КОМИТЕТ ОБРАЗОВАНИЯ И НАУКИ КУРСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«ЖЕЛЕЗНОГОРСКИЙ ГОРНО-МЕТАЛЛУРГИЧЕСКИЙ КОЛЛЕДЖ»

УТВЕРЖДАЮ

Директор ОБПОУ «ЖГМК»

_____ А.Н. Шебанов

«___» _____ 2016 г.

ПРОГРАММА

Программа по созданию безопасной информационной среды в областном бюджетном профессиональном образовательном учреждении «Железногорский горно-металлургический колледж» на 2016 – 2020 годы

Железногорск 2016

Паспорт
Программа по созданию безопасной информационной среды в областном бюджетном профессиональном образовательном учреждении «Железногорский горно-металлургический колледж» на 2016 – 2020 годы

Наименование программы	Программа по созданию безопасной информационной среды в областном бюджетном профессиональном образовательном учреждении «Железногорский горно-металлургический колледж» на 2016 – 2020 годы (далее - Программа)
Основание для разработки Программы	Приложение 1
Государственный заказчик Программы	Комитет образования и науки Курской области
Основные разработчики Программы	ОБПОУ «Железногорский горно-металлургический колледж»
Актуальность проблемы	В настоящее время активно осуществляется переход от образования в условиях ограниченного доступа к информации к образованию в условиях неограниченного доступа к информации. Современное состояние информационного пространства с использованием ИКТ таково, что оно определяется как источник трансформации воздействия информационной среды в угрозы информационной безопасности обучающихся и информации ограниченного доступа, создаваемой и используемой в профессиональной образовательной организации (ПОО). Таким образом, актуальными становятся вопросы, связанные с обеспечением безопасности информационной среды ПОО.
Основная цель Программы	Разработка мероприятий по обеспечению безопасности информационной среды образовательной организации
Основные задачи Программы	– проанализировать актуальные возможные угрозы информационной безопасности ПОО, вытекающие из направлений деятельности; – повысить эффективность мер направленных на защиту информации ограниченного доступа, циркулирующей в образовательной организации с учетом последних изменений нормативно-правовых актов РФ;

	– проанализировать эффективность используемых мер защиты обучающихся от нежелательной и запрещенной информации, распространяющейся в сети Интернет; – проанализировать мероприятия по информированию, популяризации знаний и умений в области ИБ среди участников образовательного процесса; – простимулировать развитие инновационной деятельности педагогических работников в области информационной безопасности.
Индикаторы и показатели Программы	– коэффициент нейтрализации угроз информационной безопасности; – соответствие официального сайта образовательной организации требованиям нормативно-правовых актов; – наличие мер защиты от нежелательной и запрещенной информации в образовательной организации; – информированность лиц, отвечающих за здоровье и развитие студентов, об имеющихся возможностях защиты от информации, причиняющей вред здоровью и развитию обучающихся; – повышение уровня квалификации преподавателей и сотрудников колледжа в области ИБ; – участие студентов в конференциях и конкурсах по вопросам ИБ; – динамика результатов анкетирования среди участников образовательного процесса по вопросам информационной безопасности.
Сроки и этапы реализации Программы	допрограммный этап - 2009- 2016 годы этап реализации - 2016 - 2020 годы
Источники финансирования Программы	Бюджет образовательной организации
Ожидаемые конечные результаты Программы и показатели эффективности реализации Программы	– повышение коэффициента нейтрализации угроз информационной безопасности колледжа; – полное соответствие официального сайта образовательной организации требованиям нормативно-правовых актов; – наличие мер защиты от нежелательной и запрещенной информации в образовательной организации; – 100% охват студентов занятиями по

	информационной безопасности; – повышение минимум до 85% информированности лиц, отвечающих за здоровье и развитие студентов об имеющихся возможностях защиты от информации, причиняющей вред здоровью и развитию; – полный охват преподавателей и сотрудников колледжа мероприятиями, направленными на повышение специальных знаний в области ИБ; – наличие сертификатов и грамот, подтверждающих участие студентов и преподавателей в конференциях и конкурсах по вопросам ИБ; – положительная динамика результатов анкетирования среди участников образовательного процесса по вопросам информационной безопасности.

I. ОБЩИЕ СВЕДЕНИЯ ОБ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Областное бюджетное профессиональное образовательное учреждение «Железногорский горно-металлургический колледж» в настоящее время ведет подготовку по основным профессиональным образовательным программам среднего профессионального образования - программам подготовки квалифицированных рабочих, служащих – 3 профессии, программам подготовки специалистов среднего звена – 14 специальностей по очной, очно-заочной и заочной формам обучения, ведет переподготовку и повышение квалификации специалистов и рабочих кадров для предприятий города и региона о 92 программам дополнительного профессионального образования.

Лицензия Серия 46Л01 №0000306, регистрационный номер №1784 от 15 ноября 2013 г., выданные комитетом образования и науки Курской области.

Свидетельство о государственной аккредитации Серия 46А01 № 0000199 г., регистрационный номер № 1277 от 28.02.2014.

Общественной составляющей управления колледжа является Совет колледжа, а также Попечительский совет, в который входят представители работодателей, профессионального сообщества и общественных организаций города.

Колледж действует на основе Устава.

Колледж является одним из крупнейших образовательных учреждений среднего профессионального образования Курской области, контингент которого составляет – около 1300 студентов и 1500 слушателей ежегодно.

В настоящее время колледж ведет подготовку по следующим профессиям и специальностям

Таблица 1 - Код и наименование специальностей

Наименование профессий и специальностей	Код
Мастер отделочных строительных работ	08.01.08
Сварщик (электросварочные и газосварочные работы)	15.01.05
Машинист крана (крановщик)	23.01.07
Строительство и эксплуатация зданий и сооружений	08.02.01
Компьютерные системы и комплексы	09.02.01
Программирование в компьютерных системах	09.02.03
Информационная безопасность автоматизированных систем	10.02.03
Техническая эксплуатация и обслуживание электрического и электромеханического оборудования (по отраслям)	13.02.11
Технология машиностроения	15.02.08
Обогащение полезных ископаемых	21.02.18
Металлургия черных металлов	22.02.01
Организация перевозок и управление на транспорте	23.02.01
Техническое обслуживание и ремонт автомобильного транспорта	23.02.03
Техническая эксплуатация подвижного состава железных дорог	23.02.06
Экономика и бухгалтерский учет (по отраслям)	38.02.01
Операционная деятельность в логистике	38.02.03
Правоохранительная деятельность	40.02.02

В колледже ведётся подготовка по десяти укрепленным группам

специальностей направлений подготовки. Реализуются основные профессиональные образовательные программы среднего профессионального образования: программы подготовки квалифицированных рабочих, служащих – 3, программы подготовки специалистов среднего звена - 14.

В колледже для проведения занятий имеется 39 кабинетов и 14 лабораторий, ресурсный центр на базе ПАО «Михайловский ГОК», учебно-производственные мастерские, три спортивных зала, актовый зал и библиотека. В колледже имеется центр информационных технологий, объединяющий в своем составе 10 компьютерных классов.

На территории колледжа частично огороженной забором расположены следующие здания:

- девятиэтажное общежитие с пристроенным одноэтажным центром информационных технологий;
- двухэтажное здание столовой;
- основной корпус, пятиэтажное кирпичное здание имеющее технический подвал с пристроенными одноэтажным зданием мастерских и двухэтажным спортзалом с актовым залом, в подвале организованы помещения с тренажерами;
- дополнительный корпус состоящий из двух и четырех этажных зданий соединенных переходом;
- двухэтажное здание мастерских.

Все корпуса расположены на значительном расстоянии от дорог. На территории организована система наружного видеонаблюдения.

В основном корпусе производится обработка конфиденциальной информации. Окна здания выходят на дорогу и во внутреннее пространство территории. Основной вход расположен на втором этаже здания со стороны дороги и попасть к нему можно только через переходной мостик. Запасные входы закрыты, ключи находятся на вахте и выдаются только допущенным лицам под запись. На входе в здание установлена автоматизированная система управления доступом, а также организовано рабочее место вахтера и охраны. На входе и в коридорах установлены камеры видеонаблюдения сведенные на пост охраны (Приложение 5).

Учебно-воспитательный процесс в колледже направлен на подготовку высококвалифицированных специалистов для развития экономики города Железногорска и Железногорского района Курской области, а также горно-металлургической отрасли, на воспитание активной гражданской позиции.

II. АКТУАЛИЗАЦИЯ УГРОЗ

Несмотря на все реализованные защитные меры одними только техническими и программными средствами нельзя ограничить доступ несовершеннолетних к нежелательной информации. Пока студенты мотивированы искать интересную, но одновременно и опасную для них информацию, они будут пытаться найти и находить всё новые способы обхода блокировок и контентной фильтрации. Поэтому первостепенной задачей обеспечения безопасности информационной среды является повышение информированности о последствиях неосмысленного и необдуманного

использования ресурсов сети Интернет. Причем повышение информированности распространяется на всех участников образовательного процесса (студенты, педагоги, родители, сотрудники).

Угроза	**Угроза доступа к нежелательной и запрещенной информации**			
Описание угрозы	Угроза заключается в возможности посещения несовершеннолетними сайтов, содержащих информацию, приносящую вред их здоровью и развитию			
Нарушитель	Нарушаемые свойства	Объект воздействия		Актив
Внутренний нарушитель с низким потенциалом	Нравственное, физическое, психологическое и социальное здоровье детей и молодежи	Дети и молодежь		Нравственное, физическое, психологическое и социальное здоровье детей и молодежи
Исходная степень защищенности (Y1)	Вероятность реализации угрозы (Y2)	Опасность угрозы	Возможность реализации угрозы (Y)	Актуальность угрозы
Средняя (5)	Средняя (5)	Высокая	Средняя (0,5)	**Актуальная**
Возможные предпосылки				
– наличие в сети Интернет информации, угрожающей здоровью и развитию детей; – возможность доступа в сеть Интернет				
Принятые меры			Эффективность мер	
– программные и аппаратные средства контентной фильтрации; – мероприятия по повышению информированности в области информационной безопасности			Недостаточная в виду наличия человеческого фактора	
Выводы				
В виду наличия предпосылок к реализации угрозы, а также недостаточности реализованных защитных мер, вероятность реализации угрозы считается средней В связи с возможностью значительных негативных последствий в случае реализации угрозы, опасность угрозы считается высокой Исходя из полученных показателей, угроза считается **актуальной**				

Угроза	**УБИ.004: Угроза аппаратного сброса пароля BIOS**			
Описание угрозы	Угроза заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»).			
Нарушитель	Нарушаемые свойства	Объект воздействия		Актив
Внутренний нарушитель с низким потенциалом	Целостность	Микропрограммное и аппаратное обеспечение BIOS/UEFI		ПДн, хранящиеся на сервере
Исходная степень	Вероятность реализации	Опасность угрозы	Возможность реализации угрозы	Актуальность угрозы

защищенности (Y1)	угрозы (Y2)		(Y)	
Средняя (5)	Низкая (2)	Низкая	Средняя (0,35)	неактуальная
Возможные предпосылки				
– наличие механизмов аппаратного сброса паролей, установленных в BIOS – наличие у нарушителя физического доступа к системному блоку компьютера				
Принятые меры			Эффективность мер	
– Комплекс инженерно-технических мер по ограничению физического доступа в помещение серверной			Достаточная	
Выводы				
В свете наличия предпосылок к реализации угрозы, а также достаточности реализованных защитных мер, вероятность реализации угрозы считается низкой В связи с возможностью незначительных негативных последствий в случае реализации угрозы, опасность угрозы считается низкой Исходя из полученных показателей, угроза считается неактуальной				

Угроза	**УБИ.006: Угроза внедрения кода или данных**			
Описание угрозы	Угроза заключается в возможности внедрения нарушителем в дискредитируемую информационную систему вредоносного кода, который может быть в дальнейшем запущен «вручную» пользователями или автоматически при выполнении определённого условия (наступления определённой даты, входа пользователя в систему и т.п.), а также в возможности несанкционированного внедрения нарушителем некоторых собственных данных для обработки в дискредитируемую информационную систему, фактически осуществив незаконное использование чужих вычислительных ресурсов.			
Нарушитель	Нарушаемые свойства		Объект воздействия	Актив
Внешний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность		Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	ПДн
Исходная степень защищенности (Y1)	Вероятность реализации угрозы (Y2)	Опасность угрозы	Возможность реализации угрозы (Y)	Актуальность угрозы
Средняя (5)	Средняя (5)	Средняя	Средняя (0,5)	актуальная
Возможные предпосылки				
– Вероятность наличия уязвимостей программного обеспечения – Возможная слабость мер антивирусной защиты – Работа с файлами, поступающими из недоверенных источников – наличие у пользователя привилегий установки программного обеспечения				
Принятые меры			Эффективность мер	
– комплекс средств антивирусной защиты – программные средства ограничения доступа к недоверенным ресурсам сети – ограничение привилегий пользователей – использование лицензированного ПО			Недостаточная, в виду наличия «человеческого фактора»	
Выводы				
В свете наличия предпосылок к реализации угрозы, а также недостаточности реализованных				

защитных мер, вероятность реализации угрозы считается средней В связи с возможностью негативных последствий в случае реализации угрозы, опасность угрозы считается средней Исходя из полученных показателей, угроза считается актуальной

Угроза	**УБИ.018: Угроза загрузки нештатной операционной системы**			
Описание угрозы	Угроза заключается в возможности подмены нарушителем загружаемой операционной системы путём несанкционированного переконфигурирования в BIOS/UEFI пути доступа к загрузчику операционной системы.			
Нарушитель	Нарушаемые свойства		Объект воздействия	Актив
Внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность		Микропрограммное обеспечение BIOS/UEFI	ПДн
Исходная степень защищенности (Y1)	Вероятность реализации угрозы (Y2)	Опасность угрозы	Возможность реализации угрозы (Y)	Актуальность угрозы
Средняя (5)	Низкая (2)	Низкая	Средняя (0,35)	неактуальная
Возможные предпосылки				
– слабость технологий разграничения доступа к управлению BIOS – доступность нарушителю указания источника загрузки операционной системы				
Принятые меры			Эффективность мер	
– дополнительные средства защиты BIOS			Достаточная	
Выводы				
В свете наличия предпосылок к реализации угрозы, а также достаточности реализованных защитных мер, вероятность реализации угрозы считается низкой В связи с возможностью незначительных негативных последствий в случае реализации угрозы, опасность угрозы считается низкой Исходя из полученных показателей, угроза считается неактуальной				

Угроза	**УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией**			
Описание угрозы	Угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих или заданных ему другими лицами (организациями) деструктивных целей.			
Нарушитель	Нарушаемые свойства		Объект воздействия	Актив
Внутренний нарушитель с низким потенциалом	Конфиденциальность		Аппаратное обеспечение, носители информации, объекты файловой системы	ПДн
Исходная степень защищенности (Y1)	Вероятность реализации угрозы (Y2)	Опасность угрозы	Возможность реализации угрозы (Y)	Актуальность угрозы
Средняя (5)	Средняя (5)	Средняя	Средняя (0,5)	актуальная
Возможные предпосылки				

– наличие возможности просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путём подслушивания разговоров и др. – уязвимости средств контроля доступа, ошибки в параметрах конфигурации данных средств или отсутствие указанных средств.

Принятые меры	Эффективность мер
– применение средств контроля доступа – организационные меры	Недостаточная, в виду наличия «человеческого фактора»

Выводы
В свете наличия предпосылок к реализации угрозы, а также недостаточности реализованных защитных мер, вероятность реализации угрозы считается средней В связи с возможностью негативных последствий в случае реализации угрозы, опасность угрозы считается средней Исходя из полученных показателей, угроза считается актуальной

Угроза	**УБИ.088: Угроза несанкционированного копирования защищаемой информации**			
Описание угрозы	Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы).			
Нарушитель	Нарушаемые свойства	Объект воздействия	Актив	
Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Конфиденциальность	Объекты файловой системы, машинный носитель информации	ПДн	
Исходная степень защищенности (Y1)	Вероятность реализации угрозы (Y2)	Опасность угрозы	Возможность реализации угрозы (Y)	Актуальность угрозы
Средняя (5)	Средняя (5)	Средняя	Средняя (0,5)	актуальная

Возможные предпосылки
– наличие возможности доступа к защищаемой информации – возможность использования съемных носителей информации – хранение и передача информации в незашифрованном виде

Принятые меры	Эффективность мер
– отключение возможности использования съемных носителей на программном и аппаратном уровне – организационные меры по ограничению доступа к защищаемой информации – применение криптографических средств защиты информации	Недостаточная, в виду наличия «человеческого фактора»

Выводы
В свете наличия предпосылок к реализации угрозы, а также недостаточности реализованных

защитных мер, вероятность реализации угрозы считается средней В связи с возможностью негативных последствий в случае реализации угрозы, опасность угрозы считается средней Исходя из полученных показателей, угроза считается актуальной

Угроза	**УБИ.140: Угроза приведения системы в состояние «отказ в обслуживании»**			
Описание угрозы	Угроза заключается в возможности отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой.			
Нарушитель	Нарушаемые свойства	Объект воздействия	Актив	
Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Доступность	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	Сетевые ресурсы	
Исходная степень защищенности (Y1)	Вероятность реализации угрозы (Y2)	Опасность угрозы	Возможность реализации угрозы (Y)	Актуальность угрозы
Средняя (5)	Высокая (10)	Средняя	высокая (0,75)	актуальная
Возможные предпосылки				
– возможность превышения объёма запросов над объёмами доступных для их обработки ресурсов дискредитируемой системы (таких как способность переносить повышенную нагрузку или приобретать дополнительные ресурсы для предотвращения их исчерпания) – наличие мотивации к данным действиям у потенциального нарушителя				
Принятые меры	Эффективность мер			
–				
Выводы				
В свете наличия предпосылок к реализации угрозы, а также отсутствия реализованных защитных мер, вероятность реализации угрозы считается высокой В связи с возможностью негативных последствий в случае реализации угрозы, опасность угрозы считается средней Исходя из полученных показателей, угроза считается актуальной				

Угроза	**УБИ.175: Угроза «фишинга»**
Описание угрозы	Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации/аутентификации) пользователя путём убеждения его с помощью методов социальной инженерии (в т.ч. посылкой целевых писем (т.н. spear-phishing attack), с помощью звонков с вопросом об открытии вложения письма, имитацией рекламных предложений (fake offers) или различных приложений (fake apps)) зайти на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию или открыть заражённое вложение в письме.

Нарушитель	Нарушаемые свойства	Объект воздействия	Актив
Внешний нарушитель с низким потенциалом	Конфиденциальность	Рабочая станция, сетевое программное обеспечение, сетевой трафик	

Исходная степень защищенности (Y1)	Вероятность реализации угрозы (Y2)	Опасность угрозы	Возможность реализации угрозы (Y)	Актуальность угрозы
Средняя (5)	Высокая (10)	Средняя	Высокая 0,75	Актуальная

Возможные предпосылки
– недостаточность знаний пользователей о методах и средствах «фишинга» – наличие у нарушителя сведений о конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; – наличие у нарушителя средств создания и запуска поддельного сайта – наличие у нарушителя сведений о контактах пользователя с доверенной организацией (номер телефона, адрес электронной почты и др.)

Принятые меры	Эффективность мер
–	

Выводы
В свете наличия предпосылок к реализации угрозы, а также отсутствии реализованных защитных мер, вероятность реализации угрозы считается высокой В связи с возможностью негативных последствий в случае реализации угрозы, опасность угрозы считается средней Исходя из полученных показателей, угроза считается актуальной

Угроза	**УБИ.186: Угроза внедрения вредоносного кода через рекламу, сервисы и контент**
Описание угрозы	Угроза заключается в возможности внедрения нарушителем в информационную систему вредоносного кода посредством рекламы, сервисов и (или) контента (т.е. убеждения пользователя системы активировать ссылку, код и др.) при посещении пользователем системы сайтов в сети Интернет или установкой программ с функцией показа рекламы.

Нарушитель	Нарушаемые свойства	Объект воздействия	Актив
Внутренний нарушитель с низким потенциалом	Целостность Доступность	Сетевое программное обеспечение	

Исходная степень защищенности (Y1)	Вероятность реализации угрозы (Y2)	Опасность угрозы	Возможность реализации угрозы (Y)	Актуальность угрозы
Средняя (5)	Средняя (5)	Средняя	Средняя (0,5)	актуальная

Возможные предпосылки
– слабость механизмов фильтрации сетевого трафика – слабость антивирусного контроля на уровне организации – возможность посещения пользователями с рабочих мест сайтов в сети Интернет

Принятые меры	Эффективность мер
– применение комплекса антивирусных	Недостаточная, в виду наличия «человеческого фактора»

средств и их своевременное обновление – применение программно-аппаратных средств фильтрации сетевого трафика – ограничение доступа к сети интернет отдельным группам пользователей	
Выводы	
В свете наличия предпосылок к реализации угрозы, а также недостаточности реализованных защитных мер, вероятность реализации угрозы считается средней В связи с возможностью негативных последствий в случае реализации угрозы, опасность угрозы считается средней Исходя из полученных показателей, угроза считается актуальной	

III. ОБЕСПЕЧЕНИЕ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ОТ НЕПРАВОМЕРНЫХ ДЕЙСТВИЙ

В колледже организована система контроля и учета документов на бумажных носителях:

1. Учет всей документации колледжа с классификацией по сфере применения, дате, содержанию, требованиям, предъявляемым к конфиденциальности, целостности, доступности.

2. Закрепление индивидуальной ответственности за каждый документ за конкретным сотрудником. Назначение лиц, ответственных за контроль документооборота и конфиденциального делопроизводства.

3. Регистрация и учет всех входящих/исходящих документов колледжа с фиксацией в специальном журнале информации о дате получения/отправления документа, откуда поступил, или куда отправлен, классификация документа (письмо, счет, договор, приглашение и т.п.).

4. Организация архива документов. Систематизация неиспользуемых документов в целях облегчения их нахождения в случае необходимости. А также меры защиты архива от уничтожения или повреждения в результате чрезвычайных происшествий или злонамеренных действий. Кроме того ограничение и контроль доступа к документации колледжа хранящейся в архиве.

5. Регистрация документов, с которых делаются копии с фиксацией в специальном журнале (дата копирования, количество копий, кем для кого или с какой целью производятся копии и тому подобное).

6. Особый режим уничтожения документов. Перед уничтожением документов контролируется их содержание во избежание случайного уничтожения необходимых документов и определяется их статус. Об уничтожении документов в обязательном порядке составляется акт, который подписывается ответственным лицом, а также лицами, присутствующими при уничтожении.

Для облечения системы контроля все документы разделены на три условные категории по степени конфиденциальности, содержания и уровню доступа:

- документы общего пользования;

- документы для служебного пользования;
- документы, содержащие информацию конфиденциального характера.

В колледже организованы меры по защите информации, обрабатываемой средствами вычислительной техники.

В качестве основных мер защиты информации в колледже применяются:

- документальное оформление перечня сведений конфиденциального характера с учетом специфики этих сведений;
- реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к информации и связанным с ее использованием работам, документам;
- ограничение доступа персонала и посторонних лиц в защищаемые помещения и помещения, где размещены средства информатизации и коммуникации, а также хранятся носители информации.

Для реализации данных мер был разработан комплект инструкций (Приложение 6).

Порядок обеспечения защиты конфиденциальной информации при эксплуатации информационной системы колледжа определён в Положении об обработке и защите персональных данных (Приложение 3).

В колледже документально определен перечень защищаемых помещений (ЗП) и лиц, ответственных за их эксплуатацию в соответствии с установленными требованиями по защите информации. На ЗП составлен технический паспорт, форма которого приведена в качестве примера в Приложении 7.

Защищаемые помещения размещены в пределах контролируемой зоны с учетом следующих рекомендаций:

- удаление ЗП от границ контролируемой зоны;
- ЗП не располагаются на первых этажах зданий;
- используются шторы или жалюзи на окнах.

По решению директора колледжа проводится специальная проверка защищаемого помещения и установленного в нем оборудования с целью выявления закладных устройств.

В коллеже запрещается использование радиотелефонов, оконечных устройств сотовой связи, переносных магнитофонов и других средств аудио и видеозаписи при проведении конфиденциальных мероприятий в ЗП.

В соответствии с организационно-распорядительными документами не допускается работа с документами ограниченного доступа на вычислительной технике не предназначенной для ее обработки о чем доведено до всех сотрудников допущенных к данному виду информации под роспись.

Контроль за исполнением возложен на администраторов сети колледжа.

Аттестация объектов информатизации - это комплекс организационно-технических мероприятий, в результате которых, с помощью специального

документа – «Аттестата соответствия» подтверждается, что объект информатизации соответствует требованиям стандартов и иных нормативно-технических документов по безопасности информации, утвержденных федеральным органом по сертификации и аттестации ФСТЭК РФ.

В колледже ведётся аттестация объектов информатизации (Приложение 7).

К первичным методам защиты информации в колледже относятся:

Физические меры защиты:

- развёртывание системы контроля и разграничения физического доступа к элементам автоматизированной системы (металлические двери, замки в серверной);
- создание службы охраны и физической безопасности;
- организацию механизмов контроля за перемещением сотрудников и посетителей (с использованием систем видеонаблюдения, проксимити-карт и т.д.);

Организационные меры, предусматривающие:

- разработку и внедрение регламентов, должностных инструкций и тому подобных регулирующих документов;
- регламентацию порядка работы с носителями, содержащими конфиденциальную информацию.

Сеть колледжа разбита на несколько подсетей, вход в которые доступен только определенной категории пользователей. На всех компьютерах выполнена парольная аутентификация.

В качестве вторичных методов защиты информации в колледже применяется аудит и протоколирование.

Аудиту подлежат следующие процессы:

- вход в систему (успешный или нет);
- выход из системы;
- обращение к удаленной системе;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т.п.).

При протоколировании события записывается следующая информация:

- дата и время события;
- уникальный идентификатор пользователя – инициатора действия;
- тип события;
- результат действия (успех или неудача);
- источник запроса (например, имя терминала);
- имена затронутых объектов (например, открываемых или удаляемых файлов);
- описание изменений, внесенных в базы данных защиты (например, новая *метка безопасности* объекта).

Таким образом в колледже создана и функционирует система технической защиты информации, которая в дальнейшем подлежит корректировке и модернизации.

IV. ОРГАНИЗАЦИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, в колледже обособляются от иной информации путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных используется отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами колледжа (Приложение 3).

Обработка персональных данных, осуществляемая без использования средств автоматизации, осуществляется таким образом, что в отношении каждой категории персональных данных определено место хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Защита персональных данных включает в себя установление особого режима доступа в те помещения, где хранятся такие данные, направленного на защиту последних от несанкционированных доступа, изменений или распространения.

Доступ в места хранения документов, содержащие персональные данные ограничен (помещение запирается на ключ, оснащено техническими средствами охраны). Сотрудники, обрабатывающие персональные данные ознакомлены с порядком физической защиты носителей ПДн (документов).

В помещениях где хранятся персональные данные (кроме архива) установлены металлические шкафы запирающиеся на ключ. Ключ хранится у ответственного лица назначенного приказом директора колледжа.

Обработка персональных данных, осуществляемая с использованием средств автоматизации, в колледже регламентируется Положением «Об обработке и защите персональных данных» (Приложение 3).

На основе Приказа ФСТЭК России от 18 февраля 2013 г. N 21 в колледже реализован комплекс организационных и технических мер по обеспечению

безопасности персональных данных при их автоматизированной обработке. В числе реализованных мер, прежде всего, антивирусная защита, обеспечивающая всестороннюю защиту информационных систем колледжа от потенциально нежелательного программного обеспечения. Также реализованы меры по идентификации и аутентификации пользователей системы, меры по управлению доступом субъектов доступа к объектам доступа, в том числе, разделение полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационных систем. Реализован защищенный удаленный доступ субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети (сеть интернет). С целью защиты информации, хранящейся и передающейся на отчуждаемых носителях, реализован учет машинных носителей информации, а также управление доступом к машинным носителям информации. Неотъемлемой частью системы защиты информации является система регистрация событий безопасности.

Таким образом в колледже создана и функционирует система защита персональных данных соответствующая требования законодательства, которая в дальнейшем подлежит корректировке и модернизации.

V. ОРГАНИЗАЦИЯ КОНТРОЛЯ ЗА ФУНКЦИОНИРОВАНИЕМ ОФИЦИАЛЬНОГО САЙТА ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ И РАЗМЕЩАЕМОЙ НА НЕМ ИНФОРМАЦИИ

В Железногорском горно-металлургическом колледже функционируют несколько сайтов, призванных обеспечить абитуриентов, студентов и сотрудников колледжа необходимой информацией по различным направлениям деятельности и ресурсами для обеспечения учебно-воспитательного процесса.

Официальный сайт колледжа, расположенный по адресу http://zhgmk.ru, имеет структуру, отвечающую требованиям статьи 29 «Информационная открытость образовательной организации» закона от 29.12.2012 N 273-ФЗ "Об образовании в Российской Федерации".

В соответствии с частью 5 статьи 18 «Обязанности оператора при сборе персональных данных» федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" сайт, привязанный к домену zhgmk.ru, расположен на территории Российской Федерации по адресу: г. Москва, ул. Павловская, д. 27/29 на площадке ЗАО «Хостинговые Телесистемы». О данном факте свидетельствует официальное письмо организации, владеющей оборудованием, на котором размещён сайт (Приложение 2).

Вся информация, содержащая персональные данные сотрудников или студентов, размещена на официальном сайте Железногорского горно-металлургического колледжа на основании письменного согласия на обработку персональных данных, заключённых с каждым лицом (сотрудником или студентом) участвующем в деятельности колледжа. Согласие на обработку персональных данных является частью положения «Об обработке и защите персональных данных», утверждённого приказом директора №239а от 31 августа 2015 года.

К информации содержащей персональные данные, размещённой на сайте, как правило, относятся: копии приказов, грамот и благодарностей, различные

акты и фотографии.

В соответствии с требованиями к структуре официального сайта образовательного учреждения в разделе «Сведения об образовательной организации» -> «Документы» размещены все документы, регламентирующие деятельность колледжа. В том числе в данном разделе размещено положение «Об обработке и защите персональных данных», определяющее политику в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных. Копия положения «Об обработке и защите персональных данных» имеется в Приложении 3.

VI. ЗАЩИТА УЧАЩИХСЯ ОТ НЕЖЕЛАТЕЛЬНОЙ И ЗАПРЕЩЕННОЙ ИНФОРМАЦИИ, РАСПРОСТРАНЯЮЩЕЙСЯ В СЕТИ ИНТЕРНЕТ

В колледже проходят обучение как несовершеннолетние, так и совершеннолетние лица. Для обеспечения безопасности граждан от негативного воздействия запрещённой информации применяются различные меры. К таким мерам относятся:

– контент-фильтрация;

– единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.

В колледже действует система внутренней контент-фильтрации на основе прокси-сервера. База данных с блокируемым содержимым состоит из сотен тысяч записей и обновляется автоматически.

Когда пользователь пытается получить доступ к какому-либо сетевому ресурсу, фильтр сравнивает наименование этого ресурса со списком блокируемых адресов, и в случае совпадения, отображает пользователю страницу-заглушку с указанием запрета доступа к запрашиваемому сайту.

Помимо внутренней системы фильтрации используется общедоступный сервис Яндекс.DNS, также блокирующий доступ к различного рода вредоносной информации.

Во всех учебных лабораториях колледжа отключены устройства чтения съёмных носителей (дисков, USB-накопителей), выгрузка и загрузка данных в сеть колледжа происходит сотрудниками отдела информационных технологий с контролем передаваемой информации.

Также к мерам по защите от нежелательной информации можно отнести использование провайдером «Сигнал сервис», предоставляющим колледжу выход в Интернет, вышеприведённого реестра сайтов, содержащих информацию, распространение которой в Российской Федерации запрещено.

VII. ОЦЕНКА ЭФФЕКТИВНОСТИ И ПРОГНОЗ ОЖИДАЕМЫХ СОЦИАЛЬНО - ЭКОНОМИЧЕСКИХ РЕЗУЛЬТАТОВ ОТ РЕАЛИЗАЦИИ ПРОГРАММЫ

Выполнение Программы позволит обеспечить к концу 2020 года 100% охват учащихся, их родителей, педагогов занятиями по медиабезопасности; увеличение информированности до 85% граждан об имеющихся возможностях защиты детей от информации, причиняющей вред их здоровью и развитию. Для оценки эффективности и результативности решения задач, определенных Програм мой, предлагается система целевых индикаторов и показателей по основным направлениям деятельности в рамках задач Программы, которая приведена в таблице 1

Таблица 1

п/п	**Наименование целевых индикаторов и показателей**	**Ед. изм.**	**2015 г. (базовый)**	**Динамика основных целевых индикаторов и показателей реализации Программы**				
				2016 год	**2017 год**	**2018год**	**2019 год**	**2020 год**
1	Коэффициент нейтрализации угроз информационной безопасности;		0.52	0.54	0.54	0.55	0.62	0.65
	Соответствие официального сайта образовательной организации требованиям нормативно-правовых актов;	да/нет	да	да	да	да	да	да
	Информированность лиц, отвечающих за здоровье и развитие студентов, об имеющихся возможностях защиты от информации, причиняющей вред здоровью и развитию обучающихся;	%	46	75	90	100	100	100
	Повышение уровня квалификации преподавателей и сотрудников колледжа в области ИБ;	%	21	42	63	84	100	100
	Участие студентов в семинарах, конференциях, конкурсах и др.форумах по вопросам ИБ;	кол. чел	23	38	53	68	83	98

	динамика результатов анкетирования среди участников образовательного процесса по вопросам информационной безопасности.	+/–		+	+	+	+	+

VIII. МЕРОПРИЯТИЯ ПРОГРАММЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ НА 2016-2020 ГОДЫ

№ п/п	Наименование мероприятия	Срок исполнения	Ответственные за выполнение мероприятия, участники	Ожидаемые результаты
1. Актуализация перечня возможных угроз информационной безопасности				
1.1	Составление паспорта угроз с указанием параметров вероятности реализации и опасности угрозы.	2016 год	Начальник отдела по развитию ИС и ПО	Поддержание модели угроз в актуальном состоянии. Оптимизация применяемых средств защиты в соответствии с моделью угроз
1.2	Актуализация паспорта угроз ИБ в соответствии с изменениями в законодательстве и/или в структуре информационных систем колледжа	ежегодно		
2. Повышение эффективности мер по защите информации ограниченного доступа.				
2.1	Проверка соответствия применяемых мер защиты предъявляемым требованиям	Ежегодно, до начала учебного года (июль-август)	Начальник отдела по развитию ИС и ПО	Повышение коэффициента нейтрализации актуальных угроз информационной безопасности. Повышение эффективности существующей системы информационной безопасности
2.2	Мероприятия направленные на поиск наиболее эффективных средств обеспечения защиты информации	Ежегодно		
2.3	Поддержка работоспособности системы защиты, в том числе поддержка в актуальном состоянии баз данных антивирусных программ			
3. Техническая защита обучающихся от нежелательной и запрещенной информации, распространяющейся в сети Интернет				
3.1	Поддержание работоспособности систем, исключающих доступ детей к нежелательной информации	Еженедельно	Начальник отдела по развитию ИС и ПО	100% охват рабочих мест студентов эффективными средствами контентной фильтрации
3.2	Мероприятия, направленные на борьбу с обходом блокировок со стороны студентов			
4. Популяризация знаний и умений в области ИБ среди участников образовательного процесса;				
4.1	Организация для классных руководителей	Ежегодно	Зам по ВР	повышение минимум до 85%

	обучающих семинаров по работе со студентами и родителями по вопросам безопасного использования интернет-технологий.			информированности лиц, отвечающих за здоровье и развитие студентов об имеющихся возможностях защиты от информации, причиняющей вред здоровью и развитию;
4.1.1	Подготовка презентации портала Роскомнадзора «Персональные данные. Дети»	Август – сентябрь Ежегодно	Зам по ВР Председатели ПЦК	
4.2	Круглый стол по вопросам запрещенного контента в сети интернет	Ноябрь Ежегодно	Зам по ВР Председатели ПЦК	
4.3 Неделя специальности «Информационная безопасность»				
4.3.1	Панельная дискуссия на тему «Социальные сети: зло или благо?»	Ноябрь-декабрь Ежегодно	Зам директора по ВР ЦК спец. 10.02.03	Вовлечение 100% студентов в мероприятия посвященные защите информации наличие сертификатов и грамот, подтверждающих участие студентов и преподавателей в конференциях и конкурсах по вопросам ИБ;
4.3.2	Чемпионат CTF по криптографии среди студентов		Зам директора по МР ЦК спец. 10.02.03	
4.3.3	Олимпиада профессионального мастерства среди студентов специальности 10.02.03 «Информационная безопасность автоматизированных систем»		Зам директора по МР ЦК спец. 10.02.03	
4.3.4	Конкурс социальной рекламы (плакатов, видеороликов и др.), направленной на популяризацию правил безопасного использования сети интернет		Зам директора по МР ЦК спец. 10.02.03	
4.3.5	Круглый стол с работодателями «10 лет закону 152-ФЗ О персональных данных»		Зам директора по ВД и М ЦК спец. 10.02.03	
4.3.6	Конкурс мнемонических правил для создания стойких и запоминающихся паролей		ЦК спец. 10.02.03	
4.4	Подготовка и распространение памятки «Базовые правила информационной безопасности»	Сентябрь-октябрь ежегодно	Зам директора по ВР ЦК спец. 10.02.03	100% охват студентов занятиями по информационной безопасности;
4.5	Подготовка и распространение буклетов «Безопасный интернет»	Сентябрь-октябрь ежегодно	Зам директора по ВР ЦК спец. 10.02.03	
4.6	Разработка методического пособия для	Сентябрь-октябрь	Зам директора по МР	

	проведения уроков информационной безопасности	ежегодно	ЦК спец. 10.02.03	
4.7	Уроки-семинары для школьников «Безопасный интернет»	Октябрь – апрель ежегодно	Зам директора по МР ЦК спец. 10.02.03	
4.8	Обучающие семинары для сотрудников колледжа по информационной безопасности.	2017-2020 годы	Зам директора по МР ЦК спец. 10.02.03	полный охват преподавателей и сотрудников колледжа мероприятиями, направленными на повышение специальных знаний в области ИБ;
4.9	Семинары для родителей первокурсников «Риски пропаганды в интернете»	Сентябрь, ежегодно	Зам директора по ВР ЦК спец. 10.02.03	повышение минимум до 85% информированности лиц, отвечающих за здоровье и развитие студентов об имеющихся возможностях защиты от информации, причиняющей вред здоровью и развитию;
5. Развитие инновационной деятельности педагогических работников в области информационной безопасности.				
5.1	Организация недели специальности «Информационная безопасность», приуроченной ко Дню информационной безопасности 30 ноября.	Ежегодно	Зам директора по ВР Зам директора по МР ЦК спец. 10.02.03	Вовлечение всего педагогического состава в инновационную деятельность в области информационной безопасности
5.2	Конкурс классных часов на тему «Социальное поведение в интернете» для классных руководителей первых курсов	Сентябрь 2017	Зам директора по ВР ЦК спец. 10.02.03	

IX. УПРАВЛЕНИЕ И КОНТРОЛЬ РЕАЛИЗАЦИИ ПРОГРАММЫ

К должностным лицам, непосредственно отвечающим за защиту информации, относятся: начальник отдела по развитию информационной системы и программного обеспечения, руководители подразделений, ведущих обработку персональных данных, а также администратор безопасности, назначенный соответствующим приказом директора колледжа.

Полномочия данных лиц определены в: трудовых договорах, комплектах инструкций по обеспечению безопасности информационных систем, приказах директора колледжа и иных нормативно-правовых актах.

Для реализации Программы используются два механизма: функциональный и финансовый.

Функциональный механизм реализации Программы включает:

— регулярный сбор достоверной информации по реализации Программы;
— мониторинг хода реализации мероприятий Программы;
— регулярный комплексный анализ выполнения Программы, включая промежуточные этапы;
— привлечение общественности к обсуждению мероприятий Программы, реализации и оценке её результатов;
—информационная открытость реализации Программы.
—системный мониторинг реализации Программы на основе целевых индикаторов и показателей Программы.

Финансовый механизм реализации Программы строится на следующих принципах:

— использование в Программе различных форм долевого участия средств областного бюджета с привлечением средств внебюджетных источников, в т.ч. средств частно - государственного партнерства;
— перераспределение средств между программными мероприятиями в соответствии со степенью их приоритетности;
— ежегодное уточнение объемов и направленности финансирования в разрезе действующей Программы.

Структура управления колледжем представлена в Приложении 4.

Внешний контроль за реализацией Программы осуществляет комитет образования и науки Курской области. Внутренний контроль за исполнением Программы - директор колледжа.

Промежуточные результаты заслушиваются на: заседании Попечительского совета, педагогических советах, советах колледжа, административных совещаниях, научно-методических советах.

По результатам календарного и учебного года составляются итоговые отчеты по направлениям Программы.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1

Основания для разработки Программы по созданию безопасной информационной среды в ОБПОУ «Железногорский горно-металлургический колледж»

1. Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена"

2. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 06.07.2016) "Об информации, информационных технологиях и о защите информации"

3. Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 29.06.2015) "О защите детей от информации, причиняющей вред их здоровью и развитию"

4. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015)

5. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 30.12.2015) "Об электронной подписи" (с изм. и доп., вступ. в силу с 08.07.2016)

6. Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) "О государственной тайне"

7. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

8. Постановление Правительства РФ от 26.10.2012 N 1101 (ред. от 12.10.2015) "О единой автоматизированной информационной системе "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено" (вместе с "Правилами создания, формирования и ведения

единой автоматизированной информационной системы "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "интернет", содержащие информацию, распространение которой в российской федерации запрещено"

9. Постановление Правительства РФ от 21.03.2012 N 211 (ред. от 06.09.2014) "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"

10. Распоряжение Правительства РФ от 02.12.2015 N 2471-р <Об утверждении Концепции информационной безопасности детей>

11. Постановление Совета Министров – Правительства Российской Федерации от 15.09.1993 №912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от утечки по техническим каналам»

12. 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 »

13. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные Решение Коллегии Гостехкомиссии России №7.2/02.03.2001г.

Приложение 2

ЗАО «Хостинговые Телесистемы»
www.hts.ru
Главный офис: 115093, Москва, ул. Павловская, 27/29
Телефон: +7 495 358-93-13
Факс: +7 495 358 93 13
ИНН 7725555186, КПП 772501001

Исх. №22/15 от 07.08.2015

Директору ОБПОУ «ЖГМК»
А.Н. Шебанову

В ответ на обращение №01/715 о размещении сайта Областного бюджетного профессионального образовательного учреждения «Железногорский горно-металлургический колледж» zhgmk.ru сообщаем, что на момент написания данного письма сайт, к которому привязан домен zhgmk.ru, обслуживается оборудованием, размещенном на площадке ЗАО «Хостинговые Телесистемы» и находящимся по адресу: г. Москва, ул. Павловская, д. 27/29 в рамках договора-оферты для абонента №27889.

Генеральный директор
ЗАО «Хостинговые Телесистемы» **Лавренов А.В.**

Приложение 3

КОМИТЕТ ОБРАЗОВАНИЯ И НАУКИ КУРСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ЖЕЛЕЗНОГОРСКИЙ ГОРНО-МЕТАЛЛУРГИЧЕСКИЙ КОЛЛЕДЖ»

РАССМОТРЕНО
на Совете колледжа
18 июня 2014 г., протокол № 12

УТВЕРЖДЕНО
приказом директора
№ 239а от 31 августа 2015 г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих 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 (далее информационные системы).

Порядок получения, обработки, использования, хранения и гарантии конфиденциальности персональных данных физических лиц, необходимых для осуществления деятельности ОБПОУ «ЖГМК» в соответствии с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ «О персональных данных», нормативно-правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора.

2. ЦЕЛЬ И ЗАДАЧИ ПОЛОЖЕНИЯ

2.1. Цель данного Положения - защита персональных данных от несанкционированного доступа.

2.2. Сбор, хранение, использование и распространение информации о частной жизни лица без письменного его согласия не допускаются. Персональные данные относятся к категории конфиденциальной информации.

2.3. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

2.4. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

2.5. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

2.6. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

2.7. Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъектов, действующих на основании статей 14 и 15 Федерального закона и законодательства о персональных данных.

2.8. Настоящее положение утверждается директором ОБПОУ «ЖГМК» и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным работников, учащихся и выпускников.

3. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ.

3.1. Персональные данные – любая информация, необходимая, относящаяся к определенному или определяемому на основании такой информации физическому лицу, определяемая нормативно- правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора, Положением об обработке и защите персональных данных и приказами Федерального государственного образовательного учреждения среднего - профессионального образования «Железногорский горно- металлургический колледж».

3.2. Состав персональных данных работника, учащегося и выпускника:

- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики.

Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

3.3 Оператором персональных данных является ОБПОУ «ЖГМК» (далее Учреждение)

3.4. Субъектом персональных данных является работник, учащийся и выпускник (далее студент)

4. Обязанности Оператора персональных данных

4.1. В целях обеспечения прав и свобод человека и гражданина ОБПОУ «ЖГМК» и его представители при обработке персональных данных работника или студента обязаны соблюдать следующие общие требования:

4.1.1. Обработка персональных данных работника или студента может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам, учащимся и выпускникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников или студентов, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

4.1.2. При определении объема и содержания обрабатываемых персональных данных работника или студента Учреждение должно руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора;

4.1.3. Все персональные данные работника или студента следует получать у него самого. Если персональные данные работника или студента возможно получить только у третьей стороны, то работник или студент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Учреждение должен сообщить работнику или студенту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника или студента дать письменное согласие на их получение;

4.1.4. Учреждение не имеет права получать и обрабатывать персональные данные работника или студента о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений и отношений в сфере образовательных услуг, в соответствии со статьей 24 Конституции Российской Федерации Учреждение вправе получать и обрабатывать данные о частной жизни работника или студента только с его письменного согласия;

4.1.5. Учреждение не имеет права получать и обрабатывать персональные данные работника или студента о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом;

4.1.6. При принятии решений, затрагивающих интересы работника или студента, Учреждение не имеет права основываться на персональных данных работника или студента, полученных исключительно в результате их автоматизированной обработки или электронного получения;

4.1.7. Защита персональных данных работника или студента от неправомерного их использования или утраты должна быть обеспечена Учреждением за счет его средств в порядке, установленном федеральным законом;

4.1.8. Работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

4.1.9. Работники не должны отказываться от своих прав на сохранение и защиту тайны;

5. Обязанности субъекта персональных данных

5.1. Передавать Учреждению или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора;

5.2. Своевременно сообщать Учреждению об изменении своих персональных данных;

6. Права субъекта персональных данных

6.1. Требовать исключения или исправления неверных или неполных персональных данных;

6.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

6.3. Персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

6.4. Определять своих представителей для защиты своих персональных данных;

6.5. На сохранение и защиту своей личной и семейной тайны.

7. Сбор, обработка и хранение персональных данных

7.1. Обработка персональных данных работника или студента – получение, хранение, комбинирование, передача или любое другое использование персональных данных работника или студента.

7.2. Порядок получения персональных данных.

7.2.1. Все персональные данные работника или студента следует получать у него самого. Если персональные данные работника или студента возможно получить только у третьей стороны, то работник или студент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Учреждение должно сообщить работнику или студенту о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника или студента дать письменное согласие на их получение.

7.2.2. Учреждение не имеет права получать и обрабатывать персональные данные работника или студента о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ Учреждение вправе получать и обрабатывать данные о частной жизни работника или студента только с его письменного согласия.

7.2.3. Учреждение не имеет право получать и обрабатывать персональные данные работника или студента о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

7.3. Обработка, передача и хранение персональных данных работника или студента.

К обработке, передаче и хранению персональных данных работника или студента могут иметь доступ сотрудники:

- администрация колледжа;
- бухгалтерии;
- сотрудники отдела кадров;
- кураторы студенческих групп;
- сотрудники компьютерных отделов.

7.4. При передаче персональных данных работника или студента Учреждение должно соблюдать следующие требования:

- не сообщать персональные данные работника или студента третьей стороне без письменного согласия работника или студента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или студента, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные работника или студента в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника или студента, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника или студента, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника или студента, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника или студента, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции, а студентом учебной;

- передавать персональные данные работника или студента представителям работников или студентов в порядке, установленном Трудовым Кодексом, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора, и ограничивать эту информацию только теми персональными данными работника или студента, которые необходимы для выполнения указанными представителями их функций.

7.5. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

7.6. При передаче персональных данных работника или студента потребителям (в том числе и в коммерческих целях) за пределы ОБПОУ «ЖГМК». Учреждение не должно сообщать эти данные третьей стороне без письменного согласия работника или студента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или студента или в случаях, установленных федеральным законом.

7.7. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

7.8. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

7.9. По возможности персональные данные обезличиваются.

8. Доступ к персональным данным

8.1. Внутренний доступ (доступ внутри организации).

Право доступа к персональным данным сотрудника или студента имеют:

- директор ОБПОУ «ЖГМК»;

- руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения);

- при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового подразделения;

- кураторы студенческих групп (доступ к личным данным только студентов своей группы);

- сам работник или студент, носитель данных.

Другие сотрудники организации имеют доступ к персональным данным работника или студента только с письменного согласия самого работника или студента, носителя данных.

8.2. Внешний доступ.

8.2.1. К числу массовых потребителей персональных данных вне Учреждения можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления;

8.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

8.2.3. Организации, в которые сотрудник или студент может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника или студента только в случае его письменного разрешения.

8.2.4. Другие организации.

Сведения о работающем сотруднике, обучающемся студенте или уже уволенном (отчисленном) могут быть предоставлены другой организации только с письменного запроса на бланке Учреждения, с приложением копии нотариально заверенного заявления работника или студента.

8.2.5. Родственники и члены семей.

Персональные данные работника или студента могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника или студента.

В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия. (УК РФ).

9. Защита персональных данных

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном

счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Учреждения.

9.1. «Внутренняя защита».

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами Учреждения. Для защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится серверное оборудование и системы хранения данных;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только директору колледжа и в исключительных случаях, по письменному разрешению директора, руководителю структурного подразделения.

9.1.1. Защита персональных данных сотрудника или студента на электронных носителях. При обработке персональных данных в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

9.2. «Внешняя защита».

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности компании, посетители, работники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

9.2.1. Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим компании;
- учет и порядок выдачи удостоверений;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

9.2.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника или студента, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

9.2.3. Все лица, связанные с получением, обработкой и защитой персональных данных обязаны заключить «Соглашение о неразглашении персональных данных сотрудников или студентов Учреждения».

10. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными.

10.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

10.2. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

10.3. Каждый сотрудник Учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

10.4. Лица, виновные в нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) несут дисциплинарную, административную, гражданско–правовую или уголовную ответственность в соответствии с федеральным законом.

Приложение №1 к «Положению о защите и обработке персональных данных»

СОГЛАСИЕ

на обработку персональных данных

г. Железногорск «___» _____ 20___ г.

Заполняется только лицами, достигшими совершеннолетия:

Я, _____
(Фамилия, Имя, Отчество полностью)

_____ серия _____ № _____
(вид документа, удостоверяющий личность)

Выдан(о) _____, «__»____20__г.,
(кем и когда)

проживающий(ая) по адресу _____,

контактный телефон(ы) _____

Заполняется только родителями (представителями или опекунами) несовершеннолетних:

Я, _____,
ФИО родителя (законного представителя полностью)

проживающий по адресу _____,

паспорт серия _____ номер _____, выдан: _____

_____ «__»____20__г.,
(кем и когда)

являясь родителем (законным представителем) _____,
(ФИО ребенка (подопечного) полностью)

на основании _____,
(реквизиты доверенности или иного документа, подтверждающего полномочия представителя)

контактный телефон(ы) _____.

в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», подтверждаю свое согласие на обработку персональных данных, включающих:

- фамилию, имя, отчество;
- наименование, серию и номер документа, удостоверяющего личность;
- гражданство;
- пол;
- дату рождения;
- адрес;
- семейное положение,
- данные о родителях;
- социальное положение;
- сведения об образовании, месте получения образования, результаты образования;
- право на льготы;
- трудовой стаж;
- данные о состоянии здоровья;

с целью внесения их в базу данных поступающих в областное бюджетное профессиональное образовательное учреждение «Железногорский горно-металлургический колледж» (далее Оператор), расположенную по адресу: 307170, Курская обл. г. Железногорск, ул. Голенькова, д.2., а также для размещения (при необходимости) данных на официальном сайте колледжа в сети Интернет по адресу: zhgmk.ru.

Предоставляю Оператору право осуществлять все действия (операции) с персональными данными, включая их сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение. Оператор вправе обрабатывать персональные данные посредством внесения их в базу данных о студентах, обучающихся в колледже, а также размещать данные о ФИО и учебных группах студентов на своём официальном сайте в сети Интернет, расположенном по адресу: zhgmk.ru.

Передача персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Настоящее согласие дано мной «____»_____20__г. и действует до окончания обучения.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении, либо вручен лично под расписку представителю Оператора.

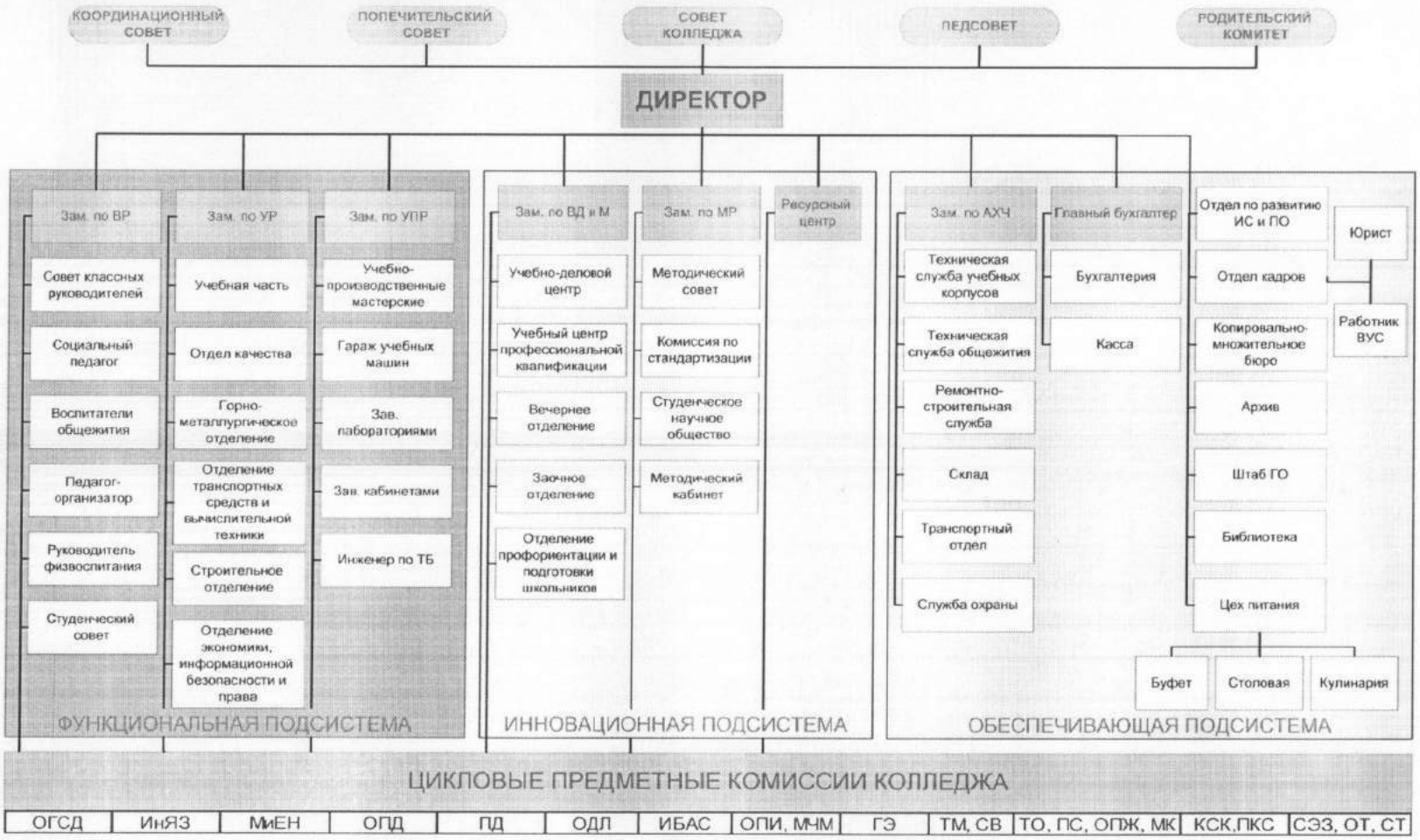
В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных, Оператор обязан немедленно прекратить их обработку.

С Уставом и Лицензией колледжа ознакомлен.

Подпись: _____ _____
(Ф.И.О. полностью)

ОРГАНИЗАЦИОННАЯ СТРУКТУРА

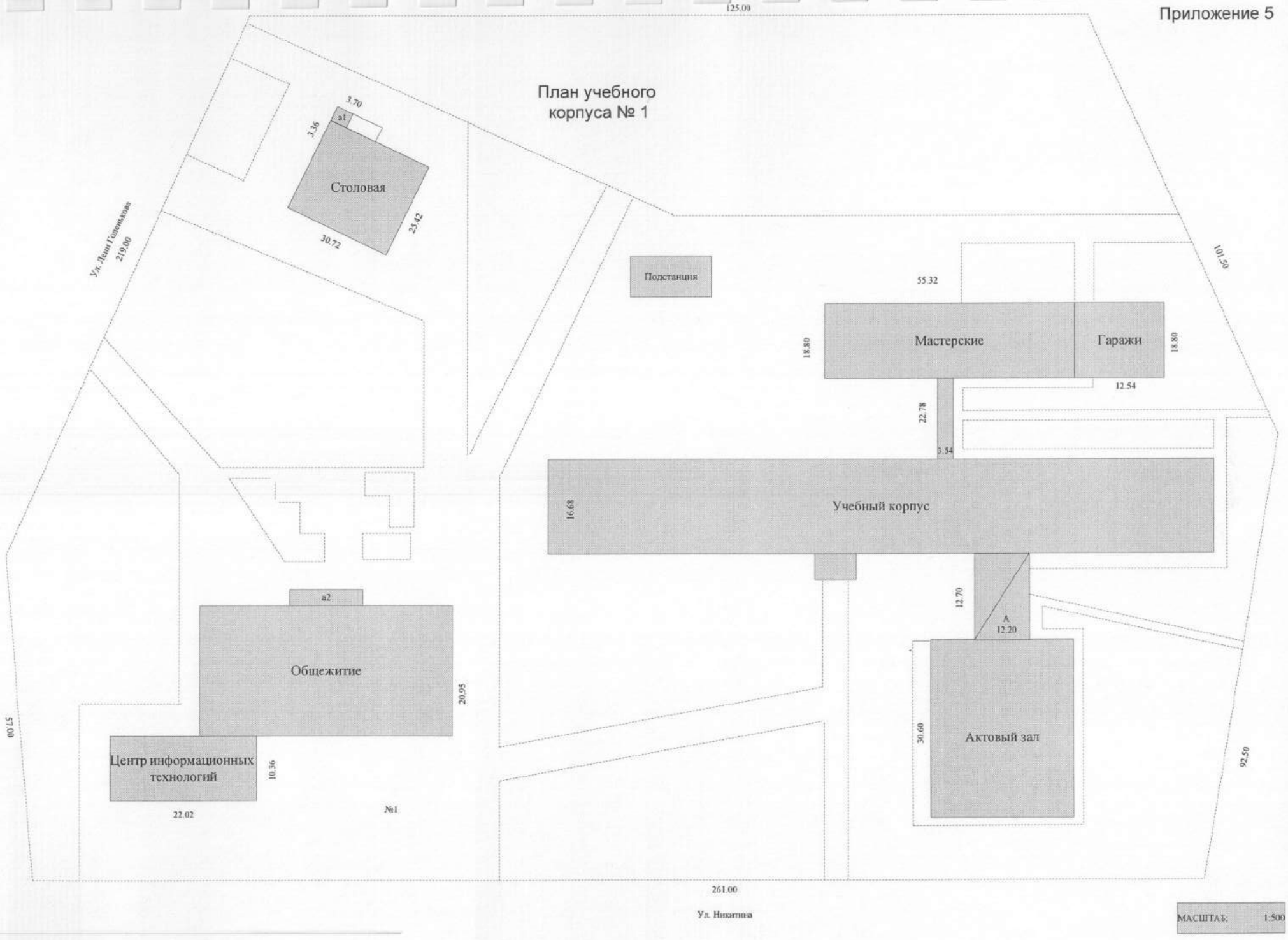
ОБЛАСТНОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ЖЕЛЕЗНОГОРСКИЙ ГОРНО-МЕТАЛЛУРГИЧЕСКИЙ КОЛЛЕДЖ»



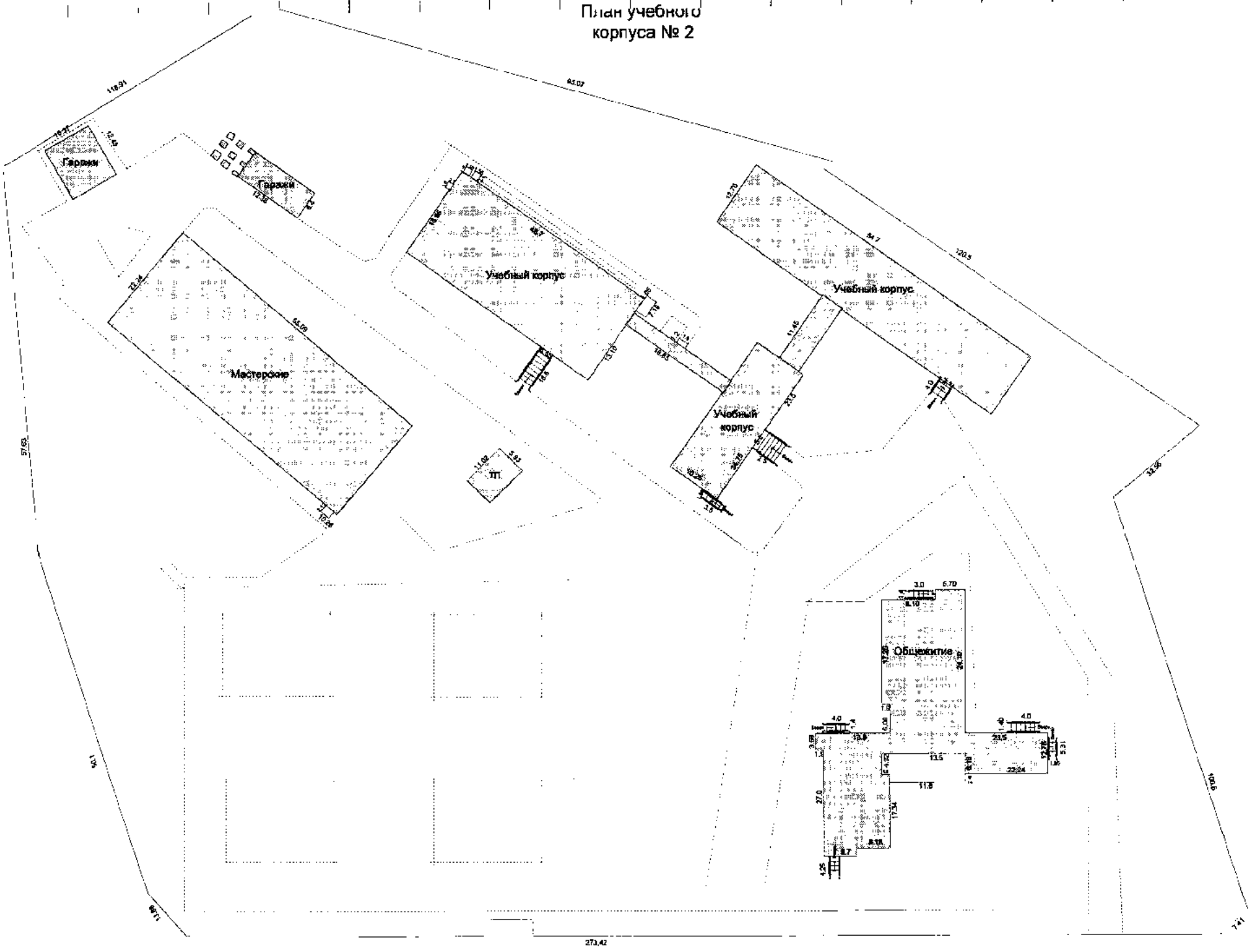
Приложение 4

Приложение 5

План учебного корпуса № 1



План учебного корпуса № 2



Приложение 6

УТВЕРЖДАЮ

Директор
ОБПОУ «ЖГМК»

_____ А.Н. Шебанов

«____» _____ 2016 г.

Комплект инструкций
администраторам системы и пользователям
по обеспечению безопасности информации в государственной информационной системе Ведения региональной информационной системы в сфере образования в ОБПОУ «ЖГМК»

Общие положения

Настоящая Инструкция определяет функции, права и обязанности администратора безопасности информации и пользователей государственной информационной системы Ведения региональной информационной системы в сфере образования в ОБПОУ «ЖГМК» (далее ГИС) и ИСПДн в её составе по вопросам обеспечения информационной безопасности при работе с информацией ограниченного доступа.

Настоящие инструкции являются дополнением к действующим нормативным документам по вопросам обеспечения безопасности информации и защите информации, и не исключают обязательного выполнения их требований.

Инструкция администратору безопасности информации

Администратор безопасности информации назначается приказом директора ОБПОУ «ЖГМК».

Администратор обеспечивает правильность использования и нормальное функционирование системы защиты информации (СЗИ) на объекте информатизации.

Основные функции администратора:

- контроль за выполнением требований действующих нормативных документов по вопросам обеспечения режима конфиденциальности, при проведении работ в ГИС;
- настройка и сопровождение в процессе эксплуатации подсистемы управления доступом в ГИС;
- контроль доступа лиц в помещение ГИС;
- контроль за проведением периодической смены паролей для доступа пользователей в ГИС;
- настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в ГИС;
- сопровождение подсистемы обеспечения целостности информации в ГИС;
- сопровождение подсистемы защиты информации от утечки за счет ПЭМИН, контроль соблюдения требований по размещению и использованию технических средств и систем, указанных в Предписании на эксплуатацию;
- анализировать данные журналов аудита ГИС с целью выявления возможных нарушений требований защиты;
- оценивать возможность и последствия внесения изменений в состав ГИС с учетом требований по защите, подготавливать свои предложения;
- контролировать физическую сохранность средств и оборудования ГИС;

– своевременно анализировать журналы учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;

– осуществлять выявление, анализ и устранение уязвимостей информационной системы, в том числе путём установки обновлений общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств, средств защиты информации из доверенных источников с требуемой особенностями применяемых информационных технологий и технических средств периодичностью, но не реже 1 раза в год;

– контролировать работоспособность, параметры настройки и правильности функционирования программного обеспечения и средств защиты информации, установку обновлений программного обеспечения;

– в период профилактических работ на рабочих станциях ГИС снимать при необходимости средства защиты информации с эксплуатации с обязательным обеспечением сохранности информации;

– периодически (не реже 1 раза в год) предоставлять директору ОБПОУ «ЖГМК» отчет о состоянии защиты ГИС и о нештатных ситуациях и допущенных пользователями нарушений установленных требований по защите информации.

Администратор безопасности информации имеет право:

– участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

– требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

– блокировать учетные записи пользователей, осуществивших несанкционированный доступ к защищаемым ресурсам;

– участвовать в любых проверках в ГИС;

– запрещать устанавливать на серверах и рабочих станциях нештатное программное и аппаратное обеспечение;

– вести контроль за процессом резервирования и дублирования важных ресурсов ГИС;

– участвовать в приемке новых программных средств;

– уточнять в установленном порядке обязанности пользователей ГИС по поддержанию уровня защиты;

– вносить предложения по совершенствованию уровня защиты ГИС;

– запрещать и немедленно блокировать попытки изменения программно-аппаратной среды ГИС без согласования порядка ввода новых (отремонтированных) технических и программных средств и средств защиты информации;

– запрещать и немедленно блокировать применение пользователями ГИС программ, с помощью которых возможны факты несанкционированного доступа к ресурсам ГИС;

– незамедлительно докладывать директору ОБПОУ «ЖГМК» обо всех попытках нарушения защиты ГИС;

– анализировать состояние защиты ГИС и ее отдельных подсистем;

– контролировать состояние средств и систем защиты информации и их параметры и критерии;

– контролировать правильность применения пользователями средств защиты информации;

– оказывать помощь пользователям в части применения средств защиты;

– не допускать установку, использование, хранение и размножение в ГИС программных средств, не связанных с выполнением функциональных задач;

– осуществлять контроль за соблюдением установленных правил и параметров регистрации и учета бумажных носителей информации;

– осуществлять контроль уничтожения (стирание) информации на машинных носителях при их передаче между пользователями и в сторонние организации;

– контролировать установленный порядок и правила антивирусной защиты информации;

– контролировать отсутствие на машинных носителях остаточной информации по окончании работы;

– не допускать к работе на рабочих станциях ГИС посторонних лиц.

Администратор безопасности информации обязан:

– знать в совершенстве применяемые информационные технологии;

– участвовать в контрольных и тестовых испытаниях и проверках ГИС;

– знать права доступа пользователей по обработке, хранению и передаче защищаемой информации;

– обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных функций;

– проводить инструктаж пользователей по правилам работы в ГИС;

– в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

– докладывать директору ОБПОУ «ЖГМК» о неправомерных действиях пользователя, приводящих к нарушению требований по защите информации;

– вести документацию в ГИС, в соответствии с требованиями нормативных документов;

– настраивать только те параметры системы, которые определяют права доступа пользователей к информации;

– производить периодическое тестирование всех реализованных программно-техническими средствами функций и требований по обеспечению информационной безопасности;

– в соответствии с приказом директора ОБПОУ «ЖГМК» и разрешительной системой доступа осуществлять добавление, блокирование, удаление и назначение прав доступа пользователям в системе;

– определить начальное значение паролей пользователя;

– восстанавливать настройки средств защиты информации при сбоях;

– хранить журналы аудита средств защиты информации на весь срок исковой давности действий и 5 лет после его окончания.

При выявлении факта несанкционированного доступа администратор безопасности информации обязан:

– блокировать доступ к информации ограниченного доступа;

– проанализировать характер несанкционированного доступа;

– доложить директору ОБПОУ «ЖГМК» запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

– принять меры к защите от несанкционированного доступа;

– по решению директора ОБПОУ «ЖГМК» возобновить работу.

Администратору безопасности информации запрещается:

– производить действия по настройке параметров системного и специального программного обеспечения;

– устанавливать срок действия учетной записи пользователя более 1 (одного) года;

– по истечении указанного срока в соответствии с разрешительной системой доступа производится продление действия учетной записи либо определение прав на такое продление;

– производить установку прикладного и специального программного обеспечения;

– фиксировать учетные данные пользователя (пароли, идентификаторы, ключи и др.) на твердых носителях, а также сообщать их кому бы то ни было, кроме самого пользователя.

При возникновении ситуаций, не описываемых руководящими документами, решение принимает администратор безопасности информации, руководствуясь действующим законодательством РФ.

Ответственность за сохранность информации ограниченного доступа несет администратор безопасности информации, действия которых фиксируются в протоколах аудита.

Администратор безопасности информации несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования этих учетных записей.

При нарушениях администратором безопасности информации правил, связанных с информационной безопасностью, они несут ответственность, установленную действующим законодательством Российской Федерации.

Инструкция по работе пользователей в ГИС

Допуск пользователей для работы в ГИС осуществляется в соответствии с утверждённым «Списком лиц, допущенных к работе в государственной информационной системе Ведения региональной информационной системы в сфере образования в ОБПОУ «ЖГМК» и разрешительной системой доступа.

Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам компьютера. При этом для хранения файлов, содержащих информацию ограниченного доступа, разрешается использовать только специально выделенные каталоги на несъемных носителях информации, а также соответствующим образом учтенные съёмные носители информации.

Присвоение пользователю полномочий доступа к ресурсам компьютера, состав необходимого системного и прикладного программного обеспечения для решения поставленных задач и определение возможного времени работы пользователя в ГИС осуществляется при первичной регистрации пользователя администратором безопасности информации.

Пользователь отвечает за правильность включения и выключения технических средств и систем, входа в систему и все действия при работе в ГИС.

Вход пользователя в систему осуществляется на основе ввода имени, присвоенного при первичной регистрации и ввода личного пароля. Требования к парольной защите определяется инструкцией по парольной защите.

В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам пользователя осуществляется периодическая (раз в месяц) замена пароля постоянного пользователя. Замена личного пароля осуществляется пользователем самостоятельно.

При работе со съемными носителями информации пользователь каждый раз перед началом работы обязан проверить их на наличие вирусов с использованием установленных антивирусных программ, в соответствии с Инструкцией по антивирусной защите.

При передаче съемных носителей информации между пользователями либо в сторонние организации для ремонта или утилизации пользователь производит уничтожение (стирание) информации ограниченного доступа на таких машинных носителях после чего осуществляет контроль уничтожения (стирания) информации. Уничтожение (стирание) информации производится внедренными в ГИС

сертифицированными средствами защиты информации с использованием механизмов очистки остаточной информации в соответствии с эксплуатационной документацией на такие средства защиты. Уничтожение (стирание) информации ограниченного доступа при передаче между пользователями может не производиться пользователем только при условии предварительного шифрования такой информации средствами криптографической защиты информации, если таковые внедрены в ГИС.

Пользователь обязан:

– знать и строго выполнять установленные правила и обязанности по доступу к защищаемым ресурсам и соблюдению принятого режима информационной безопасности;

– обеспечить правильность вводимых данных;

– своевременно сообщать администратору безопасности об изменениях статуса пользователя;

– незамедлительно сообщить администратору безопасности факты выявления инцидентов с доступом к информации ограниченного доступа.

В процессе работы пользователю запрещается:

– использовать для постоянного хранения и обработки информации ограниченного доступа каталоги несъемных носителей информации, за исключением выделенных каталогов;

– осуществлять попытки несанкционированного доступа к ресурсам операционной системы;

– в рамках выделенных ресурсов и полномочий доступа к ним обрабатывать информацию с уровнем конфиденциальности, выше заявленного при регистрации;

– пытаться подменять функции администратора по перераспределению времени работы и полномочий доступа к ресурсам компьютера;

– покидать помещение с незаблокированной учетной записью;

– отключать установленные средства защиты информации;

– использовать машинные носители без их предварительной проверки антивирусными средствами;

– устанавливать программное обеспечение;

– менять параметры конфигурации ранее установленных программных средств;

– использовать пароль, предоставленный администратором безопасности для первоначального доступа в качестве постоянного рабочего пароля;

– использование различными пользователями одной и той же учетной записи, даже если пользователи имеют одинаковые полномочия по доступу;

– запрещается передавать в любом виде или сообщать идентификаторы и пароли для доступа другим лицам, в том числе и своим руководителям;

– хранение пароля на любых твердых носителях, позволяющих другим лицам получить информацию о пароле;

– использовать информацию, полученную в результате доступа к БД, в целях, не предусмотренных его функциональными обязанностями.

Ответственность за сохранность и правильное использование информации, ставшей известной в процессе обработки информации ограниченного доступа несет пользователь.

Возможность получения технического доступа к информации ограниченного доступа не дает права пользователям обработки такой информации, если им не предоставлены права доступа к этой информации. Такие действия рассматриваются как попытки несанкционированного доступа.

При выявлении инцидентов с доступом к информации ограниченного доступа доступ пользователей к ней может быть ограничен до окончания расследования инцидента, о чем пользователь уведомляется в кратчайшие сроки. По результатам служебного расследования нарушитель может быть лишен прав доступа к информации ограниченного дос-

тупа, материалы расследования могут быть направлены в соответствующие службы для привлечения нарушителя к ответственности.

Пользователь несет ответственность за все действия, совершенные от имени его учетной записи, если не доказан факт несанкционированного использования этой учетной записи.

При нарушениях пользователем правил, связанных с информационной безопасностью, он несет ответственность, установленную действующим законодательством Российской Федерации.

Инструкция по парольной защите

Данная инструкция призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной системе организации, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ГИС и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности.

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 8 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Для генерации «стойких» значений паролей могут применяться специальные программные средства.

При наличии технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение администратору безопасности.

Опечатанные конверты с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов должны применяться личные печати владельцев паролей.

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий должна производиться администратором безопасности немедленно.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий администраторов и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой.

В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры по внеплановой смене паролей.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Инструкция по антивирусной защите

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности информации ГИС.

К применению в ГИС допускаются сертифицированные ФСБ и ФСТЭК России антивирусные средства.

В ГИС запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

Пользователи ГИС при работе со съемными носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

Ярлык для запуска антивирусной программы должен быть вынесен в окно «Рабочий стол» операционной системы Windows.

Администратор безопасности информации осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

Администратор безопасности информации проводит периодическое тестирование всего установленного программного обеспечения на предмет отсутствия компьютерных вирусов.

При обнаружении компьютерного вируса пользователь обязан сообщить об этом факте администратору безопасности.

В случае обнаружения на сменных носителях информации нового вируса, не поддающегося лечению, администратор безопасности информации обязан запретить (приостановить) использование этих носителей до обезвреживания вируса, передать вирус в компанию производитель применяемого антивирусного средства и сообщить об этом факте директору ОБПОУ «ЖГМК».

Инструкция по учету и маркированию машинных носителей персональных данных

С целью реализации режима ограниченного доступа к персональным данным в ОБПОУ «ЖГМК» и недопущению бесконтрольного использования машинных носителей, содержащих персональные данные, вводится их маркирование и поэкземплярный учет.

При маркировании на машинный носитель должна быть нанесена следующая информация:

- надпись «Содержит персональные данные»;
- ОБПОУ «ЖГМК»;
- учетный/инвентарный номер.

Организация и контроль за выполнением учета машинных носителей, содержащих персональные данные, возлагается на лицо, ответственное за обеспечение безопасности персональных данных в государственной информационной системе Ведения региональной информационной системы в сфере образования в ОБПОУ «ЖГМК».

Учет машинных носителей, содержащих персональные данные, осуществляется по «Журналу регистрации и учета машинных носителей персональных данных ОБПОУ «ЖГМК».

Начальник отдела по развитию ИСПО ОБПОУ «ЖГМК» _____ М.В. Ковальцов

Приложение 7

УТВЕРЖДАЮ

Директор
ОБПОУ «ЖГМК»

_____ А.Н. Шебанов

«___» _____ 2016 г.

ТЕХНИЧЕСКИЙ ПАСПОРТ
государственной информационной системы
Ведения региональной информационной системы в сфере образования
в ОБПОУ «ЖГМК»
расположенной по адресу: 307170, Курская область, г. Железногорск, ул. Л. Голенькова, д. 2, 3 этаж, кабинет №376 «заведующий учебной частью»

2016 г.

1. **Общие сведения об объекте информатизации**

1.1. Наименование объекта: государственная информационная система Ведения региональной информационной системы в сфере образования в ОБПОУ «ЖГМК» и ИСПДн в её составе – далее «ГИС».

1.2. Расположение объекта: 307170, Курская область, г. Железногорск, ул. Л. Голенькова, д. 2, 3 этаж, кабинет №376 «заведующий учебной частью».

2. **Состав оборудования ГИС**

2.1. Состав ОТСС объекта:

Таблица 1. Перечень основных технических средств и систем, входящих в состав ГИС

№ п/п	Тип ОТСС	Заводской (инвентарный) номер	Размещение ОТСС на объекте	Сведения по сертификации, специсследованиям и спецпроверкам	Примечание
Кабинет №376 «заведующий учебной частью»					
ПЭВМ №24031641					
1.	Системный блок	24031641	Кабинет №376 «заведующий учебной частью»		
2.	НЖМД в составе сист. блока, Seagate Barrakuda 7200. 12	5VMPW133			
3.	USB носитель Verbatim	151021190004G68AAJ			
4.	Монитор Benq GL2023-TA	ETX8F04495019			
5.	Клавиатура CBR KB107	КЛ-02			
6.	Мышь оптич. Genius NetScroll 100x	X4K89455109010			
7.	Сетевой фильтр	б/н			

2.2. Состав ВТСС объекта:

Таблица 2. Перечень вспомогательных технических средств, установленных в помещениях ГИС

№ п/п	Тип ВТСС	Заводской (инвентарный) номер	Примечание
Кабинет №376 «заведующий учебной частью»			
1.	Лампа освещения	б/н	
2.	Датчик пожарной сигнализации	б/н	
3.	Датчик пожарной сигнализации	б/н	
4.	Телефонный аппарат Panasonic KX-TS2360RUF	1JBF024513	
5.	Коммутатор Complex	95287054	
ПЭВМ №24031632			
6.	Системный блок	24031632	
7.	Монитор LG Flatron L1730P	0000162568	
8.	Аудиоколонки Genius SP-G10	JA091C4477	

№ п/п	Тип ВТСС	Заводской (инвентарный) номер	Примечание
9.	МФУ HP LaserJet	CNB7HD65LH	
10.	Клавиатура CBR KB107	КЛ-01	
11.	Мышь оптич. Genius NetScroll	X49209801178	
12.	Сетевой фильтр	б/н	
ПЭВМ №000162809			
13.	Системный блок	000162809	
14.	Монитор Benq ET-0005-NA	ETX3803676026	
15.	Клавиатура Genius KB-06X2	XEAC01120505	
16.	Мышь оптич. Genius NetScroll 100	X4B86169604405	
17.	Сетевой фильтр	б/н	

2.3. Структура, топология и размещение ОТСС относительно границ контролируемой зоны объекта.

2.3.1. Структурная (топологическая) схема с указанием информационных связей между устройствами.

Структурная (топологическая) схема с указанием информационных связей между устройствами автоматизированного рабочего места представлена на Рисунке 1. Функциональные и технологические связи между объектами ГИС представлены на Рисунке 2.

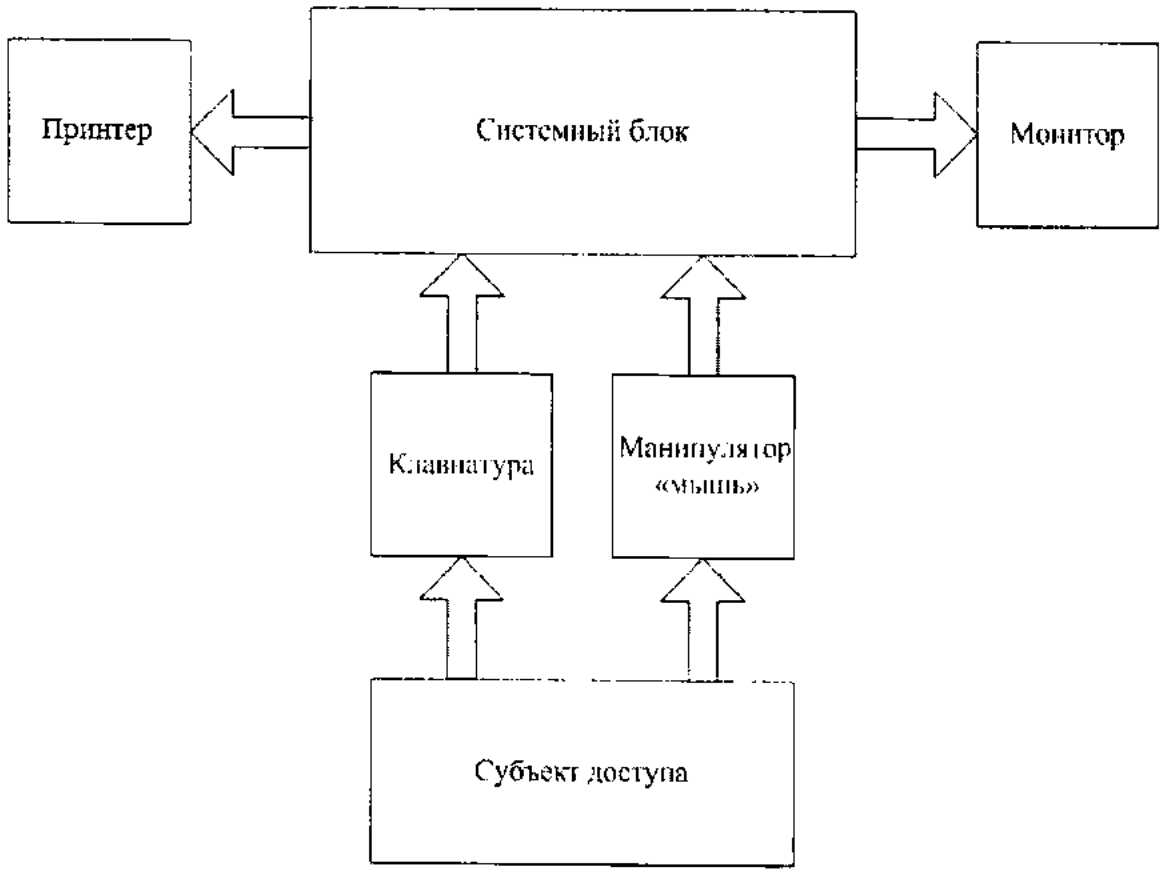


Рисунок 1. Структурная (топологическая) схема информационных связей между устройствами автоматизированного рабочего места.

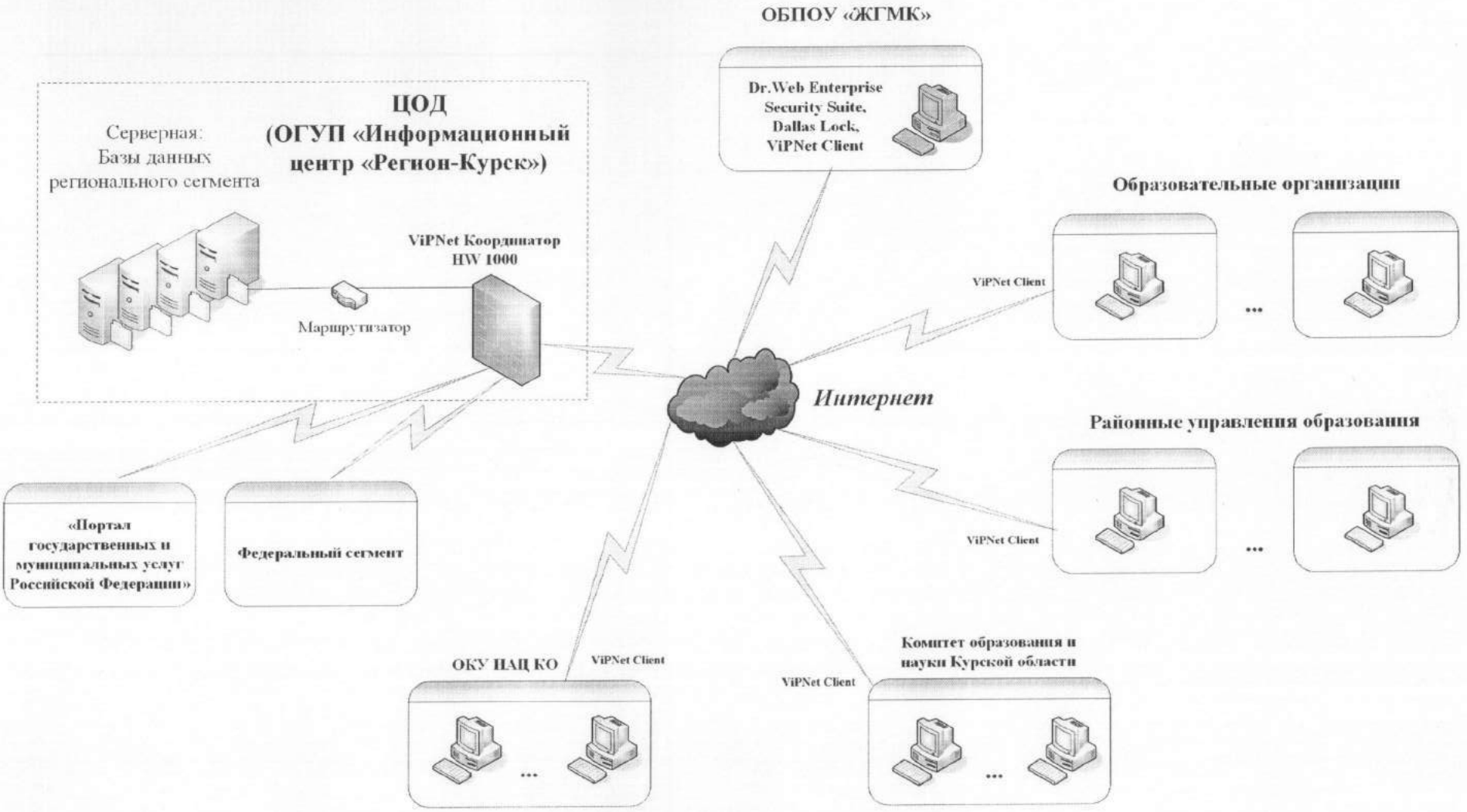


Рисунок 2. Функциональные и технологические связи между объектами ГИС с учетом применения средств защиты информации.

2.3.2. Схема размещения и расположения ОТСС на объекте с привязкой к границам контролируемой зоны.
Размещение и расположения ОТСС на объекте с привязкой к границам контролируемой зоны представлено на Рисунках 3-6.

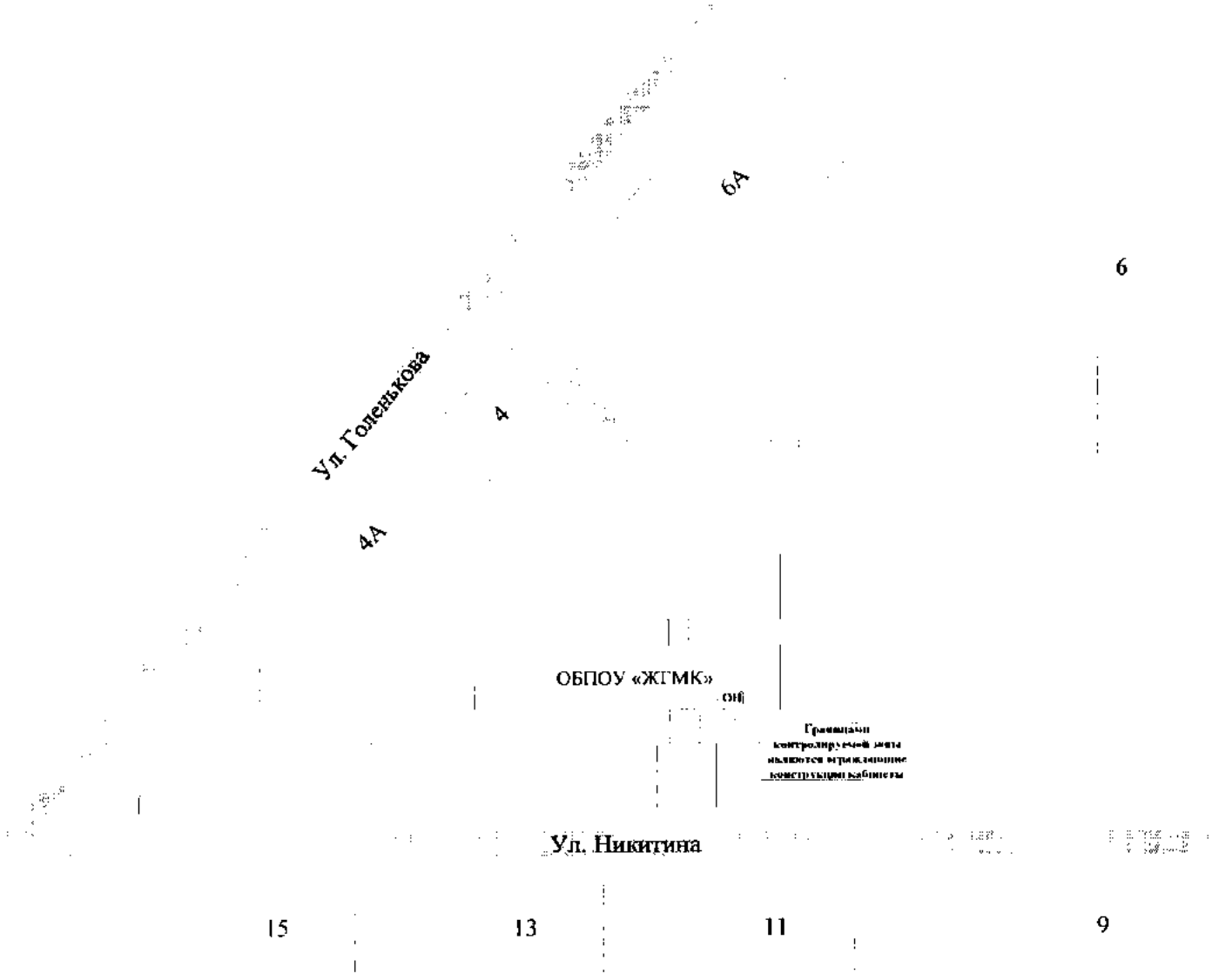


Рисунок 3. Схема размещения объекта информатизации с привязкой к границам контролируемой зоны.

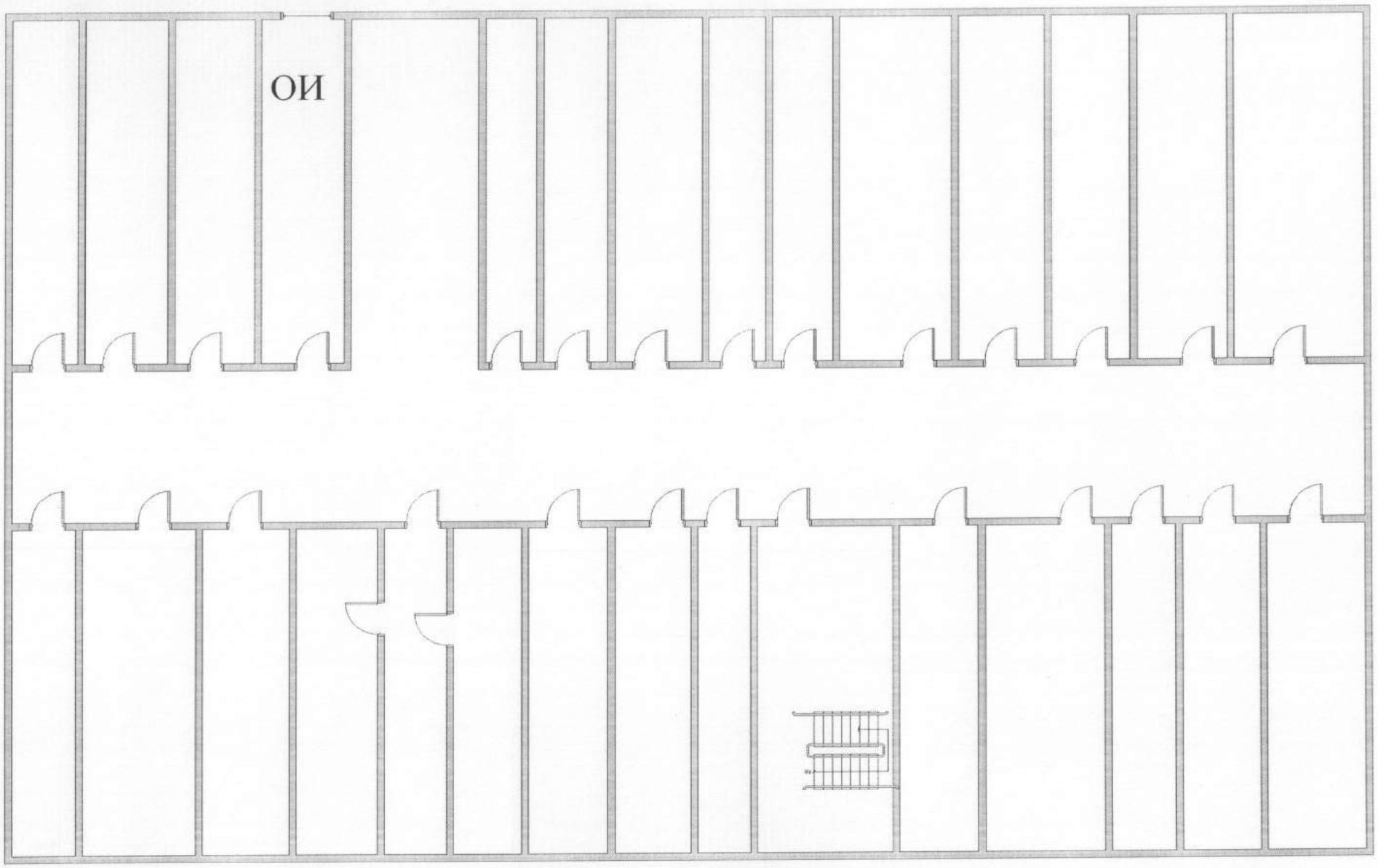


Рисунок 4. Схема 3 этажа с расположением объекта информатизации.

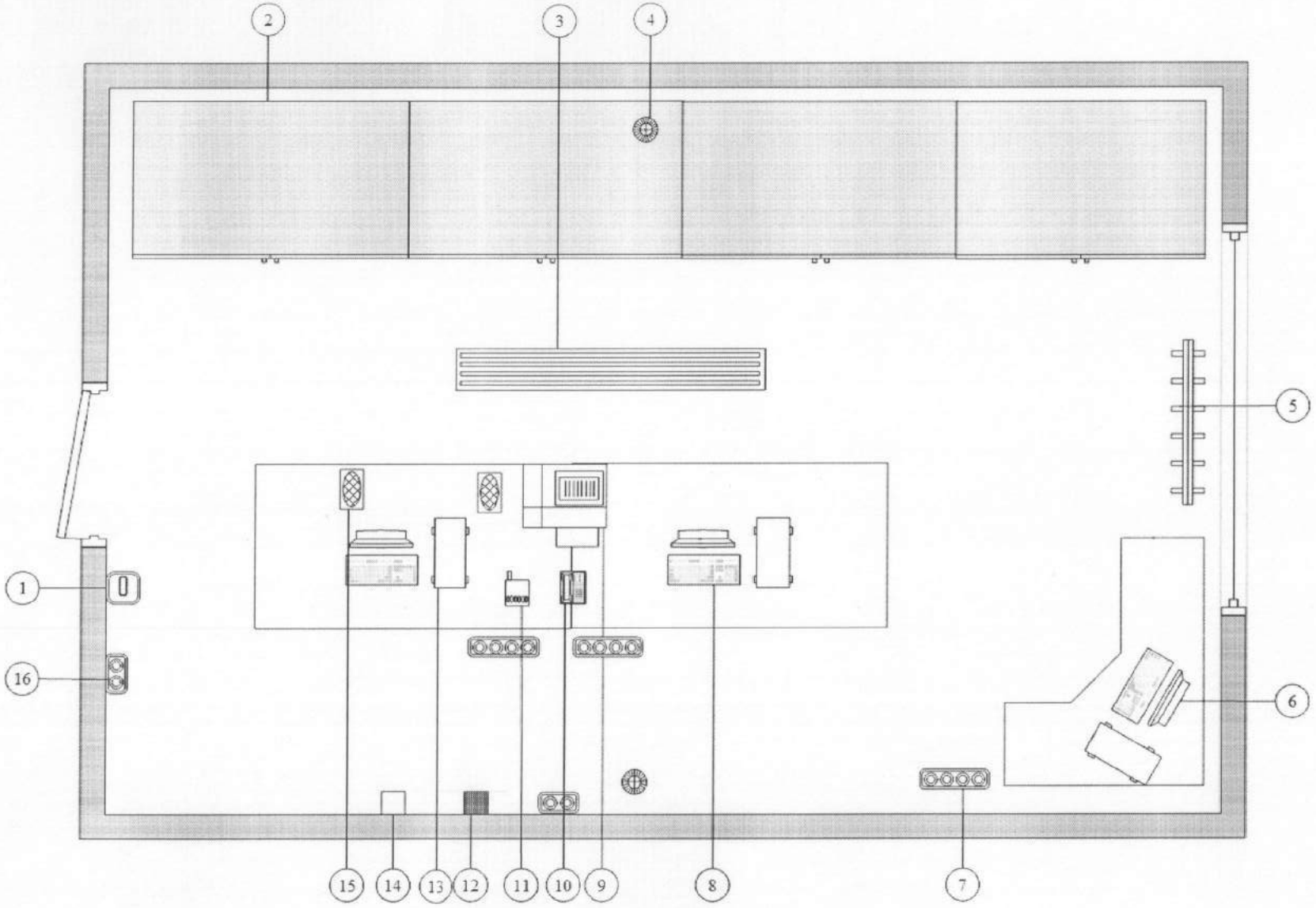


Рисунок 5. Схема кабинета №376 «заведующий учебной частью» (1 – выключатель, 2 – шкаф, 3 – лампа освещения, 4 – датчик пожарной сигнализации, 5 – батарея, 6 – ПЭВМ №24031641 (ОТСС), 7 – сетевой фильтр, 8 – ПЭВМ №000162809 (ВТСС), 9 – принтер, 10 – телефонный аппарат, 11 – коммутатор, 12 – розетка ЛВС, 13 – ПЭВМ №24031632 (ВТСС), 14 – розетка АТС, 15 – аудиоколонки, 16 – розетка электропитания).

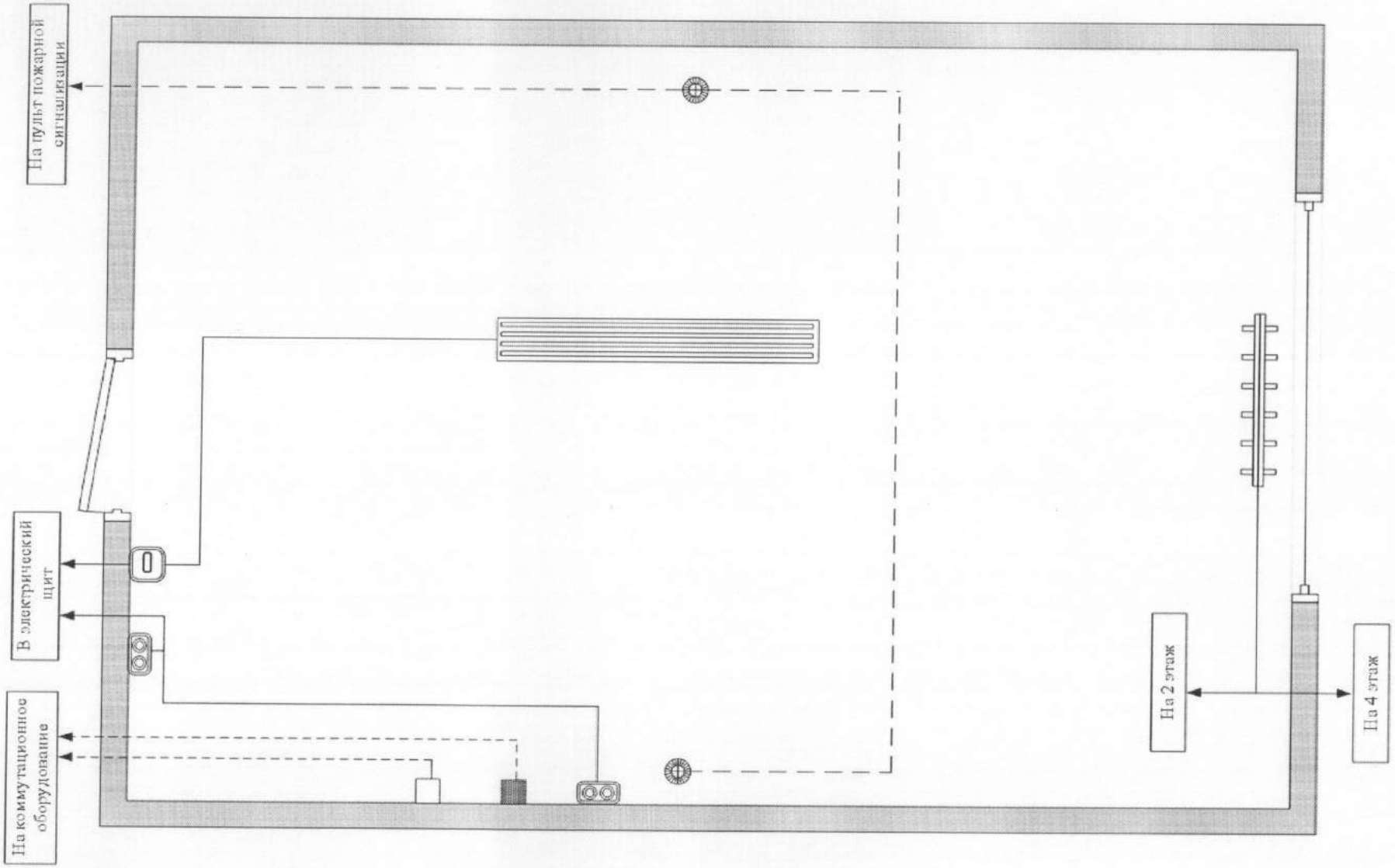


Рисунок 6. Схема размещения и расположения линий электропитания розеточной и осветительной сети, линий пожарной сигнализации, телефонных линий, трубопроводов отопления на объекте информатизации (кабинет №376 «заведующий учебной частью»).

2.4. Размещение ВТСС, расположение линий и коммуникаций.

2.4.1. Схемы размещения ВТСС и прокладки линий и коммуникаций, выходящих из помещений объекта.

Схемы расположения ВТСС, телефонных линий, трубопроводов отопления, линий пожарной сигнализации представлены на Рисунках 5, 6. Система охраны и пожаротушения выполнена по проводной схеме, и имеет выход за пределы контролируемой зоны.

2.4.2. Системы электропитания и заземления.

Схема электропитания ОТСС объекта, схемы электропитания розеточной и осветительной сети объекта приведена на Рисунке 6. Электрическая подстанция располагается за пределами контролируемой зоны.

2.5. Перечень средств защиты, установленных на объекте информатизации.

Перечень средств защиты информации, установленных в ГИС приведен в Таблице 3.

Таблица 3. Перечень средств защиты информации, установленных в ГИС

№ п/п	Наименование продукции	Заводской (инвентарный) номер	Сведения о сертификате, знаке соответствия (ЗС)
Кабинет №376 «заведующий учебной частью»			
ПЭВМ №24031641			
1.	Dr.Web Enterprise Security Suite версия 6.0	Сер. ном. ZY2Y-NQDP-HWQL-RT26	Сертификат ФСТЭК России №2446, выдан 20.09.2014, действителен до 20.09.2017
		СЗЗ К112922	Сертификат ФСБ России №СФ/019-1518, выдан 04.08.2010, действителен до 31.12.2016
2.	Система защиты информации от несанкционированного доступа «Dallas Lock 8.0-К»	Зав. ном. 7357-1217-775 (1)	Сертификат ФСТЭК России №2720, выдан 25.09.2012, действителен до 25.09.2018
		СЗЗ К665968	
3.	Средство криптографической защиты информации ViPNet Client 3.2 КС2	Рег. Ном. 637С-062874	Сертификат ФСТЭК России №1549/1, выдан 26.05.2010, действителен до 26.05.2016
		Номер дистр. КлКС2-3.2-92491	Сертификат ФСБ России №СФ/124-2796, выдан 11.02.2016, действителен до 30.11.2017

2.6. Перечень используемых программных средств (средств доступа к информации).

Таблица 4. Перечень используемых программных средств (средств доступа к информации)

№ п/п	Наименование программных средств	Версия	Разработчик
Кабинет №376 «заведующий учебной частью»			
ПЭВМ №24031641			
1.	ОС Windows	7 Профессиональная	Microsoft Corporation
2.	Microsoft.NET Framework 4 Client	4.0.30319	Microsoft Corporation

№ п/п	Наименование программных средств	Версия	Разработчик
	Profile		
3.	Microsoft.NET Framework 4 Extended	4.0.30319	Microsoft Corporation
4.	Microsoft Office Профессиональный плюс 2007	12.0.4518.1014	Microsoft Corporation
5.	Microsoft Visual C++ 2008 Redistributable – x86	9.0.30729.6161	Microsoft Corporation
6.	Microsoft Visual C++ 2010 x86 Redistributable	10.0.40219	Microsoft Corporation
7.	WinRAR (32-разрядная)	5.20.0	Yevgeniy Roshal
8.	Yandex браузер	б/н	Яндекс

3. Описание технологического процесса обработки информации

Технологический процесс обработки персональных данных в ОБПОУ «ЖГМК» при ведении региональной информационной системы в сфере образования в Курской области определяется:

- Федеральным законом РФ от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;
- Федеральным законом РФ от 27.07.2006 №152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2010 №210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
- Распоряжением Правительства РФ от 17.12.2009 №1993-р «Об утверждении сводного перечня первоочередных государственных и муниципальных услуг, предоставляемых в электронном виде»;
- Постановлением Правительства РФ от 08.06.2011 №451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме»;
- Распоряжением Правительства РФ от 25.10.2014 №2125-р, «Об утверждении Концепции создания единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам»;
- Распоряжением Правительства РФ от 14.02.2015 №236-р «Об утверждении плана мероприятий («дорожной карты») по созданию единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам»;
- Постановлением Губернатора Курской области №537-пг от 03.12.2013 «О создании региональной информационной системы в сфере образования»;
- иными принятым в исполнение вышеуказанных НПА документами.

Обработка информации ведется со следующими целями:

- получение информации о контингенте обучающихся субъекта РФ;
- получение оперативной информации об очередях на зачисление в организации образования субъекта РФ;
- учет обучающихся в организациях образования субъекта РФ,
- формирование полного набора данных об этапах обучения и достижениях обучающихся при их обучении в организациях образования субъекта РФ, включая результаты дополнительного образования;

– получение информации о влиянии образовательного процесса на состояние здоровья обучающихся;

– повышение доступности для населения информации об организациях образования субъекта РФ, и оказываемых ими образовательных услугах через государственные информационные порталы;

– организация возможности подачи заявлений о зачислении обучающихся в дошкольные образовательные организации и общеобразовательные организации в электронном виде;

– сокращение количества документов и информации, подлежащих представлению заявителями для получения государственных и муниципальных услуг в сфере образования.

Сотрудник, допущенный приказом директора ОБПОУ «ЖГМК» с помощью веб-браузера по защищенному каналу VPN обращается к ресурсам региональной информационной системы в сфере образования в Курской области, базы данных которой располагаются в Центре обработки данных (ЦОД) в ОГУП «Информационный центр «Регион-Курск». Сотрудник заполняет в информационной системе данные по ОБПОУ «ЖГМК» и, при необходимости, просматривает данные по другим образовательных организациях Курской области.

Функциональные связи и каналы передачи информации при различных вариантах обработки информации представлены на Рисунке 7.

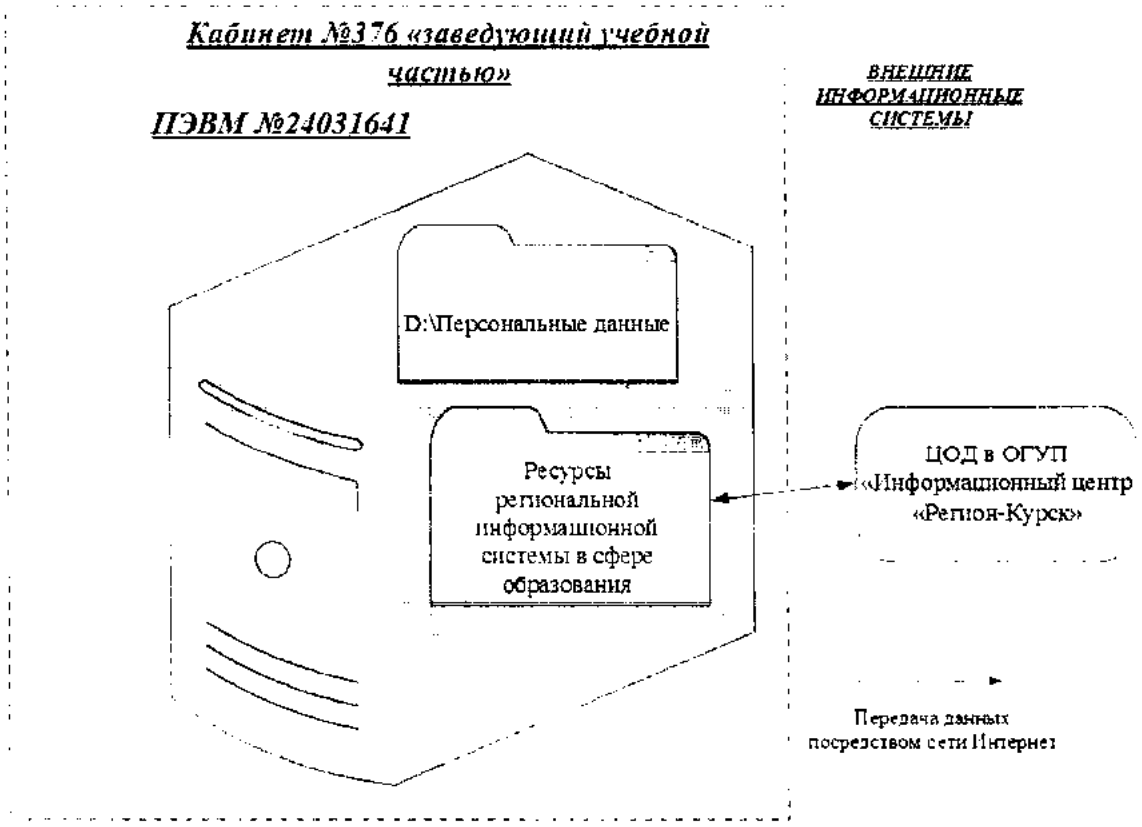


Рисунок 7. Функциональные связи в ГИС Ведения региональной информационной системы в сфере образования в ОБПОУ «ЖГМК».

4. Разрешительная система доступа (матрицы доступа) к информационным (программным) ресурсам

Требования по доступу к аппаратным ресурсам представлены в Таблице 5:

Таблица 5. Требования по доступу к аппаратным ресурсам

№ п/п	Режимы обработки информации	Значения, параметры, порты	Примечание
1.	Набор текста с клавиатуры	+	
2.	Запись/считывание информации с НЖМД	+/+	
3.	Запись/считывание информации с оптических носителей	+/+	
4.	Запись/считывание информации с USB-накопителей	+/+	
5.	Запись/считывание информации с flash-накопителей	-/-	
6.	Вывод информации на печать	+	

Перечень субъектов доступа ГИС и уровень их полномочий приведен в Таблице 6:

Таблица 6. Перечень субъектов доступа ГИС и уровень их полномочий

№ п/п	Должность	ФИО	Имя пользователя в АС (login)	Уровень полномочий в АС
1.	Заведующий учебной частью ОБПОУ «ЖГМК»	Копылова Наталья Анатольевна	КопыловаНА	пользователь
2.	Заместитель директора по учебной работе ОБПОУ «ЖГМК»	Проценко Татьяна Николаевна	ПроценкоТН	пользователь
3.	Ведущий программист отдела по развитию ИСПО ОБПОУ «ЖГМК»	Миронов Андрей Викторович	Администратор	администратор

Перечень объектов доступа ГИС приведен в Таблице 7:

Таблица 7. Перечень объектов доступа

№ п/п	Тип информации	Объекты доступа в АС
1.	Удаленные ресурсы.	//1.8.106.10/ //1.8.106.11/ //1.8.106.12/ //1.8.106.13/
2.	Файлы с информацией на жестком магнитном диске.	D:\Персональные данные
3.	Входящие/Исходящие документы, на CD (DVD-R/RW)-дисках,	x:\Документы\Персональные данные
		x:\Документы\Конфиденциально

№ п/п	Тип информации	Объекты доступа в АС
	USB-носителях	x:\Документы\Неконфиденциально
4.	Основные конфигурационные файлы ОС и драйверы	C:\Windows
5.	Основные конфигурационные файлы средств защиты информации	C:\DLLOCK80\
		C:\Program Files\InfoTeCS\ViPNet Client\
		C:\Program Files\DrWeb\

Описание реализованных правил разграничения доступа (матрица доступа) к программным средствам приведено в Таблице 8:

Таблица 8. Перечень объектов доступа

№ п/п	Программное обеспечение	Имя пользователя в АС (login)		
		КопыловаНА	ПроценкоТН	Администратор
Кабинет «заместитель директора»				
ПЭВМ №9С327820R				
1.	ОС Windows	В	В	В
2.	Microsoft.NET Framework 4 Client Profile	В	В	З
3.	Microsoft.NET Framework 4 Extended	В	В	З
4.	Microsoft Office Профессиональный плюс 2007	В	В	З
5.	Microsoft Visual C++ 2008 Redistributable – x86	В	В	З
6.	Microsoft Visual C++ 2010 x86 Redistributable	В	В	З
7.	WinRAR (32-разрядная)	В	В	З
8.	Yandex браузер	В	В	З

В	-	выполнение
З	-	запрет выполнения (запуска)

Описание реализованных правил разграничения доступа (матрица доступа) к объектам приведено в Таблице 9:

Таблица 9. Описание реализованных правил разграничения доступа (матрица доступа) к объектам

№ п/п	Информационные ресурсы	Имя пользователя в АС (login)		
		КопыловаНА	ПроценкоТН	Администратор
1.	//1.8.106.10/	ВИЧУП	ВИЧУП	-
2.	//1.8.106.11/	ВИЧУП	ВИЧУП	-
3.	//1.8.106.12/	ВИЧУП	ВИЧУП	-
4.	//1.8.106.13/	ВИЧУП	ВИЧУП	-
5.	D:\Персональные данные	ВИЧУП	ВИЧУП	-
6.	C:\Windows	ВЧ	ВЧ	ВИЧ
7.	C:\DLLOCK80\	ВЧ	ВЧ	ВИЧУ
8.	C:\Program	ВЧ	ВЧ	ВИЧУ

№ п/п	Информационные ресурсы	Имя пользователя в АС (login)		
		КопыловаНА	ПроценкоТН	Администратор
	Files\InfoTeCS\ViPNet Client\			
9.	C:\Program Files\DrWeb\	ВЧ	ВЧ	ВИЧУ

В	(X)	-	выполнение (создание)
И	(A)	-	изменение
Ч	(R)	-	чтение
У	(D)	-	удаление
П	(P)	-	печать

Описание реализованных правил разграничения доступа (матрица доступа) к аппаратным средствам приведено в Таблице 10:

Таблица 10. Описание реализованных правил разграничения доступа (матрица доступа) к аппаратным средствам

№ п/п	Имя пользователя в АС (login)	Привилегии		
		Вывод защищаемой информации		Загрузка ПЭВМ со съемных машинных носителей информации
		на CD/DVD- диски	на USB-носители	
1.	КопыловаНА	+	+	-
2.	ПроценкоТН	+	+	-
3.	Администратор	-	-	-

+	-	разрешено
-	-	запрещено

5. Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации

Инвентарные номера аттестата соответствия, заключения по результатам аттестационных испытаний, протоколов испытаний и даты их регистрации приведены в Таблице 11:

Таблица 11. Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации

№ п/п	Наименование документа	Номер документа	Дата регистрации
1.	Аттестат соответствия		
2.	Заключение по результатам аттестационных испытаний		
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

6. Результаты периодического контроля

Сведения о результатах периодического контроля объекта информатизации на соответствие требованиям по безопасности информации приведены в Таблице 12:

Таблица 12. Сведения о результатах периодического контроля объекта информатизации на соответствие требованиям по безопасности информации

№ п/п	Наименование организации, проводившей проверку	Дата проведения проверки	Номер протокола	Примечание
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				

7. Лист регистрации изменений

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Таблица 13. Сведения о регистрации изменений объекта информатизации на соответствие требованиям по безопасности информации

Порядковый № и дата введения изменений	Наименование документа, фиксирующего изменения	№№ замененных (исправленных) листов технического паспорта	Подпись лица, внесшего изменения

Приложение 8

ОБОУ СПО «Железногорский горно-металлургический колледж»

24-30 ноября 2015 года

Неделя специальности 090305 «Информационная безопасность автоматизированных систем»

Наша специальность призвана готовить специалистов способных противостоять всем возможным угрозам в области информационной безопасности.

Наша специальность – специальность настоящего и будущего!!!

Первый набор на специальность «Информационная безопасность» в Железногорском горно–металлургическом колледже был осуществлен в 2009 году. В 2014 году нам исполнилось **5 лет**!

С 2009 года осуществлено два выпуска по специальности «Информационная безопасность».

С 2011 года в колледже осуществляется набор в группы по специальности 090305 «Информационная безопасность автоматизированных систем». Сейчас по данной специальности в колледже с 1 курса по 4 курс обучаются четыре группы.

ПРОГРАММА НЕДЕЛИ СПЕЦИАЛЬНОСТИ
090305 «Информационная безопасность автоматизированных систем»

Дата проведения	*Время проведения*	*Мероприятие*	*Место проведения*	*Участники*	*Ответственные*
24.11.14	*В течение дня*	*– Конкурс презентаций и газет «Информационная безопасность – прошлое, настоящее, будущее»*	*3 этаж колледжа*	*Студенты группы И-14*	*Милютина Е.В.*
25.11.14	*10:00 – 12:00*	*– Открытая защита курсовых проектов (работ) по ПМ 01 «Эксплуатация подсистем безопасности автоматизированных систем»*	*ЦИТ «Айвенго»*	*Студенты группы И-11*	*Петрушин С.Д. Жигалева О.Л. Чекърска Ю.И.*
	14:00-14:40 16:00-16:40	*– Классные часы – Профориентация*	*Читальный зал*	*Студенты группы И-12*	*Милютина Е.В. Жигалева О.Л.*
	В течение дня	*– Конкурс по криптоанализу для всех желающих студентов колледжа*	*Весь колледж*	*Все желающие студенты*	*Чекърска Ю.И. Мажуга А. Борисова А.*
26.11.14	*В течение дня*	*– День самоуправления*	*аудитории согласно расписанию*	*Студенты групп И-12, И-11*	*Петрушин С.Д., Жигалева О.Л.*
27.11.14	*14:00-14:40 16:00-16:40*	*– Классные часы – Профориентация*	*Читальный зал*	*Студенты группы И-12*	*Милютина Е.В. Жигалева О.Л.*
	18:00-19:00	*– Круглый стол с представителями предприятий и организаций г.Железногорска по актуальным вопросам защиты информации*	*ЦИТ «Айвенго»*	*Студенты групп И-12, И-13, И-11*	*Петрушин С.Д., Жигалева О.Л., Чекърска Ю.И.*
28.11.14	*14:00-15:00*	*– Олимпиады по специальности*	*ЦИТ «Айвенго»*	*Студенты групп И-12, И-11*	*Петрушин С.Д., Жигалева О.Л., Чекърска Ю.И.*
30.11.14	*11:00-12:00*	*– Викторина по основам информационной безопасности.*	*ЦИТ «Айвенго»*	*Студенты групп И-12, И-11, ЮЗГУ*	*Петрушин С.Д., Жигалева О.Л., Чекърска Ю.И.*
	12:10-13:00	*– Вручение наград. Закрытие недели специальности. Концерт.*	*Актовый зал*	*Студенты колледжа*	*Жигалева О.Л., Головачева Л.Н.*

Темы для классных часов и профориентации:

1. О защите детей от информации, причиняющей вред их здоровью и развитию
2. А взламывали ли сегодня ваш аккаунт в соцсети?

3. Черные и белые хакеры

Приложение 9

А ВЗЛАМЫВАЛИ ЛИ СЕГОДНЯ ВАШ АККАУНТ В СОЦСЕТИ?

Мажуга Анастасия Сергеевна
Руководители:
Жигалева Ольга Леонидовна,
Чекърска Юлия Игоревна
ОБОУ СПО «Железногорский горно-металлургический колледж»

Сегодня особой популярностью пользуются социальные сети. Русскоязычные пользователи очень полюбили сеть «ВКонтакте», не менее популярны и «Одноклассники». Эти социальные сети используются для самых разных целей, кто-то заходит в Вконтакте чтобы послушать музыку, кто-то чтобы пообщаться, а кто-то чтобы посмотреть фильм. Люди привыкли общаться в сети, обмениваться личной информацией и фотоснимками. Но многие глубоко заблуждаются, когда думают, что их аккаунт в соцсетях надежно защищен.

Целью нашего исследования стало определение наиболее актуальных способов взлома аккаунта в социальных сетях и подбор наиболее эффективных механизмов защиты.

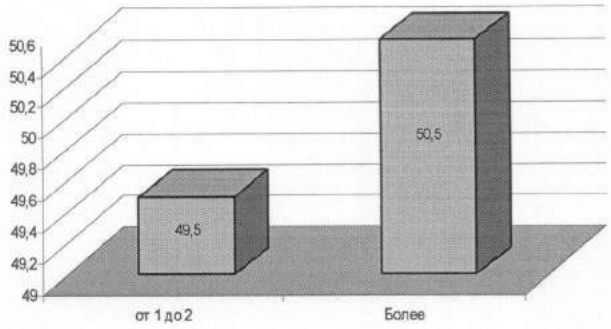
В рамках нашего исследования для определения актуальности рассматриваемого вопроса и понимания ее рядовыми пользователями в Железногорском горно-металлургическом колледже было проведено анкетирование, в котором приняли участие 185 студентов.

Вопрос	Варианты ответов	Результат	
		абс	%
Зарегистрированы ли Вы в социальных сетях?	Да	184	99,5
	Нет	1	0,5

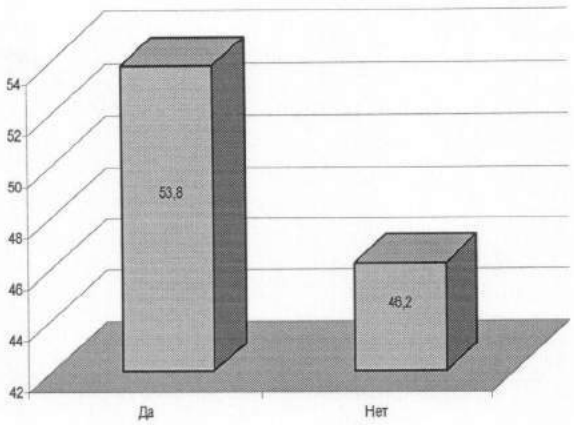
Результаты данного опроса подтверждают неразрывность общения молодежи с общением в социальных сетях.

Вопрос	Варианты ответов	Результат	
		абс	%
В скольких социальных сетях Вы зарегистрированы?	1-2	91	49,5
	Более	93	50,5
Взламывали ли когда-нибудь Ваш аккаунт?	Да	99	53,8
	Нет	85	46,2

На рисунке 1 представлено графическое отображение результатов опроса, которое показывает, что зачастую пользователи (50,5%) ищут общения в разных соцсетях, а не отдают предпочтение какой-то одной.



В скольких социальных сетях Вы зарегистрированы?



Взламывали ли когда-нибудь Ваш аккаунт?

Рисунок 1 – Результаты анкетирования

Также интересным фактом является то, что большая часть опрошенных нами респондентов (53,8%) явно заметили взлом своего аккаунта. А вот среди тех, кто заявил, что его аккаунт никогда не взламывался (46,2%), скорей всего определенная часть просто об взломе не догадывается. Это связано с существующими способами взломов.

В рамках анкетирования были и другие вопросы:

Вопрос	Варианты ответа
Что может по Вашему мнению стать причиной взлома аккаунта?	простой пароль
	посещение непроверенных сайтов
	неизвестные люди в друзьях
	другое
Для каких целей может использоваться Ваш аккаунт?	просто хулиганство хакеров
	рассылка спама и рекламы
	в личных целях
	другое

Многие студенты считают, что причиной взлома может стать простой пароль и посещение непроверенных сайтов, но также некоторые считают, что неизвестные люди в друзьях могут нарушить безопасность их аккаунта.

Основными целями взлома большинство опрошенных считают хулиганство хакеров (75%) и взлом в личных целях (69%).

Далее рассмотрим самые распространенные способы, которыми пользуются для взлома аккаунта в социальной сети:

1. Самым распространенны способом является открытие аккаунта с помощью подборки паролей. В этом случае просто перебирают самые распространенные простые пароли и слова. Защититься от этого метода легко, достаточно всего хорошо продумать свои пароли.

2. Часто в интернет-кафе стоят специальные программы, улавливающие все нажатия на кнопки клавиатуры. Такие программы называются KeyLogger'ами. Кроме того к их основным функциям

дополняется запись всех нажатий на клавиатуре в определенные файлы. От этого метода защититься можно только выходом в интернет только со своего проверенного компьютера.

3. Если вы частый пользователь социальных сетей , то вам нужно быть внимательным к защите своего компьютера от вирусов. Ведь многие вирусы, такие как трояны, высылают свои хозяевам данные вашего аккаунта. Самой надежной защитой вашего компьютера от вирусов будет установка проверенного антивируса.

4. Способ социальной инженерии. Этот метод применяется непосредственно при общении с человеком. В этом случае нужно просто внимательно относиться к разговорам с незнакомыми людьми. Ведь если эти люди профессионалы своего дела, то вы не заметите, как они разведают у вас нужную им информацию.

5. Многие опытные интернет-мошенники пользуются специальным программным обеспечением, которое позволяет находить ошибки в кодах сайтов. Так можно получить доступ к основным базам данных и паролям. В этом случае восстановлением данных занимаются сами администраторы.

6. Часто взломом личных аккаунтов занимаются через почтовые рассылки. В полученных письмах содержится специально продуманное сообщение, ответ на которое подразумевает указание своих данных, в том числе и паролей. Чтобы защититься от этого метода достаточно внимательно относиться к полученным письмами отвечать только на проверенные вами письма, ведь самым тяжелым последствием этого метода может быть потеря не только личной почты, но и всех аккаунтов.

7. Еще бывают такие вредоносные сайты, которые визуально похожи на сайт социальной сети. На них даже видна Ваша страничка, с Вашей фотографией, но адрес этого сайта отличается от адреса нужного Вам сайта. Возможно добавление к строчке справа и слева символов или разбавление адреса какими-то символами. В общем, все сделано, так чтобы человек не заметил подмены адреса сайта и свободно вводил на нем Логин и Пароль от своей странички в социальной сети. От этого метода можно защититься лишь внимательным просмотром адреса сайта.

Результатом нашего исследования стало рассмотрение методов защиты от влома в социальных сетях. Мы рекомендуем следующие мероприятия:

1. Создавайте только уникальные пароли для всех ваших аккаунтов в социальных сетях.

Однажды взломав вашу учетную запись в одной соцсети злоумышленники получают доступ ко всем вашим аккаунтам в других социальных сетях, они смогут беспрепятственно зайти во все ваши профили, если вы используете один и тот же пароль. Если для вас трудно запоминать кучу паролей, то воспользуйтесь специальными приложениями генерации и хранения паролей, хотя для большей безопасности не стоит ими злоупотреблять, так как любое приложение также можно взломать. Пароль обязательно должен содержать цифры, буквы (желательно на английской раскладке) и специальные символы (например, восклицательный знак или

знак подчеркивания). Длинна пароля должна быть не меньше 8 знаком. Все это очень затруднит работу хакеру, поскольку взломать пароль методом простого перебора он не сможет.

2. Мониторинг сторонних приложений.

Проходя авторизацию на любом стороннем сервисе или используя сторонний сервис для более удобного общения в соцсетях, вы тем самым даете доступ к своему аккаунту. Трудно отслеживать все приложения, которым вы дали разрешение на доступ в профили в социальных сетях, но важно знать и понимать, что внешние сайты могут привести вас к взлому вашего профиля. В каждой из соцсетей в настройках есть функция отключения сторонних приложений.

3. Не переходите по ссылкам, о природе которых вы не знаете.

Вы получили в личные сообщения или в комментарий в ленте какую-то ссылку. Не нажимайте, если вы подозреваете, что ссылка может вести на вредоносный ресурс. Особенно, никогда не нажимайте сокращенную ссылку, по которой не видно на какой вообще сайт она вас перенаправляет. По статистике, 84% всех сокращенных ссылок ведут на вредоносные сайты.

4. Обновляйте операционную систему и антивирусные программы на своем гаджете.

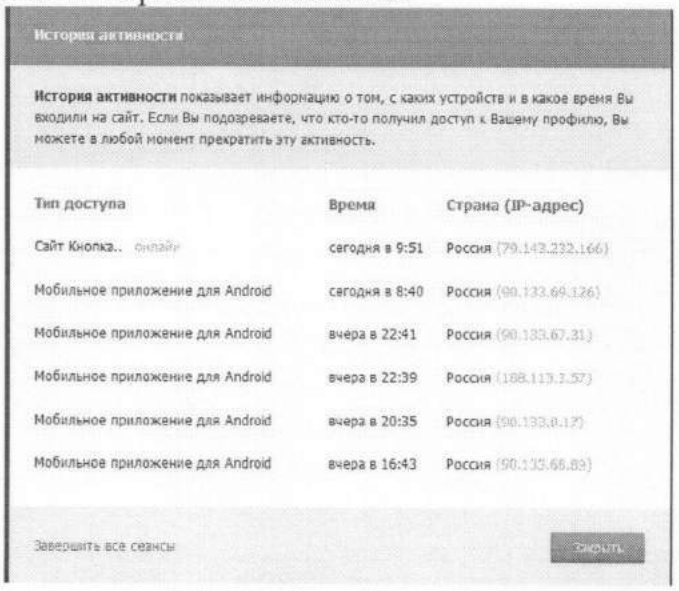
Этим вы избавите себя от «дыр» в системе, которые успевают найти злоумышленники и использовать их в своих зловредных целях.

5. Всегда выходите из своих аккаунтов по завершении работы.

Особенно это касается, если вы вошли в свой профиль с чужого компьютера. Да и на своем гаджете нужно взять в привычку совершать выход из соцсети, лучше лишний раз завтра набрать пароль, чем быть взломанным по такой простой причине.

Так как большинство студентов предпочитают общаться в соцсети ВКонтакте, то мы рассмотрели, какие рекомендации дает служба поддержки по отслеживанию посещения (взлома) аккаута пользователя.

Заходим в настройки, находим «Безопасность Вашей страницы», открываем «Посмотреть историю активности»



По типу доступа мы можем отследить: откуда и когда заходил на аккаунт пользователь. Следовательно, если Вы в указанное место не пользовались своим аккаунтом, то им воспользовался кто-то другой. Делайте вывод!

Кроме того, команда «Завершить все сеансы» позволит Вам в любое время с любого компьютера выполнить завершение всех случайно не завершенных сеансов. Но лучше не забывать завершать сеанс сразу!

Делая вывод по выполненному исследованию, рекомендуем всем помнить: если вы хотите жить в информационном и безопасном обществе, то каждый из нас должен задуматься, о том какую культуру личной безопасности он несет через использование социальных сетей.

Источники

1. http://www.ugrozenet.ru/kompyuternaya-bezopasnost/143-zaschita-ot-vzloma-v-socialnyh-setyah.html - сайт Информационная программа безопасности граждан

2. http://flapps.ru/istoriya-aktivnosti-v-kontakte - сайт Советы пользователям ВК

3. http://vostanovlenie-dannyx.ru/obsuzhdeniya/266 - сайт Восстановление данных (программы, советы, обсуждения)

Приложение 10

ОПИСАНИЕ ПРОЕКТА

Номинация – МОЯ РАЗРАБОТКА

Тема проекта – ОРГАНИЗАЦИЯ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ДЕТЕЙ ОТ НЕЖЕЛАТЕЛЬНОЙ (ВРЕДОНОСНОЙ) ИНФОРМАЦИИ ИЗ СЕТИ ИНТЕРНЕТ

Авторы проекта: Положенцев Илья, Милютиков Павел
Научные руководители: Жигалева О.Л., Ковальцов М.В.
ОБОУ СПО «Железногорский горно-металлургический колледж»,
г. Железногорск Курской области

Актуальность исследования. Значимость Интернета в современной жизнедеятельности человека очень важна. Сегодня любой человек, имеющий доступ к компьютеру с подключением Интернет, может получить любую информацию за пару кликов и нажатий на кнопки клавиатуры. Численность аудитории Интернета растёт с очень большой скоростью.

Интернет предоставляет большие возможности для получения самой разнообразной информации, но при этом **противоречие** заключается в том, что часть содержания информации на различных сайтах практически никак не контролируется и носит нежелательный характер для восприятия определенными возрастными группами людей.

Проблема исследования. Законодательство РФ определяет ряд требований и ограничений по разработке, размещению, использованию и передаче информации, которая может причинить вред здоровью и развитию детей. На различных сайтах Интернета размещена информация с рекомендациями по применению программно-аппаратных средств для обеспечения безопасности детей. Однако, зачастую родители или лица, ответственные за детей, по разным причинам (незнание, халатность), не отслеживают получение детьми из глобальной сети информации, в том числе нежелательной (вредоносной). Проблема состоит в отсутствии механизма ознакомления взрослых с правовыми и программными средствами обеспечения защиты детей от нежелательной (вредоносной) информации из сети Интернет.

Объект исследования: обеспечение защиты от нежелательной информации из сети Интернет.

Предмет исследования: правовые и программные средства обеспечения защиты детей от нежелательной (вредоносной) информации из сети Интернет.

Цель проекта: подготовка и организация мероприятий по пропаганде применения эффективных программно-аппаратных средств обеспечения защиты детей от нежелательной информации из сети Интернет среди родителей и лиц, ответственных за здоровье и развитие детей.

Задачи проекта (уже реализованные):

- изучить различные источники по проблеме защиты детей от вредоносной информации;
- проанализировать законодательную базу Российской Федерации по защите детей от информации, которая может нанести им вред;
- проанализировать возможности программного регулирования по обеспечению защиты детей от вредоносной информации из сети Интернет;
- разработать оптимальный комплекс программно-аппаратных средств, которые смогут эффективно обеспечивать защиту ребёнка от вредоносной информации при нахождении в сети Интернет;
- разработать анкету для родителей с целью тестирования и получения статистических данных по проблеме исследования;
- разработать памятку с рекомендациями для родителей и лиц, ответственных за здоровье и развитие детей, по защите детей от нежелательной (вредоносной) информации из сети Интернет..

Задачи проекта (требующие реализации):

- проведение мероприятий по пропаганде безопасного для детей Интернета через применение комплекса программно-аппаратных средств защиты.

Информационную базу исследования составили Федеральные законы РФ в области защиты детей от информации, причиняющей вред их здоровью и развитию, сайты производителей программно-аппаратных средств защиты (антивирусные программы, программы блокирования рекламы), статьи по исследованию проблемы защиты детей от информации, причиняющей вред.

Сроки реализации

Проект готов к реализации.

Проект с учетом постоянного обновления рекомендаций по программно-аппаратному обеспечению является **бессрочным**.

Актуальность проекта может регулироваться через проведение мониторингов.

Общие сведения по проблеме исследования

В настоящее время, время информационных войн, очень важно уметь правильно и объективно оценивать текущую ситуацию во многих областях жизнедеятельности человека. Через средства массовой информации и телекоммуникационные сети ведется интеллектуальная борьба. И если официальные каналы телевидения выполняют определенные функции цензуры, то контролирование информации на сайтах безграничного Интернета связано с рядом сложностей.

Сетью Интернет пользуется глобальная аудитория, которая состоит из разных полов, возрастов, этнических групп, интеллектуальной развитости. Многие люди, видя информацию в сети Интернет, начинают ей сразу доверять, не понимая при этом, что информация эта «не фильтрована» и может нести в себе самую разнообразную негативную информацию. Самым доверчивым

звеном в нашем обществе являются пожилые люди и дети. Мы обратили внимание на детей.

В рамках проекта были изучены законы РФ, такие как ФЗ РФ от 24 июля 1998 г. N 124-ФЗ "Об основных гарантиях прав ребенка в Российской Федерации", ФЗ РФ от 13 марта 2006 г. N 38-ФЗ «О рекламе», ФЗ от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Данные законы вводят ряд ограничений на производство, использование и размещение вредоносной информации в местах доступных для детей.

Дети очень любознательны, поэтому всюду ищут информацию, от любимого супергероя, до звёзд Вселенной. И в этом им очень помогает «Кладезь информации» - Интернет. Открывая сайты, ребенок не обращает внимания на ряд факторов: название сайта, ссылку, на которую осуществится переход, иконку сайта, пометку от поисковой системы, является ли этот сайт вредоносным или нет, и получает доступ к нежелательной информации. К такой информации могут относиться любые сведения, к которым ребёнок не должен получить доступ: экстремистская, суицидальная, расистская, очень жестокая (насильственная) информация, информация с эротическим содержанием.

Очень часто «благодаря» родителям уже с раннего возраста дети получают доступ в мировую паутину. Мы не будем отрицать, что Интернет несёт в себе много хорошего – возможность быстрого поиска, огромное количество познавательной информации, развлечения и многое другое. Но наличие большого количества сайтов, которые несут в себе материалы, не предназначенные для детской психики, определяет необходимость контролирования ресурсов, которые посещает ребёнок.

На страницах Интернета мы можем найти много описаний способов, которые помогут оградить ребёнка от нежелательной информации. Способы можно условно разделить на две группы: теоретические и практические.

Мы считаем, что для обеспечения полноценной безопасности необходимо соблюдать все аспекты:

1. Теоретический аспект - законодательное регулирование со стороны государства, пропаганда среди родителей безопасного использования Интернет детьми, правил поведения в нём.

2. Практический (программный) аспект - установка плагинов, программ, утилит.

Полностью оградить ребёнка от нежелательной информации в Интернете можно только отключив подключение к нему, так как программные средства совершенствуются с каждым днём, а компании, разрабатывающие защиту от нежелательной информацией, не успевают вносить в реестр способы защиты от неё. Но можно обеспечить приближенную к максимальной степени защиту, установив специальный комплекс программ, плагинов и утилит.

Главное правило, чтобы эти программные средства были совместимы и не конфликтовали между собой.

К таким программным и программно-аппаратным средствам относятся:

1. Надёжный браузер.
2. Антивирусная программа.
3. Программы, блокирующие рекламу, «всплывающие» сайты.
4. Настройка через DNS.
5. Дополнительно можно использовать плагины и утилиты для браузеров или работающие самостоятельно.

В ходе реализации проекта нами были изучены возможности разных программных или программно-аппаратных средств из указанного списка. Что позволило разработать наиболее оптимальный комплекс, позволяющий обеспечить защиту детей от нежелательной (вредоносной) информации из сети Интернет. Данный комплекс входит в рекомендации для родителей и лиц, ответственных за здоровье и развитее детей (Приложение 1).

Для установления сложившейся обстановки в городе по вопросам регулирования родителями доступа детей в Интернет была разработана анкета (Приложение 2), которая также позволит осуществлять мониторинг результатов проведения пропагандистской деятельности по применению программно-аппаратных средств, позволяющих обеспечить защиту детей от нежелательной (вредоносной) информации из сети Интернет

Если при работе с интернетом выполнены хотя бы 3 пункта из предложенного комплекса, то защита будет обеспечена на 60-70%. А если все 5 – то до 95%. Остальные проценты будут всегда присутствовать из-за человеческого фактора.

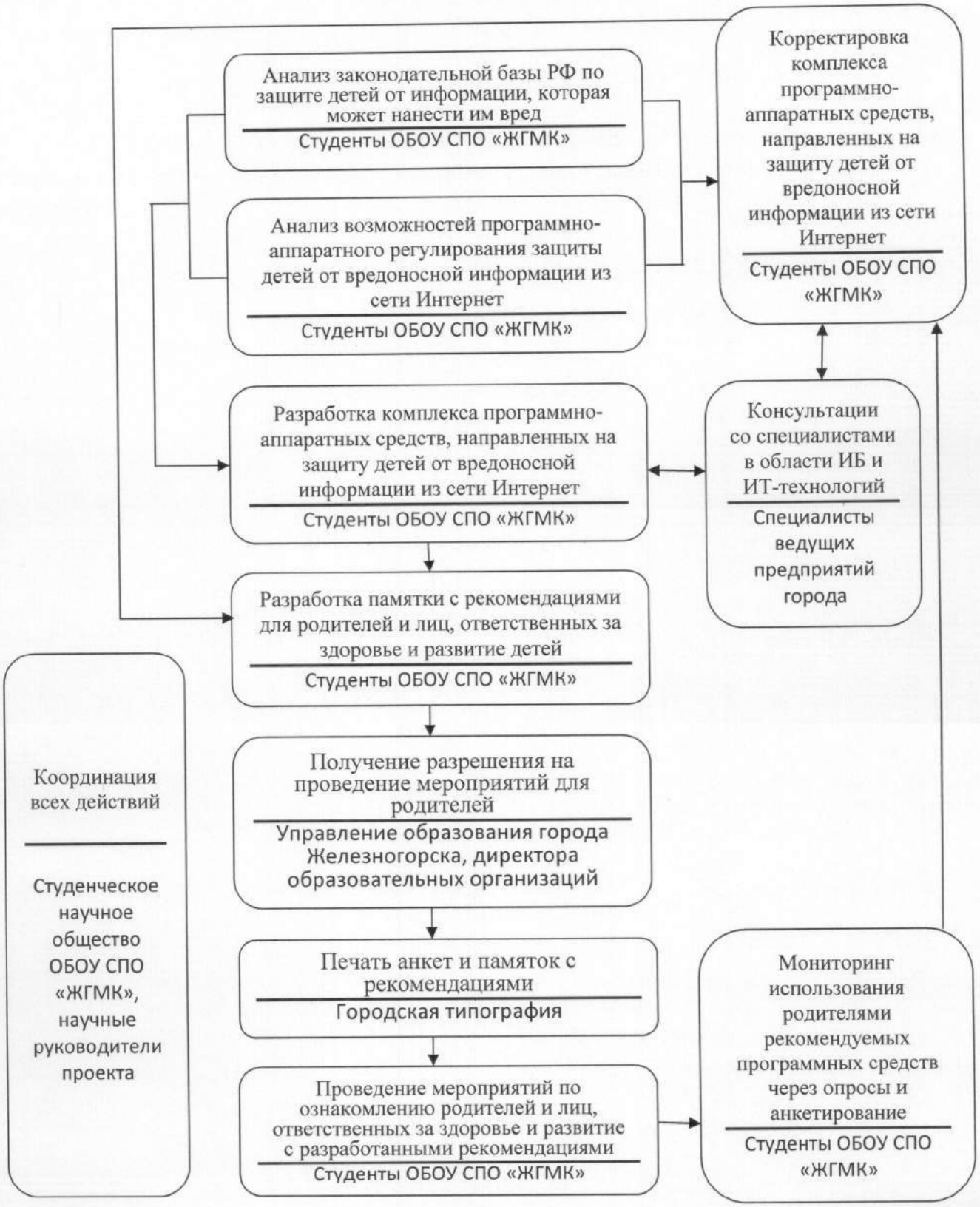
Не стоит также забывать, что информационные технологии развиваются стремительно и необходимо отслеживать обновления для используемых программных продуктов. Иначе предложенные средства станут неэффективными.

План реализации проекта

1. Постоянное изучение различных источников по проблеме защиты детей от вредоносной информации;
2. Проведение систематического анализа законодательной базы Российской Федерации по защите детей от информации, которая может нанести им вред;
3. Проведение систематического анализа возможностей программно-аппаратного регулирования защиты детей от вредоносной информации из сети Интернет;
4. Разработка и корректировка перечня рекомендуемых программно-аппаратных средств, которые направлены на обеспечение защиты детей от вредоносной информации при нахождении их в сети Интернет;
5. Внесение актуальных изменений в памятку с рекомендациями для родителей и лиц, ответственных за здоровье и развитие детей, по защите детей от нежелательной (вредоносной) информации из сети Интернет.
6. Печать материалов для проведения пропагандистской деятельности в рамках реализации проекта.

7. Проведение мероприятий по пропаганде безопасного для детей Интернета через применение комплекса программно-аппаратных средств защиты.

Механизм реализации проекта и схема управления проектом в рамках территории



Кадровое обеспечение проекта с описанием количественного и качественного потенциала команды проекта

Кадровое обеспечение проекта	Обязанности в рамках реализации проекта	Количество
Студенты специальности 10.02.03 «Информационная безопасность автоматизированных систем» или специальностей связанных с IT-технологиями	Отслеживание новых технологий в области защиты от нежелательной (вредоносной) информации с помощью программно-аппаратных средств.	1
Студенты специальности 10.02.03 «Информационная безопасность автоматизированных систем» или специальностей связанных правовой деятельностью	Анализ законодательной базы РФ в области защиты детей от нежелательной (вредоносной) информации.	1
Специалисты в области ИБ и ИТ-технологий ведущих предприятий города	Консультирование по вопросам актуальности рекомендуемых средств защиты детей от вредоносной информации из сети Интернет	2-3
Студенты образовательных учреждений города	Волонтеры, осуществляющие деятельность по пропаганде безопасного для детей Интернета через применение комплекса программно-аппаратных средств защиты.	4-7 (зависит от количества ОУ, в которых необходимо провести мероприятия)
Председатель студенческого научного общества и научные руководители проекта	Общая координирующая деятельность	2-3
	Всего:	10-15

Критерии оценки эффективности проекта

Основными критериями эффективности проекта являются показатели мониторинга использования рекомендованных программно-аппаратных средств защиты от нежелательной (вредоносной) информации, проводимого среди родителей и лиц, ответственных за здоровье и развитие детей.

Мониторинг может проводиться:

- в форме опроса респондентов;
- в форме анкетирования респондентов.

Предполагаемые конечные результаты, перспективы развития проекта, долгосрочный результат

Прогнозируемые конечные результаты реализации проекта:

– выполнение законодательства РФ в области защиты детей от нежелательной (вредоносной) информации из сети Интернет;

– формирование информационной культуры у родителей, лиц, ответственных за детей, студентов – будущих родителей, у детей.

Пропагандистская деятельность призвана повысить ответственность родителей за воспитание и за будущее своих детей. Правильное использование информации из сети Интернет, которая не будет наносить вред здоровью и развитию детей, послужит основой для гармоничных отношений в семье, в обществе.

Ресурсное обеспечение проекта

Для реализации проекта необходимы материальные затраты на печатную продукцию:

- анкеты;
- памятки с рекомендациями,

а также на транспортные расходы для волонтеров для поездок в ОУ для проведения мероприятий описанных в проекте.

Порядок контроля и оценки результатов проекта

Контроль за реализацией проекта возлагается на Студенческое Научное Общество образовательного учреждения (в нашем случае - колледжа), на ежемесячных заседаниях которого заслушиваются результаты проведенных мероприятий. Координационную деятельность осуществляют научные руководители проектов. План проведения мероприятий согласовывается с Управлением образования города и директорами ОУ.

Результаты проведения мероприятий представляются на конференциях, в виде статей по обмены опытом.

Главную оценку эффективности реализации проекта дают родители, учителя, воспитатели по результатам их анкетирования.

Приложение 1

ПАМЯТКА И РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ДЕТЕЙ ОТ НЕЖЕЛАТЕЛЬНОЙ (ВРЕДОНОСНОЙ) ИНФОРМАЦИИ ИЗ СЕТИ ИНТЕРНЕТ

Уважаемые родители и лица, ответственные за здоровье и развитие детей!

ПОМНИТЕ, что кроме полезной информации, получаемой из сети Интернет, ваши дети могут получить доступ к информации несущей экстремистский, суицидальный, расистский характер, к жестокой (насильственной) информации, информации с эротическим содержанием.

Последствия ознакомления ребенка с нежелательной информацией.

	Расстройства психики	Зависимость	Физический вред здоровью	Оскорбление чувств
Реклама	–	–	+	+
Сайты для взрослых	+	+	+	+
Сайты пропаганды	+	+	+	+
Наркотики	+	+	+	–
Насилие	+	–	+	–

Парадокс Интернета: соединяет людей находящихся далеко друг от друга, разъединяет тех, кто рядом.

Поэтому, если Вы хотите быть ближе к своим детям и защитить их, в Ваших интересах должно быть соблюдение самими и донесение до детей следующей информации:

1. Необходимо следить за адресами, на которые ведут ссылки. Для того, чтобы узнать адрес, на который ведет ссылка необходимо просто навести на неё курсор. Если Вам предлагают перейти на сайт с одним адресом, а ссылка ведет на совершенно другой, то тут что-то не так.

2. Перед вводом личной информации проверяйте адресную строку браузера. Если Вы там увидите что-то вроде vkontokte.ru вместо привычного vkontakte.ru, то можете быть уверенны, что Вы находитесь на поддельном сайте и у Вас пытаются украсть пароль для доступа к Вашему аккаунту.

3. Не переходите по незнакомым ссылкам, которые приходят Вам на почту, в социальные сети или другие файлообменные ресурсы. Даже если ссылка пришла от знакомого человека необходимо быть максимально внимательным. Вполне возможно аккаунт вашего знакомого уже взломан, и теперь от его имени рассылают вирусы.

4. Не скачивайте неизвестные файлы, даже если файл пришел от Вашего знакомого. Перед тем как скачивать его уточните у отправителя, что он представляет собой, для чего он.

5. Современные поисковые системы и браузеры, например, такие как GoogleChrome, умеют предупреждать пользователя, когда он пытается зайти на сайт распространяющий вирусы или вредоносные программы. Необходимо внимательно относиться к таким предупреждениям.

6. Не кликайте по рекламным баннерам.

7. Относитесь с подозрением к программам для «взлома» онлайн сервисов, игр и программ. В результате использования таких программ жертвой «взлома» можете стать именно Вы.

8. Будьте внимательны к файлам, загружаемым через файлообменные ресурсы. Пользователи данных сетей могут распространять вирусы, даже не подозревая об этом.

9. Не используйте старые версии InternetExplorer, так как они «не фильтруют» ссылки, которые открываются в процессе работы в Интернете. Если Вы используете этот браузер, то используйте последние версии, более новые, например, версию 11.

10. Отключите JavaScript. Большая часть сайтов отлично работает без его использования. Для браузера MozillaFirefox можно использовать плагин Noscript, данное расширение позволяет отключать выполнение скриптов только для неизвестных сайтов, что очень важно в нашем аспекте.

продолжение Приложения 1

Комплекс программных средств, позволяющих обеспечить защиту Ваших детей от доступа к вредоносной информации в Интернет

Вид защиты	Рекомендуемые программно-аппаратные средства
Браузеры	Maxthon (Версия 4). Google Chrome (плагин Adblockplus) ComodoIceDragon.
Антивирусные программы	PandaCloudAntivirus. AVG AntiVirusFree. AvastFreeAntivirus.
Программы, блокирующие рекламу, «всплывающие» сайты	Adguard Pop-Up Stopper (Версияот 3.10.1014)
Фильтрация DNS	Яндекс.DNS OpenDNSFamilyShield (OpenDNS Семейный Щит)

Рекомендуется установить стандартную страницу поиска Семейный поиск Яндекс, который поможет вам оградить ребёнка уже с самого начала запуска браузера. Для этого необходимо выполнить следующие действия:

1. Войдите в настройки браузера: Верхний правый значок из трёх горизонтальных линий → Настройки.
2. Выберите: Начальная группа → Следующие страницы.
3. Нажмите Добавить, в поле Добавить страницу впишите «http://family.yandex.ru»

Настройка фильтрации DNS на мобильных устройствах (смартфонах, планшетах) осуществляется следующим образом:

1. Введите IP-адрес роутера в браузере, чтобы зайти в панель администратора.
2. Введите имя пользователя и пароль.
3. В меню управления роутером найдите настройки DNS-сервера.
4. Пропишите адрес Яндекс.DNS (77.88.8.7) в качестве Primary DNS-сервера и сохраните изменения. В поле Secondary DNS-сервера пропишите адрес OpenDNSFamilyShield (208.67.222.123).

Настройка фильтрации DNS для компьютера (ноутбука) выполняется следующим образом:

1. Откройте меню Пуск → Настройка → Панель управления → Сетевые подключения.
2. Щелкните правой кнопкой мыши на нужном сетевом подключении и выберите пункт Свойства.
3. В окне свойств подключения выберите пункт Протокол Интернета (TCP/IP) и нажмите кнопку Свойства.
4. В открывшемся окне выберите пункт Использовать следующие адреса DNS-серверов.
5. Введите адрес Яндекс.DNS 77.88.8.7 в качестве Предпочитаемый DNS-сервер. В поле Альтернативный DNS-сервер пропишите адрес OpenDNSFamilyShield 208.67.222.123. И сохраните изменения кнопкой Ок.

Данный метод защиты через DNS описан для ОС Windows, для других операционных систем настройка DNS практически идентична.

Если у вас стоит браузер GoogleChrome, то необходимо установить плагин Adblockplus, который поможет в ограждении вашего ребёнка от непристойных баннеров и сайтов с нежелательной информацией. Для этого необходимо выполнить следующие действия:

1. Войдите в настройки браузера: Верхний правый значок из трёх горизонтальных линий → Настройки.
2. Выберите слева Расширения → Ещё расширения.
3. Поищите AdBlock, который появится в категории Расширения.
4. Установите кнопкой Бесплатно.

Так же можно установить программу «Интернет Цензор Лайт», которая устанавливается как дополнение к веб-браузеру MozillaFirefox и обеспечивает фильтрацию только для данного браузера.

Описанные программно-аппаратные средства Вы можете установить самостоятельно или это может сделать по Вашей просьбе специалист при установке программного обеспечения на Ваш компьютер.

ПОМНИТЕ, ЧТО ВЫ В ОТВЕТЕ ЗА ВАШИХ ДЕТЕЙ!

Приложение 2

Анкета по определению использования средств защиты детей от нежелательной (вредоносной) информации из сети Интернет

1. Имеет ли Ваш ребенок доступ к Интернету?
a) Да
b) Нет
c) Не знаю

2. Много ли вы знаете о том, что делает ваш ребёнок в Интернете?
a) Много
b) Умеренное количество
c) Немного
d) Нисколько

3. Есть ли у Вашего ребёнка электронная почта?
a) Да
b) Нет
c) Не знаю

4. Знаете ли вы пароли от учётных записей электронной почты, социальных сетей Вашего ребёнка?
a) Да
b) Нет
c) Не все

5. Где чаще всего использует Интернет Ваш ребёнок?
a) Дома, в своей собственной комнате
b) Дома, в комнате, где другие члены семьи тоже имеют доступ к нему
c) В школе
d) В доме друга
e) В другом месте (указать) _____

6. Как часто вы позволяете Вашему ребёнку пользоваться Интернетом одному (без наблюдения и учета времени)?
a) Всегда
b) Большую часть времени
c) Около половины всего времени
d) Изредка
e) Никогда не позволяем

7. Сколько времени проводит Ваш ребенок в сети Интернет.
a) До одного часа в день
b) Примерно час в день
c) До трех часов в день
d) Более трех часов в день
e) Не знаю

8. Вы используете на домашнем компьютере антивирусные программы.
a) Да. Укажите, какие программы _____
b) Нет. Укажите почему _____

10. Какие программные средства Вы применяете, чтобы обеспечить безопасную работу Вашего ребенка в сети Интернет:
a) самостоятельно устанавливаю программное обеспечение, позволяющее отключать доступ к нежелательным сайтам. Укажите, какие программы _____
b) при покупке домашнего компьютера, нам установили программное обеспечение, позволяющее отключать доступ к нежелательным сайтам. Укажите, какие программы _____
_____
c) ни каких мер не принимаю, так как ничего об этом не знаю
d) ни каких мер не принимаю, так как считаю это бесполезным занятием.

СПАСИБО ЗА УЧАСТИЕ В АНКЕТИРОВАНИИ!

Приложение 11

РАССМОТРЕНО

на заседании цикловой комиссии
специальности 090305
Протокол № 3 от 14.11.2013
Председатель ЦК

_____ О.Л. Жигалева

14.11.2013

СОГЛАСОВАНО

Зам.директора по ВР

_____ Л.Н. Головачева

15.11.2013

ПРОГРАММА
недели специальности 090305
«Информационная безопасность автоматизированных систем»

25.11.13 – открытие недели специальности, демонстрация презентаций и газет

26.11.13 – классные часы в группах 1, 2, 3, 4 курсов колледжа и на отделении профориентации и подготовки школьников

27.11.13 – день самоуправления

28.11.13 – классные часы в группах 1, 2, 3, 4 курсов колледжа и на отделении профориентации и подготовки школьников

29.11.13 – олимпиада по специальности 090305

30.11.13 – Подведение итогов недели специальности.
Международный день защиты информации!

ТЕМАТИКА КЛАССНЫХ ЧАСОВ:

1) Защита персональных данных в законодательстве Российской Федерации

2) Защита персональных данных в социальных сетях

3) Развитие хакерства

4) Вирусы: особенности, последствия

5) История криптографии

Приложение 12

УДК
Медведева Ангелина Алексеевна
retro7999@yandex.ru
Научный руководитель – к.п.н., Жигалева Ольга Леонидовна
ОБПОУ «Железногорский горно-металлургический колледж»

Анализ редакций Федерального закона N 149-ФЗ «Об информации, информационных технологиях и защите информации»

Правовая защита в информационной сфере является составляющей информационной безопасности, которая представляет собою совокупность решений, законов, нормативов, регламентирующих как общую организацию работ по обеспечению информационной безопасности, так и создание и функционирование систем защиты информации на конкретных объектах.

Создаваемые в ходе работы по обеспечению информационной безопасности организационно-правовые базы обеспечивают нормативную сторону юридической защиты информации. Также они создаются и для выполнения следующих функций:

1.Разработка основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации;

2. Определение системы органов и должностных лиц, ответственных за обеспечение ИБ в стране и порядка регулирования деятельности предприятия и организации в этой области.

Определение основных понятий информации, информационных технологий и защиты информации, мер ответственности за нарушения правил защиты, а также определение порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации регулируется Федеральным законом № 149-ФЗ "Об информации, информатизации и защите информации".

В связи со стремительными изменениями в области IT-технологий и в области защиты информации, необходимы изменения и в юридической защите информации, но разработка законодательной базы – это более длительный процесс и связана с различными аспектами.

ФЗ № 149 "Об информации, информационных технологиях и о защите информации" был принят Государственной Думой 8 июля 2006 года. Попытаемся проанализировать редакции ФЗ «Об информации, информационных технологиях и защите информации» за последние пять лет.

В 2010 году было внесено определение электронного документа (ст 2 п.11.1), а также требование к государственным органам и органам местного самоуправления по обеспечению доступа к информации о своей

деятельности с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» (ч.5 ст.8).

В статье 11 части 3 было определено, что «электронный документ, электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признаются равнозначными документу, подписанному собственноручной подписью, в случаях, если иное не установлено федеральными законами». Для информации, содержащейся в ГИС должны быть обеспечены актуальность и достоверность, а также ее защита от любых неправомерных действий (ч.9 ст.14).

В 2010 году был принят Федеральный закон от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" и появилась необходимость внесения изменений связанных с согласованием с этим новым законом в виде дополнения в части 1 статье 12 дополнение «4) обеспечение информационной безопасности детей». Также в связи с принятием нового Федерального закона от 06.04.2011 N 63-ФЗ "Об электронной подписи" были внесены изменения в статью 11 части 4, в которой понятие «цифровая электронная подпись» заменено на «цифровая подпись».

Редакции 2012 года связаны с вопросами сайтов в сети Интернет (ст.2 п. 13-18). Введены новые понятия: сайт в сети «Интернет», страница сайта, доменное имя, сетевой адрес, владелец сайта, провайдер хостинга. И была добавлена статья 15.1 «Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено».

В 2013 году было три редакции ФЗ, они также затрагивали вопросы распространения информации через сеть «Интернет». Например, была введена статья 15.3. Порядок ограничения доступа к информации, распространяемой с нарушением закона.: «1. В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, включая случай поступления уведомления о распространении такой информации от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан, Генеральный прокурор Российской Федерации или его заместители направляют требование в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению доступа к

информационным ресурсам, распространяющим такую информацию…».

Редакция ФЗ от 28.12.2013 связана с внесением изменений в законодательные акты по контрактной системе (размещению заказов) в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд. Данные работы выполняются через сервисы Интернет и поэтому требуют защиты конфиденциальной информации.

Изменения и дополнения, касающиеся интеллектуальной деятельности были внесены в соответствии с Федеральным законом от 02.07.2013 N 187-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях" и были определены в основном определением порядка ограничения доступа к информации, распространяемой с нарушением исключительных прав на фильмы, в том числе кинофильмы, телефильмы. Были добавлены новые понятия, например, «единая система идентификации и аутентификации - федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах».

Дополнены пункты о общедоступной информации, размещаемой ее обладателем в сети «Интернет» и об информации составляющей государственную тайну.

В 2014 году было четыре редакции ФЗ.

Была дополнена статья 10. Распространение информации или предоставление информации следующими статьями:

– Статья 10.1. Обязанности организатора распространения информации в сети "Интернет";

– Статья 10.2. Особенности распространения блогером общедоступной информации.

Продолжено дополнение статьи 15 по использованию информационно-телекоммуникационных сетей, связанное с порядком ограничения доступа к информации, распространяемой с нарушением закона (ст. 15.3).

Следующая редакция была связана с дополнениями, касающимися государственного регулирования деятельности по организации и проведению азартных игр и запрета деятельности по организации и проведению азартных игр и лотерей с использованием сети "Интернет" и иных средств связи.

Редакция от 24.11.2014 внесла много изменений и дополнений в статью 15, большинство из которых были связаны с защитой смежных и авторских прав. Дополненная статья 15.5. рассматривает порядок ограничения доступа к информации, обрабатываемой с нарушением

законодательства Российской Федерации в области персональных данных.

Важное дополнение то, что обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить нахождение на территории РФ баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации. А также технические средства информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями, должны размещаться на территории Российской Федерации.

Редакции 2015 года касались обязанностей оператора поисковой системы (ст.10.3), который обязан прекратить выдачу сведений об указателе страницы сайта в сети "Интернет", позволяющих получить доступ к информации о заявителе, распространяемой с нарушением законодательства Российской Федерации. Статья 12.1. Особенности государственного регулирования в сфере использования российских программ для электронных вычислительных машин и баз данных добавлена «в целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из Российской Федерации, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки создается единый реестр российских программ для электронных вычислительных машин и баз данных».

Последняя редакция, вступившая в силу 10.01.2016 связана с требованиями к электронному документообороту органов государственной власти и органов местного самоуправления, что в свою очередь связано с увеличением электронного документооборота при взаимодействии физических и юридических лиц с органами государственной власти и органами местного самоуправления.

Таким образом, из сделанного обзора редакций ФЗ «Об информации, информационных технологиях и защите информации» можно сделать вывод, что необходимо отслеживать изменения и дополнения в основные законодательные акты в сфере защиты информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Сёмкин С.Н., Сёмкина А.Н. Основы правового обеспечения защиты информации. – М.: Горячая Линия - Телеком, 2008. — 238 с.

2. https://www.consultant.ru/document/cons_doc_LAW_61798/ – Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 13.07.2015) "Об информации, информационных технологиях и о защите информации" (с

изм. и доп., вступ. в силу с 10.01.2016)

3. https://www.consultant.ru/document/cons_doc_LAW_103797/5d573377380450dceccfaf1074551bcfcedd8173/#dst100019 – Обзор изменений Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

Приложение 13

Теребрина Анастасия Сергеевна
E-mail: terebrina99@mail.ru
Научный руководитель – к.п.н., Жигалева Ольга Леонидовна
ОБПОУ «Железногорский горно-металлургический колледж»

ИССЛЕДОВАНИЯ POSITIVE TECHNOLOGIES И АНКЕТИРОВАНИЕ РЕСПОНДЕНТОВ ПО ПАРОЛЬНОЙ ЗАЩИТЕ

В процессе обучения по специальности 10.02.03 Информационная безопасность автоматизированных систем в ОБПОУ «ЖГМК» изучаются программные продукты компании Positive Technologies, которая более 10 лет аккумулирует экспертные знания по практической безопасности и является одним из мировых лидеров в области комплексной защиты крупных информационных систем от современных киберугроз. Продукты и услуги Positive Technologies обеспечивают:

- анализ защищенности и оценку соответствия стандартам;
- мониторинг событий безопасности и предотвращение вторжений;
- блокирование атак, включая ранее неизвестные (0-day);
- расследование инцидентов и оценку защитных мер;
- анализ безопасности кода приложений и построение безопасной разработки.

Наиболее распространенной уязвимостью ресурсов внутренней сети, которой уделяют постоянное внимание исследователи компании Positive Technologies, является использование слабых паролей, которые были обнаружены во всех исследованных системах (рисунок 1).

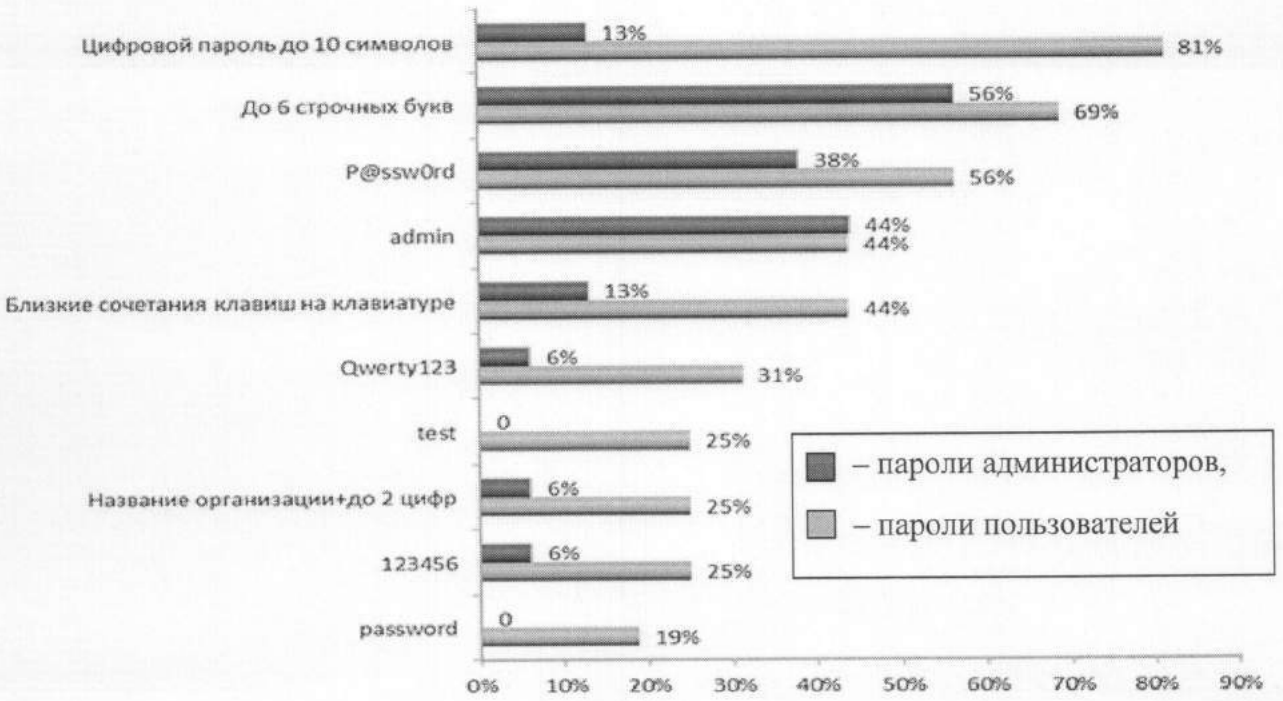
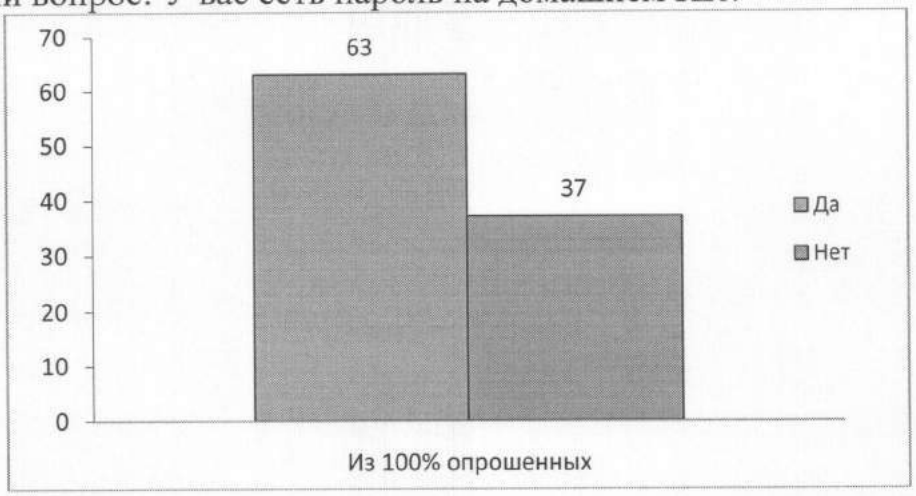


Рисунок 1 – Доли систем со словарными паролями в 2014 году.

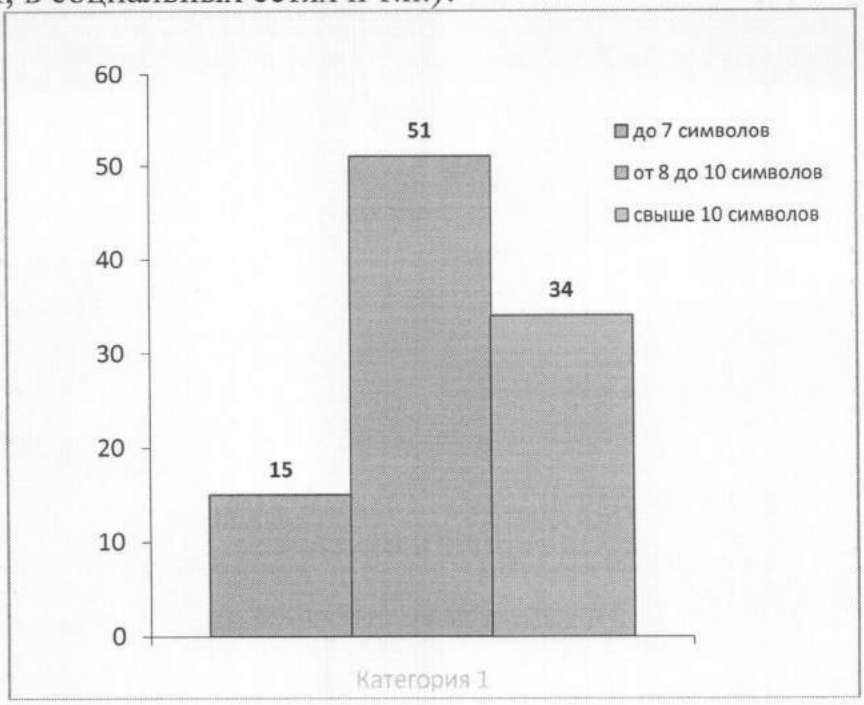
Хотя эксперты из области информационной безопасности уже устали постоянно предупреждать всех о том, что неосторожность людей — это главный фактор потери конфиденциальной информации, пользователи, как всегда думают, что им ничего не грозит. Результат такой самонадеянности очевиден – утраченная информация, взломанные аккаунты, обвинения в рассылке спама и прочие неприятности.

В колледже было проведено анонимное анкетирование респондентов, в качестве которых выступали как студенты, так и преподаватели. Всего было задано 5 вопросов, на которые они должны были ответить максимально честно. Было опрошено 209 человек

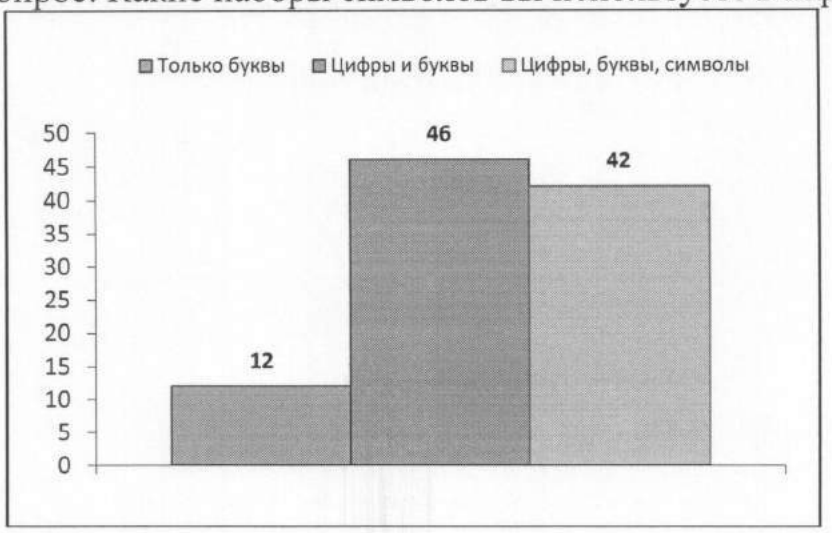
Первый вопрос: У вас есть пароль на домашнем ПК?



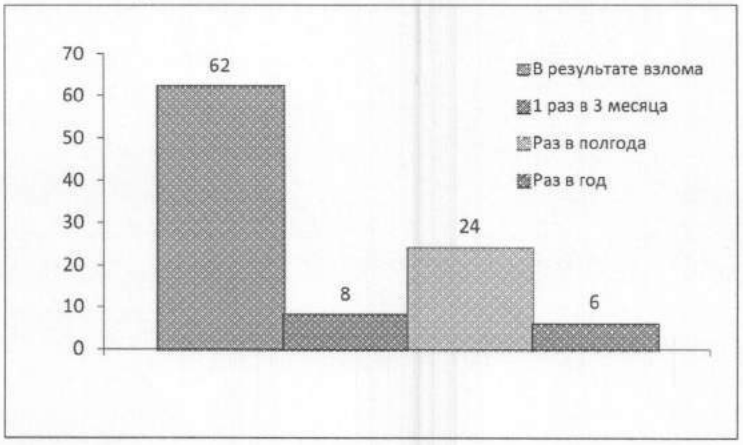
Второй вопрос: Какая длина используемого вами пароля (на домашнем ПК, в социальных сетях и т.п.)?



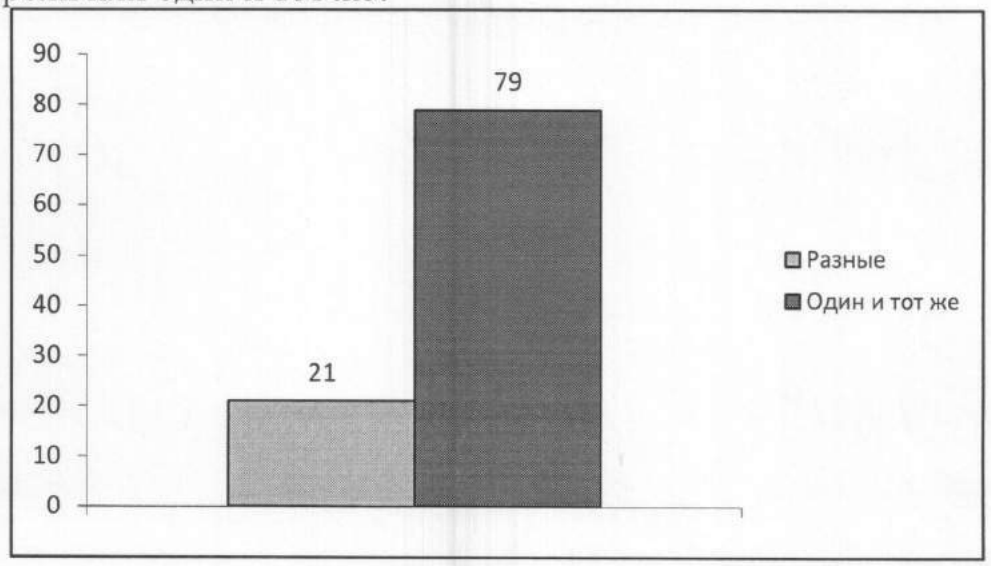
Третий вопрос: Какие наборы символов вы используете в паролях?



Четвертый вопрос: Как часто вы меняете свой пароль?



Пятый вопрос: При разных аккаунтах и профилях Вы используете разные пароли или один и тот же?



По результатам анкетирования можно сделать вывод, что у большинства опрашиваемых респондентов есть пароль на домашнем ПК, но в большинстве случаев пароль ненадежный, к сожалению, большое число респондентов меняет пароль только в случае явного обнаружения взлома и на разных аккаунтах использует один и тот же пароль.

Проведенный анализ показывает на необходимость проведения системных разъяснительных мероприятий для молодых людей, которые в скором будущем придут на предприятия и могут стать внутренними нарушителями из-за того, что недостаточно осведомлены в вопросах защиты информации и не владеют культурой информационной безопасности.

К основным рекомендациям по парольной защите для рядового пользователя являются: длина – не менее 8-ми символов, использование верхнего и нижнего регистров, цифр, букв и символов, смена пароля раз в 3 месяца, а также не рекомендуется использовать один и тот же пароль на разных учетных записях и аккаунтах. Это очень актуально в связи с тем, что большинство взломов сегодня происходит через сеть Интернет.

Источники:

http://www.ptsecurity.ru/about/news/40925/?sphrase_id=24726 – Главные уязвимости корпоративных информационных систем в 2014 году: веб-приложения, пароли и сотрудники

Приложение 14

Мероприятия (регионального, всероссийского и международного уровней), на которых представлялись работы студентов и преподавателей с тематикой по информационной безопасности (2013-2016 гг.)

2013-2014 учебный год

II Межрегиональная студенческая НПК «НОВЫЙВЗГЛЯД», посвященная70-тилетию Курской битвы. ОБОУ СПО «ЖПК» 26сентября 2013г.(публикация)

История развития отечественной криптографии, Мажуга А. С..рук Жигалева О.Л. (диплом 2 степени)

XXI Всероссийская студенческая конференция «Молодежь и наука » XXI века, 17-18 апреля 2014 г., г. Железногорск

А взламывали ли сегодня ваш аккаунт в соцсети? Мажуга А.С., рук. Жигалева О.Л., (диплом)

Система контроля управления доступом, Милютиков П.Н., рук. Петрушин С.Д., (диплом)

Всероссийский конкурс методических работ, проводимый Ассоциацией учебных заведений металлургического комплекса России (место проведения г. Москва, политехнический колледж, участники - Ростовская обл., Мурманская обл., Владимировская обл., Вологодская обл., Курская обл., Нижний Новгород, Липецкая обл., Белгородская обл., Владикавказ, регионы Урала, регионы Сибири)

Жигалева О.Л. «Методическое пособие по МДК 01.03. Организация и эксплуатация комплексной системы защиты информации», диплом 1 степени в номинации «Учебные пособия»

2014-2015 учебный год

XXII Всероссийская студенческая научно-техническая конференция «Молодежь и наука XXI века», посвященная 70-летию Победы в Великой Отечественной войне, ОБПОУ «ЖГМК» апрель 2015 года

Диплом в номинации «Информационные и телекоммуникационные технологии», «Мероприятия по защите детей от нежелательной (вредоносной) информации из сети интернет» (Положенцев И., Милютиков П.)

Грамота, «Культура информационной безопасности» (Мельников В.О., Глазков Д.К.)

Всероссийская олимпиада профессионального мастерства обучающихся по специальности СПО «Информационная безопасность автоматизированных систем», г. Саратов, апрель 2015 – Милютиков П. (диплом 2 степени)

I МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ «Вопросы кибербезопасности, моделирования и обработки информации в современных социотехнических системах» «Информ-2015», КГУ, Курск, 26 - 27 мая 2015 г.

10 участников конференции

2015-2016 учебный год

II МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ «Вопросы кибербезопасности, моделирования и обработки информации в современных социотехнических системах» «Информ-2016», КГУ, Курск, 20 - 21 мая 2016 г.

Исследования Positive Technologies и анкетирование респондентов по парольной защите

Теребрина Анастасия Сергеевна

Научный руководитель – к.п.н., Жигалева Ольга Леонидовна

Анализ редакций Федерального закона N 149-ФЗ «Об информации, информационных технологиях и защите информации»

Медведева Ангелина Алексеевна

Научный руководитель – к.п.н., Жигалева Ольга Леонидовна

Проблемы обеспечения информационной безопасности при создании системы автоматизации «Умный дом» на базе контроллера ARDUINO и программно-аппаратной платформы FLPROG

Положенцев Илья Эдуардович

Научный руководитель – Чекърска Юлия Игоревна

Всероссийская олимпиада профессионального мастерства обучающихся по специальности СПО «Информационная безопасность автоматизированных систем», г. Уфа, апрель 2016 – Милютиков П. (диплом 2 степени)