бюджетное профессиональное образовательное учреждение Вологодской области «Великоустюгский многопрофильный колледж»

УТВЕРЖДЕНА
приказом директора колледжа
от «19» 02 2019 г. № 74

ИНСТРУКЦИЯ

«19» 02 2019 г. № 28

г. Великий Устюг

администратора безопасности автоматизированных систем

1. Общие положения

1.1. Настоящая инструкция является руководящим документом для администратора безопасности (уполномоченного по безопасности) автоматизированной системы объекта информатизации (далее - администратор) в бюджетном профессиональном образовательном учреждении Вологодской области «Великоустюгский многопрофильный колледж» (далее – колледж).

Требования настоящей инструкции должны выполняться во всех режимах функционирования автоматизированной системы (далее - АС).

1.2. Нарушение установленных требований и норм по защите информации по степени важности делятся на три категории:

- первая - невыполнение требований и норм по защите информации, в результате чего имелась или имеется реальная возможность ее утечки по техническим каналам или несанкционированного доступа к ней (далее - НСД);
- вторая - невыполнение требований и норм по защите информации, в результате чего создаются предпосылки к ее утечке по техническим каналам или НСД;
- третья - невыполнение других требований по защите информации.

При выявлении нарушения первой категории администратор обязан немедленно прекратить работы на АС и подать служебную записку директору колледжа, в которой изложить факт нарушения, предпринятые и/или рекомендуемые им действия.

При выявлении нарушений второй и третьей категорий администратор обязан подать служебную записку директору колледжа, в которой изложить факт нарушения, предпринятые и/или рекомендуемые им действия.

1.3. Помимо настоящей инструкции в своей повседневной деятельности администратор руководствуется другими документами, регламентирующими защиту конфиденциальной информации от утечки по техническим каналам и НСД, и эксплуатационной документацией на установленные на объекте информатизации системы защиты от несанкционированного доступа к информации (далее - СЗИ НСД) и от утечки информации по техническим каналам.

2. Общие обязанности Администратора

2.1. Администратор отвечает за:

- соблюдение требований по противодействию утечке информации по техническим каналам;
- обеспечение пользователей АС параметрами опознания;
- обеспечение установленных правил разграничения доступа пользователей к защищаемым информационным ресурсам АС;
- анализ работоспособности СЗИ НСД;
- контроль за соблюдением пользователями установленных правил работы с конфиденциальной информацией;
- обеспечение неизменности системного и прикладного программного обеспечения АС, в том числе и программного обеспечения СЗИ НСД.

2.2. Администратор обязан:

- знать требования документов, регламентирующих защиту конфиденциальной информации от утечки по техническим каналам и НСД, выявлять возможные каналы утечки информации и способы совершения НСД и готовить предложения по их устранению;
- не допускать использования, хранения и размножения на АРМ АС программных продуктов и носителей информации, непосредственно не связанных со служебной деятельностью на данном рабочем месте;
- разработать и утвердить в установленном порядке инструкцию по обеспечению безопасности информации в случаях возникновения чрезвычайных обстоятельств на объекте информатизации, предусматривающую систему мер и действий при стихийном бедствии, пожаре, аварии систем жизнеобеспечения объекта, заражении АРМ компьютерными вирусами, фактов НСД к информации, фактов компрометации параметров идентификации пользователя и т.п.;
- не допускать к работе на АРМ АС посторонних лиц;
- следить за сохранностью голографических наклеек на корпусах ПЭВМ, целостностью печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных ПЭВМ и других устройствах;
- организовывать и координировать работы по защите информации;
- участвовать в планировании эксплуатации АРМ при изменении условий его эксплуатации, контролируя выполнение требований Аттестата соответствия объекта информатизации;
- участвовать в разработке организационных мероприятий по обеспечению защиты информации в подразделении при обработке конфиденциальной информации;
- знать уровень конфиденциальности обрабатываемой информации, следить за тем, чтобы обработка информации производилась только с использованием учтенных съемных и несъемных носителей информации, причем уровень конфиденциальности последних должен быть не ниже уровня конфиденциальности обрабатываемой информации;
- контролировать соблюдение требований по учету, хранению и пересылке носителей конфиденциальной информации;

- вести документацию, предусмотренную документами, регламентирующими защиту конфиденциальной информации от утечки по техническим каналам и НСД;
- при выявлении нарушений действовать в соответствии с п.1.2 настоящей Инструкции;
- знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС), установленных и смонтированных в автоматизированной системе (далее - АС), перечень используемого программного обеспечения (далее - ПО) в АС;
- производить необходимые настройки подсистемы управления доступом установленных в АС средств защиты информации от несанкционированного доступа (далее - СЗИ от НСД) и сопровождать их в процессе эксплуатации, при этом:

а) реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

б) вводить описания пользователей АС в информационную базу СЗИ от НСД;

в) своевременно удалять описания пользователей из базы данных СЗИ от НСД при изменении списка допущенных к работе лиц;
- контролировать доступ лиц в помещение в соответствии со списком сотрудников, допущенных к работе в АС;
- проводить инструктаж работников колледжа - пользователей ПЭВМ по правилам работы с используемыми техническими средствами и системами защиты информации;
- контролировать своевременное проведение смены паролей для доступа пользователей к ПЭВМ;
- обеспечивать постоянный контроль выполнения работниками колледжа установленного комплекса мероприятий по обеспечению безопасности информации в АС;
- осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;
- настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе на ПЭВМ;
- вводить в базу данных СЗИ от НСД описания событий, подлежащих регистрации в системном журнале;
- проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в 10 дней;
- организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации. Сопровождать подсистемы обеспечения целостности информации на ПЭВМ в АС;
- периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;
- восстанавливать программную среду, программные средства и настройки СЗИ от НСД при сбоях;

- вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;
- контролировать отсутствие на магнитных носителях остаточной информации по окончании работы пользователей;
- периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядка и правил проведения антивирусного тестирования;
- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования АС и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;
- контролировать соответствие документально утвержденного состава аппаратной и программной части АС реальным конфигурациям АС, вести учет изменений аппаратно-программной конфигурации;
- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания АС и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта);
- присутствовать (участвовать) при работах по внесению изменений в аппаратно-программную конфигурацию АС;
- вести Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств ПЭВМ;
- поддерживать установленный порядок проведения антивирусного контроля согласно требований Инструкции по антивирусной защите, в случае отказа средств и систем защиты информации принимать меры по их восстановлению;
- докладывать ответственному за осуществление контроля за состоянием уровня защищенности информационных ресурсов и обеспечением защиты информации о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;
- вести документацию на АС в соответствии с требованиями нормативных документов.
- постоянно повышать свою квалификацию.

3. Обязанности Администратора по предотвращению утечки информации по техническим каналам

3.1. Администратор обязан сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований по размещению и использованию технических средств АС.

3.2. Администратор обязан не допускать:
- изменение состава, размещения и изменения уровней излучения средств активной защиты информации, если они установлены в помещениях объекта;
- внесение несанкционированных изменений в системы электроснабжения, заземления и других проводных коммуникаций объекта;

- обработку конфиденциальной информации при выключенных средствах активной защиты информации.

3.3. Администратор обязан периодически (не реже одного раза в месяц) осуществляет контроль работоспособности системы активной защиты согласно эксплуатационной документации на систему.

4. Права Администратора безопасности

4.1. Администратор безопасности имеет право:

- требовать от работников колледжа - пользователей АС соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в АС;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов АС;
- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

СОГЛАСОВАНО
Советом Учреждения
Протокол № 2
«18» 02 20 19 г.

В дело № 01-14
«19» 02 20 19 г.