СОГЛАСОВАНО:
Председатель Профсоюзного комитета Государственного бюджетного профессионального образовательного учреждения Республики Крым «Симферопольский колледж сферы обслуживания и дизайна»
_____ Б.В. Ячменев
«30» 12 2021 г.

УТВЕРЖДАЮ:
Директор Государственного бюджетного профессионального образовательного учреждения Республики Крым «Симферопольский колледж сферы обслуживания и дизайна»
_____ Е.С. Назарова
«30» 12 2021 г.

Введено в действие приказом
от «30» 12 2021 г. № 356-О

Положение
об информационной безопасности Государственного бюджетного профессионального образовательного учреждения Республики Крым «Симферопольский колледж сферы обслуживания и дизайна»

г. Симферополь
2021 год

Содержание

Вводные положения

1.1. Введение

Положение информационной безопасности Государственного бюджетного профессионального образовательного учреждения Республики Крым «Симферопольский колледж сферы обслуживания и дизайна» (далее – Колледж, Положение) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Колледж в своей деятельности.

1.2. Цели

Основными целями Положения являются защита информации Колледжа и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в Уставе.

Общее руководство обеспечением ИБ осуществляет специалист по противопожарной профилактике и чрезвычайным ситуациям. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет системный администратор, выполняющий функции администратора информационной безопасности в Колледже (далее - администратор информационной безопасности).

Сотрудники Колледжа обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящего Положения и других документов ИБ.

1.3. Задачи

Положение информационной безопасности направлено на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Задачами настоящего Положения являются описание организации системы управления информационной безопасностью в Колледже; определение политики учетных записей; регламент предоставления доступа к информационному ресурсу; регламент защиты АРМ;

1.4. Область действия

Настоящее Положение распространяется на всех сотрудников Колледжа и обязателен для исполнения всеми сотрудниками. Требования настоящего Положения применимы для использования во внутренних нормативных и методических документах, а также в договорах.

1.5. Период действия и порядок внесения изменений

Настоящее Положение вводится в действие приказом директора Колледжа.

Положение признается утратившим силу на основании приказа директора Колледжа,

Изменения в Положение вносятся приказом директора Колледжа.

Инициаторами внесения изменений в Положение информационной безопасности являются:

- директор Колледжа;

- специалист по противопожарной профилактике и чрезвычайным ситуациям;

- администратор информационной безопасности.

Плановая актуализация настоящего Положения производится ежегодно и имеет целью приведение в соответствие определенных защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация Положения информационной безопасности производится в обязательном порядке в следующих случаях:

- при изменении политики РФ в области информационной безопасности, указов и законов РФ в области защиты информации;

- при изменении внутренних нормативных документов (инструкций, положений, рекомендаций), касающихся информационной безопасности Колледжа;

- при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, влекущего ущерб Колледжа.

Ответственность за актуализацию Положения об информационной безопасности (плановую и внеплановую) несет администратор информационной безопасности.

Контроль за исполнением требований настоящего Положения и поддержанием ее в актуальном состоянии возлагается на специалиста по противопожарной профилактике и чрезвычайным ситуациям.

2. Термины и определения

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

Администратор информационной безопасности – специалист Колледжа (системный администратор), осуществляющий контроль за обеспечением защиты информации, а также осуществляющий организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Аудит информационной безопасности – процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как Колледжем (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит). Результаты проверки документально оформляются свидетельством аудита.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

Доступ к информации – возможность получения информации и ее использования.

Защищенный канал передачи данных – логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных (средствами VPN), либо путем их физической изоляции и размещения на охраняемой территории.

Идентификатор доступа – уникальный признак субъекта или объекта доступа.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – это актив, который, подобно другим активам общества, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов общества.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач отделов Колледжа. В Колледже используются различные типы информационных систем для решения управленческих, учетных, обучающих и других задач.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационные активы – информационные системы, информационные средства, информационные ресурсы.

Информационные средства – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

Инцидент информационной безопасности – действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов учреждения.

Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

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

Конфиденциальность – доступ к информации только авторизованных пользователей.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование отделов Колледжа, привести к причинению материального или иного вида ущерба.

Локальная вычислительная сеть (ЛВС) – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Межсетевой экран (МЭ) – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав сети, а также между сетью Колледжа и внешними сетями (сетью Интернет).

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Регламент информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в Колледже для обеспечения его информационной безопасности.

Пользователь ЛВС – сотрудник Колледжа, а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Регистрационная (учетная) запись пользователя – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название отдела, телефоны, E-mail и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Системный администратор – сотрудник Колледжа, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети учреждения и ПК.

Собственник – лицо или организация, которые имеют утвержденные обязательства по менеджменту для контроля разработки, поддержки, использования и безопасности активов. Термин «собственник» не означает, что лицо действительно имеет какие-либо права собственности на актив.

Средства криптографической защиты информации – средства шифрования, средства электронной подписи, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Угрозы информационным данным – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Управление информационной безопасностью – совокупность целенаправленных действий, осуществляемых в рамках политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности учреждения при реализации угроз в информационной сфере.

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

ЭВМ – электронная - вычислительная машина, персональный компьютер.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца ключа подписи, а также установить отсутствие искажения информации в электронном документе.

VPN (VIRTUAL PRIVATE NETWORK) – «Виртуальная частная сеть»: технология и организация систематической удаленной связи между выбранными группами узлов в крупных распределенных сетях.

3. Обозначения и сокращения

АРМ – Автоматизированное рабочее место.

АС – Автоматизированная система.

БД – База данных.

ЗИ – Защита информации.

ИБ – Информационная безопасность.

ИС – Информационная система.

ИТС – Информационно-телекоммуникационная система.

КЗ – Контролируемая зона.

МЭ – Межсетевой экран.

НСД – Несанкционированный доступ.

ОС – Операционная система.

ПБ – Политики безопасности.

ПО – Программное обеспечение.

СВТ – Средства вычислительной техники.

СЗИ – Средство защиты информации.

СКЗИ – Средство криптографической защиты информации.

СПД – Система передачи данных.

СУБД – Система управления базами данных.

СУИБ – Система управления информационной безопасностью.

СЭД – Система электронного документооборота.

ЭВМ – Электронная - вычислительная машина, персональный компьютер.

ЭЦП – Электронная цифровая подпись.

4. Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются следующие:

- Постоянный и всесторонний анализ информационного пространства с целью выявления уязвимостей информационных активов.

- Своевременное обнаружение проблем, потенциально способных повлиять на ИБ, корректировка моделей угроз и нарушителя.

- Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию.

- Персонификация и адекватное разделение ролей и ответственности между сотрудниками учреждения, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

5. Соответствие Положения действующему законодательству

Правовую основу составляют законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

6. Ответственность за реализацию политики информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт администратор информационной безопасности.

Ответственность за реализацию Положения возлагается:

в части, касающейся исполнения правил Положения, – на каждого сотрудника Колледжа, согласно должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящего Положения.

7. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация просвещения сотрудников Колледжа в области информационной безопасности возлагается на администратора информационной безопасности. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности». Обучение сотрудников Колледжа правилам обращения с конфиденциальной информацией, проводится путем:

- проведения администратором информационной безопасности инструктивных занятий с сотрудниками, принимаемыми на работу в Колледж;

- самостоятельного изучения сотрудниками внутренних нормативных документов Колледжа.

Допуск сотрудников к работе с защищаемыми информационными ресурсами Колледжа осуществляется только после его ознакомления с настоящими Положением. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками Колледжа, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

8. Регламент информационной безопасности Колледжа

Регламент информационной безопасности Колледжа – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в Колледже.

Под Регламентами безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Регламент информационной безопасности относятся к административным мерам обеспечения информационной безопасности и определяют стратегию Колледжа в области ИБ.

Регламенты информационной безопасности определяют эффективную работу средств защиты информации.

8.1. Регламент предоставления доступа к информационному ресурсу

8.1.1. Назначение

Настоящий Регламент определяет основные правила предоставления сотрудникам доступа к защищаемым информационным ресурсам Колледжа.

8.1.2. Положение Регламента

К работе с информационным ресурсом допускаются сотрудники, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящим Регламентом.

Каждому сотруднику Колледжа, допущенному к работе с конкретным информационным ресурсом, должно быть сопоставлено персональное уникальное имя (учетная запись), под которым он будет регистрироваться и работать в ИС.

В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в Колледже одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

8.1.3. Порядок создания (продления) учетной записи пользователя

Процедура регистрации (создания учетной записи), так же продления срока действия временной учетной записи пользователя для сотрудника Колледжа инициируется заявкой (Приложение № 1).

В заявке указывается:

- должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;

- основание для регистрации учетной записи (номер приказа о принятии на работу в Колледж или иного договорного документа, определяющего необходимость предоставления сотруднику доступа к информационным ресурсам Колледжа).

Заявку подписывает специалист кадровой службы, подтверждающий, что указанный сотрудник действительно принят в штат Колледжа.

Администратор информационной безопасности рассматривает представленную заявку и совершает необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и минимальных прав доступа к ресурсам Колледжа.

По окончании регистрации учетной записи пользователя в заявке делается отметка о выполнении задания за подписями исполнителей.

Минимальные права в ИС, определенные выше, а также присвоение начального пароля производится администратором информационной безопасности, при согласовании заявки на предоставление (изменение) прав доступа пользователя к информационным ресурсам.

8.1.4. Порядок удаления учетной записи пользователя

При прекращении срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться.

В заявке указывается:

- должность сотрудника, фамилия, имя и отчество сотрудника;

- имя пользователя (учетной записи) данного сотрудника;

- дата прекращения полномочий пользователя.

Заявку подписывает специалист кадровой службы, утверждая тем самым факт прекращения срока действия полномочий пользователя.

Администратор информационной безопасности рассматривает представленную заявку и совершает необходимые операции по удалению учетной записи пользователя. По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.

В случае необходимости сохранения персональных документов на АРМ сотрудника, после прекращения срока действия его полномочий, сотрудник (или его непосредственный руководитель) должен своевременно (не позднее, чем за 3 суток до момента прекращения срока действия своих полномочий) подать заявку на блокирование учетной записи пользователя с указанием срока хранения указанной информации.

8.2. Регламент защиты АРМ

8.2.1. Назначение

Настоящий Регламент определяет основные правила и требования по защите персональных данных и иной конфиденциальной информации Колледжа от неавторизованного доступа, утраты или модификации.

8.2.2. Положения Регламента

Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.

Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только администратору информационной безопасности. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к администратору информационной безопасности.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

Программное обеспечение должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.

Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию - регламентированы.

АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками Колледжа. Запрещается использование указанных АРМ другими пользователями без согласования с администратором информационной безопасности Колледжа. При передаче указанного АРМ другому пользователю, должна производиться гарантированная очистка диска (форматирование).

8.3. Регламент учетных записей

8.3.1. Назначение

Настоящий Регламент определяет основные правила присвоения учетных записей пользователям информационных активов Колледжа.

8.3.2. Положение Регламента

Регистрационные учетные записи подразделяются на:

- пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов Колледжа;

- системные – используемые для нужд операционной системы;

- служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов Колледжа назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

9. Профилактика нарушений информационной безопасности

Под профилактикой нарушений информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений информационной безопасности в Колледже и проведение разъяснительной работы по информационной безопасности среди пользователей.

Проведение в ИС Колледжа регламентных работ по защите информации предполагает выполнение процедур контрольного тестирования (проверки) функций СЗИ, что гарантирует ее работоспособность с точностью до периода тестирования. Контрольное тестирование функций СЗИ может быть частичным или полным и должно проводиться с установленной в ИС Колледжа степенью периодичности.

Задача предупреждения в ИС Колледжа возможных нарушений информационной безопасности решается по мере наступления следующих событий:

- включение в состав ИС Колледжа новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Колледжа;

- изменение конфигурации программных и технических средств ИС (изменение конфигурации программного обеспечения рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Колледжа;

- при появлении сведений о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения технических средств, используемых в ИС Колледжа.

Администратор информационной безопасности (возможно, при помощи сторонней организации специализирующейся в области информационной безопасности) собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения относительно ИС Колледжа. Источниками подобного рода сведений могут

служить официальные издания и публикации различных компаний, общественных объединений и других организаций, специализирующихся в области защиты информации.

Администратор информационной безопасности (возможно, при помощи сторонней организации, специализирующейся в области информационной безопасности) организовывает периодическую проверку СЗИ ИС Колледжа путем моделирования возможных попыток осуществления НСД к защищаемым информационным ресурсам.

Плановая разъяснительная работа по настоящим правилам, а также инструктаж сотрудников Колледжа по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в Колледже, проводится администратором информационной безопасности ежеквартально.

Внеплановая разъяснительная работа по настоящим правилам, а также инструктаж сотрудников Колледжа по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в Колледже, проводится при пересмотре настоящих правил, при возникновении инцидента нарушения правил.

Прием на работу новых сотрудников должен сопровождаться ознакомлением их с настоящим Положением.

10. Ликвидация последствий нарушения информационной безопасности

Администратор информационной безопасности, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения информационной безопасности, факты осуществления НСД к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения информационной безопасности или осуществления НСД к защищаемым информационным ресурсам ИС рекомендуется уведомить администратора информационной безопасности, и далее следовать его указаниям.

Действия администратора информационной безопасности при признаках нарушения политики информационной безопасности регламентируются следующими внутренними документами:

- Инструкцией пользователя автоматизированной системы;

- Должностными обязанностями администратора информационной безопасности;

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

11. Ответственность нарушителей Положения информационной безопасности

Ответственность за нарушение информационной безопасности несет каждый сотрудник Колледжа в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования Положения, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный Колледжу в результате нарушения ими Положения (Ст. 238 Трудового кодекса РФ).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники Колледжа несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

12. Регулирующие законодательные нормативные документы

При организации и обеспечении работ по информационной безопасности сотрудники Колледжа должны руководствоваться следующими законодательными нормативными документами:

12.1. Основополагающие нормативные документы

К основополагающим нормативным документам относятся:

- Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ от 5 декабря 2016 г. № Пр-646).

12.2. Законы Российской Федерации

- Федеральный закон Российской Федерации от 28.12.2010 г. «О безопасности» № 390-ФЗ (с изменениями от 05.10.2015 г.)

- Гражданский кодекс Российской Федерации;

- Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (с изменениями от 23 июня 2016 г.);

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Уголовный кодекс РФ;

- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (с изменениями от 05.04.2016 г.);

- Федеральный закон от 04.05.2011 г. № 99-ФЗ « О лицензировании отдельных видов деятельности» (с изменениями от 30.12.2015 г.).

12.3. Указы и распоряжения президента Российской Федерации

- Указ Президента Российской Федерации от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации» (с изменениями от 26 июля 1995 г., 17 января, 9 июля 1997 г.);

- Указ Президента Российской Федерации от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» (с изменениями от 25 июля 2000 г.);

- Указ Президента Российской Федерации от 3 июля 1995 г. № 662 «О мерах по формированию общероссийской телекоммуникационной системы и обеспечению прав собственников при хранении ценных бумаг и расчетах на фондовом рынке Российской Федерации» (с изменениями от 16 октября 2010 г.);

- Указ Президента Российской Федерации от 9 января 1996 г. № 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» (с изменениями от 30 декабря 2000 г.);

- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями от 13 июля 2015 г.).

12.4. Постановления и распоряжения правительства Российской Федерации

- Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» (с изменениями от 18.03.2016г.);

- Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации» (с изменениями от 21 апреля 2010 г.).

- Постановление Правительства от 15 сентября 2008 г. N 687 «Об утверждении положения об особенностях обработки персональных данных осуществляемой без использования средств автоматизации».

- Постановление Правительства от 1 ноября 2012 г. n 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

12.5. Нормативные и руководящие документы Федеральных служб РФ

- Приказ ФСТЭК России от 11.02.2013 г. №17 «Об утверждении Требований о защите информации не составляющей государственную тайну, содержащейся в государственных информационных системах» (Зарегистрировано в Минюсте России 31.05.2013 г. № 28608);

- Приказ ФСТЭК России от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

- Приказ ФСБ России №416, ФСТЭК России №489 от 31.08.2010 г. «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования (Зарегистрировано в Минюсте России 13.10.2010 г. №18904:

- Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.).

Положение разработано системным администратором

_____ С.И. Самсоновым

Всего прошито, пронумеровано и скреплено печатью

20 (двадцать)

) листов

Начальник общего отдела
ГБПОУ РК «СКССОиД»
_____ Е.В. Киреева