**СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ «ОТДЕЛ КАДРОВ ОРГАНИЗАЦИИ»****MEANS OF INFORMATION SECURITY PROTECTION OF THE AUTOMATED
SYSTEM "PERSONNEL DEPARTMENT OF THE ORGANIZATION"****ЧЕКУЛАЕВА Е.Н.,
ГУЩИНА Е.В.****CHEKULAEVA E.N.,
GUSHCHINA E.V..***Поволжский государственный
технологический университет**Volga state University of technology**en_281287@mail.ru**doi: 10.18411/pivsn-03-2019-05**idsp: sciencepub-pivsn-03-2019-05***АННОТАЦИЯ**

В статье рассматривается краткая характеристика и анализ обеспечения защиты автоматизированной системы. Отражено программное обеспечение автоматизированной системы «Отдел кадров организации», а также выбраны основные средства защиты автоматизированной системы «Отдел кадров организации».

КЛЮЧЕВЫЕ СЛОВА: автоматизированное рабочее место, информационная безопасность, несанкционированный доступ, антивирусная защита, средства защиты автоматизированной системы.

ABSTRACT

The article deals with a brief description and analysis of the protection of the automated system. The software of the automated system "personnel Department of the organization" is reflected, and also the main means of protection of the automated system "personnel Department of the organization" are chosen.

KEY WORDS: automated workplace, information security, unauthorized access, anti-virus protection, means of protection of the automated system.

ВВЕДЕНИЕ

Каждое автоматизированное рабочее место (АРМ) предназначено для работы в многопользовательском режиме, доступ исполнителей к работе осуществляется в соответствии с установленной разграничительной системой доступа, пользователи имеют равные права доступа к информации. Пользователи имеют право постоянного хранения файлов с защищаемыми данными на жестких магнитных дисках, входящих в состав ПЭВМ, в специально выделенных администратором каталогах. Для хранения файлов с конфиденциальными данными могут также использоваться учтенные установленным порядком машинные носители информации. Доступ к информационным ресурсам АРМ осуществляется по паролю конкретного пользователя, с регистрацией в Журнале приема-передачи ПЭВМ и учета времени решения задач, при этом пользователь получает установленные системным администратором права доступа к устройствам, каталогам и файлам, и программам ПЭВМ.

ЦЕЛЬ ИССЛЕДОВАНИЯ

В работе поставлена цель обработать и определить средства защиты безопасности информации для автоматизированной системы «Отдел кадров организации». На основании поставленной цели, выделим следующие задачи:

1. Изучить краткую характеристику и анализ обеспечения защиты автоматизированной системы.
2. Рассмотреть программное обеспечение автоматизированной системы «Отдел кадров организации».
3. Определить основные средства защиты автоматизированной системы «Отдел кадров организации».

Совместное использование пользователями данной автоматизированной системы позволит руководителю организации и отделу кадров активно изучить основные средства защиты, а также определить программное обеспечение и безопасность информации о персональных данных сотрудников.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

В работе отдела кадров можно выделить следующие важные составляющие: заключение трудового договора с сотрудниками, ведение личной карточки (включает в себя персональные данные сотрудников: паспортные данные, ИНН, адрес проживания, телефоны), составление штатного расписания, графика отпусков, создание различных приказов. Проблема автоматизации кадрового делопроизводства является актуальной, поэтому существует большое количество программного обеспечения для работы отдела кадров. Эти программы можно разделить на несколько групп:

1. свободно распространяемые программы, написанные непрофессионалами («WDATEOK», «Кадры», «Отдел кадров и ДОУ», «Табель»);
2. программы, которые разрабатываются собственными программистами для своей организации («SLS-Кадры», «STAFF-Кадры», «Triamant» и др);
3. бухгалтерские системы, в состав которых включен функциональный модуль «Кадры» («1С Зарплата и кадры», «Platinum», «Ultima-S», «Scala», «Галактика», «БОСС-Кадровик» и др);
4. комплексные системы автоматизации деятельности предприятия, основанные на использовании системы баз данных, охватывающих все сферы деятельности предприятия («Orakl-Кадры» и «NS2000»).

Документы хранятся на сервере и компьютерах специалистов по работе с кадрами. Вся информация считается общедоступной, кроме персональных данных, которые считаются конфиденциальными и требуют защиты. Для эффективного выполнения своих функций кадровой службе необходимо постоянно и тесно взаимодействовать с другими отделами предприятия: взаимодействие с бухгалтерией организации, с юридическим отделом и со всеми структурными подразделениями компании.

В целях безопасности информации от несанкционированного доступа на АРМ установлена программно-аппаратная система защиты информации от НСД «Панцирь-К». Настройку системы защиты от НСД для конкретных пользователей и контроль ее работы осуществляет системный администратор.

Функции, права и обязанности Администратора и пользователей на АРМ регламентируются в соответствии с «Инструкцией по защите конфиденциальной информации при обработке с помощью СВТ», «Инструкциями пользователей АРМ» и «Инструкцией системного администратора».

На ПЭВМ, входящей в состав АРМ, установлена операционная система Windows 7. Копия операционной системы, системы защиты информации от НСД «Панцирь-К» хранятся у Администратора. Для разработки документов пользователей на АРМ установлен программный пакет Microsoft Office 2016.

Права доступа пользователей к программам, каталогам и файлам на АРМ определены в документации по разрешительной системе доступа персонала к защищаемым ресурсам АРМ и реализованы на АРМ средствами системы защиты от НСД «Панцирь-К». Антивирусная защита осуществляется пользователями АРМ с применением

программного средства "Dr. Web" в соответствии с Инструкцией по проведению антивирусного контроля.

ИС «Отдел кадров организации», обработка информации с использованием средств автоматизации.

Упрощенная схема отдела кадров приведена на рисунке 1.

Рисунок 1. Схема ОК

Угрозы несанкционированного доступа к АРМам сотрудников может быть реализованы посредством следующих уязвимостей:

- Отсутствие пломбирования корпуса АРМ;
- Отсутствие регламента доступа к АРМ;
- Отсутствие средств защиты от НСД.

Для осуществления технологического процесса обработки информации на используется следующее программное обеспечение (ПО) (таблица 1):

Таблица 1

Программное обеспечение

№ п/п	Название ПО	Назначение	Место установки (папка на ЖМД)
1	Microsoft Windows 7 Home Edition	Операционная система	C:\Windows
2	Панцирь-К	Средство защиты информации от НСД	C:\Program Files\Панцирь
3	Microsoft Office 2016	Пакет офисных программ	C:\Program Files\Microsoft office
4	Антивирус Dr. Web 11.5	Программа антивирусного контроля	C:\Program Files\DrWeb
5	Adobe Acrobat Reader DC 2019	Программа просмотра pdf-файлов	C:\Program Files\Adobe\Acrobat Reader DC
6	Принтер HP LaserJet Pro 400	Драйвер принтера	C:\Windows
7	VipNet Coordinator HW1000	Шлюз безопасности	-

В состав системы защиты ИСПДн «Отдел кадров» входят следующие СЗИ:

1. Dr. Web 11.5;

Dr.Web – комплексная защита от всех видов интернет-угроз. Антивирус, фаервол, антиспам, веб-антивирус SpIDer Gate, защита данных и информации.

2. VipNet Coordinator HW 1000;

ViPNet Coordinator HW1000 - шлюз безопасности (решение в сфере компьютерной безопасности, обеспечивающее мощную комплексную защиту от сетевых угроз. Эта технология появилась как реакция на новые изощренные атаки, с которыми привычные файерволы уже не справлялись.

3. Панцирь-К;

Система предназначена для защиты информации, обрабатываемой на компьютерах в составе корпоративной сети. КСЗИ служит для эффективного противодействия, как известным, так и потенциально возможным атакам на защищаемые ресурсы, что обеспечивается устранением архитектурных недостатков защиты современных ОС.

Основные механизмы защиты КСЗИ реализованы в виде системных драйверов. Все возможности защиты, предоставляемые КСЗИ, реализованы собственными средствами (не использованы встроенные механизмы ОС).

ЗАКЛЮЧЕНИЯ

В ходе обработки и определения средств защиты безопасности информации для автоматизированной системы «Отдел кадров организации». Можно сделать следующие выводы:

1. Документы хранятся на сервере и компьютерах специалистов по работе с кадрами. Вся информация считается общедоступной, кроме персональных данных, которые считаются конфиденциальными и требуют защиты. Для эффективного выполнения своих функций кадровой службе необходимо постоянно и тесно взаимодействовать с другими отделами предприятия.

2. В целях безопасности информации от несанкционированного доступа на АРМ установлена программно-аппаратная система защиты информации от НСД «Панцирь-К». Настройку системы защиты от НСД для конкретных пользователей и контроль ее работы осуществляет системный администратор.

В результате был проведен анализ, позволяющий совместное использование пользователями данной автоматизированной системы руководителем организации и отделом кадров активно изучать основные средства защиты, а также определять программное обеспечение и безопасность информации о персональных данных сотрудников.

1. Источник номер 1 Грушо А.А. Теоретические основы компьютерной безопасности [Текст]: [учеб. пособие для вузов по специальностям группы 090100 "Информ. безопасность"] / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. - М.: Академия, 2009. – 267 с.
2. Источник номер 2 Бизнес-планирование [Текст]: [учеб. пособие для студентов вузов по направлениям "Экономика" и "Менеджмент"] / [В. З. Черняк и др.]; под ред. В. З. Черняка. - 4-е изд., перераб. и доп. - М.: ЮНИТИ, 2012. – 590 с.
3. Источник номер 3 Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности [Текст]: [учеб. пособие для студентов вузов по направлениям] / Ю.А. Родичев. – Питер, 2017. – 256 с.