МИНИСТЕРСТВО ОБРАЗОВАНИЯСТАВРОПОЛЬСКОГО КРАЯ

государственное бюджетное профессиональное образовательное учреждение «Ставропольский колледж сервисных технологий и коммерции»
ГБПОУ СКСТиК

Приложение 6

к приказу директора
ГБПОУ «Ставропольский колледж сервисных технологий и коммерции»
от 17.05.2022 № 99-од

ПОЛОЖЕНИЕ
об информационной безопасности
в государственном бюджетном профессиональном образовательном учреждении «Ставропольский колледж сервисных технологий и коммерции»

I. Общие положения

1.1. Настоящее Положение об информационной безопасности (далее - Положение) в государственном бюджетном профессиональном образовательном учреждении «Ставропольский колледж сервисных технологий и коммерции» (далее - колледж) является локальным нормативным актом, разработанным в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенными в Положении об обработке и защите персональных данных ГБПОУ «Ставропольский колледж сервисных технологий и коммерции»

1.2. Целью настоящего Положения, является обеспечение безопасности объектов защиты колледжа от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональным данным (далее по тексту – УБПДн).

1.3. Безопасность персональных данных достигается путем исключения несанкционированного или случайного доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей.

Должно осуществляться своевременное обнаружение и реагирование на УБПДн. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

2. Определения

В настоящем документе используются следующие термины и их определения.

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

Аутентификация отправителя данных - подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные - сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) -получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации - возможность получения информации и ее использования.

Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

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

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Неавтоматизированная обработка персональных данных - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Раскрытие персональных данных - умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации - способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. Обозначения и сокращения

АРМ – автоматизированное рабочее место.

ИСПДн – информационная система персональных данных.

ЛВС – локальная вычислительная сеть.

НСД – несанкционированный доступ.

ОС – операционная система.

ПДн – персональные данные. ПО – программное обеспечение.

СЗПДн – система (подсистема) защиты персональных данных.

УБПДн – угрозы безопасности персональных данных.

4. Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

отчета об обследовании ИСПДн и результатах проведения внутренней проверки защиты ПДн на бумажных носителях.

перечня персональных данных, подлежащих защите;

акта классификации информационной системы персональных данных;

модели угроз безопасности персональных данных;

матрицы доступа пользователей к защищаемым информационным ресурсам ИСПДн;

руководящих документов ФСТЭК России и ФСБ России.

На основе этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн колледже.

На основании анализа актуальных угроз безопасности ПДн, описанного в Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

Для ИСПДн составляется список используемых технических средств защиты (далее - Список), а также программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

АРМ пользователей;

Сервера приложений;

СУБД;

границы ЛВС;

каналов передачи в сети общего пользования, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

антивирусные средства для рабочих станций пользователей и серверов;

средства межсетевого экранирования;

средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Список функций защиты может включать:

управление и разграничение доступа пользователей;

регистрацию и учет действий с информацией;

обеспечивать целостность данных;

производить обнаружений вторжений.

Список используемых технических средств отражается в «План мероприятий по обеспечению защиты персональных данных».

Список используемых средств должен поддерживаться в актуальном состоянии.

5. **Требования к составу системы защиты персональных данных СЗПДн** включает в себя следующие подсистемы:

управления доступом, регистрации и учета;

обеспечения целостности и доступности;

антивирусной защиты;

межсетевого экранирования;

анализа защищенности;

обнаружения вторжений;

криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в документе «Акт классификации информационной системы персональных данных».

5.1. Подсистемы управления доступом, регистрации и учета

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;

идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;

регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.

регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД).

5.2. Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн колледжа, а также средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.

5.3. Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн колледжа.

Средства антивирусной защиты предназначены для реализации следующих функций:

резидентный антивирусный мониторинг;

антивирусное сканирование;

скрипт-блокирование;

централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

автоматизированное обновление антивирусных баз;

ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

5.4. Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

фильтрации открытого и зашифрованного (закрытого) IP-трафика;

фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;

регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;

контроля целостности своей программной и информационной части;

фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

регистрации и учета запрашиваемых сервисов прикладного уровня;

блокирования доступа объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛВС.

5.5. Подсистема анализа защищенности

Подсистема анализа защищенности должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

5.6. Подсистема обнаружения вторжений

Подсистема обнаружения вторжений должна обеспечивать выявление сетевых атак на элементы ИСПДн, подключенные к сетям общего пользования и (или) международного обмена. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

5.7. Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для исключения несанкционированного доступа к защищаемой информации в ИСПДн колледжа при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

6. Пользователи ИСПДн

Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Пользователем ИСПДн является любой работник колледжа имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его должностными обязанностями.

Пользователи ИСПДн делятся на три категории:

администраторы информационной безопасности;

администраторы ИСПДн;

операторы ИСПДн.

Администраторы информационной безопасности – это работники колледжа, которые занимаются настройкой, внедрением и сопровождением систем безопасности.

Администратор ИБ обладает следующим уровнем доступа:

обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

обладает полной информацией о технических средствах и конфигурации ИСПДн;

имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

Администраторы ИСПДн - это работники колледжа, ответственные за настройку, внедрение и сопровождение ИСПДн.

Обеспечивают функционирование подсистемы управления доступом ИСПДн и уполномочены осуществлять предоставление и разграничение доступа конечного пользователя (Оператора ИСПРд) к элементам, хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

обладает полной информацией о технических средствах и конфигурации ИСПДн;

имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

обладает правами конфигурирования и административной настройки технических средств ИСПДн.

Операторы ИСПДн – работники колледжа, участвующие в процессе эксплуатации ИСПДн.

Оператор ИСПДн обладает следующим уровнем доступа:

обладает необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

располагает конфиденциальными данными, к которым имеет доступ;

осуществляют непосредственную обработку персональных данных в рамках своих полномочий, определяемых должностной инструкцией, с соблюдений требований настоящей

7. Требования к пользователю по обеспечению защиты ПДн

7.1. Обязанности пользователя

Не разглашать персональные данные, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных обязанностей.

Не сообщать устно или письменно, не передавать в каком-либо виде третьим лицам и не раскрывать публично персональные данные без соответствующего разрешения директора колледжа.

Знать и выполнять требования законодательных актов Российской Федерации, настоящей Инструкции и других внутренних документов, регламентирующих порядок обработки персональных данных.

Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры обработки персональных данных, которые определены должностной инструкцией.

Знать и соблюдать установленные требования обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных.

Использовать для хранения персональных данных только определенные места хранения и учтенные носители персональных данных.

Незамедлительно, в кратчайшие сроки, сообщать директору колледжа об утрате или недостаче носителей информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов и о других фактах, которые могут привести к разглашению персональных данных.

При прекращении работ (трудовых отношений) все материальные носители, содержащие персональные данные (флеш-накопители, дискеты, оптические диски, документы, черновики, распечатки на принтерах, кино- и фотоматериалы, модели, промышленные образцы и пр.), передать директору по акту приема-передачи.

Соблюдать требования парольной политики.

Соблюдать требования антивирусной защиты.

Пользователи, имеющие выход в Интернет, обязаны соблюдать правила при работе в сетях связи общего пользования и (или) сетях международного информационного обмена.

Пользователи, работающие с электронной подписью или использующие шифрование, обязаны соблюдать Инструкцию по обращению со средствами криптографической защиты информации.

Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

Обо всех выявленных нарушениях, связанных с порядком обработки персональных данных, а также для получений консультаций по вопросам обработки персональных данных, необходимо обращаться к ответственному за организацию обработки персональных данных.

7.2. Пользователям запрещается:

✓ Нарушать установленные в колледже инструкции по работе с персональных данных.

✓ Использовать компоненты программного и аппаратного обеспечения колледжа в неслужебных целях.

✓ Оставлять свое рабочее место без присмотра, предварительно не заблокировав (штатными средствами операционной системы Windows — комбинацией клавиш [WIN] + [L] или [CTRL] + [ALT] + [DEL] с дальнейшим нажатием кнопки «Блокировка» появившегося меню, либо при помощи штатных средств защиты информации от несанкционированного доступа при их наличии).

✓ Оставлять без присмотра или неубранными в хранилища (шкаф, сейф) носители или документы, содержащие персональные данные.

✓ Записывать и хранить персональные данные на неучтенных носителях информации (оптических дисках, гибких магнитных дисках, флеш- накопителях и т.п.).

- ✓ Самовольно изменять состав и конфигурацию используемых программных, аппаратных, программно-аппаратных средств, самовольно устанавливать программное обеспечение, отключать/подключать оборудование или изменять режимы его работы.
- ✓ Изменять IP-адрес, MAC-адрес и иные настройки сети АРМ.
- ✓ Производить действия, направленные на получение несанкционированного доступа к АРМ и серверам, равно как и любым другим узлам локально-вычислительной сети колледжа или Интернет, в том числе:

действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого сетевого оборудования или программного обеспечения);

установка программного обеспечения, осуществляющего перехват информации (информационных пакетов), адресованной другим пользователям;

действия, направленные на получение несанкционированного доступа к информационным ресурсам, в последующем использовании такого доступа;

уничтожение, модификация программного обеспечения или данных без согласования с директором или владельцами этого ресурса;

попытки подбора паролей к любым информационным ресурсам методом перебора всех возможных вариантов паролей, либо атак по словарю;

умышленные действия по созданию, использованию и распространению вредоносных программ, в том числе направленных на получение несанкционированного доступа к любым информационным и служебным ресурсам (как внутри колледжа, так и вне), либо на нарушение целостности и работоспособности этих систем;

действия по сканированию локальной сети с целью определения ее внутренней структуры, списков открытых портов, наличия существующих сервисов и уязвимостей.

- ✓ Самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать.
- ✓ Самостоятельно разрабатывать или использовать нерегламентированные (без разрешения директора, не относящиеся к производственному процессу) программы (например: игры; IM-клиенты, такие как Google Messenger, ICQ и т.п.; P2P-клиенты: Kazaa, eMule и т.п.).
- ✓ Разрешать посторонним лицам работать под своей учетной записью в ИСПДн.
- ✓ Пересылать персональные данные по каналам связи в открытом виде, в том числе Интернет, по телефону, факсу, электронной почте и т.п. (без использования средств шифрования).
- ✓ Получать доступ к персональным данным с рабочих мест, не оборудованными необходимыми средствами защиты информации.
- ✓ Самовольно создавать совместно используемые сетевые ресурсы (папки общего доступа) на своих компьютерах и файловых серверах, не санкционированно удалять или изменять права доступа к ним.

✓ В случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения.

✓ Препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

✓ Удалять или искажать программы и файлы с персональными данными и иной важной информацией, необходимой для пользования с персональными данными.

✓ Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению внештатной ситуации. Об обнаружении такого рода ошибок - ставить в известность руководителя своего подразделения и сотрудников, ответственных за установку и (или) сопровождение программного обеспечения (Администратора безопасности персональных данных в информационных системах персональных данных (далее - администратор безопасности)).

✓ Подключать к локально-вычислительной сети личные средства вычислительной техники: ноутбуки, карманные компьютеры, смартфоны и т.п., а также личные носители и накопители информации. В случае необходимости переноса информации.

7.3. Ответственность пользователя

В соответствии со ст. 24 Федерального закона Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей.

Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей. При нарушениях пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

8. Парольная политика

8.1. Общие требования к паролям:

Первичный пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые системным администратором при создании новой учетной записи.

Установку первичного пароля производит работник колледжа, назначенный приказом (далее - системный администратор) при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на системном администраторе.

Основной пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику организации, используемая для подтверждения подлинности владельца учетной записи.

Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

Административный пароль - комбинация символом (буквы, цифры, знаки препинания, специальные символы), известная системному администратору (администратору БД, администратору приложения), используемая при настройке служебных учетных записей, учетных записей служб и сервисов, а также специальных учетных записей.

Системный администратор несет персональную ответственность за сохранение в тайне административного пароля. Запрещается сообщать пароль другим лицам, в том числе работникам колледжа, записывать его, а также пересылать открытым текстом в электронных сообщениях.

Системный администратор обязан не реже одного раза в месяц производить смену административного пароля, соблюдая требования настоящего документа.

В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом заведующему сектором программно-информационного обеспечения и изменить административный пароль.

Копии административных паролей должны храниться в опечатанном конверте в отделе информационного обеспечения.

8. 2. Требования к паролям

Пароли НЕ ДОЛЖНЫ состоять из:

вашего имени, отчества или фамилии ни в каком виде (т.е. написаны в строчном, в прописном, в смешанном виде, задом наперед, два раза и т.д.);

вашего идентификатора входа (login) ни в каком виде;

имен вашей(его) супруги(а) или детей;

не используйте какую-либо информацию о себе;

сюда входят: номера телефонов, номера в пропусках и других документах, номер или марка вашего автомобиля, ваш почтовый адрес и т.д. и т.п.;

только цифр или одинаковых букв;

слов, которые можно найти в словаре (любом, включая иностранные) или в каком-либо списке слов;

меньше, чем восьми символов;

Пароли ДОЛЖНЫ:

содержать строчные и прописные буквы;

содержать небуквенные символы (т.е. цифры, знаки пунктуации, специальные символы);

быть легко запоминаемы, чтобы не было необходимости записывать их;

быть составлены так, чтобы вы могли быстро набрать их на клавиатуре. Это осложнит возможность подглядеть пароль.

Минимальное требование: буквенно-цифровой пароль.

Желательно использовать буквы в верхнем или нижнем регистрах, цифры или специальные символы (например: ~ ! @ # $ % л & * ( ) _ - + = | \ ? / . , : ; ’] [{ } < > . .

Несмотря на такие жесткие требования, есть несколько способов выбора паролей, которые все ж е соответствуют этим правилам:

*• * Выберите предложение из песни или стихотворения, и отберите только первые буквы каждого слова (хотя в примере использовано английское предложение,*

Вы можете воспользоваться и другими языками)

Pretty woman walking down the street становится Pwwdts.

*• * Выберите два коротких слова и соедините их с помощью*

• пунктуационных знаков и спец символов: Dog+rain, kidю.

8.3. Правила использования паролей:

хранить в тайне свой пароль, не сообщать его другим лицам.

не предоставлять доступ в ИСПДн другим лицам под своей учетной записью и паролем.

изменять свой пароль при первом требовании политики паролей операционной системы и/или ИСПДн.

во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

запрещается записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе АРМ, на обратной стороне клавиатуры и т.д.

8.4. **Смена, удаление личного пароля любого Пользователя производится в следующих случаях:**

в случае подозрения на компрометацию пароля;

по окончании срока действия;

в случае прекращения полномочий (увольнение, переход на другую работу внутри колледжа) Пользователя после окончания последнего сеанса работы в информационных системах персональных данных;

по указанию ответственного работника за организацию обработки персональных данных.

При увольнении, переходе на новую должность сотрудника, имеющего доступ помимо своей учетной записи к другим ресурсам (межсетевые экраны, маршрутизаторы, серверы, другие учетные записи и т.п.) также производится внеплановая смена паролей к таким ресурсам.

9. Модель нарушителя безопасности

Под нарушителем понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты

Нарушители подразделяются по признаку принадлежности к ИСПДн.

Все нарушители делятся на две группы:

внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн. Классификация нарушителей представлена в Модели угроз безопасности персональных данных каждой ИСПДн.

10. Модель угроз безопасности

Для ИСПДн ГБПОУ «Ставропольский колледж сервисных технологий и коммерции» выделяются следующие основные категории угроз безопасности персональных данных:

1. Угрозы утечки по техническим каналам.

2. Угрозы несанкционированного доступа к информации:

угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн;

угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;

угрозы преднамеренных действий внутренних нарушителей;

угрозы несанкционированного доступа по каналам связи.