УТВЕРЖДЕНО
приказом директора
ГБПОУ МО
«Воскресенский колледж»
от 02 февраля 2019 № 21/20
Директор ГБПОУ МО
«Воскресенский колледж»
_____А.Ю.Лунина
« 02 » _____02_____ 2019 г.

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите информации в государственном бюджетном профессиональном образовательном учреждении Московской области «Воскресенский колледж»

Действует с 03 февраля 2019 года

Положение принято решением
Управляющего совета колледжа
Протокол от 01 февраля 2019 №1

г. Воскресенск,
2019 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящее Положение разработано на основании требований:

- федерального закона Российской Федерации «О персональных данных» от 27.07.2006 № 152;
- федерального закона Российской Федерации от 27.07.2006 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- постановления Правительства Российской Федерации «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 17.11.2007 № 781
- постановления Правительства Московской области «Об утверждении положения о порядке обращения с информацией ограниченного доступа в исполнительных органах государственной власти Московской области, государственных органах и государственных учреждений Московской области» от 27.11.2002 № 573/46.

1.2 Под информацией, требующей защиты, понимаются сведения из «Перечня сведений конфиденциального характера в ГБПОУ МО «Воскресенский колледж», разработанного на основе Указа Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 6.03.1997 № 188, действующего законодательства и «Сводного перечня сведений конфиденциального характера», утвержденного постановлением Правительства Московской области от 27.11. 2002 № 573/46.

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 ГБПОУ МО «Воскресенский 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 его руководитель.

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

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

Проведения работ по защите информации в АС с помощью встроенных средств безопасности лицензионных операционных систем и антивирусного программного обеспечения возлагается на программиста.

Контроль выполнения требований настоящего Положения возлагается на Заместителя директора колледжа по безопасности (далее –ответственный).

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

1.11 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 техникума и циркулирующая в локальной вычислительной сети (ЛВС) бухгалтерии, а также представленная в виде носителей на бумажной, магнитной и иной основе.

2.2. Объекты защиты (объекты информатизации):

- АС различного уровня и назначения, участвующие в обработке информации, в отделах бухгалтерского учета и отчетности, кадров.
- 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 техникума, 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.

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

2.7. 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. ПОРЯДОК АТТЕСТАЦИИ И ВВОДА В ЭКСПЛУАТАЦИЮ АС

3.1. Все АС должны быть аттестованы на соответствие требованиям по безопасности информации в соответствии с требованиями ФСТЭК России. Это мероприятие является необходимым условием для ввода в эксплуатацию АС.

3.2. Аттестационные испытания проводятся аттестационной комиссией, формируемой аккредитованным ФСТЭК России органом по аттестации по программе, согласованной с колледжем.

3.3. Для проведения испытаний аттестационной комиссии, утвержденной приказом руководителя коледжа, подготавливаются и представляются на объект информатизации:

- акты категорирования и классификации по требованиям защиты от НСД к информации
- технический паспорт;
- состав технических и программных средств;
- перечень сведений конфиденциального характера;
- организационно-распорядительную документацию разрешительной системы доступа персонала к защищаемым ресурсам;
- инструкции пользователям и ответственному за защиту конфиденциальной информации;
- инструкции по эксплуатации средств защиты информации;
- предписания на эксплуатацию технических средств и систем;
- сертификаты соответствия требованиям по безопасности информации на используемые средства защиты информации.

3.6. Аттестационные испытания АС проводятся до полного их завершения в соответствии с программой испытаний вне зависимости от промежуточных результатов испытаний и завершаются выдачей «Аттестата соответствия».

3.7. Перечень характеристик, об изменениях которых требуется обязательно извещать орган по аттестации, указывается в «Аттестате соответствия».

3.8. Разрешение на использование АС выдается руководителем техникума в письменной форме на основании результатов аттестации.

3.9. По результатам аттестации ответственным разрабатываются и доводятся до исполнителей инструкции и рекомендации о порядке выполнения мероприятий по защите информации.

3.10. Обработка конфиденциальной информации до окончания аттестации и распоряжения о вводе в строй объектов информатизации запрещается.

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

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

- использование встроенных средств безопасности операционной системы, установленной на компьютере;
- использование технических средств, сертифицированных по требованиям безопасности информации;
- предотвращение организационными мерами НСД к обрабатываемой информации;
- запрет на подключение СВТ 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.

4.5. Документальное оформление мероприятий по защите объекта информатизации включает:

- приказ о вводе в эксплуатацию;
- акт классификации;
- технический паспорт;

- «Аттестат соответствия».

5. ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ

5.1Директор:
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 Заместитель директора колледжа по безопасности отвечает за организацию работ по защите информации в колледже:

- обеспечение безопасности обработки информации с помощью СВТ;
- 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, организовывает 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 СВТ (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, организовывает 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 руководителю колледжа ;
- в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.

5.3. **Ответственный** 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.

5.6. 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 составляется годовой план работ по защите информации.

6.3. Контроль выполнения годового плана возлагается на руководителя 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.

7.4. Периодический контроль может осуществляться представителями отдела мобилизационной подготовки и защиты информации Министерства образования Московской области и ГУРБ Московской области.

7.5. Ответственный обязан присутствовать при всех проверках по вопросам защиты информации

7.6. Результаты проверок отражаются в Актах проверок.

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

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

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

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