информации, их уничтожение, либо контроль процедуры их уничтожения, вести **«Журнал учета машинных носителей информации» в АНО ДПО «Учебно-курсовой комбинат».**

3.5.Осуществлять учёт и периодический контроль над составом и полномочиями пользователей автоматизированных рабочих мест (далее АРМ).

3.6.Осуществлять оперативный контроль за работой пользователей защищённых АРМ и адекватно реагировать на возникающие нештатные ситуации, фиксировать их в **«Журнале учета работ в ИСПДн».**

3.7.Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

3.8.Реагировать на попытки несанкционированного доступа к информации в установленном гл.8 настоящей Инструкции порядке.

3.9.Устанавливать и осуществлять настройку средств защиты информации в рамках компетенции.

3.10.По мере необходимости вносить изменения в конфигурацию технических средств ИСПДн, отражать соответствующие изменения в **«Техническом паспорте информационной системы персональных данных».**

3.11.Осуществлять непосредственное управление и контроль режимов работы функционирования применяемых в ИСПДн средств защиты информации, осуществлять проверку правильности их настройки (выборочное тестирование).

3.12.Периодически контролировать целостность печатей (пломб, наклеек) технических средств, используемых для обработки персональных данных.

3.13.Проводить работу по выявлению возможных каналов утечки персональных данных, изучать текущие тенденции в области защиты персональных данных.

3.14.Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты

информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

3.15.Предоставлять доступ к ИСПДн новым пользователям, предоставлять им возможность задать пароль, соответствующий требованиям настоящей Инструкции и **«Инструкции пользователя информационной системы персональных данных».**

3.16.Производить мероприятия по внеплановой смене паролей.

3.17.Вносить плановые и внеплановые изменения в учётную запись пользователей ИСПДн, в том числе по требованию руководителя организации и в случае увольнения сотрудника.

3.18.Осуществлять периодическое резервное копирование баз персональных данных и сопутствующей защищаемой информации, а также осуществлять внеплановое создание резервных копий по требованию пользователей ИСПДн и в иных случаях, когда это необходимо для обеспечения сохранности персональных данных.

3.19.Осуществлять восстановление информации из резервных копий по требованию пользователей ИСПДн и в иных случаях, когда это необходимо для восстановления утраченных сведений.

3.20.Хранить дистрибутивы программного обеспечения, установленного в ИСПДн, в том числе дистрибутивы средств защиты информации, в месте, исключающем несанкционированный доступ к ним третьих лиц.

3.21.Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.

3.22.Заниматься обслуживанием установленных средств криптографической защиты информации (в том числе персональных данных).

3.23.Знать законодательство РФ о защите персональных данных, следить за его изменениями.

3.24.Выполнять иные мероприятия, требуемые техническими и программными средствами ИСПДн для поддержания их функционирования.

4. ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

4.1.К использованию в Организации допускаются только лицензионные средства антивирусной защиты, централизованно закупленные у разработчиков или поставщиков данных средств, которые регистрируются в «Журнале учета средств защиты информации, эксплуатационной и технической документации к ним в АНО ДПО «Учебно-курсовой комбинат».

4.2.Установка средств антивирусного контроля на компьютерах и серверах ИСПДнОрганизации осуществляется администратором безопасности ИСПДнили под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК РФ в области защиты персональных данных.

4.3.Антивирусный контроль должен быть настроен в режиме постоянной антивирусной защиты.

4.4.Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ, передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после её приёма. При передаче файлов, запакованных в архивы, без их распаковки, должна вручную инициироваться антивирусная проверка этих архивов.

4.5.Процедура обновления баз средства антивирусной защиты должна проводиться в автоматическом режиме не реже 1 (Одного) раза в день на всех АРМ ИСПДн, работающих в сети, не реже 1 (Одного) раза в неделю для всех АРМ ИСПДн, работающих автономно.

4.6.Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором безопасности ИСПДн на предмет отсутствия вредоносного программного обеспечения.

4.7.Подключаемые к компьютеру внешние устройства и носители информации должны проверяться антивирусным ПО непосредственно после подключения.

4.8.Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности средств антивирусной защиты) в ИСПДнОрганизации, осуществляется администратором безопасности ИСПДн и всеми должностными лицами, настраивающими и сопровождающими средства антивирусной защиты в ИСПДнОрганизации.

5. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

5.1.Временный пароль, заданный администратором безопасности ИСПДнпри регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему на постоянный пароль, который необходимо менять ежегодно.

5.2.Опечатанные конверты (пеналы) с паролями сотрудников должны храниться в сейфе, к которому исключён доступ других сотрудников Организации и третьих лиц. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии), либо печать администратора безопасности ИСПДн (или печать организации). Все конверты (пеналы) с паролями в обязательном порядке фиксируются в **«Журнале учёта паролей пользователей информационной системы персональных данных».**

5.3.В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

5.4.Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственных за организацию обработки персональных данных, администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

5.5.Администратор безопасности ИСПДнведёт **«Журнал учета паролей пользователя информационной системы персональных данных»,** в котором он отмечает причины внеплановой смены паролей пользователей.

6. ПОРЯДОК РАБОТЫ С МАШИННЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1.Под машинными носителями в настоящей инструкции понимаются следующие носители информации:

- оптические диски (CD, DVD) однократной и многократной записи;
- электронные накопители информации (флэш-память, съемные жесткие диски).

6.2.Машинные носители, содержащие персональные данные, подлежат обязательному учету администратором безопасности ИСПДн в «Журнале учета машинных носителей информации».

6.3.Носители, содержащие персональные данные, должны иметь специальную маркировку. Тип маркировки выбирается администратором безопасности ИСПДн.

6.4.Носители должны храниться в сейфе, расположенном в помещении Организации, и изыматься только для выполнения должностных обязанностей.

6.5.При поступлении нового машинного носителя, который будет использоваться для хранения или передачи персональных данных, администратор безопасности ИСПДн регистрирует его в **«Журнале учета машинных носителей».**

6.6.Учет выдачи машинных носителей ведётся в «Журнале учета машинных носителей», в котором указывается маркировка носителя, дата, время, фамилия, имя и отчество должностного лица, получившего материальный носитель, его подпись.

6.7.В случае возврата должностным лицом машинного носителя в «Журнале учета машинных носителей» администратором безопасности ИСПДн проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.

7. РАЗГРАНИЧЕНИЕ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ИНФОРМАЦИОННЫМ РЕСУРСАМ И СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ

Защита от несанкционированного доступа осуществляется:

7.1.Идентификацией и проверкой подлинности пользователей ИСПДн при доступе к информационным ресурсам Организации.

7.2.Разграничением доступа к обрабатываемым базам данных. Пользователь ИСПДн имеет доступ только к тем информационным ресурсам, которые разрешены для него согласно приказу руководителя Организации. Для осуществления доступа к информационным ресурсам, администратор безопасности ИСПДн назначает конкретному пользователю ИСПДнидентифицирующее имя пользователя и персональный пароль доступа.

7.3.Администратор безопасности ИСПДн должен осуществлять мероприятия по обеспечению защиты информационных ресурсов Организации от несанкционированного доступа и непреднамеренных изменений и разрушений, а также иметь в наличии средства восстановления, резервные копии, предусматривающие процедуру восстановления свойств информационных ресурсов после сбоев и отказов оборудования.

8. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

8.1.К попыткам несанкционированного доступа относятся:

- сеансы работы сИСПДн незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;
- действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

8.2.Привыявлении факта несанкционированного доступа администратор безопасности ИСПДн обязан:

- прекратить несанкционированный доступ кИСПДн;
- доложить руководителю Организации служебной запиской о факте несанкционированного доступа, егорезультате (успешный, неуспешный) и предпринятых действиях;
- известить руководителя организации, в которой работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

9. ПРАВА

Администратор безопасности ИСПДн имеет право:

9.1.Требовать от пользователей ИСПДн выполнения инструкций в части работы с программными, аппаратными средствами ИСПДн и персональными данными.

9.2.Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.

9.3.Проводить внеплановые антивирусные проверки при возникновении угрозы появления вредоносных программ.

9.4.Производить периодические попытки взлома паролей пользователей в целях тестирования системы контроля доступа на наличие уязвимостей. В случае успешной попытки – вправе требовать у пользователя изменения пароля.

9.5.Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

10. ОТВЕТСТВЕННОСТЬ

10.1.Администратор ИСПДн несёт персональную ответственность за соблюдение требований настоящей Инструкции, за средства защиты информации, применяемые в ИСПДнОрганизации, за качество проводимых им работ по обеспечению безопасности персональных данных и завсе действия, совершенные отимени егоучётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

10.2.Администратор ИСПДн при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

10.3.Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) Организации, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник Организации, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Организации (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

10.4.В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии с действующим законодательством об административных правонарушениях РФ.

10.5.В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.