Утверждено
приказом «НКЛПиС»
от 12.01.2016 № 4.2

Положение о порядке организации и проведения работ по защите конфиденциальной информации в ГАПОУ НСО «Новосибирский колледж легкой промышленности и сервиса»

I. Общие положения

1. Настоящее Положение определяет общие требования по защите информации конфиденциального характера (далее - конфиденциальной информации), циркулирующей в ГАПОУ НСО «Новосибирский колледж легкой промышленности и сервиса (далее – колледж) и порядок организации работы по обеспечению ее защиты.

2. Требования Положения являются обязательными для выполнения должностными лицами и работниками (далее – работниками) структурных подразделений.

3. Для подготовки Перечня сведений приказом руководителя создается постоянно действующая комиссия.

4. Отнесение сведений к категории конфиденциальной информации осуществляется на основании Перечня сведений, содержащих конфиденциальную информацию в колледже (далее – Перечень сведений).

5. Перечень сведений разрабатывается комиссией на основе предложений руководителей структурных подразделений колледжа и утверждается решением руководителя.

6. При подготовке предложений о внесении сведений в Перечень сведений руководителями структурных подразделений колледжа должны быть учтены целесообразность отнесения конкретных сведений к категории конфиденциальной информации, вероятные экономические и иные последствия такого отнесения.

7. Руководители структурных подразделений колледжа несут персональную ответственность за принятое ими решение о необходимости отнесения конкретных сведений к информации конфиденциального характера и определения срока действия ограничения на распространение этих сведений.

8. Перечень сведений периодически пересматривается, но не реже, чем через каждые 3 года, в части обоснованности отнесения сведений к категории конфиденциальной информации.

9. Решение о снятии ранее введенных ограничений на распространение информации принимается Экспертной комиссией и утверждается руководителем :

- по предложению руководителей структурных подразделений , в ведении которых находятся документы, содержащие конфиденциальную информацию;
- по результатам проведения комиссией проверки документов.

10. Защита конфиденциальной информации в автоматизированных системах осуществляется путем выполнения комплекса организационных, программных, технических средств и мер по предотвращению утечки ее по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий на нее с целью нарушения, уничтожения, блокирования или искажения информации в процессе обработки, передачи, хранения.

11. Ответственность за выполнение требований по защите конфиденциальной информации в структурных подразделениях колледжа возлагается на их руководителей.

Ответственность за обеспечение защиты конфиденциальной информации на рабочих местах возлагается на пользователей конфиденциальной информации.

12. Разработку мероприятий по защите конфиденциальной информации в автоматизированной системе осуществляют работники, ответственные за защиту информации в колледже.

13. Допуск работников к работе с конфиденциальной информацией, обрабатываемой в автоматизированных системах, осуществляется в соответствии с Инструкцией о порядке работы с конфиденциальной информацией в колледже.

14. Финансирование мероприятий по защите конфиденциальной информации и государственных информационных ресурсов в колледже предусматривается в сметах расходов на его содержание.

II. Термины, сокращения и определения

15. Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

16. Документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

17.. Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

18. Конфиденциальный документ – документ на материальном носителе, имеющий гриф ограничения доступа.

19. Персональные данные – сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

20. СВТ – средства вычислительной техники.

III. Охраняемые средства и сведения.

23. Цель защиты автоматизированных систем, предназначенных для обработки конфиденциальной информации, состоит в предотвращении или существенном снижении ущерба от утечки конфиденциальной информации по техническим каналам, несанкционированного доступа и преднамеренного программно-технического воздействия на конфиденциальную информацию и программные средства.

24. При обработке в автоматизированных системах защите подлежат:

- носители конфиденциальной информации;
- средства вычислительной техники, на базе которых эксплуатируются автоматизированные системы, предназначенные для обработки конфиденциальной информации;
- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые в автоматизированных системах для осуществления приёма, обработки, хранения и передачи конфиденциальной информации;
- технические средства и системы, обрабатывающие информацию, которая не является конфиденциальной, но размещённые в помещениях, где циркулирует конфиденциальная информация, а также помещения, в которых размещаются автоматизированные системы.

25. К охраняемым сведениям автоматизированных систем, предназначенных для обработки конфиденциальной информации, относятся также:

- настройки программных и технических средств защиты информации (включая данные идентификации и авторизации администраторов и пользователей);
- конфигурации автоматизированных систем;
- таблицы разграничения доступа работников к защищаемой информации.

IV. Оценка угроз безопасности информации.

26. Основными угрозами для конфиденциальной информации, обрабатываемой в автоматизированных системах, являются:

- несанкционированное копирование (тиражирование) конфиденциальной информации;
- несанкционированное считывание конфиденциальной информации; хищение носителей конфиденциальной информации; программные вирусы; несанкционированный доступ к сетевым ресурсам;
- перехват конфиденциальной информации, передаваемой по открытым каналам передачи данных;
- аппаратные и программные закладки;
- аппаратные неисправности средств вычислительной техники в составе автоматизированной системы;
- хищение (кража) средств вычислительной техники из состава автоматизированной системы.

V. Мероприятия по защите информации.

27. Организационные мероприятия по защите информации.

1) Выполнение организационных мероприятий по защите конфиденциальной информации, обрабатываемой в автоматизированных системах, предусматривает:

- документальное оформление Перечня сведений конфиденциального характера, подлежащих защите в колледже;
- определение круга работников, допущенных к автоматизированной обработке конфиденциальной информации;
- определение состава технических средств, с помощью которых производится обработка конфиденциальной информации, и её носителей;
- создание системы защиты конфиденциальной информации, определение обязательных требований к ней, а также порядка и условий её эксплуатации;
- назначение работников, ответственных за защиту информации в колледже;

2) Основанием для защиты конфиденциальной информации на автоматизированной системе является обязательное наличие выписки из Перечня сведений конфиденциального характера.

3). Допуск работника к обработке конфиденциальной информации на автоматизированной системе и закрепление за ним оборудования автоматизированной системы, размещённого на его рабочем месте и предназначенного для обработки конфиденциальной информации, осуществляется при наличии в должностном регламенте работника права/обязанности по работе с информацией конфиденциального содержания.

4). Работник, допущенный к обработке конфиденциальной информации на автоматизированной системе, несёт ответственность за соблюдение им установленного в колледже порядка обеспечения режима защиты конфиденциальной информации и неразглашение ставших известными ему сведений конфиденциального характера.

Нарушение конфиденциальности информации работником влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

5). Автоматизированные системы, предназначенные для обработки конфиденциальной информации, комплектуются техническими средствами в соответствии с решаемыми задачами. Их состав должен удовлетворять требованиям стандартов Российской Федерации по электромагнитной совместимости, безопасности, санитарным нормам.

Повышение уровня защищённости конфиденциальной информации при её обработке на автоматизированных системах достигается использованием сертифицированных по требованию безопасности информации средств вычислительной техники.

6). Обработка конфиденциальной информации в автоматизированных системах, подключенных к локальной или распределенной вычислительной сети. разрешается при использовании сертифицированных ФСТЭК России межсетевых экранов;

7) Помещения, в которых размещены автоматизированные системы, предназначенные для обработки конфиденциальной информации, должны исключать возможность бесконтрольного проникновения посторонних лиц и гарантировать сохранность находящихся в них носителей конфиденциальной информации.

28. Технические мероприятия по защите информации.

Технические мероприятия по защите конфиденциальной информации на автоматизированных системах предусматривают технические решения, направленные на предотвращение утечки защищаемой информации по техническим каналам.

1) Сеть передачи конфиденциальной информации должна быть выделенной, т.е. не иметь подключений других автоматизированных систем, в том числе

автоматизированных рабочих мест, на которых производится обработка общедоступной (открытой) информации и имеющих выход в международные информационные сети типа Интернет.

Допускается подключение автоматизированных систем и автоматизированных рабочих мест, обрабатывающих общедоступную (открытую) информацию к выделенной сети передачи данных через сертифицированные межсетевые экраны соответствующего класса защищённости.

Для защиты конфиденциальной информации используются сертифицированные по требованиям безопасности информации технические средства защиты информации.

29. Программные и программно-технические средства по защите информации.

1) Обеспечение требуемого уровня защиты конфиденциальной информации от перехвата её при передаче по открытым каналам связи, несанкционированного доступа к ней и вирусного поражения её достигается применением сертифицированных средств защиты информации.

2) Защита конфиденциальной информации, обрабатываемой на автоматизированных системах, от вирусного поражения предусматривает:

– еженедельное обновление антивирусных баз на рабочих местах;

– обязательную антивирусную проверку любой информации, получаемой и передаваемой по телекоммуникационным каналам, а также информации на съёмных носителях;

– соблюдение на рабочих местах требований инструкции по антивирусной защите;

– установку сертифицированных антивирусных программ на автоматизированные рабочие места осуществляет работник подразделения, ответственного за обслуживание СВТ.

3) Устанавливаемое системное и прикладное программное обеспечение на автоматизированную систему подлежит предварительной проверке на отсутствие вирусов. Проверка осуществляется на обособленном автоматизированном рабочем месте работником департамента, ответственного за обслуживание СВТ.

4) Факт выполнения антивирусной проверки после установки программного обеспечения на автоматизированном рабочем месте регистрируется в специальном журнале подразделения, ответственного за обслуживание СВТ, за подписью работника, проводившего антивирусную проверку (в случае, если журнал не ведется автоматически централизованно на антивирусном сервере).

5) При обнаружении зараженной вирусом информации работник, проводивший проверку, обязан:

- приостановить обработку информации;
- немедленно известить о факте обнаружения зараженной вирусом руководителя подразделения, ответственного за обслуживание СВТ, работника, ответственного за защиту информации, работника, предоставившего зараженную вирусом информацию;
- провести лечение или уничтожение зараженной вирусом информации;
- при обнаружении нового вируса, не поддающегося лечению применяемыми антивирусными программами, направить зараженную вирусом информацию в структурное подразделение, ответственное за обслуживание автоматизированной системы, для дальнейшей передачи его в организацию, с которой заключён договор на антивирусную поддержку.

6) Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах автоматизированной системы и контроль за действиями работников подразделения, ответственного за обслуживание автоматизированной системы, при работе с паролями возлагается на работника, ответственного за защиту информации.

7) Пароли для работников автоматизированной системы генерируются и распределяются централизовано. Пароль содержит не менее 8 символов (с использованием верхнего и нижнего регистров). Новое значение пароля должно отличаться от предыдущего не менее, чем 6 символами.

8) В случае компрометации пароля работник, ответственный за обслуживание СВТ обязан:

- заблокировать автоматизированное рабочее место;
- исключить скомпрометированный пароль;
- ввести в автоматизированную систему новый пароль.

Смена паролей всех работников автоматизированной системы производится при прекращении полномочий работников, которым были предоставлены полномочия по управлению парольной защитой подсистем автоматизированной системы.

Хранение паролей на бумажном носителе допускается в журнале паролей подразделения, обрабатывающего конфиденциальную информацию.

VI. Ответственность должностных лиц по защите информации.

Ответственность за организацию и состояние работ по защите конфиденциальной информации возлагается на руководителей структурных подразделений колледжа, осуществляющих работы со сведениями конфиденциального характера и государственными информационными ресурсами.

Руководство работами по технической защите информации в колледже осуществляется руководителем колледжа через ответственных за техническую защиту информации.

Назначение на должность и освобождение от должности ответственного за техническую защиту информации производится приказом руководителя колледжа.

VII. Планирование работы по защите информации.

30. Работа по защите конфиденциальной информации в автоматизированной системе проводится в соответствии с утверждённым комплексным планом работ по защите конфиденциальной информации (далее - план). Организационные и технические мероприятия плана направлены на обеспечение требуемого уровня защиты конфиденциальной информации.

31. Разработку плана осуществляют ответственные за техническую защиту информации. План подписывает его разработчик и утверждает руководитель по согласованию с Комитетом компьютерных технологий министерства труда, занятости и трудовых ресурсов Новосибирской области.

VIII. Контроль состояния защиты информации.

32. Контроль защиты конфиденциальной информации на автоматизированных системах осуществляется в целях своевременного выявления и предотвращения утечки конфиденциальной информации по техническим каналам, не санкционированного доступа к ней, преднамеренных программно-технических воздействий на неё.

33. Основными задачами контроля являются:

- получение объективной оценки состояния защиты конфиденциальной информации;
- оценка эффективности решения программно-технических вопросов обеспечения защиты конфиденциальной информации;
- оценка качества выполнения требований законодательства Российской Федерации, нормативных актов Губернатора Новосибирской области и решений органов защиты государственной тайны по вопросам защиты конфиденциальной информации.

В соответствии со своей компетенцией контроль могут осуществлять должностные лица или комиссии от Управления ФСТЭК России по Сибирскому федеральному округу, Управления ФСБ России по Новосибирской области.

34. Результаты контроля защиты конфиденциальной информации на автоматизированной системе оформляются справкой с отражением в ней состояния защиты конфиденциальной информации в структурных подразделениях департамента. На основании справки составляется план мероприятий по устранению выявленных недостатков и реализации предложений, содержащихся в справке.

Об устранении выявленных недостатков и реализации предложений, в установленные сроки представляется отчет в орган, проводивший контроль.

IX. Аттестация рабочих мест

35. Право на обработку конфиденциальной информации на автоматизированной системе подтверждается Аттестатом соответствия, который выдаётся (оформляется) по результатам аттестационной проверки. Данная проверка проводится органом по аттестации объектов информатизации по требованиям безопасности информации, аккредитованным ФСТЭК России (далее - орган аттестации).

Аттестация автоматизированной системы по требованиям безопасности конфиденциальной информации вызвана необходимостью официального подтверждения эффективности комплекса используемых мер и средств защиты.

36. Инициирует аттестационную проверку автоматизированной системы органом аттестации руководитель колледжа. В этих целях руководитель о принятом решении извещает отдел компьютерных технологий Минтруда Новосибирской области и с его методической помощью осуществляет подготовку заявки и необходимых документов для проведения аттестационной проверки.

37. Оплата расходов по выполнению поставок оборудования и услуг при аттестации автоматизированной системы производится в соответствии с договором между колледжем и органом аттестации.

38. Выдача Аттестата соответствия осуществляется органом аттестации на период не более трёх лет, в течение которого обеспечивается неизменность условий функционирования как автоматизированной системы, так и технологии обработки конфиденциальной информации.

При изменении условий функционирования или технологии обработки конфиденциальной информации на автоматизированной системе его руководитель - владелец Аттестата соответствия, обязан известить об этом соответствующий орган аттестации, который принимает решение о

необходимости проведения дополнительной проверки эффективности системы защиты конфиденциальной информации.

XI. Вопросы взаимодействия

39. В вопросах защиты информации колледж взаимодействует самостоятельно или с помощью министерства труда, занятости и трудовых ресурсов Новосибирской области с:

- Комиссией Новосибирской области по информационной безопасности;
- Федеральной службой по техническому и экспортному контролю (Управлением ФСТЭК России по Сибирскому федеральному округу);
- Федеральной службой безопасности Российской Федерации (Управлением ФСБ России по Новосибирской области);
- Службой специальной связи и информации Федеральной службы охраны Российской Федерации (Управлением специальной связи и информации ФСО России в Сибирском федеральном округе);
- Главным управлением внутренних дел по Новосибирской области;
- организациями, имеющими лицензии на осуществление деятельности в сфере защиты информации;