

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите
конфиденциальной информации в
государственном профессиональном образовательном учреждении
Тульской области "Донской политехнический колледж"

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о порядке организации и проведения работ по защите конфиденциальной информации в ГПОУ ТО "ДПК" (далее - Положение) разработано на основании требований:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федерального закона от 27.07.2006 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- постановления Совета Министров - Правительства Российской Федерации от 15 сентября 1993г. № 912-51 «Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам»;
- постановления Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Специальных требований и рекомендаций по технической защите конфиденциальной информации», утвержденных приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

1.2. Под информацией, требующей защиты, понимаются сведения об ГПОУ ТО «ДПК» (далее - колледж) и её деятельности, на распространение которых накладываются ограничения Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

1.3. Персональные данные являются составной частью конфиденциальной информации (далее - информация).

1.4. Цель данного Положения - на основании действующих законодательных актов и руководящих документов по защите информации создать необходимые организационно-правовые основы для построения эффективной системы защиты информации от несанкционированного доступа (СЗИ НСД) при обработке в автоматизированных системах ГПОУ ТО "ДПК" (далее- колледж).

1.5. Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

1.6. Положение определяет порядок организации в колледже работ по разработке и эксплуатации СЗИ НСД к АС.

1.7. Положение предназначено для практического использования должностным лицам ответственным за защиту информации.

1.8. Требования настоящего Положения являются обязательными для исполнения во всех структурных подразделениях, всеми должностными лицами колледжа.

1.9. За общее состояние защиты информации в колледже отвечает директор колледжа.

1.10. Персональная ответственность за организацию и выполнение мероприятий по защите информации в структурных подразделениях колледжа возлагается на руководителей этих подразделений.

1.11. Ответственность за обеспечение защиты информации возлагается непосредственно на пользователя информации в соответствии с инструкцией «По работе пользователей с конфиденциальной информацией на АРМ», утвержденной директором колледжа.

1.12. Проведение работ по защите информации в АС с помощью встроенных средств безопасности лицензионных операционных систем и антивирусного программного обеспечения возлагается на заведующего центром ИКТ.

1.13. Контроль выполнения требований настоящего Положения возлагается на ответственного за защиту конфиденциальной информации.

1.14. Для оказания услуг в области аттестации объектов вычислительной техники необходимо привлекать специализированные организации, имеющие лицензию на этот вид деятельности.

1.15. Используемые аппаратные и программные средства защиты информации должны быть сертифицированы в соответствии с требованиями «Положения о сертификации...», утвержденного постановлением Правительства Российской Федерации от 26.06. 1995 № 608.

2. ОХРАНЯЕМЫЕ СВЕДЕНИЯ И ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ

2.1 Охраняемые сведения - информация, обрабатываемая средствами вычислительной техники (СВТ) АС в структурных подразделениях колледжа, а также представленная в виде носителей на бумажной, магнитной и иной основе.

2.2 Объекты защиты (объекты информатизации):

- АС различного назначения, участвующие в обработке информации;
- технические средства и системы, не обрабатывающие непосредственно информацию, но размещенные в помещениях, где она обрабатывается;
- помещения, где установлены АС.

2.3 Потенциальные угрозы безопасности объектов информатизации.

В качестве угроз безопасности объектов информатизации в колледже рассматриваются:

- использование технических средств для несанкционированного доступа (НСД) к информационным ресурсам АС с целью получения, разрушения, искажения и блокирования информации;
- преднамеренные действия нарушителей посредством НСД к АРМ, к носителям информации, к вводимой и выводимой информации, к программному обеспечению;
- непреднамеренные действия сотрудников колледжа, приводящие к утечке, искажению, разрушению информации, в том числе ошибки эксплуатации СВТ.

2.4 Перехват информации или воздействие на неё с использованием технических средств могут вестись:

- из-за границы контролируемой зоны из близлежащих строений и транспортных средств;
- при посещении колледжа посторонними лицами.

2.5 Применение средства технической разведки для перехвата информации, циркулирующей на объектах информатизации колледжа маловероятно с учётом её характера - персональные данные на сотрудников и обучающихся детей.

2.6 Основное внимание должно быть уделено защите информации, в отношении которой угрозы безопасности реализуются без применения сложных технических средств:

- обрабатываемой АС от НСД и непреднамеренных действий;
- выводимой на экраны мониторов компьютеров;
- хранящейся на физических носителях;
- циркулирующей в ЛВС при несанкционированном подключении к данной сети.

3. ДЕКЛАРИРОВАНИЯ СООТВЕТСТВИЯ И ВВОД В ЭКСПЛУАТАЦИЮ АС

3.1 Необходимым условием для ввода в эксплуатацию АС является её соответствие требованиям ФСТЭК России по безопасности информации. Директор колледжа при условии классификации информационной системы персональных данных (ИСПДн) по 3 классу проводит её оценку соответствия декларированием соответствия АС требованиям нормативно-методической документации ФСТЭК России.

3.2 Для декларирования соответствия аттестационной комиссии, утвержденной приказом директора колледжа, подготавливаются и представляются на объект информатизации:

- перечень сведений конфиденциального характера;
- организационно-распорядительную документацию разрешительной системы доступа персонала к защищаемым ресурсам;
- технический паспорт АС;
- модель угроз для конкретной АС;
- акт категорирования АС;

- акт классификации ИСПДн;
- инструкции пользователям и ответственному за защиту конфиденциальной информации;

- инструкции по эксплуатации средств защиты информации;

3.3 При декларировании соответствия АС требованиям безопасности информации настройки СЗИ с помощью встроенных средств защиты операционной системы компьютера от НСД проводятся силами колледжа.

3.4 По результатам декларирования соответствия ответственным разрабатываются и доводятся до исполнителей инструкции и рекомендации о порядке выполнения мероприятий по защите информации.

4. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

4.1 Замыслом достижения целей защиты информации является обеспечение защиты информации путем строгого соблюдения действующих норм и требований ФСТЭК России, созданием СЗИ НСД к АС и принятием эффективных организационных мер, предписанных руководящими документами.

4.2 Целями технической защиты информации в колледжа являются:

- исключение утечки информации с помощью технических средств разведки;

- предотвращение НСД посторонних лиц к информации, ее разрушения, искажения, уничтожения, блокировки и несанкционированного копирования.

4.3 Целями организационных мероприятий по защите информации в колледже являются:

- исключение непреднамеренных действий сотрудников колледжа, приводящих к утечке, искажению, разрушению информации, в том числе ошибки эксплуатации АС;

- сведение к минимуму возможности нарушения политик безопасности с помощью любых средств, не связанных непосредственно с использованием АС (физический вынос информации на электронном носителе).

4.4 С целью закрытия возможных каналов утечки информации при её обработке и хранении на АС применяются следующие меры защиты:

- использование встроенных средств защиты операционной системы, установленной на компьютере;

- использование технических средств, сертифицированных по требованиям безопасности информации;

- предотвращение организационными мерами НСД к обрабатываемой информации;

- выполнение положений «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», утвержденных приказом Гостехкомиссии России от 30 августа 2002 г. № 282, при организации обработки информации в локальных вычислительных сетях;

- запрет на подключение АС к информационно-телекоммуникационным сетям международного информационного обмена (п.1. Указа Президента РФ от 17.03. 2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»);

- осуществление учета машинных носителей информации и их хранение в надежно запираемых и опечатываемых шкафах;

- организация процесса резервного копирования и архивирования как неотъемлемой части политики защиты информации.

4.5 Документальное оформление мероприятий по защите объекта информатизации включает:

- приказ о вводе в эксплуатацию;

- акт классификации ИСПДн;

- акт категорирования АС по требованиям защиты от НСД к информации;

- технический паспорт;

- «Аттестат соответствия» или декларацию о соответствии.

5. ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ

5.1 Директор колледжа:

- отвечает за организацию работ по защите информации в колледже;

- утверждает перечни сведений конфиденциального характера, защищаемых помещений, основных технических систем и средств, также другие документы по вопросам защиты информации;

- утверждает акты классификации и категорирования АС.

5.2 Ответственный за защиту информации:

- обеспечение безопасности обработки информации с помощью АС;

- порядок подготовки, учета и хранения документов конфиденциального характера, а также машинных носителей конфиденциальной информации;

- порядок передачи информации другим органам и организациям, а также между структурными подразделениями своей организации.

- разрабатывает организационно-распорядительные документы по вопросам защиты информации;

- обеспечивает защиту информации, циркулирующей на объектах информатизации, организывает работы по аттестации объекта вычислительной техники на соответствие нормативным требованиям;

- проводит систематический контроль работы СЗИ, применяемых на объектах информатизации, а также за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;

- не допускает подключения к АС (ЛВС) устройств, не прошедших специальные исследования, не имеющих предписания на эксплуатацию;

- совместно с заведующими структурными подразделениями осуществляет планирование мероприятий по подготовке АС к работе со сведениями

конфиденциального характера, организывает их выполнение и контроль их эффективности;

- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в случае выявления попыток НСД к информации или попыток хищения, копирования, изменения незамедлительно принимает меры пресечения и докладывает директору колледжа;

- в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.

5.3 Ответственный за защиту информации имеет право:

- контролировать исполнение приказов и распоряжений вышестоящих организаций по вопросам обеспечения безопасности информации;

- требовать от руководителей проверяемых подразделений устранения выявленных нарушений и недостатков, давать обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;

- требовать от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;

- рекомендовать запрещать эксплуатацию систем обработки и передачи информации при несоблюдении требований по защите информации;

- определяет порядок и осуществляет контроль ремонта сертифицированных АС;

- вносить предложения по совершенствованию СЗИ НСД, изменению категорий объектов информатизации, степени конфиденциальности обрабатываемой информации.

5.4 Руководители структурных подразделений:

- лично отвечают за защиту информации в структурных подразделениях, сохранность машинных и иных носителей информации;

- организуют выполнение мероприятий по защите информации при использовании технических средств;

- участвуют в определении мест установки и количества АРМ, необходимых для обработки информации, а также пользователей этих АС;

- участвуют в определении правил разграничения доступа к информации в системах и средствах информатизации, используемых в колледже.

6. ПЛАНИРОВАНИЕ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

6.1 Планирование работ по защите информации проводится на основании:

- рекомендаций актов проверок контрольными органами;
- результатов анализа деятельности в области защиты информации;
- рекомендаций и указаний ФСТЭК России;

6.2 Для подготовки и реализации организационных и технических мероприятий по защите информации ответственный составляет годовой план работ по защите информации.

6.3 Контроль выполнения годового плана возлагается на директора колледжа.

7. КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

7.1 С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения НСД к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность систем информатизации, осуществляется контроль состояния и эффективности СЗИ.

7.2 Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

7.3 Повседневный контроль выполнения организационных и технических мероприятий, направленных на обеспечение защиты информации, проводится руководителями структурных подразделений колледжа и ответственным за защиту информации.

7.4 Периодический контроль может осуществляться представителями ФСТЭК России, территориальных органов ФСБ России.

7.5 Допуск представителей этих органов для проведения контроля состояния защиты информации осуществляется в установленном порядке по предъявлению служебных удостоверений и предписаний на право проверки, подписанных руководителем (заместителем) соответствующего органа.

7.6 Ответственный за защиту информации обязан присутствовать при всех проверках по вопросам защиты информации.

7.7 Результаты проверок отражаются в Актах проверок.

7.8 По результатам проверок контролирующими органами ответственный с привлечением заинтересованных должностных лиц в десятидневный срок разрабатывает план устранения выявленных недостатков.

7.9 Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам.

7.10 Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

7.11 При обнаружении нарушений директор принимает необходимые меры по их устранению в сроки, согласованные с органом или должностным лицом, проводившим проверку.