МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)
ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ

Кафедра автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

Разработка рекомендаций системы защиты персональных данных в профессиональной образовательной организации

Магистерская диссертация
по направлению: 44.04.04 Профессиональное обучение (по отраслям)
Направленность (профиль): Управление информационной безопасностью в профессиональном образовании
Форма обучения заочная

Проверка на объем заимствований:
77 % авторского текста

Работа рекомендована к защите
«18» 01 2021г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнила:
Студентка группы ЗФ-309-210-2-1
Мельник Нина Юрьевна

Научный руководитель:
Уварина Наталья Викторовна, д.п.н,
профессор

Челябинск
2021

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время развитие технических средств позволяет собирать и обрабатывать большие объемы социально значимой информации, которые необходимы для жизнедеятельности человека, общества и государства. А развитие компьютерной техники дает возможность получать доступ и использовать различные банки данных почти о любом субъекте. Кто владеет информацией, тот владеет миром, - верно полагают философы. Информация является безусловно условием жизни и социальной деятельности субъектов, предметом их постоянного внимания. Все же всякая информация может быть использована как на благо, так и во вред людям[1]. Правовой режим защиты персональных данных в современных условиях приобретает важное значение ввиду того, что российским законодательством, и в первую очередь Конституцией РФ, объявлен принцип невмешательства в частную жизнь лица. Поэтому работодатели могут получать от работников информацию только в добровольном порядке и строго ограниченную целями, определенными в законодательстве. Эта тема в данное время особенно актуальна, так как активное использование средств компьютерной техники и информационно-обрабатывающих технологий, а также увеличивающийся объем массивов информации вызывает возникновение новых проблем, требующих от работодателей принятия адекватных мер реагирования[1].

Создание информационных систем (ИС) повышает производительность труда любой организации, с любой формой собственности. Пользователи данной системы могут быстро получать данные необходимые для выполнения их служебных обязанностей. Однако у процесса компьютеризации есть и другая сторона: облегчение доступа к массивам и базам данных получают и злоумышленники. Обладая доступом к различным базам данных (БД), злоумышленники могут использовать их для вымогания денег, других ценных сведений, материальных ценностей и

прочего.

Поэтому в наше «цифровое» время защита информации стоит как никогда остро. Чаще всего злоумышленников интересуют сведения, хранящиеся в БД государственных структур, таких как МВД, ФНС и прочих, а также подконтрольных им организациям, таким как учреждения здравоохранения, образования.

Основным законом, регулирующим обработку персональных данных различными субъектами, является Федеральный закон «О персональных данных» от 27.07.2006 года №152-ФЗ (далее – закон 152-ФЗ). Под его сферу попадают субъекты, которые осуществляют действия по обработке персональных данных с применением средств автоматизации (учитывая информационно-телекоммуникационные сети), либо без использования таких средств, при условии, что подобные действия позволяют совершать поиск или предоставлять доступ к персональным данным в базах, размещенных на материальном носителе или находящихся в картотеках, либо других систематизированных собраниях данных. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» определяет:

1. Основные понятия, связанные с обработкой персональных данных;
2. Принципы и условия обработки персональных данных;
3. Обязанности оператора;
4. Права субъекта персональных данных;
5. Виды ответственности за нарушение требований, установленных Федеральным законом № 152-ФЗ;
6. Государственные органы, осуществляющие контроль и надзор за соблюдением требований, установленных Федеральным законом № 152-ФЗ.

Защита персональных данных является актуальной темой в нашей стране, поскольку законодательная база существует менее 10 лет. В связи с тем, часто лица, ответственные за обработку персональных данных не

знаю элементарных правил безопасности доверенной им информации. Поэтому на специалистов по информационной безопасности ложиться не только ответственность за безопасность информационной системы, но система обучения персонала.

Данная работа посвящена разработке системы защиты персональных данных в профессиональной образовательной организации.

Цель работы: повышение эффективности защиты персональных данных сотрудников и студентов в «Челябинском энергетическом колледже им. С. М. Кирова».

Для достижения цели работы необходимо выполнить следующие задачи:

- Рассмотреть теоретические основы вопроса: понятие и сущность персональных данных;
- Изучить особенности персональных данных и определить их отличия от иной информации;
- Выявить общие требования к обработке персональных данных;
- Рассмотреть работу кадровой службы с персональными данными;
- Изучить особенности получения, передачи и защиты персональных данных, а также их защиты при работе на ЭВМ.

Объектом исследования в научно-исследовательской работе является персональные данные субъекта Российской Федерации.

Предметом исследования – основы защиты персональных данных.

При написании работы использовались следующие методы исследования: теоретический анализ и обобщение научной литературы, обобщение опыта практической работы.

Теоретическая значимость работы заключается в том, что результаты, полученные в ходе исследования дополняют точку зрения авторов, работающих по данной теме.

Информационной базой исследования послужили, нормативно-справочные и научно-публицистические материалы по рассматриваемой теме, а также данные, собранные самостоятельно.

Теоретической базой исследования послужил анализ литературы и источников по данной теме. Для анализа существующей защиты персональных данных использована внутренняя документация ГБПОУ ЧЭнК.

Практическая значимость работы заключается в том, что результаты исследования могут использоваться в дальнейшем развитии и повышения эффективности защиты в области персональных данных, обрабатываемых в информационных системах персональных данных в образовательной организации.

Структура работы: введение, три главы, заключение, список используемой литературы.

ГЛАВА 1. ОСНОВЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1 Основные определения, используемые в законодательстве.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Персональные данные – это любая информация о физическом лице, в частности, ФИО, место и дата рождения, место проживания и регистрации, социальное, имущественное и семейное положение, профессия, образование, доходы и другое (п. 1 ст. 3 ФЗ«О персональных данных»)[2].

Защита персональных данных - комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определенному физическому лицу. При поступлении на работу это данные отдела кадров работодателя, которые работник указывает в личной карточке, автобиографии, других документах, заполняемых при подписании трудового договора[3].

Оператором является лицо получившее разрешение к персональным данным, осуществляющий их обработку, не допускает их распространение без согласия владельца персональных данных или наличия иного законного основания. Оператор при рассмотрении персональных данных должен принимать все обязательные организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение, (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), 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.

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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.

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

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.

В процессе трудовой деятельности работника работодатель накапливает и хранит документы, содержащие персональные данные работника. В образовательных учреждениях персональные данные содержатся в документации отдела кадров[4].

Под угрозой (в общем смысле) обычно понимают потенциально возможное событие (воздействие, процесс или явление), которое может привести к нанесению ущерба чьим-либо интересам, в частности под угрозой безопасности автоматизированных систем (АС) обработки информации понимается возможность воздействия на АС, которое прямо или косвенно может нанести ущерб ее безопасности. АС является наиболее уязвимой частью информационной системы персональных данных (ИСПДн), поскольку предоставляет злоумышленнику самый быстрый доступ к информации, во отличии от базы данных (БД), хранящихся на бумажных носителях.

Ошибки в программном обеспечении (ПО) являются распространенным видом компьютерных нарушений. ПО серверов, рабочих станций, маршрутизаторов и т.д. написано людьми, поэтому оно практически всегда содержит ошибки. Чем выше сложность подобного ПО, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляют никакой опасности, некоторые же могут привести к серьезным последствиям, таким как получение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов (использование компьютера в качестве плацдарма для атаки и т.п.). Обычно подобные ошибки устраняются с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких пакетов является необходимым условием безопасности информации[4].

Преднамеренные угрозы связаны с целенаправленными действиями

нарушителя. В качестве нарушителя может быть служащий, посетитель, конкурент, наемник и т.д. Действия нарушителя могут быть обусловлены разными мотивами: недовольством служащего своей карьерой, сугубо материальным интересом (взятка), любопытством, конкурентной борьбой, стремлением самоутвердиться любой ценой и т.п.

1.2 Законодательные основы защиты персональных данных

В настоящее время, на территории Российской Федерации осуществляется государственное регулирование в области обеспечения безопасности персональных данных (далее - ПДн). Правовое регулирование вопросов обработки ПДн осуществляется в соответствии с Конституцией Российской Федерации и международными договорами Российской Федерации, на основании вступившего в силу с 2007 года Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятых во исполнение его положений, нормативно-правовых актов и методических документов.

В силу требований указанного Федерального закона «О персональных данных» все информационные системы персональных данных (далее - ИСПДн), созданные до введения его в действие, должны быть приведены в соответствие установленным требованиям не позднее 1 июля 2011 года.[1]

Другими нормативными актами, оказывающие правовое регулирование в области защиты персональных данных в медицинских организациях являются:

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

Трудовой кодекс Российской Федерации (глава 14).

Постановление Правительства РФ от 17 ноября 2007 г. №781 «Об

утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

Постановление Правительства РФ от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Правила обработки персональных данных, осуществляемой с использованием автоматизации и без использования средств автоматизации, должны применяться с учетом требований вышеуказанных положений. Приказом Федеральной службы по техническому и экспортному контролю от 05.02.2010 №58 утверждено Положение о методах и способах защиты информации в информационных системах персональных данных, которое подробно регламентирует вопросы, связанные с порядком применения методов и способов защиты информации в информационных системах персональных данных оператором или уполномоченным им лицом.

Чтобы защитить персональные данные работников в образовательном учреждении, надо создать режим обработки персональных данных, который включает:

- создание внутренней документации по работе с персональными данными;

- организацию системы защиты персональных данных;

- внедрение технических мер защиты персональных данных.

Широкое распространение информационных технологий дает возможность свободно получать, обрабатывать и распространять сведения о людях. В последнее время распространение баз данных с номерами телефонов, местом жительства и другой информацией стало доступным, и это привело к нарушению прав граждан на конфиденциальность сведений о личной жизни.

Необходимо выделить требования, которые данные акты

предъявляют к организациям. Условно их можно разделить на административные и технические. К административным относятся требования организационного характера, создание внутренних нормативных и правовых актов. К техническим требованиям относят внедрение программных и аппаратных средств защиты, а также средства контроля и ограничения доступа. Составим таблицу 1, в которую занесем требования законодательства Российской Федерации в области персональных данных, предъявляемые организациям.

Таблица 1–Требования законодательства Российской федерации

Название документа	Административные требования	Технические требования
Федеральный закон от 27.07.2006 №152 - ФЗ «О персональных данных»	Назначение оператором ответственного за обработку персональных данных	Обнаружение фактов несанкционированного доступа и принятие мер
	Издание оператором документов, определяющим его политику безопасности в области обработки персональных данных	Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним
	Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных	Создание информационной системы обработки персональных данных
	Ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных	-
	Публикация или осуществление беспрепятственного доступа к документу, определяющего политику безопасности в области обработки персональных данных оператора	
	Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы	
	Учет машинных носителей персональных данных	Обеспечение сохранности носителей персональных данных

Продолжение таблицы 1

Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных	Организация режима обеспечения безопасности помещений	Использование средств защиты информации в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз
	Утверждение руководителем документа, определяющего перечень лиц, допущенных к обработке персональных данных	Наличие электронного журнала безопасности
	Ограничение доступа к журналу безопасности	-
	Определение класса информационной системы персональных данных	-
Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Идентификация и аутентификация субъектов доступа и объектов доступа	Ограничение программной среды
	Управление доступом субъектов доступа к объектам доступа	Защита машинных носителей
	Регистрация событий безопасности	Управление конфигурацией информационной системы
	Контроль безопасности персональных данных	Антивирусная защита
	Выявление инцидентов	Системы Обнаружения вторжений (ids/ips)
	-	Защита среды виртуализации
Приказ ФСБ России от 10.07.2014 №378	Утверждение правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях	Оснащение помещений входными дверьми с замками
	Утверждение перечня лиц, имеющих право доступа в Помещение	Хранение носителей персональных данных в сейфах, оборудованных внутренними замками
	Ведение журнала учета носителей персональных данных	Обеспечение информационной системы автоматизированными средствами, регистрирующими запросы пользователей на получение персональных данных

Продолжение таблицы 1

Приказ ФСБ России от 10.07.2014 №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке при их обработке в информационных системах с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации	Поддержание в актуальном состоянии документ, определяющий перечень лиц, допущенных к работе с персональными данными	Обеспечение информационной системы автоматизированными средствами, исключающими доступ к содержанию электронного журнала сообщений лиц, не указанных в утвержденном руководителем оператора списке лиц, допущенных к содержанию электронного журнала сообщений
	Назначение обладающего достаточными навыками должностного лица оператора ответственным за обеспечение безопасности персональных данных в информационной системе	Обеспечение информационной системы автоматизированными средствами, позволяющими автоматически регистрировать в электронном журнале безопасности изменения
	Обеспечение периодического контроля работоспособности автоматизированных средств	Полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе
	Назначение оператором лица, ответственного за периодический контроль ведения электронного журнала безопасности и соответствия отраженных в нем полномочий сотрудников оператора их должностным обязанностям	Оборудование окнами и дверьми Помещений, в которых размещены серверы информационной системы, металлическими решетками, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения

Продолжение таблицы 1

Постановление Правительства от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"	Необходимо обеспечивать раздельное хранение персональных данных, обработка которых осуществляется в различных целях	-
	Не допускается фиксация на одном материальном носителе персональных данных, цели обработки заведомо не совместимы	-
	Лица, осуществляющие обработку, должны быть проинформированы о факте обработки ими персональных данных	-
Постановление Правительства от 21.03.2012 №211 "Об утверждении перечня мер, направленных на выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными и правовыми актами, операторами являющимися государственными или муниципальными органами	Должны быть утверждены правила обработки персональных данных, устанавливающие процедуры, направление на выявление и предотвращение нарушений законодательства РФ в сфере персональных данных	-
	Должны быть утверждены правила рассмотрения запросов субъектов персональных данных или их представителей	-
	Должны быть утверждены правила обезличивания персональных данных	-
	Должны быть утверждены правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных	-
	Должен быть утвержден должностной регламент (должностные обязанности) или должностная инструкция ответственного за организацию обработки персональных данных	-
	Должна быть утверждена типовая форма согласия на обработку персональных данных сотрудников или иных субъектов персональных данных	-
	Должен быть определен порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных	-
«Трудовой кодекс Российской Федерации» от 30.12.2001 №197-ФЗ	Работники должны быть ознакомлены под роспись с документами организации, устанавливающие порядок обработки ПДн	-

Составив таблицу с требованиями, можно легко отследить какие из них выполняются в организации, а какие еще необходимо выполнить. Большинство требований, указанных в данной таблице остаются очень общими. Что приводит к вольной трактовке и страдает качество их выполнения внутри организации.

1.3 Информационная система персональных данных

ИСПДн представляет собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации [2].

Состав и содержание угроз безопасности ПДн (УБПДн) определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

К характеристикам ИСПДн, обусловливающим возникновение УБПДн, можно отнести категорию и объем обрабатываемых в ИСПДн персональных данных, структуру ИСПДн, наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности ПДн, обрабатываемых в ИСПДн, режимы обработки персональных данных, режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

База данных (БД) представляет собой совокупность специальным образом организованных данных, хранимых в памяти вычислительной системы и отображающих состояние объектов и их взаимосвязей в рассматриваемой предметной области.

Рассмотрев различные модели представления данных, перейдём к детальному описанию БД ПДн. В образовательной организации можно выделить два основных подразделения обрабатывающих информацию, в которую включены ПДн:

Учебное (состоит из сбора, обработки, хранения, уточнения, модификации, уничтожения персональных данных студентов);

Бухгалтерия и кадры (обработка персональных данных сотрудников)

Каждое из подразделений формируют свою БД, отвечающей их специфики деятельности. В зависимости от требований нормативных и руководящих документов, а также внутренних приказов и распоряжений, база может варьироваться. Чаще всего, главную роль в создании БД оказывает ПО, имеющееся в наличии, например, СУБД MS Access, поставляющееся в комплекте MS Office, позволяет в короткие сроки создать БД. Рассмотрим примеры БД каждого из вышеуказанных подразделений.

В образовательном учреждении БД храниться на бумажных носителях (база анкет студентов) и на серверах БД (в роли сервера может выступить любая ПЭВМ, как отдельно стоящая, в случае локальной БД, так и включённая в сеть, в случае использовании клиент-серверной технологии).

БД образовательного учреждения создаются и используются несколькими типами программ: Office Access 2003, либо Microsoft Office Access 2007 (данные хранятся в формате mdb, реже accdb);Office Excel 2003, либо Microsoft Office Excel 2007 (данные хранятся в формате xls);

Достоинства данных СУБД:

- быстрота разработки;
- совместимость с большинством ПЭВМ под управлением ОС Windows

Недостатки:

- отсутствие защиты, либо низкая защита данных;

- проблемы с многопользовательским доступом (для xls, dbf более 2, для mdb более 5 пользователей);
- низкая скорость работы с большим объёмом данных;
- циркуляция большого объёма данных в сети при многопользовательском доступе;

Достижение высокого уровня безопасности невозможно без принятия должных организационных мер. С одной стороны, эти меры должны быть направлены на обеспечение правильности функционирования механизмов защиты и выполняться администратором безопасности системы. С другой стороны, руководство организации, эксплуатирующей средства автоматизации, должно регламентировать правила автоматизированной обработки информации, включая и правила ее защиты, а также установить меру ответственности за нарушение этих правил.

Для непосредственной организации (построения) и эффективного функционирования системы защиты информации в АС может быть (а при больших объемах защищаемой информации - должна быть) создана специальная штатная служба защиты (служба компьютерной безопасности) [10].

Служба компьютерной безопасности представляет собой штатное или нештатное подразделение, создаваемое для организации квалифицированной разработки системы защиты информации и обеспечения ее функционирования.

Основные функции службы заключаются в следующем [10]:

- формирование требований к системе защиты в процессе создания АС;
- участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;
- планирование, организация и обеспечение функционирования

системы защиты информации в процессе функционирования АС;

- распределение между пользователями необходимых реквизитов защиты;
- наблюдение за функционированием системы защиты и ее элементов;
- организация проверок надежности функционирования системы защиты;
- обучение пользователей и персонала АС правилам безопасной обработки информации;
- контроль за соблюдением пользователями и персоналом АС установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;
- принятие мер при попытках НСД к информации и при нарушениях правил функционирования системы защиты.

Организационно-правовой статус службы защиты определяется следующим образом:

- численность службы защиты должна быть достаточной для выполнения всех перечисленных выше функций;
- служба защиты должна подчиняться тому лицу, которое в данном учреждении несет персональную ответственность за соблюдение правил обращения с защищаемой информацией;
- штатный состав службы защиты не должен иметь других обязанностей, связанных с функционированием АС;
- сотрудники службы защиты должны иметь право доступа во все помещения, где установлена аппаратура АС и право прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации;
- руководителю службы защиты должно быть предоставлено право запрещать включение в число действующих новые элементы АС,

если они не отвечают требованиям защиты информации;

- службе защиты информации должны обеспечиваться все условия, необходимые для выполнения своих функций.

Все эти задачи не под силу одному человеку, особенно если организация довольно велика. Более того, службу компьютерной безопасности могут входить сотрудники с разными функциональными обязанностями. Обычно выделяют четыре группы сотрудников (по возрастанию иерархии).

Сотрудник группы безопасности. В его обязанности входит обеспечение должного контроля за защитой наборов данных и программ, помощь пользователям и организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности. При децентрализованном управлении каждая подсистема АС имеет своего сотрудника группы безопасности.

Администратор безопасности системы. В его обязанности входит ежемесячное опубликование нововведений в области защиты, новых стандартов, а также контроль за выполнением планов непрерывной работы и восстановления (если в этом возникает необходимость) и за хранением резервных копий.

Администратор безопасности данных. В его обязанности входит реализация и изменение средств защиты данных, контроль за состоянием защиты наборов данных, ужесточение защиты в случае необходимости, а также координирование работы с другими администраторами.

Руководитель (начальник) группы по управлению обработкой информации и защитой. В его обязанности входит разработка и поддержка эффективных мер защиты при обработке информации для обеспечения сохранности данных, оборудования и программного обеспечения; контроль за выполнением плана восстановления и общее руководство административными группами в подсистемах АС (при децентрализованном управлении).

Существуют различные варианты детально разработанного штатного расписания такой группы, включающие перечень функциональных обязанностей, необходимых знаний и навыков, распределение времени и усилий. При организации защиты существование такой группы и детально разработанные обязанности ее сотрудников совершенно необходимы [13].

Основные организационные и организационно-технические мероприятия по созданию и поддержанию функционирования комплексной системы защиты

Они включают:

- разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений) мероприятия;
- мероприятия, проводимые при осуществлении или возникновении определенных изменений в самой защищаемой АС или внешней среде (по необходимости);
- периодически проводимые (через определенное время) мероприятия;
- постоянно (непрерывно или дискретно в случайные моменты времени) проводимые мероприятия.

К разовым мероприятиям относят:

- общесистемные мероприятия по созданию научно-технических и методологических основ (концепции и других руководящих документов) защиты АС;
- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов АС (исключение возможности тайного проникновения в помещения, исключение возможности установки прослушивающей аппаратуры и т.п.);
- мероприятия, осуществляемые при проектировании, разработке и вводе в эксплуатацию технических средств и программного обеспечения (проверка и сертификация используемых технических и

программных средств, документирование и т.п.);

- проведение спецпроверок всех применяемых в АС средств вычислительной техники и проведения мероприятий по защите информации от утечки по каналам побочных электромагнитных излучений и наводок;
- разработка и утверждение функциональных обязанностей должностных лиц службы компьютерной безопасности;
- внесение необходимых изменений и дополнений во все организационно-распорядительные документы (положения о подразделениях, функциональные обязанности должностных лиц, инструкции пользователей системы и т.п.) по вопросам обеспечения безопасности программно-информационных ресурсов АС и действиям в случае возникновения кризисных ситуаций;
- оформление юридических документов (в форме договоров, приказов и распоряжений руководства организации) по вопросам регламентации отношений с пользователями (клиентами), работающими в автоматизированной системе, между участниками информационного обмена и третьей стороной (арбитражем, третейским судом) о правилах разрешения споров, связанных с применением электронной подписи;
- определение порядка назначения, изменения, утверждения и предоставления конкретным должностным лицам необходимых полномочий по доступу к ресурсам системы;
- мероприятия по созданию системы защиты АС и созданию инфраструктуры;
- мероприятия по разработке правил управления доступом к ресурсам системы (определение перечня задач, решаемых структурными подразделениями организации с использованием АС, а также используемых при их решении режимов обработки и доступа к данным; определение перечня файлов и баз данных, содержащих сведения,

составляющие коммерческую и служебную тайну, а также требования к уровням их защищенности от НСД при передаче, хранении и обработке в АС; выявление наиболее вероятных угроз для данной АС, выявление уязвимых мест процесса обработки информации и каналов доступа к ней; оценку возможного ущерба, вызванного нарушением безопасности информации, разработку адекватных требований по основным направлениям защиты);

- организацию надежного пропускного режима;
- определение порядка учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих эталонные и резервные копии программ и массивов информации, архивные данные и т.п.;
- организацию учета, хранения, использования и уничтожения документов и носителей с закрытой информацией;
- определение порядка проектирования, разработки, отладки, модификации, приобретения, специсследования, приема в эксплуатацию, хранения и контроля целостности программных продуктов, а также порядок обновления версий используемых и установки новых системных и прикладных программ на рабочих местах защищенной системы (кто обладает правом разрешения таких действий, кто осуществляет, кто контролирует и что при этом они должны делать);
- создание отделов (служб) компьютерной безопасности или, в случае небольших организаций и подразделений, назначение нештатных ответственных, осуществляющих единое руководство, организацию и контроль за соблюдением всеми категориями должностных лиц требований по обеспечению безопасности программно-информационных ресурсов автоматизированной системы обработки информации;
- определение перечня необходимых регулярно проводимых превентивных мер и оперативных действий персонала по обеспечению

непрерывной работы и восстановлению вычислительного процесса АС в критических ситуациях, возникающих как следствие НСД, сбоев и отказов СВТ, ошибок в программах и действиях персонала, стихийных бедствий.

К периодически проводимым мероприятиям относят:

- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);
- анализ системных журналов, принятие мер по обнаруженным нарушениям правил работы;
- мероприятия по пересмотру правил разграничения доступа пользователей к информации в организации;
- периодически с привлечением сторонних специалистов осуществление анализа состояния и оценки эффективности мер и применяемых средств защиты. На основе полученной в результате такого анализа информации принимать необходимые меры по совершенствованию системы защиты;
- мероприятия по пересмотру состава и построения системы защиты.

К мероприятиям, проводимым по необходимости, относят:

- мероприятия, осуществляемые при кадровых изменениях в составе персонала системы;
- мероприятия, осуществляемые при ремонте и модификациях оборудования и программного обеспечения (строгое санкционирование, рассмотрение и утверждение всех изменений, проверка их на удовлетворение требованиям защиты, документальное отражение изменений и т.п.);
- мероприятия по подбору и расстановке кадров (проверка принимаемых на работу, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, создание условий, при которых персоналу было бы невыгодно

нарушать свои обязанности и т.д.).

Постоянно проводимые мероприятия включают:

- мероприятия по обеспечению достаточного уровня физической защиты всех компонентов АС (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности СВТ, носителей информации и т.п.).
- мероприятия по непрерывной поддержке функционирования и управлению используемыми средствами защиты;
- явный и скрытый контроль за работой персонала системы;
- контроль за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй и функционирования АС;
- постоянно (силами отдела (службы) безопасности) и периодически (с привлечением сторонних специалистов) осуществляемый анализ состояния и оценка эффективности мер и применяемых средств защиты.

Для организации и обеспечения эффективного функционирования комплексной системы компьютерной безопасности должны быть разработаны следующие группы организационно-распорядительных документов:

- документы, определяющие порядок и правила обеспечения безопасности информации при ее обработке в АС (план защиты информации в АС, план обеспечения непрерывной работы и восстановления информации);
- документы, определяющие ответственность взаимодействующих организаций (субъектов) при обмене электронными документами (договор об организации обмена электронными документами).

План защиты информации в АС должен содержать следующие сведения:

- описание защищаемой системы (основные характеристики защищаемого объекта): назначение АС, перечень решаемых АС задач, конфигурация, характеристики и размещение технических средств и программного обеспечения, перечень категорий информации (пакетов, файлов, наборов и баз данных, в которых они содержатся), подлежащих защите в АС и требований по обеспечению доступности, конфиденциальности, целостности этих категорий информации, список пользователей и их полномочий по доступу к ресурсам системы и т.п.; цель защиты системы и пути обеспечения безопасности АС и циркулирующей в ней информации;
- перечень значимых угроз безопасности АС, от которых требуется защита и наиболее вероятных путей нанесения ущерба;
- основные требования к организации процесса функционирования АС и мерам обеспечения безопасности обрабатываемой информации;
- требования к условиям применения и определение зон ответственности установленных в системе технических средств защиты от НСД;
- основные правила, регламентирующие деятельность персонала по вопросам обеспечения безопасности АС (особые обязанности должностных лиц АС).

План обеспечения непрерывной работы и восстановления информации должен отражать следующие вопросы системы.

Договор о порядке организации обмена электронными документами должен включать документы, в которых отражаются следующие вопросы:

- разграничение ответственности субъектов, участвующих в процессах обмена электронными документами;
- определение порядка подготовки, оформления, передачи, приема, проверки подлинности и целостности электронных документов;

- определение порядка генерации, сертификации и распространения ключевой информации (ключей, паролей и т.п.);
- определение порядка разрешения споров в случае возникновения конфликтов.

Обработка персональных данных требует создание специального режима, в котором четко определены технология их обработки, порядок и условия существования ПДн на каждом этапе их жизненного цикла. Это предусматривает разработку и внедрение процедур их сбора, приема, учета, регистрации, хранения, использования, уничтожения и т.п. Большое значение при этом имеет срок хранения ПДн, а также наличие системы контроля обработки ПДн на всех этапах их жизненного цикла.

Определение сроков обработки ПДн крайне важно потому, что Федеральный закон определяет, что «в случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки».

Сроки обработки также определяются на основании других нормативно-правовых актов. Так, требованиями трудового, гражданского, пенсионного законодательства, отраслевых нормативных актов устанавливаются определенные сроки обработки персональных данных. Например, для карточек Т-2 - это 75 лет (Постановление Госкомстата № 1), а для сведений о предоставленных абоненту услугах связи - 3 года (Постановление Правительства № 538)[3].

ГЛАВА 2. ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ «ЧЭнК ИМ. С. М. КИРОВА»

2.1 База персональных данных

Челябинский энергетический техникум был создан приказом ВСНХ№1731 от 27 июля 1930 г., а в 1936 г. ему было присвоено имя С.М. Кирова.

В 2003 г. Челябинский энергетический техникум преобразован в колледж и объединен с Челябинским индустриальным колледжем. Результатом этого слияния стали два образовательных корпус: Энергетический корпус и Индустриальный корпус.

На сегодняшний день – это Государственное бюджетное образовательное учреждение среднего профессионального образования «Челябинский энергетический колледж имени С. М. Кирова».

В учреждении имеются два корпуса:

1. 454006, г. Челябинск, ул. Российская 23,
2. 454087, г. Челябинск ул. Блюхера 91,

Режим работы учебного заведения:

– понедельник – четверг с 8-00 до 17.00

– пятница с 8.00-15.45.

Колледж осуществляет образовательную деятельность в соответствии с Уставом, утвержденным приказом Министерства образования и науки Челябинской области по следующим специальностям:

– Тепловые электрические станции;

– Теплоснабжение и теплоэнергетическое оборудование;

– Электрические станции, сети и системы;

– Электроснабжение;

– Техническая эксплуатация и обслуживание электрического и электромеханического оборудования;

– Сетевое и системное администрирование;

– Информационные системы и программирование;

– Монтаж, наладка и эксплуатация электрооборудования промышленных и гражданских зданий;

– Монтаж и техническая эксплуатация промышленного оборудования;

– Монтаж и техническое обслуживание и ремонт промышленного оборудования;

– Экономика и бухгалтерский учет;

– Сооружение и эксплуатация газонефтепроводов и газонефтехранилищ;

– Земельно-имущественные отношения;

– Сварочное производство;

– Техническое обслуживание и ремонт автомобильного транспорта;

– Техническое обслуживание и ремонт двигателей, систем и агрегатов автомобилей;

– Строительство и эксплуатация зданий и сооружений;

– Монтаж, наладка и эксплуатация электрооборудования промышленных и гражданских зданий;

– Управление, эксплуатация и обслуживание многоквартирного дома.

На данный момент в колледже обучается 1720 человек (очное-1471 , заочное-168 , очно-заочное-81). Из них за счет средств областного бюджета 1473 человек, за счет вне бюджета 247 человек.

Педагогический состав ЧЭнК укомплектован полностью. Средний возраст преподавателей 42 года, административных работников – 40 лет. Основное количество педагогического состава имеет возраст от 35 до 42 лет.

Управление колледжем осуществляется в соответствии с Законом «Об образовании в Российской Федерации», Уставом и локальными актами колледжа на принципах единоначалия и самоуправления, демократичности, открытости, приоритета общечеловеческих ценностей, охраны жизни и здоровья человека, свободного развития личности. В соответствии с основными задачами колледжа выстраивается система управления образовательным процессом. Структура управления представляет собой комбинацию линейной и программно-целевой структур управления. В соответствии с линейной структурой (по вертикали) строится управление по отдельным направлениям деятельности колледжа: учебно-методическое, учебно-воспитательное, учебно-производственное и т.д.

Общее руководство деятельностью Государственного бюджетного профессионального образовательного учреждения «Челябинский энергетический колледж» осуществляет директор (по содержанию – это уровень стратегического управления), который определяет совместно с Управляющим Советом колледжа стратегию развития, представляет интересы колледжа в государственных и общественных инстанциях. Несет персональную юридическую ответственность за организацию жизнедеятельности колледжа, создает благоприятные условия для развития.

Педагогический совет - совещательный орган при директоре колледжа и под его председательством, в состав которого входят преподаватели, мастера производственного обучения и другие педагогические работники, заместители директора, председатели цикловых методических комиссий.
Педагогический совет, непосредственно участвует:

- В процессе обучения и воспитания;
- Решает задачи совершенствования образовательного процесса;

- Оценивает достигнутые результаты учебно-методической и воспитательной работы.

Методический совет - возглавляет целевую систему внутри колледжного контроля, основанную на координации деятельности всех подразделений и должностных лиц по осуществлению контрольных мероприятий на единой методической основе. Председатели Методсовета назначаются приказом директора их числа наиболее квалифицированных преподавателей и работников структурных подразделений колледжа. Методические комиссии отвечают:

- за соответствие программы требованиям ФГОС СПО;
- своевременность разработки, качество и достаточность содержания программы;
- планируют и реализуют программу учебно-методического, учебно-воспитательного процесса.

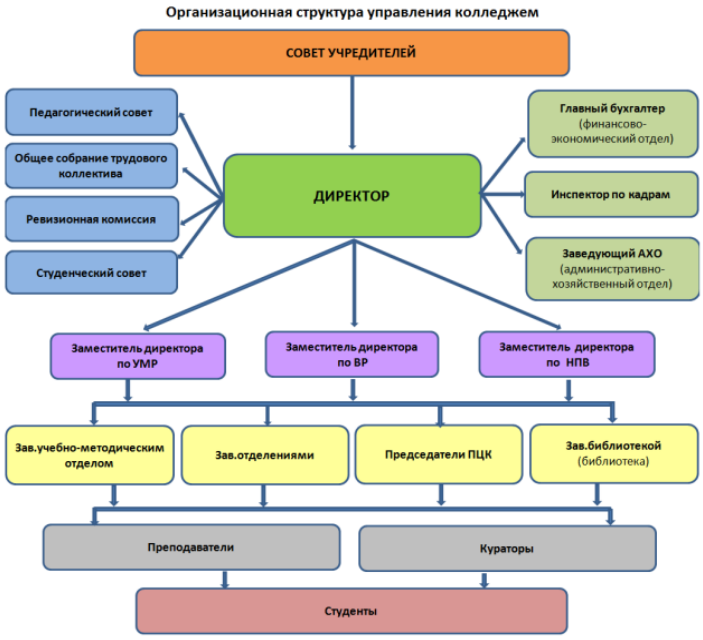

Рисунок 1– Организационная структура управления колледжем.

В профессиональной образовательной организации можно выделить два основных подразделения обрабатывающих информацию, в которую включены ПДн: Бухгалтерия и кадры (обработка персональных данных сотрудников и студентов).

БД, хранящиеся в ЭВМ, могут весьма разнообразны, поскольку требуется наиболее детально осветить различные аспекты деятельности предприятия. Существенным отличием от бумажного аналога является скорость доступа и объём сведений получаемым при автоматизированной обработке БД. Поэтому для защиты информации в БД, а также уменьшения занимаемого места на диске, используют:

Сегментацию. Физическая или логическая сегментация БД в ИСПДн по классам обрабатываемой информации, выделение сегментов сети, в которых происходит автоматизированная обработка персональных данных.

Обезличивание. Введение в процесс обработки персональных данных процедуры обезличивания существенно упростит задачи по защите персональных данных. Обезличивание можно провести путем нормализации баз данных, либо кодированием, либо шифрованием.

Разделение ПДн на части. В этом случае возможно уменьшение количества субъектов ПДн, обрабатываемых в системе. Это может быть достигнуто, например, за счет использования таблиц перекрестных ссылок в базах данных.

Абстрагирование ПДн. Зачастую на некоторых участках обработки или сегментах сети персональные данные можно сделать менее точными, например, путем группирования общих характеристик.

Состав ИСПДн «Кадры»:

Персональные данные сотрудников организации:

1) фамилия, имя, отчество;

2) дата и место рождения;

3) пол;

4) паспортные данные (серия, номер паспорта, кем и когда выдан);

5) информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование:

наименование, номер, дата выдачи, специальность);

6) информация о трудовой деятельности до приема на работу;

7) информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);

8) семейное положение;

9) адреса регистрации и фактического проживания;

10) номера контактных телефонов;

11) индивидуальный номер налогоплательщика;

12) номер страхового свидетельства пенсионного страхования;

13) номер полиса обязательного медицинского страхования;

14) данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);

15) данные об аттестации работников;

16) данные о повышении квалификации;

17) данные о наградах, медалях, поощрениях, почетных званиях;

18) информация об отпусках;

19) информация о командировках;

20) информация о болезнях.

В информационной системе одновременно обрабатываются данные 236 субъектов персональных данных (сотрудников) в пределах Организации.

2.2 Средства защиты информации

Средства защиты информации - это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

Аппаратные средства - это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они препятствуют доступу к информации, в том числе с помощью её маскировки. К аппаратным средствам относятся: генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны - недостаточная гибкость, относительно большие объём и масса, высокая стоимость[12].

К основным аппаратным средствам защиты информации относятся:

устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т.п.);

устройства для шифрования информации;

устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы).

устройства уничтожения информации на носителях;

устройства сигнализации о попытках несанкционированных действий пользователей компьютерной системы и др[13].

Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств - универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки - ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств)[12].

К программным средства относят:

встроенные в ОС средства защиты информации (механизмы идентификации и аутентификации, разграничение доступа, аудит и пр);

антивирусная программа (антивирус) - программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики - предотвращения заражения файлов или операционной системы вредоносным кодом (наиболее известные антивирусы ESET NOD32, Kaspersky Antivirus, Dr. Web;

криптографические методы защиты информации - это методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования. Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней (например, зашифрованный файл нельзя прочесть даже в случае кражи носителя). Криптографические программы делятся на встраиваемые в операционную систему (cryptographic services provider (CSP) - криптопровайдер) и выполненные в виде отдельных приложений.

Самыми распростаранёными являются Microsoft Base Cryptographic Provider, КриптоПро CSP, ViPNet CSP, Shipka CSP;

Межсетевой экран (firewall) - это устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных. Существуют два основных типа межсетевых экранов: межсетевые экраны прикладного уровня и межсетевые экраны с пакетной фильтрацией. В их основе лежат различные принципы работы, но при правильной настройке оба типа устройств обеспечивают правильное выполнение функций безопасности, заключающихся в блокировке запрещенного трафика.

сервер (от англ. proxy - «представитель, уполномоченный») - служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, e-mail), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша (в случаях, если прокси имеет свой кэш). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях. Также прокси-сервер позволяет защищать клиентский компьютер от некоторых сетевых атак и помогает сохранять анонимность клиента. Наиболее распространенными являются 3proxy, Kerio Control, Squid, UserGate.

Защищенной виртуальной сетью VPN называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

Наиболее распространёнными программами для создания VPN являются: OpenVPN, CiscoWork VPN, ViPNeT Custom, CSP VPN, StoneGate SSL VPN.

Системы обнаружения вторжений (IDS) - программное средство,

предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Классификация IDS может быть выполнена:

по способу реагирования;

способу выявления атаки;

способу сбора информации об атаке.

По способу реагирования различают пассивные и активные IDS. Пассивные IDS просто фиксируют факт атаки, записывают данные в файл журнала и выдают предупреждения. Активные IDS пытаются противодействовать атаке, например, путем реконфигурации МЭ или генерации списков доступа маршрутизатора.

По способу выявления атаки системы IDS принято делить на две категории:

обнаружение аномального поведения (anomaly-based);

обнаружениезлоупотреблений (misuse detection или signature-based).

Классификация по способу сбора информации об атаке:

обнаружение атак на уровне сети (network-based)

обнаружение атак на уровне хоста (host-based)

обнаружение атак на уровне приложения (application-based).

Программно-аппартные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства[12].

Данные средства, как правило, состоят из нескольких частей:

аппаратный ключ, обеспечивающий идентификацию и аутентификацию пользователя (например iButton, eToken, Rutoken);

считыватель;

плата PCI для интеграции механизмов защиты в ПЭВМ.

2.3 Цикл обработки персональных данных

Обработка персональных данных требует создание специального режима, в котором четко определены технология их обработки, порядок и условия существования ПДн на каждом этапе их жизненного цикла. Это предусматривает разработку и внедрение процедур их сбора, приема, учета, регистрации, хранения, использования, уничтожения и т.п. Большое значение при этом имеет срок хранения ПДн, а также наличие системы контроля обработки ПДн на всех этапах их жизненного цикла.

Определение сроков обработки ПДн крайне важно потому, что Федеральный закон определяет, что «в случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки». Сроки обработки также определяются на основании других нормативно-правовых актов. В основе деятельности по созданию и использованию ИТ (ИСПДн является частным его звеном) лежит понятие жизненный цикл (ЖЦ), которое является одним из базовых понятий методологии проектирования САПР и многих других ИС. В настоящее время существует ряд общих методологий разработки ИС. Главное в них - единая дисциплина работы на всех этапах жизненного цикла системы, учет критических задач и контроль их решения, применение развитых инструментальных средств поддержки процессов анализа, проектирования и реализации ИС.

В общем случае под термином жизненный цикл системы (System Life Cycle) понимается определенная эволюция, период времени и совокупность работ, меняющих состояние системы от появления замысла и начала ее разработки до окончания эксплуатации. Обычно разбивается на отдельные стадии - анализ требований, проектирование, реализация (конструирование), верификация и эксплуатация. Стадии ЖЦ системы

могут повторяться итерационным образом в связи с постепенным уточнением требований к системе и/или с необходимостью ее адаптации к тем изменениям, которые возникают в предметной области системы.

Понятие ЖЦ системы позволяет определить понятие жизненный цикл ИС (ЖЦ ИС) - это модель создания и использования (эволюция) ИС, отражающая ее различные состояния, начиная с момента возникновения необходимости в данном комплексе средств создания и обмена информацией, и заканчивая моментом ее полного выхода из употребления у пользователей.

ЖЦ ИС - это период времени и совокупность работ, от момента возникновения и обоснования необходимости создания до момента нецелесообразности дальнейшей ее эксплуатации, т.е. это совокупность взаимосвязанных процессов создания и последовательного изменения состояния ИС, меняющих состояние системы, от формирования исходных требований к ней до окончания эксплуатации и утилизации комплекса средств автоматизации ИС. Обычно разбивается на отдельные стадии - анализ требований, проектирование, реализация (конструирование), верификация и эксплуатация. Стадии жизненного цикла системы могут повторяться итерационным образом в связи с постепенным уточнением требований к системе и/или с необходимостью ее адаптации к тем изменениям, которые возникают в предметной области системы. Такой цикл проходят все технические, технологические и иные информационные системы и в каждом случае они должны быть экономически обоснованы и привязаны к конкретным условиям производства[18].

2.4 Классификация угроз безопасности персональных данных в ИСПДн

2.4.1 Общее описание угроз безопасности ПДн, обрабатываемых в ИСПДн

При обработке ПДн в ИСПДн «Челябинский энергетический колледж им С. М. Кирова» возможна реализация следующих видов УБПДн:

- угрозы утечки информации по техническим каналам;
- угрозы НСД к ПДн, обрабатываемым в ИСПДн.

2.4.1 Угрозы утечки информации по техническим каналам.

Основными элементами угроз утечки информации по техническим каналам являются:

1. источник угрозы (физические лица, не имеющие доступа к ИСПДн, а также организации (в том числе конкурирующие или террористические), криминальные группировки, осуществляющие перехват (съем) информации с использованием технических средств регистрации, приема или фотографирования информации);

2. среда (путь) распространения информативного сигнала (физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником);

3. носитель защищаемой информации (пользователь ИСПДн, осуществляющий голосовой ввод ПДн в ИСПДн, акустическая система ИСПДн, воспроизводящая ПДн, а также технические средства ИСПДн и ВТСС, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин).

При обработке ПДн в ИСПДн возможно возникновение УБПДн за счет реализации следующих технических каналов утечки информации:

1. угрозы утечки акустической (речевой) информации;
2. угрозы утечки видовой информации;
3. угрозы утечки информации по каналам ПЭМИН.

Возникновение угроз утечки акустической (речевой) информации, содержащаяся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций

голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

2.4.2 Угрозы несанкционированного доступа.

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения), целостности (уничтожения, изменения) и доступности (блокирования) ПДн, и включают в себя:

1. Угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения*;*

Угрозы доступа (проникновения) в операционную среду ИСПДн с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа.

Угрозы непосредственного доступа осуществляются с использованием программных и программно-аппаратных средств ввода/вывода компьютера.

Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

2. Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.; Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств - это угрозы «Отказа в обслуживании». Их реализация обусловлена тем, что при разработке системного или прикладного программного обеспечения не учитывается возможность преднамеренных действий по целенаправленному изменению:

- содержания служебной информации в пакетах сообщений, передаваемых по сети;
- условий обработки данных (например, игнорирование ограничений на длину пакета сообщения);
- форматов представления данных (с несоответствием измененных форматов, установленных для обработки по протоколам сетевого взаимодействия);
- программного обеспечения обработки данных.

В результате реализации угроз «Отказа в обслуживании» происходит переполнение буферов и блокирование процедур обработки, «зацикливание» процедур обработки и «зависание» компьютера, отбрасывание пакетов сообщений и др.

3. Угрозы внедрения вредоносных программ (программно-математического воздействия).

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы. Это обусловлено тем, что, во-первых, количество вредоносных программ сегодня уже значительно превышает сто тысяч. Во-вторых, при организации защиты информации на

практике, как правило, достаточно лишь знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования).

Оценка опасности угроз ИСПДн:

Оценка опасности производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет 3 значения:

- низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности с учетом приведенных критерием представлена в таблице 2.

Таблица 2 – Оценка опасности

Угроза безопасности ПДн	Опасность угроз
угроза модификации базовой системы ввода/вывода (BIOS),	низкая
угроза перехвата управления загрузкой	низкая
угроза НСД с применением стандартных функций операционной системы	низкая
угроза НСД с помощью прикладной программы	низкая
угроза НСД с применением специально созданных для этого программ	низкая
угроза утечки информации с использованием копирования ее на съемные носители;	низкая

Продолжение таблицы 2

угроза утечки информации за счет ее несанкционированной передачи по каналам связи	низкая
угроза внедрения вредоносных программ с использованием съемных носителей	низкая
угроза «Анализа сетевого трафика»	низкая
угроза сканирования направленного на выявление открытых портов и служб, открытых соединений и др	низкая
угроза обхода системы идентификации и аутентификации сообщений	низкая
угроза обхода системы идентификации и аутентификации сетевых объектов	низкая
угроза внедрения ложного объекта сети	низкая
угроза навязывания ложного маршрута	низкая
угроза перехвата и взлома паролей	низкая
угроза подбора паролей доступа	низкая
угроза типа «Отказ в обслуживании	низкая
угроза внедрения троянских программ	низкая
угроза атаки типа «переполнение буфера»;	низкая
угроза удаленного запуска приложений с использованием средств удаленного управления	низкая
угроза внедрения вредоносных программ через почтовые сообщения	низкая
угроза внедрения вредоносных программ через обмен и загрузку файлов	низкая
угроза заражения сетевыми червями, использующими уязвимости сетевого ПО	низкая

ГЛАВА 3. РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

3.1Разработка положения об обработке персональных данных

В связи с актуальностью вопросов организации и осуществления в образовательных учреждениях мероприятий по обеспечению защиты персональных данных работников нами были разработаны Рекомендации по защите персональных данных работников образовательных организаций.

Рекомендации основаны на положениях законодательства Российской Федерации, действующих в сфере защиты персональных данных, и ориентированы в первую очередь на оказание практической помощи руководителям образовательных учреждений по выработке мер защиты персональных данных работников.

Защита персональных данных представляет собой комплекс мер технического, организационного и правового характера, направленных на защиту сведений, относящихся к персональной (личной) информации.

Общие и специальные положения о защите персональных данных работников регламентируются в соответствии с Конституцией Российской:

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

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ о персональных данных);

Трудовым кодексом Российской Федерации (далее – ТК РФ).

Персональные данные относящиеся к категории личной информации. Следовательно, работодатель, получающий доступ к персональным данным, должен обеспечить конфиденциальность таких данных.

К сведениям, которые не могут составлять секретную, отнесены в частности:

сведения о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений.

Образовательные учреждения, являющиеся некоммерческими организациями и обязаны в установленных федеральным законодательством случаях, в том числе в рамках реализации предусмотренного Федеральным законом «О профессиональных союзах, их правах и гарантиях деятельности» права на информацию (ст. 17), представлять по запросу профсоюзной организации сведения о численности и об оплате труда работников учреждения.

ФЗ о персональных данных определяет требования к сбору и обработке (хранению, актуализации, использованию, раскрытию и предоставлению) персональных данных физических лиц во всех сферах, где используются персональные данные, в том числе в сфере трудовых правоотношений, возникающих в образовательных учреждениях, с учетом особенностей, предусмотренных ТК РФ.

Именно образовательные учреждения должны в первую очередь отреагировать на требования законодательства о защите персональных данных участников образовательного процесса с учетом того, что фактически речь идет не просто о защите какого-то абстрактного вида информации, а о защите сведений, незаконное использование которых может серьезно отразиться на правах граждан.

Планирование мероприятий по защите персональных данных

работников

При планировании и осуществлении мероприятий, связанных с защитой персональных данных работников, рекомендуется привлекать юристов, специалистов отдела кадров (по кадровым вопросам), специалистов по информационной работе (компьютерным технологиям). Правовая составляющая должна стать обязательным элементом всей деятельности учреждения в этом направлении, поскольку необходимо:

разработать локальные акты (нормативные и правовые), связанные не только с организационной и правовой, но и технической защитой персональных данных; проработать механизмы взаимоотношений с органами, осуществляющими управление в сфере образования, профсоюзными организациями, органами контроля и надзора и т.д.

Особое внимание следует уделить передаче персональных данных третьим лицам как с точки зрения наличия основания для такой передачи, предусмотренного федеральными законами, или в виде согласия субъекта персональных данных (например, закрепленного в договоре на оказание услуг), так и с точки зрения обязательного наличия договора с этим третьим лицом, существенным условием которого должна быть обязанность обеспечения указанным лицом конфиденциальности и безопасности персональных данных при их обработке.

Защита персональных данных работников в образовательном учреждении по сути сводится к созданию режима обработки персональных данных, включающего:

создание внутренней документации по работе с персональными данными;

создание организационной системы защиты персональных данных;

внедрение технических мер защиты персональных данных.

Правовое регулирование вопросов обеспечения защиты персональных данных работников на локальном уровне

В соответствии со ст. 85 ТК РФ к персональным данным

работника относится информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Согласно порядку документального оформления в сфере трудовых отношений на каждого работника работодателем заводится личное дело, в котором хранятся сведения, относящиеся к персональным данным работника:

копия паспорта (паспортные данные работника);

копия страхового свидетельства государственного пенсионного страхования;

копия документа воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);

копия документа об образовании, квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);

анкетные данные, заполненные работником при поступлении на работу или в процессе работы (в т.ч. автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);

иные документы, которые с учетом специфики работы и в соответствии с законодательством РФ должны быть предъявлены работником при заключении трудового договора или в период его действия (например, медицинские заключения, предъявляемые работником при прохождении обязательных предварительных и периодических медицинских осмотров);

трудовой договор (соглашения о внесении изменений и дополнений в него);

копии приказов о приеме, переводах, увольнении, повышении заработной платы, премировании, поощрениях и взысканиях;

личная карточка по форме Т-2;

заявления, объяснительные и служебные записки работника;

документы о прохождении работником аттестации, собеседования, повышения квалификации (аттестационный лист);

иные документы, содержащие сведения о работнике, нахождение которых в личном деле работника необходимо для документального оформления трудовых правоотношений с работником.

Статьей 87 Трудового кодекса РФ предусмотрено, что порядок хранения и использования персональных данных работников устанавливается работодателем с учетом требований ТК РФ и иных федеральных законов, что подразумевает регулирование порядка обработки персональных данных работников локальными нормативными и иными актами.

Основным таким локальным нормативным актом должно быть Положение о защите персональных данных работников, которое принимается с учетом мнения выборного органа первичной профсоюзной организации учреждения в порядке, предусмотренном ст. 372 ТК РФ Данный локальный нормативный акт является обязательным, поэтому его отсутствие может быть квалифицировано государственным и иным органом контроля и надзора (федеральной инспекцией труда и др.) как нарушение работодателем трудового законодательства.

Наряду с Положением о защите персональных данных работников в образовательном учреждении также необходимо наличие следующих документов:

В процессе получения персональных данных работников:

- согласие работника на получение работодателем персональных данных от третьих лиц

- уведомление работника о получении его персональных данных от третьих

При осуществлении обработки персональных данных работников:

- согласие работника на обработку его персональных данных.

При хранении персональных данных работников:

- приказ об утверждении списка лиц, имеющих доступ к персональным данным работников

- обязательство о неразглашении персональных данных работников

При передаче персональных данных работников:

- согласие работника на передачу его персональных данных третьим лицам

Поскольку на работодателя возложена обязанность соблюдения режима секретности персональных данных, то необходимо в целях обеспечения выполнения этого требования вести журналы учета персональных данных, их выдачи и передачи другим лицам и представителям различных организаций, органам контроля и надзора, правоохранительным органам, которые обеспечат документальную фиксацию внутреннего и внешнего доступа к персональным данным работников.

В журнале учета внутреннего доступа к персональным данным (доступа работников учреждения к персональным данным других работников) следует указывать такие сведения, как дата выдачи и возврата документов (личных дел), срок пользования, цели выдачи, наименование выдаваемых документов (личных дел). Лицо, которое возвращает документ (личное дело), должно обязательно присутствовать при проверке наличия всех имеющихся документов по описи, если выданные документы составлены более чем на одном листе.

Помимо этого, также необходимо вести журнал учета внутреннего доступа к персональным данным работников в учреждении;

журнал учета выдачи персональных данных работников учреждения организациям и государственным органам (журнал учета внешнего доступа к персональным данным работников);

журнал проверок наличия документов, содержащих персональные данные работников.

журнала учета применяемых работодателем носителей информации.

Порядок передачи работодателем персональных данных работников

По общему правилу, персональные данные работника не могут быть переданы работодателем третьей стороне. Исключением из данного правила являются следующие случаи:

выдача работником письменного согласия на передачу персональных данных третьей стороне;

передача персональных данных работника в целях предупреждения угрозы жизни и здоровью самого работника;

другие случаи, установленные федеральным законом.

получателями персональных данных работника на законном основании являются:

органы социального страхования, органы пенсионного обеспечения, налоговые органы, органы прокуратуры и другие правоохранительные органы, федеральная инспекция труда профессиональные союзы (в соответствии с Федеральным законом «О профессиональных союзах, их правах и гарантиях деятельности» и ТК РФ профсоюзы имеют право на получение информации от работодателей по социально-трудовым вопросам для осуществления своей уставной деятельности, а также право на осуществление общественного контроля за соблюдением работодателями, должностными лицами трудового законодательства);

другие органы и организации в случаях, предусмотренных федеральным законом.

Реализация прав профсоюзов, связанных с доступом к персональным данным работников

В соответствии со ст. 17 Федерального закона «О профессиональных союзах, их правах и гарантиях деятельности» для

осуществления своей уставной деятельности профсоюзы вправе бесплатно и беспрепятственно получать от работодателей, их объединений (союзов, ассоциаций), органов государственной власти и органов местного самоуправления информацию по социально- трудовым вопросам.

Согласно ст. 11 Федерального закона «О профессиональных союзах, их правах и гарантиях деятельности» профсоюзные представители вправе беспрепятственно посещать организации и рабочие места, где работают члены соответствующих профсоюзов, для реализации уставных задач и предоставленных профсоюзам прав.

В соответствии со статьей 19 указанного федерального закона профсоюзы имеют право на осуществление профсоюзного контроля за соблюдением работодателями, должностными лицами трудового законодательства, в том числе по вопросам защиты персональных данных, трудового договора, рабочего времени и времени отдыха, оплаты труда, гарантий и компенсаций, льгот и преимуществ, а также по другим социально-трудовым вопросам в организациях, в которых работают члены данного профсоюза, и имеют право требовать устранения выявленных нарушений. Работодатели, должностные лица обязаны в недельный срок с момента получения требования об устранении выявленных нарушений сообщить профсоюзу о результатах его рассмотрения и принятых мерах.

Право на осуществление профсоюзами контроля за соблюдением работодателями и их представителями трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права, в том числе по вопросам защиты персональных данных работников, выполнением ими условий коллективных договоров, соглашений установлено также статьей 370 Трудового кодекса РФ.

Профсоюзные инспекторы труда в установленном порядке имеют право беспрепятственно посещать любых работодателей (организации,

независимо от их организационно-правовых форм и форм собственности), у которых работают члены данного профессионального союза.

Таким образом, в целях реализации полномочий, установленных федеральными законами и предусмотренных в Уставе Профсоюза и иных профсоюзных нормативных документах, профсоюзные организации вправе запрашивать в определенных целях и получать от работодателя информацию, в том числе относящуюся к персональным данным работников, которую обязаны использовать исключительно в целях, которые заявлялись при запросе соответствующей информации, а также не разглашать такую информацию, т.е. обеспечивать в соответствии с требованиями законодательства ее секретность.

Права и обязанности работников, связанные с обработкой и защитой их персональных данных

Согласно п. 8 ст. 86 Трудового кодекса РФ работники и их представители должны быть ознакомлены под роспись с документами, устанавливающими порядок обработки и защиты персональных данных, а также их права и обязанности в этой области.

В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники в соответствии со ст. 89 ТК РФ имеют право на:

полную информацию об их персональных данных и обработке этих данных;

свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

определение своих представителей для защиты своих персональных данных;

доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

требование об исключении или исправлении неверных или неполных персональных данных, а также

данных, обработанных с нарушением требований ТК РФ или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Работники обязаны в разумный срок информировать работодателя об изменении персональных данных.

Ответственность за нарушение требований по защите персональных данных

В соответствии со ст. 24 ФЗ о персональных данных лица, виновные в нарушении требований этого федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

В соответствии со ст. 90 ТК РФ, устанавливающей ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника, лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в

порядке, установленном ТК РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Так, к работнику, отвечающему за хранение персональных данных в силу его трудовых обязанностей, работодатель вправе применить одно из дисциплинарных взысканий, предусмотренных ст. 192 ТК РФ (замечание, выговор, увольнение).

Помимо этого работники, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, могут быть привлечены к материальной и уголовной ответственности.

Система государственного надзора и контроля в области персональных данных

уполномоченный орган по защите прав субъектов персональных данных - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), территориальные органы которой действуют в каждом субъекте РФ. Вторым регулятором, осуществляющим контроль за осуществлением мер по технической защите информационных систем обработки персональных данных, является Федеральная служба по техническому и экспортному контролю (ФСТЭК) и ее территориальные органы.

Третьим регулятором является федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, - Федеральная служба безопасности.

ПРИМЕРНОЕ ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

I. Общие положения

1.Примерное положение о защите персональных данных работников образовательного учреждения (далее – Положение) разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации (далее – ТК РФ), Федеральным законом «О персональных данных», Федеральным законом «Об информации, информационных технологиях и о защите информации», другими федеральными законами и иными нормативными правовыми актами.

2. Положение является локальным нормативным актом, регламентирующим порядок обеспечения защиты персональных данных работников при их обработке в образовательном учреждении, в том числе защиты от несанкционированного доступа, неправомерного их использования или утраты.

3. Настоящим Положением определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных работника, права и обязанности работников и руководителя образовательного учреждения, а также ответственность лиц, имеющих доступ к персональным данным работников, за невыполнение правовых норм, регулирующих обработку и защиту персональных данных работников.

4. В настоящем Положении используются следующие основные понятия и термины:

персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его

фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

защита персональных данных – комплекс мер технического, организационного и организационно-технического, правового характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных – работнику);

персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника;

общедоступные персональные данные работника – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

работник – физическое лицо, вступившее в трудовые отношения с работодателем (образовательным учреждением);

работодатель – юридическое лицо (образовательное учреждение), вступившее в трудовые отношения с работником;

оператор – юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных работника, а также определяющее цели и содержание обработки персональных данных;

обработка персональных данных работника – действия (операции) с персональными данными работника, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

информационная система персональных данных –

информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

использование персональных данных – действия (операции) с персональными данными, совершаемые работодателем (уполномоченным им лицом) в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников или других лиц либо иным образом затрагивающих права и свободы работников или других лиц;

конфиденциальность персональных данных – обязательное для соблюдения работодателем или лицом, получившим доступ к персональным данным работников, требование не допускать их распространения без согласия работника или иного законного основания;

блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

5. Персональные данные работников относятся к категории конфиденциальной информации.

6. Настоящее Положение является локальным нормативным актом, который утверждается работодателем с учетом мнения выборного органа первичной профсоюзной организации в порядке, установленном ст. 372 ТК РФ для принятия локальных нормативных актов[3].

II. Состав персональных данных работников

7. К персональным данным работников, получаемым работодателем и подлежащим хранению у работодателя в порядке, предусмотренном законодательством Российской Федерации и настоящим Положением, относятся следующие документы, содержащиеся в личных делах работников:

копия паспорта (паспортные данные работника);

копия страхового свидетельства государственного пенсионного страхования;

копия документа воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);

копия документа об образовании, квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);

анкетные данные, заполненные работником при поступлении на работу или в процессе работы (в т.ч. автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);

иные документы, которые с учетом специфики работы и в соответствии с законодательством РФ должны быть предъявлены работником при заключении трудового договора или в период его действия;

трудовой договор (соглашения о внесении изменений и дополнений в него);

заключение по данным психологического исследования (если такое имеется);

копии приказов о приеме, переводах, увольнении, повышении заработной платы, премировании, поощрениях и взысканиях;

личная карточка по форме Т-2;

заявления, объяснительные и служебные записки работника;

документы о прохождении работником аттестации, собеседования, повышения квалификации (аттестационный лист);

иные документы, содержащие сведения о работнике, нахождение которых в личном деле работника необходимо для документального оформления трудовых правоотношений с работником.

8. Документы, содержащие персональные данные работников, создаются путем:

копирования оригиналов;

внесения сведений в учетные формы (на бумажных и электронных носителях);

получения оригиналов необходимых документов.

III. Основные условия проведения обработки персональных данных работников

9. При определении объема и содержания обрабатываемых персональных данных работников работодатель должен руководствоваться Конституцией РФ, ТК РФ и иными федеральными законами.

10. Обработка персональных данных работников может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

11. Персональные данные следует получать у самого работника. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

12. При получении персональных данных работодатель должен сообщить работнику о целях, предполагаемых источниках и способах

получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

13. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны работодателем только с его письменного согласия.

14. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных ТК РФ или иными федеральными законами.

15. При получении персональных данных не от работника (за исключением случаев, если персональные данные были предоставлены работодателю на основании федерального закона или если персональные данные являются общедоступными), работодатель до начала обработки таких персональных данных обязан предоставить работнику следующую информацию:

наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

цель обработки персональных данных и ее правовое основание;

предполагаемые пользователи персональных данных;

установленные законодательством права субъекта персональных данных.

16. Обработка указанных персональных данных работников работодателем возможна без их согласия в следующих случаях: персональные данные являются общедоступными;

персональные данные относятся к состоянию здоровья работника и

их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;

по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

IV. Работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области. Хранение и передача персональных данных работников

17. Персональные данные работников образовательного учреждения хранятся на бумажных и электронных носителях в специально предназначенном для этого помещении.

18. Для организации хранения персональных данных в образовательном учреждении специалисты по информационной работе и другие специалисты проводят мероприятия по определению круга информационных систем и совокупности обрабатываемых персональных данных, категорированию персональных данных и предварительной классификации информационных систем.

19. В процессе хранения персональных данных работников необходимо обеспечивать:

требования законодательства, устанавливающие правила хранения конфиденциальных сведений;

сохранность имеющихся данных, ограничение доступа к ним в соответствии с законодательством РФ и настоящим Положением;

контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

20. Доступ к персональным данным работников разрешается

только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций.

21. Внутренний доступ к персональным данным работников в образовательном учреждении осуществляется в соответствии со списком лиц, уполномоченных на получение и доступ к персональным данным, утвержденным приказом руководителя образовательного учреждения.

Иные права и обязанности работников образовательного учреждения, в трудовые обязанности которых входит обработка персональных данных работников, определяются также должностными инструкциями.

22. Право внутреннего доступа к персональным данным работников образовательного учреждения имеют:

- руководитель организации;
- работник, чьи персональные данные подлежат обработке;
- работники, уполномоченные в соответствии с приказом на получение и доступ к персональным данным работников.

23. В целях обеспечения надлежащего выполнения трудовых обязанностей доступ к персональным данным работника может быть предоставлен на основании приказа руководителя образовательного учреждения иному работнику, должность которого не включена в список лиц, уполномоченных на получение и доступ к персональным данным.

24. Юридическим и физическим лицам, оказывающим услуги образовательному учреждению на основании заключенных гражданско-правовых договоров (либо на иных основаниях), которым необходим доступ к персональным данным работников образовательного учреждения в связи с выполнением ими обязательств по указанным договорам, соответствующие данные могут предоставляться

работодателем только после подписания с ними соглашения о неразглашении конфиденциальной информации.

В исключительных случаях, исходя из договорных отношений с третьими лицами, допускается наличие в договорах пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных работников.

25. Работники, осуществляющие обработку персональных данных, должны быть уведомлены в письменной форме о своей обязанности не разглашать персональные данные работников, к которым они получили доступ.

26. Получателями персональных данных работника вне образовательного учреждения на законном основании являются органы пенсионного обеспечения, органы социального страхования, определяемые в соответствии с федеральными законами о конкретных видах обязательного социального страхования; органы прокуратуры и другие правоохранительные органы; налоговые органы; федеральная инспекция труда; профессиональные союзы, а также иные органы и организации в соответствии с федеральными законами.

27. Работодатель не может сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных ТК РФ или иными федеральными законами.

28. Работодатель обязан передавать персональные данные работника представителям работников в порядке, установленном ТК РФ и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

29. Любые лица, обладающие доступом к персональным данным

работников образовательного учреждения, обязаны соблюдать специальный режим их использования и защиты. Лица, получившие персональные данные работника на законном основании, обязаны использовать их исключительно в целях, которые заявлялись при запросе соответствующей информации, а также не разглашать такую информацию (исключения из данного правила определяются только федеральными законами).

Лицо, которое получает личное дело другого работника во временное пользование, не имеет права делать в нем какие-либо пометки, исправления, вносить новые записи, извлекать документы из личного дела или помещать в него новые.

30. В целях обеспечения соблюдения режима конфиденциальности персональных данных в образовательном учреждении ведутся следующие учетные документы движения персональных данных работников:

журнал учета внутреннего доступа к персональным данным работников в учреждении;

журнал учета выдачи персональных данных работников учреждения организациям и государственным органам (журнал учета внешнего доступа к персональным данным работников);

журнал проверок наличия документов, содержащих персональные данные работников;

журнал учета применяемых работодателем носителей информации.

V. Способы защиты персональных данных работников

31. Защита персональных данных работников представляет собой регламентированный технологический, организационный и иной процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных работников образовательного учреждения и обеспечивающий надежную безопасность информации.

32. Защита персональных данных работников от неправомерного их использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном федеральным законом.

33. Для обеспечения внутренней защиты персональных данных работников работодатель:

регламентирует состав работников, функциональные обязанности которых требуют соблюдения режима конфиденциальности;

избирательно и обоснованно распределяет документы и информацию между работниками, имеющими доступ к персональным данным;

своевременно обеспечивает работников информацией о требованиях законодательства по защите персональных данных;

обеспечивает организацию порядка уничтожения информации; проводит разъяснительную работу с работниками, имеющими доступ к персональным данным, по предупреждению утраты сведений при работе с персональными данными.

34. Защита сведений, хранящихся в электронных базах данных работодателя, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается разграничением прав доступа с использованием учетной записи и системой паролей.

35. Для обеспечения внешней защиты персональных данных работников образовательное учреждение:

обеспечивает порядок приема, учета и контроля деятельности посетителей;

организует пропускной режим;

обеспечивает охрану территории, зданий, помещений, транспортных средств.

36. Все лица, связанные с получением, обработкой и защитой

персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

37. В случае выявления недостоверных персональных данных работника или неправомерных действий с ними на период проверки работодатель обязан осуществить блокирование персональных данных работника с момента обращения его самого или его законного представителя либо получения запроса уполномоченного органа по защите прав субъектов.

38. При выявлении неправомерных действий с персональными данными работника работодатель обязан устранить допущенные нарушения не более трех рабочих дней с даты такого выявления.

В случае невозможности устранения допущенных нарушений работодатель не позднее чем через три рабочих дня с даты выявления неправомерности действий с персональными данными работника обязан уничтожить персональные данные работника.

39. В случае отзыва работником согласия на обработку своих персональных данных работодатель обязан прекратить обработку персональных данных работника и уничтожить их в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между работником и работодателем.

VI. Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя

40. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на бесплатное получение полной информации о:

лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

перечне обрабатываемых персональных данных и источниках их получения;

сроках обработки персональных данных, в том числе сроках их хранения;

юридических последствиях обработки их персональных данных.

41. Работники имеют право на:

бесплатное получение полной информации о своих персональных данных и обработке этих данных;

свободный бесплатный доступ к своим персональным данным, в том числе на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом; определение своих представителей для защиты своих персональных
данных;

доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

VII. Работники не должны отказываться от своих прав на

сохранение и защиту тайны. Обязанности работников в целях обеспечения достоверности их персональных данных

42. В целях обеспечения достоверности персональных данных работники обязаны:

при приеме на работу в образовательное учреждение представлять о себе достоверные сведения в порядке и объеме, предусмотренном законодательством Российской Федерации;

в случае изменения персональных данных работника (фамилия, имя, отчество, адрес места жительства, паспортные данные, сведения об образовании, состоянии здоровья (вследствие выявления в соответствии с медицинским заключением противопоказаний для выполнения работником его должностных, трудовых обязанностей) и т.п.) сообщать об этом работодателю в разумные сроки.

VIII. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работников

43. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном ТК РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

44. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работник несет дисциплинарную и материальную ответственность в порядке, установленном ТК РФ, и иную юридическую ответственность в порядке, установленном федеральным законом.

45. Лица, в обязанность которых входит ведение персональных данных работников, обязаны обеспечить каждому возможность

ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом РФ об административных правонарушениях.

IX. Заключительные положения

46. Работодатель обязан ознакомить работников с настоящим Положением, а также с внесенными в него изменениями и дополнениями под роспись с указанием даты ознакомления.

47. Изменения и дополнения в настоящее Положение вносятся в порядке, установленном ст. 372 ТК РФ для принятия локальных нормативных актов.

ЗАКЛЮЧЕНИЕ

В ходе данной работы рассмотрены основные нормативные документы, регулирующие правовые отношения в области защиты персональных данных, приведены сведения о возможных угрозах безопасности информационной системе персональных данных, в том числе подробно приведена и рассмотрена характеристика угроз несанкционированного доступа. При рассмотрении угроз, особое внимание уделялось классификации нарушителей безопасности, поскольку они выполняют доминирующую роль в нарушении безопасности информационной системе.

Особое внимание уделено основным компонентам для построения защищённой информационной системы. Подробно рассмотрены организация хранения персональных данных в базе данных.

Все образовательные учреждения осуществляют обработку персональных данных, и каждый участник учебного процесса имеет право на защиту своих персональных данных. Согласно п. 9 ст. 86 ТК РФ они не должны отказываться от своих прав на сохранение и защиту тайны[5].

За неисполнение требований Федерального закона «О персональных данных» администрация колледжа, как и любая другая организация, обрабатывающая персональные данные, несет гражданскую, уголовную, административную, дисциплинарную ответственность, предусмотренную законодательством Российской Федерации.

В ходе исследования проанализировала особенности системы защиты персональных данных ГБПОУ ЧЭнК. Выявила общие требования к обработке персональных данных. Также рассмотрела работу кадровой службы с персональными данными и изучила особенности получения, передачи и защиты данных. Была достигнута цель и выполнены поставленные задачи. Таким образом, предлагаемые мероприятия по защите персональных данных в профессиональной образовательной организации позволят повысить защиту личных данных сотрудников.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

2. Аверченков, В. И. Защита персональных данных в организации / В.И. Аверченков. - М.: Флинта, 2016. - 260 с.

3. Бачило, И.Л. Персональные данные в структуре информационных ресурсов. Основы правового регулирования /И.Л. Бачило, Л.А. Сергиенко, Б.А. Кристальный., А.Г. Арешев // Информационное право. — 2016. — N 3

4. Бачило, ИЛ. Информационное право РФ : Учебник для вузов / И.Л. Бачило. — М.: Издательство Юрайт. 2016.- 522 с.

5. Беденкова А.А., Хоменко И.С. Правовой статус персональных данных работников // Вестник науки Сибири. 2014. № 4 (14). С. 148-151.

6. Бойкова, Ольга Феоктистовна Защита персональных данных: касается всех! Практическое пособие. Выпуск № 142 / Бойкова Ольга Феоктистовна. - М.: Либерея, 2018. - 950 с

7. Бондаренко, Э.Н. Конфиденциальная информация в трудовых отношениях. / Э.Н. Бондаренко, Иванов ДВ. — СПб.; Издательство «Юридический центр-Пресс». — 2014

8. Братищенко В.В. Проектирование информационных систем. - Иркутск: Изд-во БГУЭП, 2004. - 84 с.

9. Ветров Д.М. Защита персональных данных и защита информации на предприятии. Некоторые спорные вопросы применения // Проблемы права. - Челябинск, 2010, № 1. - С. 114-121

10. Волчихин, В.И. Нейросетевая защита персональных биометрических данных / В.И. Волчихин. - М.: Радиотехника, 2018. - 288 с.

11. Гаврюшина Н.И. Проблемы правовой защиты персональных данных // Актуальные вопросы современного российского права: межвузовский сборник научных статей. - Пенза: Изд-во ПГУ, 2010, Вып. 1. - С. 158-161

12. Емельянова, Н. З. Защита информации в персональном компьютере / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. - 368 с.

13. Журавлев М.С. Персональные данные в трудовых отношениях: допустимые пределы вмешательства в частную жизнь работника // Информационное право. 2013. № 4. С. 35-38.

14. Мазина Г.П. Персональные данные и их защита в трудовых и служебных правоотношениях // Общественная безопасность, законность и правопорядок в III тысячелетии. 2015. № 1-2. С. 180-185.

15. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости. Москва, 2009.

16. Партыка, Н. З. Емельянова. Т. Л. Партыка Защита информации в персональном компьютере. Учебное пособие / Н. З. Емельянова. Т. Л. Партыка Партыка, И.И. Попов. - М.: Форум, Инфра-М, 2018. - 368 с.

17. Пирогов, В. Ю. Информационные системы и базы данных. Организация и проектирование / В.Ю. Пирогов. - М.: БХВ-Петербург, 2016. - 528 с.

18. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

19. Проскурин, В. Г. Защита программ и данных / В.Г. Проскурин. - М.: Academia, 2018. - 208 с.

20. Филиппов, П. Б. Использование и защита персональных данных в социальных сетях Интернета / П.Б. Филиппов. - М.: Синергия, 2018. - 133 с.

21. Э. Мэйволд - Безопасность сетей [Электронный ресурс] - Режим доступа: <http://www.intuit.ru/department/security/netsec/11/1.html>.

22. Эндрю, Кин Ничего личного. Как социальные сети, поисковые системы и спецслужбы используют наши персональные данные / Кин Эндрю. - М.: Альпина Паблишер, 2016. - 854 с.