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

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

Анализ системы обеспечения информационной безопасности образовательной организации и разработка рекомендаций по ее совершенствованию

Выпускная квалификационная работа по направлению
44.04.04 Профессиональное обучение (по отраслям)
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»
Форма обучения заочная

Проверка на объем заимствований:
82,12% авторского текста

Работа рекомендована к защите
«17» января 2022 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Яковлева Валерия Витальевна

Научный руководитель:
к.п.н., старший преподаватель
Гафарова Елена Аркадьевна

Челябинск
2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В период, начавшийся с двух последних десятилетий предыдущего века, люди вышли на новую ступень своего развития – стадию создания информационного общества, знаменующую собой появление совершенно нового, непохожего на прежний, мира, во всех сферах культуры человечества также грядут неизбежные изменения.

Одним из первостепенных атрибутов современного мира является большая степень информатизации всех процессов, в том числе, тех, которые происходят в образовательных организациях. В настоящее время уже автоматизированы процессы ведения бухгалтерской отчетности, заполнения оценочных журналов, сбора данных об обучающихся и т.п. Однако, другой стороной возросшей степени информатизации является постоянное увеличение количества угроз безопасности конфиденциальных данных.

Человечество непрерывно пытается найти способы решения проблем, обозначенных выше, проводятся исследования во всех направлениях развития информационной безопасности современного общества. В Указе Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» (далее – Стратегия) также отражена актуальность проблем, связанных с угрозами безопасности данных.

Основная мысль Стратегии состоит в том, что безопасность государства неразрывно связана с решением проблем и в других областях развития страны, таких как социально-экономические и культурные аспекты. Таким образом, перед образовательными организациями возникает множество новых задач, связанных с хранением данных, в частности это повышение грамотности работников и обучающихся в сфере защиты данных, формирование регламентирующих документов в области обработки персональных данных и информации для служебного

пользования, обеспечение защиты данных на всех этапах их жизненного цикла.

Сотрудники и обучающиеся образовательных организаций, использующие в процессах деятельности информационные системы предприятия, должны быть проинформированы о возможности столкновения со всеми видами угроз и опасностей. Для обеспечения бесперебойной работы организации необходимо уметь грамотно противостоять возникающим информационным угрозам и всем видам сетевых атак, также нужно предотвратить любую возможность несанкционированного доступа к конфиденциальным данным.

На данном этапе развития информационного общества формируются требования для различных категорий специалистов, в целом направленные на создание информационной культуры с одним из главных пунктов – компетентностью в области защиты информации.

Процесс информатизации имеет непрерывный характер, также обновляются и совершенствуются различные риски и уязвимости, в связи с этим система обеспечения информационной безопасности образовательной организации нуждается в постоянной доработке и обновлении, чтобы соответствовать необходимому уровню защищенности.

Специфика деятельности образовательных организаций приводит к очевидному **противоречию**: из-за увеличения объема данных все процессы подвергаются всё большей автоматизации, а пользователи автоматизированных систем, как правило, отстают в совершенствовании своих навыков, что, в свою очередь, способствует появлению уязвимостей в системе обеспечения информационной безопасности.

Сформированность определённого набора компетенций создается в ходе образовательного процесса, а также во время трудовой деятельности; компетенции в области безопасности информации должны быть актуализированы для сотрудников образовательных организаций в целях эффективного противостояния современным угрозам.

Все нарастающая актуальность и недостаточная проработанность как теоретических, так и практических аспектов названной выше проблемы определили выбор **темы исследования: «Анализ системы обеспечения информационной безопасности образовательной организации и разработка рекомендаций по ее совершенствованию**».

Определение темы исследования обусловлено социальной значимостью вопроса, недостатком теоретической проработки в научных источниках, необходимостью в практических рекомендациях по повышению уровня безопасности информации образовательных организаций и общей актуальностью данной проблемы.

Цель исследования: разработать рекомендации по совершенствованию системы обеспечения информационной безопасности в образовательной организации.

Объект исследования: образовательная организация профессионального образования.

Предмет исследования: система обеспечения информационной безопасности в образовательной организации.

Гипотеза исследования состоит в предположении о том, что система информационной безопасности образовательной организации будет эффективнее, если привести её в соответствие с аттестационными требованиями руководящих документов для информационных систем, обрабатывающих персональные данные и информацию ограниченного распространения.

В соответствии с объектом, предметом и целью исследования были поставлены следующие **задачи:**

– изучить нормативно-методические документы и законодательные акты, различные разработки в сфере комплексной защиты информации в организациях;

–проанализировать состояние единого информационно-образовательного пространства Государственного бюджетного

профессионального образовательного учреждения «Южно-Уральского государственного технического колледжа» (ГБПОУ «ЮУрГТК»);

– проанализировать текущее состояние системы обеспечения информационной безопасности образовательной организации и составить рекомендации по её совершенствованию.

– разработать модель угроз информационой безопасности образовательной организации в соответствии с требованиями нормативных документов и на ее основе описать программу и регламент проведения аттестационных испытаний автоматизированной системы образовательной организации на соответствие требованиям безопасности информации;

– разработать методические рекомендации по совершенствованию системы информационной безопасности ГБПОУ «ЮУрГТК».

Методологической основой исследования являются фундаментальные работы в области:

– педагогических и психологических наук (Ю.К. Бабанский, В.П. Беспалько, Л.С. Выготский, П.Я. Гальперин, В.В. Давыдов, В.С. Леднев, А.Н. Леонтьев, И.Я. Лернер, Н.Д. Никандров, В.А. Сластенин, Д.И. Фельдштейн и др.);

– основной профессиональной подготовки и переподготовки преподавателя в структуре постоянного педагогического образования (С.И. Архангельский, Г.А. Бордовский, Н.В. Кузьмина, А.К. Маркова, Л.М. Митина, В.А. Сластенин, А.И. Щербаков и др.);

– сопровождения педагогики и консультирования в областях психологии и педагогики (Е.А. Александрова, В.Г. Воронцова, О.С. Газман, И.А. Колесникова, А.Е. Марон, Н.Н. Михайлова, О.С. Орлов, М.Н. Певзнер, К. Роджерс, В.В. Сохранов, С.Н. Чистякова, Н.И. Шевандрин и др.)

– информатизации обучения (Я.А. Ваграменко, С.А. Бешенков, О.А. Козлов, А.А. Кузнецов, М.П. Лапчик, Л.П. Мартиросян, И.Ш. Мухаметзянов, А.Н. Привалов, И.В. Роберт, А.Л. Семенов и др.);

– компетентностного подхода к построению учебного процесса (В.И. Байденко, А.С. Белкин, Э.Ф. Зеер, И.А. Зимняя, В.А. Кальней, А.К. Маркова, Ю.Т. Татур, А.В. Хуторской, Н.Ф. Ефремова);

– системного подхода (Н.М. Александрова, В.И. Андреев, Ю.К. Бабанский, А.П. Беляев, В.П. Беспалько, И.А. Ивлева, С.М. Маркова, Ю.Н. Петров, В.А. Сластенин, Н.Ф. Талызина);

– создания и применения компьютерных обучающих технологий в образовании (С.Г. Данилюк, А.Д. Дараган, В.Л. Латышев, Е.Н. Надеждин, А.А. Павлов, Ю.А. Романенко, В.И. Сердюков и др.);

– изучения основных проблем информационной и информационно-психологической безопасности (А.Е. Войскунский, Ю.Д. Бабаева, Л.Н. Бабанин, С.В. Бондаренко, И.В. Бурлаков, В.А. Бурова (Лоскутова), В.А. Голубев, М.С. Иванов, Л.О. Пережогин, О.В. Смыслова, Т.Л. Тропина, К. Янг и др.);

– аспекты нормативно-правового сопровождения безопаснсоти информации (В.М. Алексеев, Ю.М. Батурин, В.С. Горбатов, О.А. Городов, Р.И. Дремлюга, Ю.А. Журавлев, Г.О. Крылов, Т.А. Полякова, D.B. Thaw и др.);

– аспекты защиты информации с точки зрения педагогической проблемы (Р.В. Амелин, О.В. Казарин, А.А. Журин, П.Н. Корнюшин, А.А. Марков, В.А. Семененко, В.Н. Ясенев и др.);

– сложности обучения персонала и формирования компетенций в области защиты информации (Е.Б. Белов, Е.Н. Бояров, И.Н. Доронина, Э.В. Танова, М.Н. Швецов, E. Albrechtsen и др.);

– практические аспекты информационной безопасности и защиты информации (В.А. Галатенко, А.П. Даньков, В.Е. Козлов, А.А. Круглов, А.В. Крысин, В.В. Мельников, В.В. Минин, Ю.С. Уфимцев, В.Л. Цирлов и др.).

Научная новизна состоит в обосновании возможности необходимого обновления существующей системы информационной безопасности в образовательной организации посредством реализации программы

проведения испытаний автоматизированной системы организации на соответствие требованиям безопасности информации.

Теоретическая значимость исследования определяется расширением научных знаний в области обеспечения информационной безопасности образовательных организаций.

Практическая значимость диссертации определяется тем, что разработанная программа может применяться для совершенствования системы информационной безопасности в других образовательных организациях.

Основные этапы исследования.

На первом этапе формулировалась тема исследования, проводился сбор информации по теме исследования из различных источников, осуществлялась формулировка гипотезы, постановка цели, задач.

В ходе второго этапа осуществлялся анализ методов и средств, которые задействуются в образовательной организации по защите информации, проводился анализ научной литературы и отбор информации по теме исследования, осуществлялась публикация научных статей по теме исследования, была разработана модель угроз информационной безопасности образовательной организации.

Третий этап заключался в разработке, на основе составленной модели угроз, программы и регламента проведения испытаний автоматизированной системы организации на соответствие требованиям безопасности информации по защите информации в образовательной организации, а также методических рекомендаций по совершенствованию системы информационной безопасности ГБПОУ «Южно-Уральский государственный колледж».

Апробация результатов исследования осуществлялась путем публикации научных статей:

1. Некрасова В.В. Методы выявления и устранения некомпетентности пользователей системы информационной безопасности

образовательной организации // Профессиональное образование: методология, технологии, практика [Текст]: сборник научных статей / под. ред. Е.А. Гнатышиной. – Челябинск: изд-во «ЗАО Библиотека А. Миллера», 2020. – Выпуск 13. – 241 с.

2. Яковлева В.В. Разработка системы разграничения прав доступа к персональным данным (ПДн) как средства повышения эффективности системы обеспечения информационной безопасности образовательной организации // Студенческий вестник: электрон. научн. журн. 2021. № 14(159). URL: https://studvestnik.ru/journal/stud/herald/159

База исследования: ГБПОУ «Южно-Уральский государственный колледж» г. Челябинска.

Личное участие соискателя состоит в разработке модели угроз безопасности информации организации и создания на её основе программы и регламента проведения испытаний автоматизированной системы организации на соответствие требованиям безопасности информации, а также методических рекомендаций по совершенствованию системы информационной безопасности ГБПОУ «Южно-Уральский государственный колледж».

Структура диссертации. Диссертация состоит из введения, двух глав, заключения, приложения, списка использованной литературы, включающего 60, источников.

ГЛАВА 1. МЕТОДОЛОГИЧЕСКИЕ И ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВАНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1 Единое информационное пространство образовательной организации. Общая характеристика профессиональной образовательной организации, история учреждения, основные направления подготовки

Чтобы рассмотреть единое информационное образовательное пространство ГБПОУ «Южно-Уральского государственного технического колледжа» необходимо изначально ознакомиться с его историей, общей характеристикой, направлениями подготовки и материальным обеспечением.

Краткая история ГБПОУ «Южно-Уральского государственного технического колледжа»:

В соответствии с постановлением Совета Народных Комиссаров СССР приказом по строительству от 22.05.1940 № 89 «Об образовании профессионального учебного заведения в городе Верхняя Салда» при заводе металлоконструкций имени С. Орджоникидзе в Свердловской области появился строительный техникум.

В 1941 году, в связи с началом Великой Отечественной войны, техникум вместе с заводом переправляются в город Челябинск.

1943 год ознаменовывается переименованием учреждения в Челябинский строительный техникум (ЧСТ) в соответствии с приказом Совета Народных Комиссаров по строительству от 19.10.1943 № 654.

В 1958 году в соответствии с приказом министерства строительства РСФСР от 26.09.1958 № 304 учебное заведение вновь решено переименовать, на этот раз в Челябинский монтажный техникум (ЧМТ).

В 1991 году выпускается приказ Минмонтажспецстроя СССР от 23.10.1991 № 198 «О присвоении Челябинскому монтажному техникуму

статуса колледжа». С этого момента начата подготовка специалистов повышенного уровня.

7 сентября 2010 происходит реорганизация сращу нескольких учебных заведений – Челябинского машиностроительного техникума, Челябинского монтажного колледжа и Челябинского политехнического техникума, в результате их объединения и появляется Южно-Уральского государственного технического колледжа.

История машиностроительного комплекса:

История машиностроительного техникума неразрывно связана с развитием такого промышленного объекта как тракторный завод города Челябинска (ЧТЗ).

Челябинский тракторный техникум был основан в 1930 году, тогда же впервые зачислено 120 человек.

В мае 1931 года в учебных целях техникуму было передано около десятка аудиторий с незначительным оборудованием во вновь выстроенном здании школы, также было выделено новое здание под общежитие для иногородних студентов.

Тракторный техникум всегда выделялся своим оснащением и уровнем образования, в 1940 году заведение заняло первое место среди других техникумов Наркомсредмаша СССР.

В 1942 году происходит переименование техникума в машиностроительный, это связано с открытием нового отделения подготовки специалистов по направлениям гусеничных машин и танков. В военные годы техникум принимал значительное участие в помощи фронту и тем самым вписал себя на страницы истории Танкограда, также в то время 19 студентов и преподавателей учебного заведения погибли на фронте. В после военные годы быстро было определено направление развития – подготовка высококвалифицированных специалистов машиностроительного дивизиона.

Вечернее и заочное отделения техникума открылись только к 1956 году.

История политехнического комплекса:

Во исполнение распоряжения Совета Министров СССР от 09.06.1952 № 14333 «Об открытии в 1952-1953 учебном году филиала вечернего отделения Челябинского Машиностроительного техникума при заводе имени Орджоникидзе» Министерство транспортного машиностроения открывает 9 июня 1952 года вечерний политехнический техникум.

В тот же момент В.С. Стародубцева была назначена первым директором филиала вечернего отделения Челябинского Машиностроительного техникума.

Первым местом расположения техникума в 1953-1954 учебном году стал отдельно стоящий барак, который в настоящее время находится напротив спортзала техникума.

Первый выпускники окончили техникум в июне 1957 году, это был набор 1952 года.

Только к 1970 году у техникума появляется в собственности современное здание.

В соответствии с приказом Министра Машиностроения СССР от 10.05.1971 № 75 «О преобразовании Челябинского вечернего машиностроительного техникума» техникум был превращен в дневное учебное учреждение профессионального образования – Челябинский политехнический техникум.

Уже в 1991 году для поступающих были наборы по 10 различным специальностям, а сам техникум располагался в двух отдельно стоящих филиалах.

В историю техникума вошла Людмила Николаевна Дубровна, она была директором с 1991 по 1995 годы. В это время произошел настоящий рассвет учебного заведения, периодически появлялся набор на новые, востребованные обществом, специальности, осваивалась коммерческая

форма обучения студентов, что позволило создать современную материальную базу техникума.

Техникум с 1998 года одним из первых вводит специальность «Техническое обслуживание и ремонт автомобильного транспорта», для этого на его базе создается три, оснащенных по последнему слову техники, лаборатории.

Структура учебного заведения, которое существует на сегодняшний день выглядит так как показано на рисунке 1.

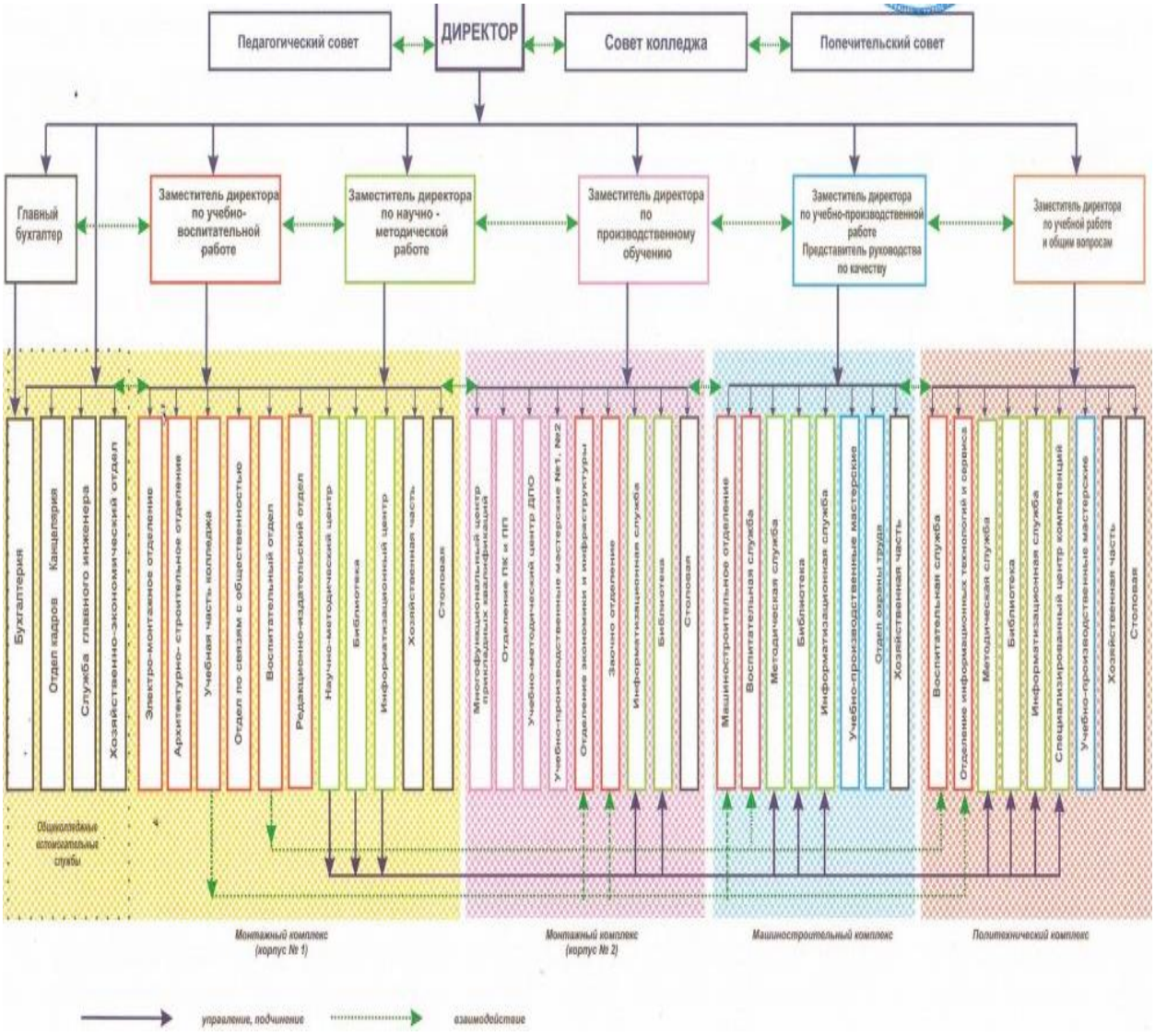

Рисунок 1 – Организационная структура ГБПОУ «Южно-Уральского государственного технического колледжа»

Сейчас колледж проводит подготовку и обучение студентов по направлениям, указанным в таблице 1.

Таблица 1 – Направления подготовки ГБПОУ Южно-Уральского государственного технического колледжа

№ п/п	Наименование направления подготовки
1.	Автоматизация технологических процессов и производств
2.	Архитектура
3.	Водоснабжение и водоотведение
4.	Земельно-имущественные отношения
5.	Инфокоммуникационные сети и системы связи
6.	Информационные системы и программирование
7.	Литейное производство черных и цветных металлов
8.	Монтаж, наладка и эксплуатация электрооборудования промышленных и гражданских зданий
9.	Монтаж и техническая эксплуатация промышленного оборудования
10.	Монтаж, техническое обслуживание и ремонт промышленного оборудования (по отраслям)
11.	Садово-парковое и ландшафтное строительство
12.	Сварочное производство
13.	Сетевое и системное администрирование
14.	Сети связи и системы коммутации
15.	Строительство и эксплуатация зданий и сооружений
16.	Техническое обслуживание и ремонт автомобильного транспорта
17.	Техническое обслуживание и ремонт двигателей, систем и агрегатов автомобилей
18.	Технология металлообрабатывающего производства
19.	Управление, эксплуатация и обслуживание многоквартирных домов
20.	Экономика и бухгалтерский учет

Во время прохождения педагогических и преддипломных практик основная работа проходила с группой студентов, обучающихся по специальности «Информационные системы и программирование», основные сведения о специальности:

обучение производится на базе основного общего образования – 3 года 10 месяцев (Квалификация: разработчик Web и мультимедийных приложений, программист).

Выпускник данной специальности по окончанию обучения должен обладать следующими компетенциями:

– способность сочетания разных художественных и творческих средств с программными продуктами, языками программирования, интерфейсами и разнообразными операционными средами для

проектирования и разработки сайтов сети Интернет различного назначения и сложности;

– способности проектировать и разрабатывать мультимедийные приложения, интерактивные мультипликации, звуковые и видео клипы широкой направленности, различные цифровые игры и программы с использованием специализированного программного обеспечения;

– способность обеспечивать безопасность веб-серверов, их непрерывное и бесперебойное функционирование, управлять доступом пользователей к созданным интернет-ресурсам, создавать ресурсы способные к восстановлению после аварий и сбоев, резервированию данных, содержащихся в них;

– способности создания такого машинного кода, который отвечает всем современным требованиям и имеет возможность интеграции с любыми другими входными данными, такими как аудио и мультимедиа файлы, языки сценариев;

– умения производить анализ и разработку Интернет-стратегий, различных методик и планов развития на основе Web.

Основные виды, которыми могут заниматься выпускники по данной программе подготовки:

– разработка и отладка компонентов общесистемного, прикладного и специализированного программного обеспечения для автоматизированных систем;

– внедрение программных модулей, их объединение и настройка;

– сопровождение, отладка и обслуживание на всех этапах жизненного цикла разнообразного программного обеспечения для автоматизированных систем;

– создание для любых целей, сопровождение, выполнение защиты безопасности содержащейся информации в базах данных.

В связи с тем, что одним из основных видов деятельности, обучающихся по данному направлению подготовки является обеспечение

безопасности web-серверов, программ, приложений, программного обеспечения и баз данных – курс информационной безопасности становится неотъемлемой частью качественной подготовки данных специалистов.

Для понимания основных принципов работы системы информационной безопасности ГБПОУ «ЮУрГТК» на сегодняшний момент рассмотрим единое информационное пространство образовательной организации.

Полное наименование организации: Государственное бюджетное образовательное учреждение среднего профессионального образования «Южно-Уральский государственный технический колледж».

Дата создания колледжа: 09.04.1940.

Учредители: учредителем ГБПОУ «Южно-Уральский государственный технический колледж» является Министерство образования и науки Челябинской области.

Директор учреждения: Тубер Игорь Иосифович.

Адрес расположения организации: 454007, Челябинская область, город Челябинск, улица Горького, дом 15.

У учреждения имеется в наличии следующее материальное обеспечение образовательного процесса:

– четыре современных учебных корпуса;

– два спортивных стадиона;

– одна лыжная база;

– две оборудованные спортивные площадки;

– пять оборудованных залов для занятий спортом;

– девять оснащенных всем необходимым оборудованием учебно-производственных мастерских для различных целей;

– три учебных полигона;

– четыре библиотеки;

– тридцать шесть оснащенных классов по общеобразовательным дисциплинам;

– восемьдесят оснащенных кабинетов для проведения дисциплин профессионального цикла;

– пятьдесят пять учебных лабораторий, в которых имеется всё необходимое оборудование, приборы и материалы;

– тридцать компьютерных аудиторий;

– двадцать пять кабинетов, оборудованных интерактивными досками или мультимедийными установками для проведения лекционных либо семинарских занятий.

Оборудование учебных лабораторий отвечает всем современным требованиям, в них имеются как учебно-лабораторные стенды, так и различное оборудование и приборы, обеспечивающие проведение на высоком уровне лабораторных работ либо практических занятий, включенных в образовательные программы по основным направлениям подготовки колледжа. Также среди материально-технических ресурсов учреждения имеются специальные технические средства обучения для коллективного или индивидуального использования лицами с ограниченными возможностями здоровья. В ходе учебного процесса применяются дистанционные образовательные технологии с использованием таких систем как e.lanbook.ru, moodle, dom.sustec.ru.

Начальная страница системы dom.sustec.ru для ГБПОУ «Южно-Уральский государственный технический колледж» показана на рисунке 2.

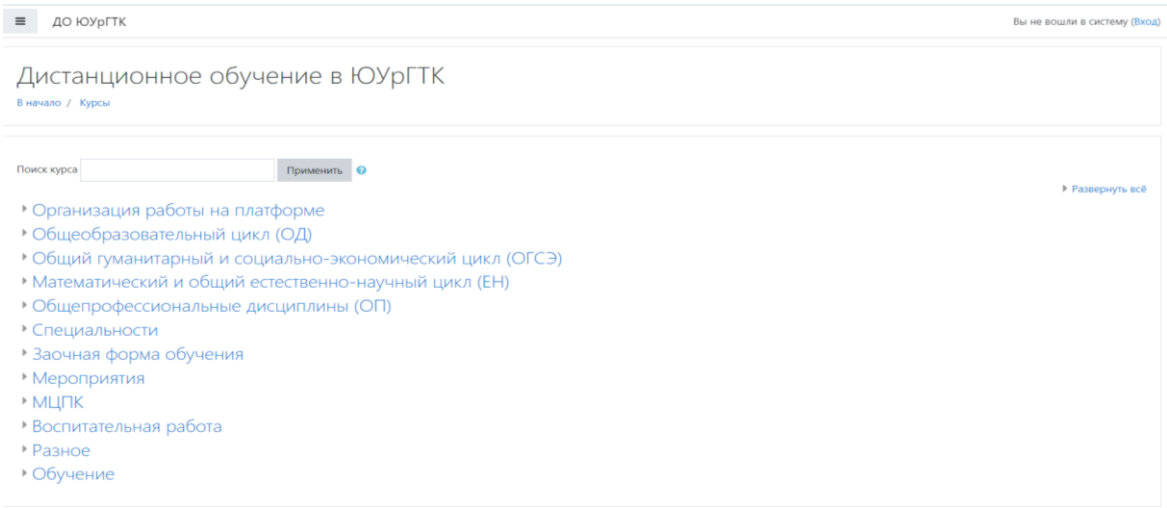

Рисунок 2 – Начальная страница информационной системы

Учебно-производственные полигоны и мастерские имеют в своем оснащении всё необходимое оборудование, приборы и материалы для возможности проведения в техникуме учебных и производственных практик студентов и для проведения аттестационных мероприятий по присвоению рабочих разрядов.

В собственности учреждения находятся все необходимые составляющие для возможности организации спортивно-оздоровительного и физкультурно-массового досуга, а именно: две спортивные площадки, оснащенные инвентарем, оборудованная лыжная база, пять спортивных залов со спортивными снарядами, один укомплектованный тренажерный зал.

Для обеспечения комфортного течения учебного процесса и улучшения проведения досуговой деятельности сотрудников и обучающихся колледжа объекты для организации спортивно-оздоровительной работы расположены во всех корпусах учебного заведения.

В целях создания благоприятных условий для всех категорий обучающихся, в том числе, для лиц с ограниченными возможностями здоровья, все учебные аудитории, кабинеты, предназначенные для проведения практических занятий, библиотечные помещения и спортивные объекты спроектированы с учетом требований всех современных нормативно-методических документов в области безопасности труда и охраны здоровья.

Из оснащения учебного заведения можно выделить следующие приспособления, для обеспечения комфортного обучения и нахождения на территории лиц с ограниченными возможностями здоровья: ко входу в машиностроительный комплекс ведут пандусы с поручнями, для лиц с нарушениями функционирования опорно-двигательного аппарата имеется специализированный вход, а также всё необходимое для беспрепятственного доступа таких обучающихся в учебные кабинеты,

библиотеку, санитарную комнату, с этой целью спроектированы специальные пандусы, поручни, расширены дверные проемы, имеются кнопки экстренного вызова персонала для оказания помощи. Все здания и сооружения колледжа соответствуют требованиям СНиП и ГОСТ.

Во всех корпусах колледжа организованы пункты горячего питания сотрудников и студентов, имеется три столовые, четыре буфета с общим количеством мест – 497.

Помещения столовых и буфетов образовательной организации соответствуют санитарно-гигиеническим требованиям Российской Федерации, оснащены всем необходимым современным техническим и технологическим оборудованием, предназначенным для приготовления пищи, утилизации отходов и обработки кухонных принадлежностей и посуды. Также обеспечены все условия для питания лиц с ограниченными возможностями здоровья. Имеется сертификат соответствия питания в столовых колледжа требованиям нормативных документов № РОСС. RU. АЯ14.М01797.

ГБПОУ «Южно-Уральский государственный технический колледж» оснащен всем необходимым для обеспечения здоровье сберегающих условий для сотрудников и обучающихся.

Также организовано медицинское обслуживание обучающихся, проводятся ежегодные медосмотры и лечебно-оздоровительная работа согласно годовым планам. У колледжа имеется два медицинских пункта, в одном из них семь оборудованных кабинетов, он расположен на территории монтажного комплекса, второй медицинский пункт находится на территории политехнического комплекса и имеет три кабинета.

Общая площадь медицинского пункта, расположенного по адресу, улица Савина, 18 составляет 200,4 м^2, в том числе:

– кабинет для врачебного осмотра: 14,2 м^2;

– процедурный кабинет: 14,3 м^2;

– кабинет для оказания стоматологических услуг: 14,2 м^2;

– кабинет медсестры: 14,2 м^2;

– кабинет функциональной диагностики: 56,8 м^2;

– гинекологический кабинет: 14,2 м^2;

– кабинеты, предназначенные для осмотров узкоспециализированными специалистами: 21,4 м^2.

Общая площадь медицинского пункта, расположенного по адресу, улица Гагарина, 7 составляет 31,9 м^2, в том числе:

– кабинет для врачебного осмотра, совмещенный с процедурным кабинетом: 16,1 м^2;

– кабинет для оказания стоматологических услуг: 15,8 м^2.

Ответственность за медицинское обслуживание обучающихся и сотрудников образовательного учреждения несут муниципальное бюджетное учреждение здравоохранения «Городская клиническая больница № 2» (в части обслуживания монтажного комплекса) и государственное бюджетное учреждение здравоохранения (в части обслуживания политехнического комплекса). Объекты медицинского обслуживания имеют лицензии на оказание медицинских услуг населению, лицензии от 13.09.2013 № ЛО-74-01-002311 и от 26.03.2012 № ЛО-74-01-001485.

Для осуществления дистанционной образовательной деятельности, размещения информации о предстоящих и прошедших мероприятиях и информирования студентов об актуальных событиях у ГБПОУ «Южно-Уральский государственный технический колледж» имеется собственный сайт (режим доступа: https://sustec.ru), отвечающий всем требованиям к подобным ресурсам образовательных организаций. Начальная страница сайта представлена на рисунке 3.

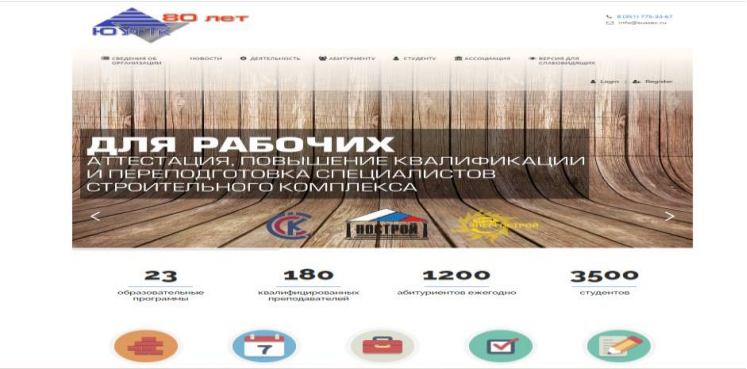

Рисунок 3 – Начальная страница сайта организации

Сайт учреждения образования – один из информационных ресурсов, создающийся в целях увеличения информационно-коммуникационного пространства организации и решающий следующие задачи:

– обеспечение необходимыми информационными сведениями всех участников образовательного процесса;

– увеличение открытости, простоты и доступности образовательной деятельности для всех вовлеченных в неё лиц;

– создание и внедрение условий для использования современных форм, средств и методов обучения и воспитания;

– формирование общей информационно-коммуникационной среды образовательной организации;

– создание благоприятного имиджа учреждения образования для обучающихся, планирующих поступать, выпускников и сотрудников;

– придание огласке инновационного опыта, полученного колледжем;

– формирование каналов для удобства общения всем участникам образовательного процесса.

У сайта ГБПОУ «Южно-Уральский государственный технический колледж» имеются следующие разделы:

– Раздел сведения об учреждении (включает в себя общие сведения об образовательной организации, структуру и органы управления

образовательной организации, сведения об учредителях, историю организации, о педагогическом и руководящем составе и т.п.).

– Раздел деятельность (содержит подразделы: информация об образовательном процессе, объединения для организации дополнительного образования, информация о повышении квалификации педагогического состава, Федеральные Государственные образовательные стандарты, регулирующие деятельность колледжа, основные образовательные программы, информация о конкурсах и олимпиадах, предстоящих в настоящем учебном году и т.п.).

– Раздел студенту (подразделы: дистанционное обучение, спортивные секции, отделения колледжа, расписание учебных занятий и т.п.).

– Раздел ассоциация (содержит сведения об ассоциации, в которой состоит учреждение).

– Раздел новости (здесь публикуется информация о всех предстоящих событиях в колледже).

В целом, на сайте можно получить доступ ко всей необходимой для обучения, поступления, и работы в учреждении информации.

Исходя из всего написанного выше, применительно к ГБПОУ «Южно-Уральский государственный технический колледж» можно выделить как актуальные следующие направления повышения информатизации:

– продолжение оснащения учебных аудиторий, лабораторий и производственных помещений компьютерной техникой;

– уход, поддержание в рабочем состоянии и администрирование уже имеющийся техники;

– повышение грамотности пользователей в части использования технических средств;

– использование новых, современных платформ, осуществляющих образовательные функции (таких как «Сетевой город. Образование» и др.)

– дальнейшие поддержка и улучшение сайта образовательной организации.

1.2 Организационно правовое обеспечение деятельности образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж»

Организационно-правовое обеспечение функционирования и развития ГБПОУ «Южно-Уральский государственный технический колледж» включает набор разных взаимосвязанных документов, регламентирующих такие особенности образовательной организации как структура, основные задачи, функции учреждения образования, специфику организации работы, права, обязанности и ответственность руководителя организации, сотрудников, обучающихся и их непосредственных представителей.

Организационно-правовое обеспечение деятельности учреждения профессионального образования определяют следующие внутренние нормативные документы:

– лицензия на право ведения деятельности в области образования граждан;

– свидетельства государственной регистрации прав собственности;

– устав организации;

– коллективный договор;

– структура и штатная численность работников организации;

– правила внутреннего трудового распорядка;

– штатное расписание учреждения;

– должностные инструкции специалистов и служащих образовательной организации.

Учредительный договор – документ, заключенный в соответствии с законодательством Российской Федерации на котором основываются и

регулируются взаимоотношения между организацией, оказывающей образовательные услуги и её учредителем.

Все основные стороны деятельности в учреждениях образования регламентируются в соответствии с Уставом организации, документом, который должен быть составлен во всех подобных организациях в соответствии с Федеральным законом «Об образовании в Российской Федерации». Устав ГБПОУ «Южно-Уральский государственный технический колледж» оформлен и утвержден приказом Министерства образования и науки Челябинской области от 30.03.2015 № 01/53.

Устав – это организационно-правовой документ организации, закрепляющий все, исходящие из Федерального закона Российской Федерации «Об образовании» основные права, функционал и обязанности учреждения образования, также, исходя из Типового положения об образовательном учреждении и других нормативных документов в области образования и науки, закрепляет полномочия, переданные образовательной организации её учредителем. Кроме того, в данном документе прописываются другие, требующие решения вопросы, касающиеся образовательного процесса и хозяйственной деятельности, которые не противоречат действующему законодательству.

Любой организации, планирующей заниматься образовательной деятельностью необходима лицензия на право оказания такого вида услуг населению, ГБПОУ «ЮУрГТК» получена данная лицензия от 19.05.2015 № 11440, на бессрочный период.

Так как наличие лицензии на проведение работ в области оказания образовательных услуг не является основанием для выдачи студентом по окончанию обучению документа государственного образца об образовании, организацией также пройдена государственная аккредитация образовательной деятельности по основным направлениям профессиональных образовательных программ в отношении каждого уровня профессионального образования по каждой укрупненной группе

профессий, специальностей и направлений подготовки. Документом, подтверждающим прохождение колледжем государственной аккредитации, является свидетельство от 18.05.2020 № 3017, срок действия до 18.05.2026.

На рисунке 4 показано приложение к свидетельству о государственной аккредитации организации с перечнем профессий и специальностей, по которым осуществляется образовательная деятельность организации.

Приложение № 1.1
к свидетельству о государственной аккредитации
от 18 мая 2020 года № 3017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ЧЕЛЯБИНСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

454007, Челябинская область, город Челябинск, улица Горького, дом 15

Профессиональное образование

№ п/п	Коды укрупненных групп профессий, специальностей и направлений подготовки профессионального образования	Наименования укрупненных групп профессий, специальностей и направлений подготовки профессионального образования	Уровень образования
1	2	3	4
1.	07.00.00	Архитектура	Среднее профессиональное образование
2.	08.00.00	Техника и технологии строительства	Среднее профессиональное образование
3.	09.00.00	Информатика и вычислительная техника	Среднее профессиональное образование
4.	11.00.00	Электроника, радиотехника и системы связи	Среднее профессиональное образование
5.	15.00.00	Машиностроение	Среднее профессиональное образование
6.	21.00.00	Прикладная геология, горное дело, нефтегазовое дело и геодезия	Среднее профессиональное образование
7.	22.00.00	Технологии материалов	Среднее профессиональное образование
8.	23.00.00	Техника и технологии наземного транспорта	Среднее профессиональное образование
9.	35.00.00	Сельское, лесное и рыбное хозяйство	Среднее профессиональное образование
10.	38.00.00	Экономика и управление	Среднее профессиональное образование

Распорядительный документ аккредитационного органа о выдаче свидетельства о государственной аккредитации:	Распорядительный документ аккредитационного органа о переоформлении свидетельства о государственной аккредитации:
приказ Министерства образования и науки Челябинской области (приказ / распоряжение) от 18 мая 2020 года № 03-ГА-54	-

Министр (должность уполномоченного лица) _____ Кузнецов Александр Игоревич (фамилия, имя, отчество уполномоченного лица)

М.П. Серия 74А02 № 0002236

Рисунок 4 – Приложение к свидетельству о государственной аккредитации

Штатное расписание организации – документ, закрепляющий количество должностей и численность по ним в учреждении.

Также одним из наиболее важных документов для любой образовательной организации, регулирующим процессы её

функционирования и развития, является коллективный договор. Трудовой договор заключается меду работодателем, либо его представителем и сотрудниками предприятия и регулирует все аспекты профессиональных, трудовых и социально-экономических отношений между ними. Законом Российской Федерации от 11.03.1992 «О коллективных договорах и соглашениях» регулируется порядок разработки, формирования и согласования коллективного договора организации. У ГБПОУ «Южно-Уральский государственный технический колледж» Коллективный договор на 2017-2020 годы утвержден профкомом и директором организации 23.03.2017, срок действия продлен на 2020-2023 года.

Должностные инструкции сотрудников – документ, описывающий основные правовые положения педагогического, административного и обслуживающего составов.

Распределение трудовых обязанностей среди сотрудников руководящего состава учреждения образования закрепляется приказами руководителя.

Весь комплект документов, описывающих вопросы организационно-правового и хозяйственного обеспечения деятельности образовательной организации, способствует наиболее эффективному управлению процессами функционирования и качественного развития учебного заведения.

В открытом доступе для пользователей на официальном сайте колледжа располагаются документы, представленные в таблице 2.

Таблица 2 – Документы ГБПОУ «ЮУрГТК», размещенные на сайте

№ п/п	Наименование документа	Вид документа
1	Лицензия на право осуществления работ в области ведения образовательной деятельности	Организационно-правовой
2	Свидетельство о прохождении государственной аккредитации	Организационно-правовой
3	Устав образовательной организации	Организационно-правовой
4	Коллективный договор организации	Организационно-распорядительный

№ п/п	Наименование документа	Вид документа
5	Рабочие программы с аннотациями	Организационно-распорядительный
6	Правила внутреннего трудового распорядка организации	Организационно-распорядительный
7	Правила внутреннего распорядка для обучающихся	Организационно-распорядительный
8	Правила приема обучающихся	Организационно-распорядительный
9	Документ о порядке оказания платных образовательных услуг	Организационно-распорядительный
10	Порядок и основания перевода, отчисления обучающихся	Организационно-распорядительный
11	План финансово-хозяйственной деятельности образовательной организации, утвержденный в установленном законодательством Российской Федерации порядке, или бюджетная смета образовательной организации	Организационно-распорядительный
12	Порядок оформления возникновения, приостановления и прекращения отношений между образовательной организацией и обучающимися и (или) родителями (законными представителями) несовершеннолетних обучающихся	Организационно-распорядительный
13	Документ об утверждении стоимости обучения по каждой образовательной программе	Организационно-распорядительный
14	Документ, определяющий политику оператора в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных	Организационно-распорядительный
15	Образец договора об оказании платных образовательных услуг	Организационно-распорядительный

ГБПОУ «ЮУрГТК» является оператором персональных данных обучающихся и их родителей (законных представителей) в полном соответствии с Положением об организации обработки и защиты персональных данных (далее – Положение), утвержденным советом колледжа (протокол от 17.09.2015 № 1)

Положение разработано в строгом соответствии с Конституцией Российской Федерации от 25.12.1993, Гражданским кодексом Российской Федерации от 30.11.1994 № 51-ФЗ, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006

№ 152- ФЗ, а также другими регламентирующими документами, действующими на территории Российской Федерации.

Положение создано с целью определения и закрепления порядка работы с персональными данными лиц, обратившихся в образовательную организацию, также других субъектов персональных данных, оператором которых является ГБПОУ «Южно-Уральский государственный технический колледж» в соответствии с имеющимися полномочиями. Положение описывает принципы защиты прав и свобод граждан, в том числе тех, которые стали субъектами обработки персональных данных колледжа, в нём говорится о защите прав на неприкосновенность частной жизни, на личную и семейную тайны. Также в нем устанавливается ответственность за неисполнение требований и норм, регулирующих обработку персональных данных, должностных лиц, имеющих оформленный официальным порядком доступ к персональным данным. В соответствии с Положением любая информация, содержащая персональные данные субъектов, является конфиденциальной и требует соблюдения особых требований в процессе его обработки, за исключением:

– персональных данных, являющихся обезличенными;

– персональных данных, которые представляются в общем доступе.

Режим конфиденциальности персональных данных может быть снят в двух случаях:

– в случае их обезличивания;

– по истечению установленного срока хранения (срок хранения может быть продлен на основании решения экспертной комиссии организации, если иное не определяется законами Российской Федерации).

В дополнении к Положению образовательной организацией выпущена Политика в отношении обработки персональных данных ГБПОУ «Южно-Уральский государственный технический колледж» (далее – Политика), утвержденная советом и директором организации от 17.09.2015

протокол № 1. Политика регламентирует принципы определяет принципы и общие подходы в части обращения с персональными данными.

Учреждением образования каждый год составляется и соблюдается план мероприятий по обеспечению информационной безопасности учебного заведения, данный документ размещается и своевременно обновляется на официальном сайте колледжа.

Исходя из написанного выше становится ясно, что ГБПОУ «Южно-Уральский государственный технический колледж» составлен и внедрен на постоянной основе весь комплект документов, регламентирующий деятельность учреждения, при этом информационная безопасность одно из основных направлений безопасности образовательной организации в комплексе.

1.3 Анализ уязвимостей (рисков) существующей системы обеспечения информационной безопасности в образовательно организации

Для проведения анализа уязвимостей существующей системы информационной безопасности ГБПОУ Южно-Уральского государственного технического колледжа наиболее оптимальным методом является разработка модели угроз.

Необходимость разработки модели угроз регламентирована рядом нормативных документов, таких как:

– часть 2 статьи 19 закона №152-ФЗ «О персональных данных»:

«2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

– состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом

Федеральной службы по техническому и экспортному контролю России (ФСТЭК России) от 18 февраля 2013г. № 21):

«4. Меры по обеспечению безопасности персональных данных реализуются, в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных».

– требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утверждены ФСТЭК России от 11 февраля 2013г. № 17):

«Формирование требований к защите информации… в том числе включает: …определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации».

– требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (утверждены приказом ФСТЭК России от 14 марта 2014 г. № 31):

«Формирование требований к защите информации в автоматизированной системе управления… в том числе включает: … определение угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования автоматизированной системы управления, и разработку на их основе модели угроз безопасности информации».

– требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утверждены приказом ФСТЭК России от 25 декабря 2017г. № 239):

«11. Разработка организационных и технических мер по обеспечению безопасности значимого объекта осуществляется субъектом критической информационной инфраструктуры… и должна включать:

а) анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии)».

Итак, отсюда следует вывод: для любых информационных систем, так или иначе подлежащих защите в соответствии с законодательством необходимо разработать модель угроз.

Необходимость создания данного документа для информационной системы ГБПОУ «Южно-Уральского государственного технического колледжа» очевидна. Наполнение модели угроз описывается в приказе ФСТЭК России от 11 февраля 2013г. № 17:

«Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации».

Таким образом, модель угроз информационной безопасности автоматизированной системы должна содержать:

– описание информационной системы;

– структурно-функциональные характеристики;

– описание угроз безопасности;

– модель нарушителя;

– возможные уязвимости;

– способы реализации угроз;

– последствия от нарушения свойств безопасности информации.

На основании Базовой модели угроз персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России от 15 февраля 2008 г., была разработана модель угроз персональных данных для ГБПОУ «Южно-Уральского государственного технического колледжа», она представлена в таблице 3. В модели угроз отражены все возможные угрозы информационной системе образовательной организации, дана вероятностная оценка реализации угрозы и представлены возможные меры по исключению риска наступления данного события.

Таблица 3 – Модель угроз безопасности персональных данных при их обработке в информационной системе ГБПОУ «Южно-Уральского государственного технического колледжа»

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1 Угрозы от утечки по техническим каналам						
1.1 Угрозы утечки акустической информации	Маловероятна	Низкая	Низкая	Неактуальная		Инструктаж пользователей в части проведения переговоров по рабочим вопросам исключительно на территории организации и с людьми, допущенными к обсуждаемой информации
1.2 Угрозы утечки видовой информации	Маловероятна	Низкая	Низкая	Неактуальная	Жалюзи на окнах; Расположение мониторов, исключающее возможность просмотра информации третьими лицами	Инструктаж пользователей в части необходимости блокировки рабочих компьютеров в случае возможности просмотра информации людьми, не допущенными к данным сведениям
1.3 Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН)	Маловероятна	Низкая	Низкая	Неактуальная		

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
2 Угрозы несанкционированного доступа к информации						
2.1 Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных (ИСПДн) носителей информации путем физического доступа к элементам ИСПДн						
2.1.1 Кража персональных электронных вычислительных машин (ПЭВМ)	Маловероятна	Низкая	Низкая	Неактуальна		Контролируемая зона для организации технической защиты конфиденциальной информации; Специализированная охрана образовательной организации
2.1.2 Кража носителей информации	Маловероятна	Низкая	Низкая	Неактуальна	Хранение носителей, исключающее несанкционированный доступ	Учет носителей; Инструктаж пользователей в части запрета выноса носителей информации с территории организации и хранения носителей в защищенных местах, исключающих возможность несанкционированного доступа
2.1.3 Кража, модификация, уничтожение информации	Маловероятна	Низкая	Низкая	Неактуальна		Контролируемая зона для организации технической защиты конфиденциальной информации с

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
						ограничением доступа посторонних лиц; Ответственность за сохранность конфиденциальной информации и ее носителей в должностных инструкциях сотрудников
2.1.4 Вывод из строя узлов ПЭВМ, каналов связи	Низкая вероятность	Средняя	Низкая	Неактуальна		Контролируемая зона для организации технической защиты конфиденциальной информации с ограничением доступа посторонних лиц; Ответственность за сохранность конфиденциальной информации и ее носителей в должностных инструкциях сотрудников
2.1.5 Несанкционированный доступ к информации при техническом обслуживании узлов ПЭВМ	Маловероятна	Низкая	Низкая	Неактуальна		Ремонт допущенными сотрудниками учреждения; Технологический процесс обработки информации содержит

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
						информацию о действиях в случае выхода из строя ПЭВМ
2.1.6 Несанкционированное отключение средств защиты	Низкая вероятность	Средняя	Низкая	Неактуальна	Настройка средств защиты	Инструктаж пользователей в части запрета каких-либо действий в отношении средств защиты; Технологический процесс обработки содержит информацию о действиях в случае выхода из строя или некорректной работе средств защиты информации
2.2 Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных средств						
2.2.1 Действия вредоносных программ (вирусов)	Низкая вероятность	Средняя	Низкая	Неактуальна	Антивирусное программное обеспечение (ПО)	Инструктаж пользователей в части действий в случае возникновения внештатных ситуаций; Технологический процесс обработки информации регламентирует действия в случае возникновения внештатных ситуаций

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
2.2.2 Недекларированные возможности системного ПО и ПО для обработки персональных данных	Маловероятна	Низкая	Низкая	Неактуальна	Настройка средств защиты	Приобретение лицензионного ПО у официальных поставщиков
2.2.3 Установка ПО не связанного с исполнением служебных обязанностей	Низкая вероятность	Средняя	Низкая	Неактуальна	Настройка средств защиты	Инструктаж пользователей в части запрета использования на рабочих ПЭВМ ПО, не задействованного для выполнения работ; Технологический процесс обработки информации регламентирует действия администраторов безопасности в случае обнаружения ПО не имеющегося в документации на систему
2.3 Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн из-за сбоев в ПО, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера						
2.3.1 Утрата атрибутов доступа	Маловероятна	Низкая	Низкая	Неактуальна		Инструктаж пользователей в части организации хранения в строго определенных местах парольных карточек; Журнал учета паролей

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
2.3.2 Непреднамеренная модификация (уничтожение) информации сотрудниками	Низкая вероятность	Средняя	Низкая	Актуальна	Настройка средств защиты; Резервное копирование информации	Инструктаж пользователей в части строгого исполнения порядка работ, предусмотренного для исполнения служебных обязанностей
2.3.3 Непреднамеренное отключение средств защиты	Маловероятна	Низкая	Низкая	Неактуальна	Доступ к установлению режимов работы средств защиты предоставляется только администратору; Настройка средств защиты	Инструктаж пользователей в части запрета каких-либо действий в отношении средств защиты
2.3.4 Выход из строя программно-аппаратных средств	Низкая вероятность	Средняя	Низкая	Неактуальна	Резервное копирование информации	
2.3.5 Сбой системы электроснабжения	Маловероятна	Низкая	Низкая	Неактуальна	Использование источников бесперебойного питания для серверов	
2.3.6 Стихийное бедствие	Маловероятна	Низкая	Низкая	Неактуальна	Пожарная сигнализация	Инструкция по действиям в случае возникновения нештатной ситуации
2.4 Угрозы преднамеренных действий внутренних нарушителей						
2.4.1 Доступ к информации,	Маловероятна	Низкая	Низкая	Неактуальна		Инструктаж пользователей в части

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
модификация, уничтожение лицами, недопущенными к её обработке						необходимости блокировки рабочих компьютеров в случае возможности просмотра информации людьми, не допущенными к данным сведениям; Парольная система доступа; Разграничение прав пользователей
2.4.2 Разглашение информации, модификация, уничтожение сотрудниками, допущенными к её обработке	Маловероятна	Низкая	Низкая	Неактуальна		Обязательства о неразглашении; Инструктаж пользователей в части проведения переговоров по рабочим вопросам исключительно на территории организации и с людьми, допущенными к обсуждаемой информации
2.5 Угрозы несанкционированного доступа по каналам связи						
2.5.1 Угрозы выявления паролей по сети	Маловероятна	Низкая	Низкая	Неактуальна	Антивирусное ПО	
2.5.2 Угрозы навязывания ложного маршрута сети	Маловероятна	Низкая	Низкая	Неактуальна	Использование межсетевого экрана	

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
2.5.3 Угрозы внедрения ложного объекта в ИСПДн	Маловероятна	Низкая	Низкая	Неактуальна	Использование межсетевого экрана	
2.5.4 Угрозы удаленного запуска приложений	Маловероятна	Низкая	Низкая	Неактуальна	Использование межсетевого экрана	
2.5.5 Угрозы внедрения по сети вредоносных программ	Низкая вероятность	Средняя	Низкая	Неактуальна	Антивирусное ПО; Использование межсетевого экрана	Инструктаж пользователей в части порядка действии в случае возникновения внештатных ситуаций

1.4 Выводы по главе 1

Информационная безопасность образовательной организации – состояние защищенности информационных ресурсов, технологий их создания и применения, а также создание набора прав субъектов информационной деятельности.

Безопасность информации – один из основных элементов системы обеспечения комплексной защиты учреждения образования.

Исходя из текущего состояния уровня защищенности информации в ГБПОУ «Южно-Уральский государственный технический колледж», руководителю организации, либо лицу, ответственному за информационную безопасность в целом и за обработку персональных данных (ПДн) в частности, необходимо предпринять комплекс мер обеспечивающий необходимый и достаточный уровень сохранности информационных данных организации.

Предпринимаемые меры защиты должны быть сопоставимы вероятности осуществления конкретного типа угроз и потенциальному ущербу, который может быть нанесен, если угроза осуществится (включая затраты на защиту от нее).

Организационные мероприятия играют важную роль в создании надежной системы защиты информации, так как возможности несанкционированного использования конфиденциальных данных в значительной мере обусловлены не техническими аспектами, а неправомерными действиями, небрежностью и необученностью пользователей и персонала защиты.

Система обеспечения информационной безопасности организации должна соответствовать следующим требованиям:

– устойчивость к произведению несанкционированного доступа;

– непрерывность совершенствования и строгое соответствие требованиям регламентирующих документов;

– конфиденциальность, не позволяющая выявить организацию системы защиты информации;

– оперативность, обеспечение возможности своевременно и действенно реагировать на внештатные ситуации и неправомерные действия со стороны нарушителей.

– обоснованность с точки зрения адекватного сопоставления уровня конфиденциальности информации, циркулирующей в системе и средств, затраченных на её защиту.

ГЛАВА 2. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО СОВЕРШЕНСТВОВАНИЮ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ (ГБПОУ «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ КОЛЛЕДЖ»)

2.1 Обоснование необходимости проведения испытаний на соответствие требованиям по безопасности информации информационной системы ГБПОУ «Южно-Уральский государственный технический колледж»

Аттестация автоматизированных систем – это комплекс организационно-технических действий, результатом завершения которых становится такой документ, как аттестат соответствия автоматизированной системы требованиям информационной безопасности, подтверждающий, что объект информатизации полностью соответствует требованиям всех регламентирующих документов по безопасности информации, действующих на территории Российской Федерации.

Для информационных систем ГБПОУ «Южно-Уральский государственный технический колледж» аттестация не является обязательной, так как в них циркулирует информация для служебного пользования и ПДн, а сами системы не относятся к государственным, однако получение подтверждающего безопасность аттестата соответствия позволит организации быть уверенной в том, что меры, реализованные в рамках системы защиты данных, достаточно эффективны и удовлетворяют всем требованиям безопасности информации. Аттестация позволит избежать конфликтов с контролирующими органами и минимизирует вероятность судебных исков за разглашение конфиденциальной информации. К тому же, требования, предъявляемые к информационным системам в Российской Федерации, с каждым годом всё сильнее

ужесточаются, поэтому существует большая вероятность, что через 3 – 5 лет аттестация информационных систем персональных данных станет необходима для всех организаций-операторов.

При этом, в случае введения обязательной аттестации для информационных систем, в которых циркулирует информация для служебного пользования и ПДн, цена на её проведение организациями, имеющими лицензию на осуществление данного вида работ, вероятнее всего значительно увеличится по сравнению с ценой, существующей в настоящее время.

В случае если образовательной организацией принято решение о не проведении аттестационных испытаний своих информационных систем, то необходимой и достаточной мерой становится выявление возможных каналов утечки данных и выполнение всех организационно-технических мероприятий для обеспечения их безопасности, подготовка документов, регламентирующих способы функционирования и защиты информационных систем. Составить программу и регламент проведения возможных аттестационных испытаний и сформировать документ, описывающий и провести проверку информационной системы в соответствии с ними собственными силами предприятия, по результатам проверки устранить все выявленные недостатки. Если такие действия выполнены, то это позволит, в случае необходимости, провести аттестационные испытания систем в кратчайшие сроки и с минимальными затратами.

Этапы подготовки автоматизированной системы к проведению испытаний, методики испытаний и способы проверки организации работ по безопасности информации в системе сформулированы в Методических рекомендациях по совершенствованию системы информационной безопасности ГБПОУ «ЮУрГТК» (Приложение 1).

2.2 Программа испытаний автоматизированной системы ГБПОУ «Южно-Уральский государственный технический колледж»

Программа испытаний – документ, в котором определяются задачи, цели, способы, определенные условия, общий объем, последовательность и методики действий в ходе испытаний на соответствие установленным требованиям информационной безопасности информации, циркулирующей в автоматизированной системе (АС) образовательной организации, расположенной по адресу: Челябинская область, г. Челябинск, ул. Горького, д. 15.

Для аттестации АС выпускается приказ руководителя организации «Об установлении контролируемой зоны для организации технической защиты конфиденциальной информации», как правило, границы контролируемой зоны соответствуют границам самой организации.

Размещение всех основных технический средств и систем (ОТСС) АС указывается в техническом паспорте системы, данный документ утверждается руководителем учреждения образования.

Объект исследования – автоматизированная система ГБПОУ «Южно-Уральский государственный технический колледж», предназначенная для информационного взаимодействия подразделений организации, а также для предоставления централизованных информационных сервисов, систем и ресурсов пользователям.

АС представляет собой локальную вычислительную сеть, функционирующую в ГБПОУ «Южно-Уральский государственный технический колледж» и расположенную в пределах контролируемой зоны образовательной организации. В качестве центра обработки данных (ЦОД) АС выделен аппаратно-программный серверный комплекс с высоконадежной дублированной сетевой инфраструктурой, системой хранения данных, системой бесперебойного питания, системой кондиционирования и системой физической защиты.

В АС одновременно обрабатывается и хранится информация разных уровней конфиденциальности – несекретная, конфиденциальная (персональные данные, информация ограниченного распространения).

Класс защищенности АС устанавливается в соответствии с Руководящим документом "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации", утвержденным по решению Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992 и Методическими рекомендациями для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости, утвержденными Министерством здравоохранения и социального развития Российской Федерации 23.12.2009. Все автоматизированные системы классифицируются по группам, исходя из следующих особенностей:

– к первой группе относятся АС, функционирующие в многопользовательском режиме, в которых единовременно циркулирует либо хранится информация различных уровней (например, несекретная и персональные данные). При этом пользователи имеют различные права по допуску к данным.

– ко второй группе относятся АС, функционирующие в многопользовательском режиме, но в отличие от первой группы, здесь пользователи имеют одинаковые права по доступу к данным.

– к третьей группе относятся АС, где допуск к работе имеет только один пользователей, имеющий право доступа ко всем данным системы.

Так как АС ГБПОУ «ЮУрГТК» многопользовательская, в которой циркулирует информация разных уровней конфиденциальности, не все пользователи имеют право доступа ко всей информации, а по обрабатывающихся в ней ПДн, как было описано ранее, можно опознать человека и узнать о нём дополнительные сведения, количество субъектов

ПДн находится в пределах от 1000 да 100000, а нарушение безопасности данных нанесет чувствительный вред субъектам, то АС устанавливается класс 1-2. Класс АС устанавливается в соответствии с актом классификации автоматизированной системы, сформированным комиссией организации и утвержденным её руководителем.

Приказом руководителя организации, проводящей аттестационные испытания, назначается аттестационная комиссия АС, в состав которой включаются эксперты органа по аттестации.

Главной целью аттестации системы становится определение соответствия АС требованиям информационной безопасности. Испытания проводятся на подтверждение соответствия системы всем требованиям нормативно-методических документов, действующих на территории Российской Федерации, относящихся к безопасности информации автоматизированных систем, обрабатывающих конфиденциальную информацию.

Ключевая задача аттестации – это определение соответствия системы и параметров её защиты нормам информационной безопасности, соблюдение которых позволит защитить данные от утечки по различным каналам передачи и от определенных воздействий на неё по причинам:

– несанкционированного доступа третьих лиц к данным, циркулирующим в АС;

– воздействий специализированного программного обеспечения, способного навредить целостности данных, циркулирующих в АС, либо работоспособности системы в целом;

– кражи носителей информации, содержащих защищаемые данные;

– получения доступа не допущенных лиц к видовой информации АС, отображающейся на экранах мониторов, путем непосредственного просмотра, либо с использованием специализированных оптических средств.

В ходе проведения испытаний используются такие методы контроля и проверок как:

метод экспертной проверки документов;

анализ способов сохранения данных от несанкционированного доступа с применением специализированных средств, проверкой экспериментального пуска системы защиты или способом осуществления попыток обходи системы защиты информации АС;

изучение совместимости и правильности функционирования всех программных, технических и организационных мер, применяющихся для защиты данных АС;

проверка средств защиты информации (СрЗИ) от несанкционированного доступа (НСД) в ходе экспериментальных попыток осуществить НСД к условной конфиденциальной информации в обход применяемой системы защиты, также с применением определенных для этого случая программ.

Метод экспертной проверки документов подразумевает анализ системы защиты информации информационной системы на соответствие требованиям информационной безопасности, в ходе исследования проверяются все документы на АС на предмет полноты и достаточности их разработки, а также на полное соответствия, описанных способов, мер по защиты и общих данных АС, реальным.

Анализ способов сохранения данных от несанкционированного доступа проводится для всей программно-технической составляющей АС в соответствие с требованиями руководящих документов по защите информации.

Соответствие системы требованиями информационной безопасности выясняется в ходе изучения всех результатов тестирования и проверок АС, в процессе анализа обнаруженных нарушений, замечаний и недочетов в системе защиты.

В ситуации обнаружения по результатам испытаний критических несоответствий АС требованиям, определенным нормативными документами, принимается решение либо о полном запрете в АС обработки защищаемой информации, либо о возможности устранения некритических несоответствий, путем выполнения следующих действий:

– переработки документов на систему;

– удаление из состава АС составных частей;

– использование дополнительных способов защиты информации (программных, технических, организационных, в зависимости от вида выявленного несоответствия);

– усилением средств защиты информации, путем использование дополнительных модулей в дополнение к уже применяющимся.

В соответствии с программой испытания АС состоят из следующих этапов:

а) изучение состава технических средств системы, условий их эксплуатации, общей структуры объекта, данный анализ включает в себя:

– изучение предоставленных первоначальных данных и их сопоставление реальным свойствам АС, в части расположение технических средств, их сборки и параметров использования;

– анализ описанного технологического процесса работы АС и сопоставление его с реальными действиями пользователей в ходе эксплуатации системы;

– изучение потоков информации системы;

– изучение реального состава использующихся для обработки информации технических средств, анализ их задействования в проведения работ.

б) анализ ходы выполнения работ в АС в части выполнения требований защиты информации, а именно:

– анализ правильности присвоения класса АС;

– изучение достаточности разработки документов, регламентирующих действия в ходе эксплуатации, организационной и проектной документации на систему;

– проверка компетентности пользователей, допущенных к работе в АС и отвечающих за сохранность информации в системе; оценка разработанности и включения в документы пунктов ответственности пользователей за сохранность информации.

в) анализ соответствия системы требованиям информационной безопасности, а именно:

– изучение разработанности требуемой документации и соответствия её требованиям нормативных документов;

– проверка компетентности пользователей, допущенных к работе в АС и отвечающих за сохранность информации в системе; оценка разработанности и включения в документы пунктов ответственности пользователей за сохранность информации;

– анализ соответствия помещений, в которых расположены технические средства АС и ведется обработка информации, требованиям регламентирующих документов.

г) проведение опытной проверки АС по сохранению информационных данных в случае совершения попыток НСД.

д) формирование итоговых документов по результатам оценки соответствия АС требованиям информационной безопасности, в том числе:

– составляется протокол оценки сохранности информации от НСД, в котором отражаются результаты испытаний системы;

– сведения о прохождении всех контрольных испытаний системы фиксируются в протоколе по итогам аттестации АС;

– общие результаты прохождения системой аттестационных испытаний оформляются в заключении по итогам аттестации АС, включающем:

анализ соответствия системы требованиям информационной безопасности Российской Федерации к данному классу АС;

список нарушений и замечаний в функционировании АС, либо её системы защиты, выявленных по итогам испытаний;

рекомендации по исправлению нарушений и замечаний в функционировании АС, либо её системы защиты, выявленных по итогам испытаний;

общее заключение по итогам испытаний с обоснованием возможности (невозможности) получения системой Аттестата соответствия требованиям информационной безопасности.

е) после аттестации системы ежегодно проводится объектовый контроль, в ходе которого устанавливается соответствие АС и её системы защиты установленным требованиям по безопасности информации, контроль неизменности условий функционирования системы. Данный контроль выполняется силами сотрудников, ответственных за сохранность информации данной АС, специалисты, проводившие аттестацию системы, привлекаются к работам только в случае необходимости.

з) объектовая проверка включает в себя исполнение следующих действий:

– проводится сопоставление документации по итогам проведения испытаний реальным условиям эксплуатации системы в настоящее время, проверка соблюдения всех требований, перечисленных в документации на АС, соответствие ведения журналов и других документов системы регламентирующим требованиям;

– проводится контроль информационной безопасности данных системы от утечки за счет НСД.

и) документы по итогам проведения ежегодной проверки оформляются в виде протокола.

2.3 Регламент проведения испытаний автоматизированной системы ГБПОУ «Южно-Уральский технический колледж» на соответствие требованиям по безопасности информации от несанкционированного доступа

Испытания проводятся на соответствие требованиям руководящего документа "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации", утвержденного решением Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992. В результате прохождения всех исследований дается заключение по защите данных системы от НСД.

Проверка способности защиты данных системы от НСД содержит следующие виды работ:

а) анализ исполнения документированного технологического процесса в реальных условиях эксплуатации системы.

Владелец представляет на испытания документированное описание технологического процесса.

Все конфиденциальные данные системы могут быть размещены только на носителях, поставленных на учет в образовательной организации в соответствии с применяющимся порядком.

В ходе проведения испытаний проверяется:

– исполнения документированного технологического процесса в реальных условиях эксплуатации системы;

– соответствие документированного описания технологического процесса обработки и хранения конфиденциальных данных реальному процессу.

б) анализ защищенности подсистемы управления доступом:

– проводится изучение наличия, работоспособности и правильности функционирования в реальных условиях подсистем идентификации и аутентификации пользователей.

Изучают способности системы разграничения прав доступа, путем попыток обращения к защищаемым файлам категорией пользователей, не допущенных к их обработке.

Во время осуществления попыток доступа системой должна производится сверка принадлежности представленных идентификационных данных всем тем, что имеются в системе. Если логин и пароль являются неизвестными системе, то системой должен прекращаться процесс предоставления доступа с записью в журнале регистрации инцидентов безопасности.

в) анализ функционирования и соответствия требованиям безопасности информации подсистемы аутентификации:

– изучают порядок прохождения субъектами процесса аутентификации. В случае, если попытка доступа несанкционированная и системе предъявляют пароль, не зарегистрированный в ней, либо если пароль не соответствует предъявляемому идентификатору, то доступ к системе должен быть прекращен средствами управления, желательно отображение попытки несанкционированного доступа в журнале событий.

Исследуют систему на возможность взлома путем подбора пароля (вручную либо с использованием специализированных программ). Также, если в описании системы прописано наличие средств, выполняющих блокировку подбора, то осуществляют проверку функционирования этих средств, путем многократных попыток ввода некорректного пароля. При превышении максимального количества попыток ввода ключей идентификации/аутентификации, установленного политикой защищенности организации, подсистема контроля доступа обязана всецело остановить возможность ввода данных идентификации/аутентификации

субъекта доступа. Права снятия блокировки системы для данного пользователя должны быть только у администратора безопасности системы.

Испытание отсутствия критериев компрометации подсистемы идентификации и аутентификации:

– проводят проверку способов хранения, выдачи, применения устройств и данных об идентификации и аутентификации. Организационные и технические события системы должны полностью исключить возможность несанкционированного получения или же кражи устройств и данных об идентификации и аутентификации.

Проводят проверку вероятности несанкционированного конфигурирования данных об идентификации и аутентификации. Доступ субъектов системы к файлам, содержащим информацию об идентификации и аутентификации, должен быть целиком заблокирован для прикладных программ. В системе обязательно отсутствие прикладных программных способов прямого доступа к устройствам и оперативной памяти, возможностей ручной разработки и отладки программ.

Проводятся испытания средств загрузки операционной системы АС в обход подсистемы идентификации и аутентификации.

Выполняют попытки загрузки операционной системы с загрузочного носителя. Настройка СрЗИ от НСД АС должна гарантировать блокировку загрузки операционной системы с носителей, не предусмотренных технологией инициализации системы.

в) проверки подсистемы регистрации и учета.

Проверки включают:

– анализ регистрации начала и завершения работ;

– испытания попыток совершения вывода из носителей системы защищаемых данных, на внешний диск;

– испытание регистрации применения программных средств;

– анализ учета защищаемых носителей информации;

– испытание возможностей отчистки освобождаемых областей памяти.

Каждый пункт рассмотрен подробно в таблице 6.

Таблица 6 – Проверки подсистемы регистрации и учета

№ п\п	Наименование проверки	Содержание проверки
1	Анализ регистрации начала и окончания работ	Ведется загрузка операционной системы и пуск программных средств АС, предусмотренных технологией инициализации системы. Производятся попытки доступа в систему с некорректными идентификатором, с корректным идентификатором доступа и некорректным паролем, с корректными идентификатором и паролем, зарегистрированными в системе. Выполняется программный останов системы. Выполняется загрузка операционной системы, пуск программных средств АС, предусмотренных технологией инициализации АС, вход в систему с использованием учетной записи администратора информационной безопасности, изучение журнала регистрации событий в отношении доступа к системе. Испытания являются успешными, когда при помощи организационных и технических способов защиты, выполняемыми в соответствии с политикой защищенности системы, гарантируется ведение журнала регистрации событий в отношении доступа (аппаратного журнала), в котором прописаны регистрация входа (выхода) субъектов доступа в систему (из системы) или регистрация загрузки и инициализации операционной системы и ее программного останова. Также регистрационные записи о всех событиях должны фиксировать: – дату и время входа (выхода) субъекта доступа в систему (из системы) или же загрузки (останова) системы; – итог попытки входа: удачная или же неуспешная, несанкционированная; – персональный идентификатор (код или же фамилия) субъекта, предъявленный при попытке доступа
2	Испытания попыток совершения вывода из устройств системы защищаемых данных, на внешний диск	Согласно с принятой в системе технологией ведется вывод из устройств защищаемых данных на внешние диски. Испытания являются успешными, в случае если организационными и техническими мерами, проводимыми согласно политике защищенности системы, гарантируется регистрация вывода из устройств защищаемых данных, в том числе

№ п\п	Наименование проверки	Содержание проверки
		программ управления, на внешние диски. В этом случае регистрационные записи должны включать в себя следующую информацию: – дату и время выдачи документа (обращения к подсистеме вывода документа); – описание устройства выдачи (логическое имя внешнего диска); – короткое описание (наименование, вид, шифр, код) и степень конфиденциальности документа; – личный номер субъекта доступа, запросившего документ
3	Испытание регистрации применения программных средств	Согласно принятой в системе технологии выполняется пуск программ обработки данных и объектами обработки выбираются файлы, входящие в список защищаемых ресурсов. Пуск программ выполняется как в штатном режиме, предусматривающем безаварийную (штатную) обработку данных и окончание работы, также и во внештатном. В последнем случае моделируется ситуация несанкционированного применения средств. В процессе анализа используются следующие способы: – задают неправильные характеристики обработки; – задают в качестве объекта обработки несуществующий файл; – осуществляют попытки запустить средства, доступ к которым ограничен подсистемой разграничения доступа. Испытания являются успешными, в случае если организационными и техническими мерами, проводимыми согласно политике защищенности системы, проводится регистрация пуска и окончания использования программ и средств, проверяемых в ходе данного этапа. Также регистрационные записи о всех событиях должны фиксировать: – дату и время запуска; – имя (идентификатор) программы (процесса, задания); – личный номер субъекта доступа, запросившего доступ к программе (процессу); – итог пуска (успешный, неуспешный – несанкционированный)
4	Анализ учета защищаемых носителей информации	Анализируется соблюдение организационных и технических мер по учету защищаемых носителей данных. Испытания являются успешными, в случае если организационными и техническими мерами,

№ п\п	Наименование проверки	Содержание проверки
		проводимыми согласно политике защищенности системы, обеспечиваются: – полный учет всех защищаемых носителей информации с применением специальной маркировки и фиксацией информации о них в журнале учета (учетной карточке); – учет в журнале (карточке) выдачи /приема защищаемых носителей; – дублирование информации о выдаче\приеме носителей пользователям
5	Испытание возможностей отчистки освобождаемых областей памяти Анализ надежности очистки внешней памяти при удалении данных	Главным методом исследования качества очистки внешней памяти при проведении испытаний системы считается средство, которое используется для контроля очистки памяти при ее освобождении на внешних носителях информации методом поиска определенных проверяющим данных. Объектами испытания являются носители на гибких и жестких магнитных дисках. Параметры поиска задают или по всему физическому диску, или в пределах логического диска. Испытания являются успешными, в случае: – если искомые проверяющим данные не были обнаружены на внешнем диске; – если отсеки, ранее заполненные искомой информацией на данный момент, содержат маскирующие данные

г) проверка подсистемы обеспечения целостности.

Выполняются испытания организационно-штатных действий по обеспечению безопасности информации:

– анализируется организационно-штатная организация сотрудников и регламентирующие документы системы на предмет наличия структуры безопасности информации.

– способом выборочного опроса выясняют наличие знаний у сотрудников, отвечающих за безопасность информации системы, их функциональных обязанностей, проверяют уровень их подготовки в области обеспечения защиты информации.

Результаты анализа считаются успешными в случае:

– если штатная организация сотрудников включает в себя администратора информационной безопасности;

– если уровень подготовки сотрудников, отвечающих за безопасность информации системы, обеспечивает исполнение требований защиты информации в системе;

– если функционал администратора информационной безопасности системы регулируется регламентирующими документами системы.

Затем проводится анализ средств и систем обеспечения целостности программных составляющих СЗИ от НСД.

В начале проведения анализа штатными средствами системы выполняется резервное копирование программных составляющих СЗИ от НСД.

Выполняется имитирование несанкционированных воздействий по искажению целостности программных составляющих СЗИ от НСД. Проводится стирание или изменение имени определенных программных компонентов СЗИ от НСД.

Проводится перезапуск системы. После завершения включения СЗИ от НСД проверяется ответная реакция компонентов подсистемы обеспечения целостности.

Результаты анализа считаются успешными в случае, если СЗИ от НСД запротоколировали изменения состава программных модулей.

Далее выполняется обследование функций СЗИ от НСД.

Анализируются регламентирующие документы системы, описывающая содержание выполнения тестирования функций СЗИ от НСД, применяющихся в системе.

Изучается наличие систем тестирования функций СЗИ от НСД, а именно параметры настройки и применения диагностических средств СЗИ от НСД.

Проводится проверка частоты выполнения тестирования функций СЗИ от НСД. Анализ проводится способом проверки эксплуатационной документации и журналов регистрации событий безопасности СЗИ от НСД.

Результаты анализа считаются успешными в случае, если средства тестирования функций СЗИ от НСД и частота проведения тестирований отвечают требованиям всех регламентирующих документов в области безопасности информации в Российской Федерации.

Следующим пунктом осуществляется анализ средств восстановления СЗИ от НСД.

Изучаются эксплуатационные и организационно-распорядительные документы системы, описывающие содержание выполнения резервного копирования СЗИ от НСД, применяющегося в системе.

Проводится проверка частоты обновления и испытание исправности работы копий. Испытания проводятся способом проверки эксплуатационных документов и журналов регистрации событий безопасности СЗИ от НСД.

Результаты анализа считаются успешными в случае, если в системе предусмотрено наличие и поддержание в работоспособном состоянии двух копий программных СЗИ от НСД.

Последним действием в ходе проведения испытаний является анализ физической защиты системы.

Результаты анализа считаются успешными в случае, если в организации имеется физическая охрана системы, включающая постоянный контроль защищенности зданий и помещений, где находятся устройства и компоненты АС. Физическая охрана может осуществляться при помощи специализированного персонала, в чьи обязанности входит защиты помещений системы от несанкционированного доступа посторонних, средств охранной сигнализации, специального оснащения помещений, в которых расположена система.

При успешном прохождении автоматизированной системой ГБПОУ «Южно-Уральский государственный технический колледж» всех проверок и испытаний, описанных выше, можно сделать вывод о её соответствии требованиям безопасности информации, предъявляемым к системам

обработки конфиденциальной информации и персональных данных в Российской Федерации. В случае принятия решения о необходимости аттестации по требованиям безопасности информации организацией, имеющей лицензию на проведение данного вида работ, данной автоматизированной системой будет получен аттестат соответствия без необходимости принятия дополнительных действий по разработке регламентирующих документов, дооснащению средствами защиты и обеспечению физической защиты объекта.

ЗАКЛЮЧЕНИЕ

В ходе написания магистерской диссертации были достигнуты все поставленные задачи, а именно:

– изучены нормативно-методические документы и законодательные акты, различные разработки в сфере защиты информации в организациях, изучен понятийный аппарат, выявлены ключевые принципы и закономерности обеспечения безопасности информации в организации;

– рассмотрено единое информационно-образовательное пространство ГБПОУ «ЮУрГТК» и выявлены ключевые моменты системы обеспечения информационной безопасности образовательной организации;

– проанализирована система обеспечения безопасности информации организации и составлены рекомендации по её совершенствованию,

–разработана модель угроз информационой безопасности образовательной организации в соответствии с требованиями нормативных документов и на ее основе описана программа и регламент проведения аттестационных испытаний автоматизированной системы образовательной организации на соответствие требованиям безопасности информации;

–разработаны методические рекомендации по совершенствованию системы информационной безопасности ГБПОУ «ЮУрГТК».

При выполнении всех рекомендаций описанных в магистерской диссертации, в случае принятия решения о необходимости аттестации автоматизированной системы образовательного учреждения по требованиям безопасности информации организацией, имеющей лицензию на проведение данного вида работ, данной системой будет получен аттестат соответствия без необходимости принятия дополнительных действий по разработке регламентирующих документов, дооснащению средствами защиты и обеспечению физической защиты объекта.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2013. – 136 с.

2. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. – М.: ДМК Пресс, 2013. – 474 с.

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: утв. Федеральной службой по техническому и экспортному контролю 15 февраля 2008г //СПС Консультант Плюс.

4. Баймакова, И.А. Обеспечение защиты персональных данных. Методическое пособие / И.А. Баймакова, А.В. Новиков, А.И. Рогачев – М.: 1С -Паблишинг, 2014. – 214 с.

5. Бекишев, К. Инновации в системе образования РК.// Естественнонаучное образование: вызовы и перспективы. Сборник под общей ред. Академика В.В.Лунина и проф. Н.Е.Кузьменко. – М.: изд-во Московского университета, 2015. – с.36-54

6. Белов, Е.Б. Основы информационной безопасности [Текст]. Учебное пособие для вузов / Е.Б.Белов, В.П.Лось, Р.В.Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2016. – 544 с.

7. Бордовский, Г.А. Проблемы педагогики информационного общества и основы педагогической информатики / Г.А. Бордовский и др. // Дидактические основы компьютерного обучения. Л.: Изд-во ЛГПИ, 1989.

8. Вараменко, Я.А. Информатизация образования: итоги и направления дальнейшей работы // Педагогическая информатика. 2017. - №1. -С. 41 -51.

9. Гершунский, Б.С. Компьютеризация в сфере образования: проблемы и перспективы./ Б.С. Гершунский М.: Педагогика, 2017. – 264 с.

10. Глинский, Б.А. Моделирование как метод научного исследования / Б.А. Глинский, Б.С. Грязнов, Б.С. Дынин. – М., 1965. 312с.

11. Гафнер В.В. Информационная безопасность: учеб.пособие. – Ростов н/Дону: Феникс, 2010. – 324 с.

12. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», утвержденного и введенного в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст. (Москва: Стандартинформ, 2007).

13. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Электронный ресурс]. //СПС Консультант Плюс.

14. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения [Электронный ресурс]. //СПС Консультант Плюс.

15. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью [Электронный ресурс]. //СПС Консультант Плюс.

16. ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».

17. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

18. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

19. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

20. Девянин П.Н. Садердинов А.А., Трайнев В.А. и др. Учебное пособие. Информационная безопасность предприятия. – М., 2006.– 335.

21. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017. — 536 с.

22. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.

23. Защита от несанкционированного доступа к информации. Термины и определения [Электронный ресурс]: утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г //СПС Консультант Плюс.

24. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей [Электронный ресурс]: утв. решением Государственной технической комиссии при Президенте РФ от 4 июня 1999 г. N114 //СПС Консультант Плюс.

25. Защита от шума [Электронный ресурс]: СНиП 23-03-2003: утв. Минрегионом РФ 28.12.10: взамен СНиП II-12-74//СПС Консультант Плюс.

26. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности. - URL: http://citforum.ru/security/articles/categorizing/3.shtml**.**

27. Красильникова, В.А. Информатизация образования: понятийный аппарат / В.А. Красильникова // Информатика и образования, № 4, 2013. С. 21 – 27.

28. Кречетников, К.Г. Методология проектирования, оценки качества и применения информационных технологий обучения / К.Г. Кречетников. – М.: Госкоорцентр, 2016 – 216с.

29. Крысин, Л.П. Толковый словарь иноязычных слов / Л.П. Крысин. – М.:Инфокнига, 2015 – 564с.

30. Кузнецов, Э.И. Общеобразовательные и профессионально-прикладные аспекты изучения информатики и вычислительной техники в педагогическом институте: автореф. дис. . д-ра пед. наук. М., 2015.

31. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. – М.: ГЛТ, 2004. – 280 с.

32. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие для вузов. / А.А. Малюк. – М.: Горячая линия – Телеком , 2004. – 280 с.

33. Мельников В.П. Информационная безопасность и защита информации: учеб.пособие для студентов высших учебных заведений.– М.: Издательский центр «Академия», 2008. – 336 с.

34. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации [Электронный ресурс]: утв. ФСБ РФ 21 февраля 2008г. N149/54-144 //СПС Консультант Плюс.

35. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости (утв. Министерством здравоохранения и социального развития РФ 23 декабря 2009 г.).

36. Моисеев, В.Б. Информационные технологии в системе высшего образования. / В.Б. Моисеев. Пенза: Изд-во Пенз. технол. ин-та, 2014. – 100с.

37. Моисеев, В.Б. Элементы информационно-образовательной среды высшего учебного, заведения. / В.Б. Моисеев. Ульяновск: Изд-во Ул. ГТУ, 2015. – 122с.

38. Рогозин В.В. Основы информационной безопасности: учеб. пособие. – М.: Юнита-Дана, 2016. – 287 с.

39. О персональных данных [Электронный ресурс]: Федеральный закон №152-ФЗ: [принят Гос. Думой 8 июля 2006 г.: одобр. Советом Федерации 14 июля 2006 года]// СПС Консультант Плюс.

40. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федер. закон: [принят Гос. Думой 8 июля 2006 г.: одобр. Советом Федерации 14 июля 2006 г.] //СПС Консультант Плюс.

41. Об образовании в Российской федерации (ред. от 29.07.2017) [Электронный ресурс]: федер. закон: [принят Гос. Думой 21.12. 2012 г.] //СПС Консультант Плюс.

42. Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: постановление Правительства РФ от 17 ноября 2007 г. N 781. //СПС Консультант Плюс.

43. Общая повестка дня России и АСЕАН в киберпространстве: противодействие глобальным угрозам, укрепление кибербезопасности и развитие сотрудничества // Индекс безопасности № 4 (111), том 20 – С. 77-92 [электронный ресурс] http://www.pircenter.org/media/content/files/18/14219241510.pdf.

44. Ожегов С.И. Толковый словарь русского языка: 80 000 слов и фразеологических выражений / С.И. Ожегов, Н.Ю. Шведова. — 4-е изд., М., 1997. — 944 с.

45. Основные направления научных исследований в области обеспечения информационной безопасности российской федерации (одобрены секцией по информационной безопасности Научного совета при Совете Безопасности Российской Федерации, протокол от 28 марта 2015г. №1) [электронный ресурс] http://www.scrf.gov.ru/security/information/document94/.

46. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. – М.: АРТА, 2012. – 296 с.

47. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну (утв. приказом ФСТЭК России от 29 апреля 2021 г. № 77).

48. Роберт, И.В. Основные понятия Единого информационного образовательного пространства / И.В. Роберт, Ю.А. Прозорова, В.А. Касторнова // Ученые записки ИИО РАО. – М.: 2015. Вып. 6. С. 5-12.

49. Роберт, И.В. Толковый словарь терминов понятийного аппарата информатизации образования / И.В. Роберт. – М.: Институт информатизации образования РАО, 2006. – 88 с.

50. Российская педагогическая энциклопедия. [электронный ресурс] – URL: http://www.gumer.info/bibliotek_Buks/Pedagog/russpenc/15.php.

51. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России, 1992 г.

52. Рыжко, А.Л. Экономика информационных систем: учебное пособие. / А.Л. Рыжко, Н.М. Лобанова, Н.А. Рыжко, Е.О. Кучинская – М.: Финансовый университет, 2014. – 204 с.

53. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [Электронный ресурс]: утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992г //СПС Консультант Плюс.

54. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [Электронный ресурс]: утв. решением Государственной технической комиссии при Президенте РФ от 25 июля 1997 г //СПС Консультант Плюс.

55. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом ФСТЭК России от 18 февраля 2013 г. № 21 (зарегистрирован Минюстом России 14 мая 2013 г., регистрационный № 28375), с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 г. № 49 (зарегистрирован Минюстом России 25 апреля 2017 г., регистрационный № 46487), приказом ФСТЭК России от 14 мая 2020 г. № 68 (зарегистрирован Минюстом России 8 июля 2020 г., регистрационный № 58877).

56. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608), с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933), приказом ФСТЭК России от 28 мая 2019 г. № 106 (зарегистрирован Минюстом России 13 сентября 2019 г., регистрационный № 55924), приказом ФСТЭК России от 27 апреля 2020 г. № 61 (зарегистрирован Минюстом России 12 мая 2020 г., регистрационный № 58322).

57. Технологии обеспечения информационной безопасности в образовательном учреждении (организации): метод. рекомендации для руководителей и педагогов образовательных учреждений (организаций) / авт.-сост. Н.Ю. Сероштанова, Е.В. Тюгаева, Н.В. Шпарута: Государственное автономное образовательное учреждение дополнительного профессионального образования Свердловской области «Институт развития образования». - Екатеринбург: ГАОУ ДПО СО «ИРО», 2014. – 44 с.

58. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие для студентов вузов,

обучающихся по специальностям в обл. информ. безопасности [Текст]/ А.Ф. Чипига. – М.:ГелиосАРМ, 2017. –336с.

59. Шарафутдинова, А.Р., Пядышев, В.С. Защита информации в образовательных учреждениях [Текст] / А.Р. Шарафутдинова, В.С. Пядышева. – URL: http://www.rusnauka.com/17_APSN_2013/Matemathics/2_140911.doc.htm.

60. Ярочкин, В.И. Информационная безопасность [Текст]: Учебник для вузов / В.И. Ярочкин. – М.: Академический Проект, 2018. – 544 с.

Приложение 1

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

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО СОВЕРШЕНСТВОВАНИЮ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГБПОУ «ЮУрГТК»

Разработал:
Студент группы ЗФ-309-210-2-1
Яковлева Валерия Витальевна

Челябинск
2022

Содержание

1 Подготовка к проведению испытаний информационной системы ГБПОУ «Южно-Уральский государственный технический колледж»

В соответствии с Положением по аттестации объектов информатизации по требованиям безопасности информации, утвержденного Государственной технической комиссией при Президенте Российской Федерации от 25.11.1994, исходные данные по аттестуемому объекту информатизации готовятся на основе следующего перечня вопросов:

– в документах должны указываться точное и полное наименование объекта аттестации, с какой целью используется объект. Данная информация указывается в техническом паспорте на автоматизированную систему.

– характер данных объекта информатизации (в случае с ГБПОУ «ЮУрГТК» данные системы носят научно-технический, экономический и социальный характер), его уровень секретности (конфиденциальности циркулирующих данных), по каким перечням конфиденциальность определена (перечнем предприятия, ведомства, отрасли, либо государства). Данные сведения указываются в акте классификации автоматизированной системы.

– документы должны содержать сведения об организационной структуре информационной системы. Эти сведения отражаются в техническом паспорте автоматизированной системы, а также в акте установки общесистемного программного обеспечения и системы защиты информации от несанкционированного доступа в автоматизированной системе.

– документы должны содержать: перечень помещений, в которых ведется обработка информации, состав набора технических средств (вспомогательных и основных) объекта аттестации. Данная информация указывается в техническом паспорте на автоматизированную систему.

– документы должны содержать сведения об особенностях и схеме расположения информационной системы с обязательным указанием границ контролируемой зоны, определенной организацией. Данная информация указывается в техническом паспорте на автоматизированную систему, также выпускается приказ руководителя организации «Об установлении контролируемой зоны для организации технической защиты конфиденциальной информации», как правило, границы контролируемой зоны соответствуют границам самой организации.

– должна быть описана структура программного обеспечения (прикладного, общесистемного и специализированного), применяющегося на объекте испытаний и использующегося для обработки информации, подлежащей защите, документы должны содержать сведения об используемых протоколах информационного обмена. Данные сведения имеются в описании технологического процесса обработки информации в автоматизированной системе.

– документы должны содержать функциональную схему информационной системы, в том числе возможные режимы обработки охраняемых сведений и общую схему потоков информации. Сведения отражаются в техническом паспорте на автоматизированную систему, матрице распределения полномочий по категориям персонала, инструкции системного администратора автоматизированной системы.

– должны быть описаны возможность взаимодействия с другими информационными системами и каким образом взаимодействие осуществляется. Сведения указываются в техническом паспорте автоматизированной системы и в инструкции системного администратора.

– в документах отражается полная характеристика системы защиты информации объекта информатизации (из чего состоит, каким образом выполняет свои функции). Сведения указываются в технологическом процессе обработки информации в автоматизированной системе.

– должно быть описание всех программных и технических средств, применяющихся в защищенном исполнении. Также проверяется наличие сертификатов соответствия средств защиты информации, эксплуатирующихся в информационной системе и применяющихся для контроля и защиты данных. Сведения размещаются в техническом паспорте автоматизированной системы и модели угроз ПДн.

– должны быть приведены сведения о лицах, занимавшихся разработкой системы защиты информации на объекте информатизации, сведения о наличии у них лицензии на осуществление данного вида работ. Сведения размещаются в техническом паспорте автоматизированной системы.

– приводится информация о присутствии в организации, которой принадлежит объект аттестации, сотрудников, занимающихся защитой информации, также о присутствии в штате организации администраторов автоматизированных систем различной направленности. Данная информация отражается в приказе о назначении администратора безопасности в автоматизированной системе, приказе о назначении системных администраторов, инструкции администратора безопасности, инструкции по проведению антивирусного контроля, инструкции по парольной защите.

– описывается структура физической защиты как самой организации, так и объекта аттестации в частности, раскрываются такие сведения как наличие охраны предприятия, хранение носителей в сейфах и .т.п. Сведения указываются в техническом паспорте, модели угроз ПДн и приказе «Об установлении контролируемой зоны для организации технической защиты конфиденциальной информации».

– проверяется эксплуатационная и проектная документация на информационную систему, оценивается её структура и содержание в части защиты информации. Информация отражается в техническом паспорте, инструкции системного администратора.

Исходя из написанного выше для проведения аттестации автоматизированной системы на соответствие требованиям безопасности информации необходимо следующие документы:

– акт классификации информационной системы;

– перечень информационных ресурсов и объектов доступа, подлежащих защите в информационной системе;

– модель угроз безопасности ПДн при их обработке в информационной системе;

– приказ о назначении администраторов безопасности информации системы;

– приказ о назначении системных администраторов;

– технический паспорт на объект аттестации;

– матрица доступа к информационным ресурсам системы;

– матрица распределения полномочий по категориям персонала объекта аттестации;

– акт установки общесистемного программного обеспечения и системы защиты информации от несанкционированного доступа в автоматизированной системе;

– описание технологического процесса обработки информации на объекте аттестации;

– инструкция системного администратора автоматизированной системы;

– инструкция администратора безопасности информации автоматизированной системы;

– инструкция по проведению антивирусного контроля в автоматизированной системе;

– инструкция по парольной защите в автоматизированной системе.

Одним из необходимых документов для определения дальнейших путей защиты информационной системы является акт классификации, чтобы его составить необходимо провести классификацию объекта.

Для правильно определения класса информационной системы изначально нужно установить категорию циркулирующих в ней ПДн:

четвертая категория – в системе содержатся общедоступные ПДн;

третья категория – в системе содержатся ПДн, по которым можно опознать человека;

вторая категория – в системе содержатся ПДн, по которым можно опознать человека и узнать о нем дополнительные сведения;

первая категория – в системе содержатся ПДн, раскрывающие религиозные и политические убеждения, национальность, расу, медицинские сведения и субъектах данных.

Помимо категории защищаемой информации нужно знать количество обрабатываемых сведений. В зависимости от количества субъектов, сведения которых обрабатывает автоматизированной системой, выделяются следующие объемы:

объем 3 – менее 1000 субъектов ПДн;

объем 2 – от 1000 до 100000 субъектов ПДн;

объем 1 – более 100000 субъектов ПДн.

Зная категорию и объем данных, можно установить класс автоматизированной системы. Существует четыре класса:

первый класс – нанесение вреда безопасности данных способно нанести значительный вред субъектам. К этому классу принадлежат системы ПДн первой категории независимо от объема, а также системы ПДн второй категории первого объема.

второй класс – нанесение вреда безопасности данных способно нанести чувствительный вред субъектам. К этому классу принадлежат системы ПДн третьей категории первого объема и второй категории второго объема.

третий класс – нанесение вреда безопасности данных способно нанести незначительный вред субъектам. К этому классу принадлежат

системы ПДн третьей категории третьего либо второго объема, а также ПДн второй категории третьего объема.

четвертый класс – нанесение вреда безопасности данных не нанесет вреда субъектам. К этому классу принадлежат системы ПДн четвертой категории любого объема.

Для более наглядного представления информации сведения о связи класса информационной системы ПДн с ее категорией и объемом циркулирующих данных отображены в таблице 1.

Таблица 1 – Зависимость класса информационной системы ПДн от категории и объема данных

Категория / Объем данных	Первая	Вторая	Третья	Четвертая
Первый	Первый класс	Первый класс	Второй класс	Четвертый класс
Второй	Первый класс	Второй класс	Третий класс	Четвертый класс
Третий	Первый класс	Третий класс	Третий класс	Четвертый класс

В соответствии с этим автоматизированной системе ГБПОУ «ЮУрГТК» присваивается второй класс, так как в ней обрабатываются ПДн, по которым можно опознать человека и узнать о нём дополнительные сведения, количество субъектов ПДн находится в пределах от 1000 до 100000, а нарушение безопасности данных может нанести чувствительный вред субъектам.

2 Методики испытаний автоматизированной системы ГБПОУ «Южно-Уральский государственный технический колледж»

В данном параграфе отражены методы испытаний системы обработки информации ГБПОУ «Южно-Уральский государственный технический колледж» для установления соответствия АС требованиям информационной безопасности.

Для проведения испытаний АС необходимы следующие материалы:

– Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден Гостехкомиссией России, 1992 год.

– документация, описывающая способы эксплуатации системы в целом, программных и технических средств защиты информации, использующихся для защиты данных АС, вспомогательного оборудования, основная техническая документация на систему.

Опытные испытания системы включают следующие действия и этапы проведения:

– изучение предоставленных первоначальных данных и их сопоставление реальным свойствам АС, в части расположение технических средств, их сборки и параметров использования, анализ описанного технологического процесса работы АС и сопоставление его с реальными действиями пользователей в ходе эксплуатации системы, изучение потоков информации системы, изучение реального состава использующихся для обработки информации технических средств, анализ их задействования в проведения работ;

– изучение организации процесса ведения работ, достаточности мер по защите информации, в процессе обработки данных, анализ правильности присвоения класса АС, изучение достаточности разработки документов, регламентирующих действия в ходе эксплуатации, организационной и проектной документации на систему, проверка компетентности пользователей, допущенных к работе в АС и отвечающих за сохранность информации в системе; оценка разработанности и включения в документы пунктов ответственности пользователей за сохранность информации;

– проведение опытной проверки АС по сохранению информационных данных в случае совершения попыток НСД и попыток воздействия на информационные данные при помощи специализированного программного обеспечения;

– формирование итоговых документов по результатам оценки соответствия АС требованиям информационной безопасности.

Изучение предоставленных первоначальных данных и их сопоставление реальным свойствам АС, в части расположение технических средств, их сборки и параметров использования, анализ описанного технологического процесса работы АС и сопоставление его с реальными действиями пользователей в ходе эксплуатации системы, изучение потоков информации системы, изучение реального состава использующихся для обработки информации технических средств, анализ их задействования в проведения работ:

– Для проведения испытаний системы должно быть обеспечено наличие следующих документов на систему:

а) список ресурсов подлежащих защите в информационной системе, с обоснованием уровня конфиденциальности каждого из них.

б) акт классификации информационной системы.

в) модель угроз безопасности ПДн при их обработке в информационной системе.

г) приказ о назначении администраторов безопасности информации системы.

д) приказ о назначении системных администраторов.

е) технический паспорт на объект аттестации.

ж) матрица доступа к информационным ресурсам системы.

з) матрица распределения полномочий по категориям персонала объекта аттестации.

и) акт установки общесистемного программного обеспечения и системы защиты информации от несанкционированного доступа в автоматизированной системе.

к) описание технологического процесса обработки информации на объекте аттестации.

л) инструкция системного администратора автоматизированной системы.

м) инструкция администратора безопасности информации автоматизированной системы.

н) инструкция по проведению антивирусного контроля в автоматизированной системе.

о) инструкция по парольной защите в автоматизированной системе.

Список необходимой документации для проведения аттестации может дополняться при необходимости выяснения более углубленных данных об АС и уточнения принципов обработки защищаемой информации, циркулирующей в ней.

– для проведения оценки правильности написания технологического процесса обработки информации АС проверяют следующие критерии:

а) изучают объект доступа, для информационной системы им являются все средства обработки данных, входящие в ее состав, такие как бумажные и электронные носители, файлы памяти вычислительных машин и др.;

б) изучают субъект доступа, им являются все лица и программные компоненты, которые имеют доступ к защищаемой информации на любом из видов носителей.

– для проведения анализа полной технологической схемы системы со всеми потоками информации изучают документы, регламентирующие порядок доступа пользователей к ресурсам АС (матрица разграничения прав доступа, матрица распределения полномочий по категориям персонала, допущенного к работе в системе и т.п.).

– для подтверждения соответствия правильности эксплуатации, функционирования и защищенности системы проводят сопоставление описанного в документах процесса обработки информации реально практикующемуся в АС.

– в целях проверки безопасности функционирования АС сравнивают первоначальные документированные данные о системе с реально существующей информацией (состав, характеристики, режимы обработки информации), изучают незащищенные уязвимые места по средствам составления модели угроз.

– для анализа безопасности данных системы изучают документы, регламентирующие доступ пользователей к различным категориям данным, исследуют достаточность разработки требований к пользователям, их ответственности, в случае выявления фактов утечки информации, разработанность инструкций, в которых задокументированы основные положения в части обработки информации.

– для исследования всех режимов функционирования АС изучают схему технологического процесса обработки информации в части работы каждого технического средства, имеющего доступ к конфиденциальной информации, с привязкой к конкретным пользователям (по должностям).

3 Проверка состояния организации работ и выполнения требований безопасности информации

Проверка состояния выполнения работ и соответствия требованиям информационной безопасности содержит пункты:

– анализ полноты разработки документации на АС в соответствии с реальными условиями функционирования системы и требованиями регламентирующих документов.

Изучают предъявляемые документы на систему, дают заключение о соответствии их содержания руководящим документам по информационной безопасности в Российской Федерации.

Сверяют сведения из документации на систему с реальными условиями расположения технических средств, документы не должны содержать противоречивых сведений об АС.

Положительные выводы по АС даются в случае полного соответствия предъявляемых документов вышеописанным требованиям.

– анализ правильности указания расположения технических средств в соответствии с предъявляемой документаций.

Сопоставляют марки, наименования, расположения технических средств информации, приведенной в представленной документации на систему.

Сравнивают состав реально установленного общесистемного и прикладного программного обеспечения, средств защиты информации с документальными данными, представленными для проверки.

Положительные выводы по АС даются в случае полного соответствия предъявляемых документов вышеописанным требованиям и отсутствия в них противоречивых сведений.

– анализ соответствия класса защищённости АС представленным документам.

Выявляют наивысшую степень конфиденциальности данных, циркулирующих в информационной системе, изучают распределение прав доступа пользователей к данным по категориям персонала, анализируют потоки данных, присваивают класс системе в соответствии с регламентирующими документами Российской Федерации.

Положительные выводы по АС даются в случае, если реальный класс испытуемой системы соответствует классу, зафиксированному документально.

– изучение уровня компетентности пользователей и достаточности закрепления ответственности по категориям персонала.

Проводят проверку изученностью пользователями всех регламентирующих работу документов. Изучают структуру распределения ответственности за соблюдение требований информационной безопасности.

Инициируют проведение тестирования всех категорий пользователей системы на предмет знания ими требований инструкций и других

руководящих документов по работе в системе. Методы выявления и устранения некомпетентности пользователей системы информационной безопасности образовательной организации приведены в параграфе 2.7.

Положительные выводы по АС даются в случае, если уровень компетентности пользователей позволяет обеспечивать необходимую степень защищенности обрабатываемых в системе данных.

– анализ соответствия помещений, где расположены составные части системы, всем требованиям информационной безопасности.

В ходе визуального осмотра изучают соответствие помещений, где расположена АС, требованиям информационной безопасности, предъявляемым к ним. Анализируют исполнение требований инструкций по безопасности информации в части функционирования и обработки информации в АС.

Проводят сверку соответствия расположения технических средств системы предъявляемым документам. Расположение мониторов должно исключать возможность несанкционированного доступа к визуальной информации, должна быть обеспечена безопасность функционирования всех устройств, участвующих в обработки информации.

Положительные выводы по АС даются в случае ее соответствия всем указанным выше требованиям.

– после проведения всех обследований составляется итоговое заключение с обоснованием соответствия (или несоответствия) представленной документации регламентирующим требованиям по информационной безопасности.

4 Методы разграничения прав доступа к персональным данным

Для повышения эффективности системы обеспечения информационной безопасности в первую очередь нужно обеспечить сохранность основных объектов защиты любой образовательной

организации – персональных данных и информации для служебного пользования. Для выполнения данной задачи необходимо совершенствовать систему разграничения прав доступа к информации в направлении усиления защиты. Актуальность исследования обусловлена тем, чт**о** в случае, если работа системы разграничения прав доступа к данным образовательной организации недостаточно налажена, при использовании автоматизированных рабочих мест (АРМ) сотрудниками организации возможен несанкционированный доступ к информации (НСД) лиц, не допущенных к процессу обработки ПДн и информации для служебного пользования.

Для совершенствования системы обеспечения информационной безопасности образовательной организации в части разграничения прав доступа к ПДн возможны следующие варианты:

а) использование организационных мер защиты систем ПДн:

– АРМ, предназначенные для хранения и обработки ПДн, не общедоступны и расположены в физически защищенных помещениях (замок на двери, жалюзи), доступ в помещения имеют только лица, допущенные к обработке ПДн.

– доступ пользователей к системе осуществляется под собственными, известными только владельцу, идентификаторами (логином и паролем), смена паролей осуществляется не реже одного раза в 3 месяца.

– доступ АРМ, предназначенного для обработки ПДн, к сети Интернет отсутствует.

– существует возможность использования только рабочих (учтенных) носителей информации, прописанных администратором безопасности в данной системе, вынос носителей информации с территории образовательной организации осуществляется в случаях необходимости по разрешению лица, ответственного за обработку ПДн в организации.

б) комплекс программно-аппаратных и организационных мер совершенствования работы системы разграничения прав доступа к ПДн:

– доступ пользователей к системе осуществляется под собственными, известными только владельцу, идентификаторами (логином и паролем), смена паролей осуществляется не реже одного раза в 3 месяца.

– доступ пользователей к каталогам и ресурсам системы разграничен администратором безопасности.

– настройка блокирования системы при отсутствии действий в течение 15 минут.

– использование лицензионного программного обеспечения (ПО).

– антивирусное ПО обновляется не реже 1 раза в месяц.

– доступ пользователей к сети Интернет ограничен (возможно использование только определенного набора разрешенных интернет сервисов).

– существует возможность использования только рабочих (учтенных) носителей информации, прописанных администратором безопасности в данной системе, вынос носителей информации с территории образовательной организации осуществляется в случаях необходимости по разрешению лица, ответственного за обработку ПДн в организации.

в) использование программных мер защиты ПДн (на примере программы Страж NT).

Использование программного продукта, позволяет:

– производить аутентификацию до загрузки операционной системы (в том числе и для виртуальной среды) с использованием аппаратных идентификаторов (USB-идентификаторов типа Guardant ID, дискета 3,5”, смарт-карт Рутокен и т.п.);

– обеспечить дискреционный принцип контроля доступа к ресурсам системы;

– создание замкнутой программной среды пользователя, позволяющей ему запуск только разрешенных приложений;

– производить регистрацию событий безопасности, в том числе и действий администратора.

– осуществлять маркировку выдаваемых на печать документов независимо от печатающего их приложения;

– обеспечивать гарантированную очистку освобождаемой оперативной памяти, содержимого защищаемых файлов при их удалении, файла(ов) подкачки при завершении работы системы;

– производить контроль целостности защищаемых ресурсов системы и компонентов системы защиты информации;

– управлять носителями информации;

– управлять устройствами;

– производить тестирование системы защиты информации.

В каждом из трех предложенных вариантов решения есть отрицательные моменты, основные из них рассмотрены в таблице 2.

Таблица 2 – Отрицательные стороны предложенных вариантов

№ п\п	Организационные меры	Комплекс программно-аппаратных и организационных мер	Программные меры (Страж NT)
1	Необходимость использования (закупки) АРМ предназначенных исключительно для обработки ПДн	Необходимость привлечения администратора безопасности	Закупка ПО (от 5 до 7,5 тыс. руб. за АРМ)
2	Невозможность работы АРМ в сети Интернет	Закупка носителей информации	Необходимость привлечения администратора безопасности
3	Организация отдельных помещений для работы с АРМ		
4	Необходимость привлечения администратора безопасности		
5	Закупка носителей информации		

При использовании ГБПОУ «ЮУрГТК» указанных выше мер защиты информации вероятность сохранности защищаемых данных значительно возрастает. Но самым надежным методом определения уровня безопасности

автоматизированной системы является прохождение ей аттестации на соответствие требованиям по безопасности информации.

5 Методы выявления и устранения некомпетентности пользователей системы информационной безопасности образовательной организации

В настоящее время основным источником угроз для безопасности, циркулирующей в информационных системах образовательных организаций, являются в первую очередь сами пользователи этой системы. В данном случае речь не идет о злом умысле и противоправных действиях, главная опасность заключается в неосведомленности участников информационных процессов основными принципами безопасности информации. В проекте Методики определения угроз безопасности информации в информационных системах (ИС) ФСТЭК России говорится: «следует, в первую очередь, уделять внимание оценке антропогенных угроз, связанных с несанкционированными (неправомерными) действиями субъектов по нарушению безопасности (конфиденциальности, целостности, доступности) информации, в том числе целенаправленными воздействиями программными (программно-техническими) средствами на информационные системы, осуществляемые в целях нарушения (прекращения) их функционирования».

Итак, основными задачами для выявления и устранения некомпетентности пользователей являются:

– определение действенных методов нахождения пробелов в знаниях информационной безопасности;

– оценка способов устранения этих пробелов;

– анализ результатов повышения грамотности в области информационной безопасности.

Для начала рассмотрим наиболее распространенные угрозы безопасности, с которыми сталкиваются пользователи информационных систем образовательных организаций:

– общедоступность персональных паролей;

– не соблюдение разграничения прав доступа к информации;

– рассылки фишинговых писем;

– не умение пользоваться программными средствами защиты информации.

Итак, в качестве первого пункта по определению пробелов пользователей в области информационной безопасности возможно проведение анкетирования персонала на знание основных принципов защиты информации, тест предлагается составить в следующем ключе:

1. Для отправки сообщений по рабочим вопросам, каким электронным почтовым ящиком вы пользуетесь:

– домашним;

– рабочим;

– по-разному.

2. Можете ли Вы сообщить пароль от рабочего ПК одному из своих коллег?

– нет;

– да;

– в зависимости от ситуации;

3. Используете ли Вы антивирусное программное обеспечение во время работы на ПК организации?

– да;

– нет;

– не всегда.

4. Как часто производится смена паролей на Вашем рабочем компьютере?

– не реже одного раза в 3 месяца;

– не реже оного раза в 6 месяцев;

– реже чем раз в 6 месяцев.

5. При возникновении необходимости покинуть рабочее место на небольшой промежуток времени с намерением дальнейшего продолжения работы, что Вы сделаете?

– выключите компьютер;

– заблокируете свой аккаунт;

– закроете все открытые приложения;

– оставите все как есть.

6. Открывали ли Вы ссылки из поступающих электронных писем с неизвестных адресов?

– да;

– нет;

– в зависимости от ситуации.

Затем производится проверка данного теста и оглашение работникам результатов и правильных ответов.

Далее предлагается произвести проверку пользователей на практическое выполнение вопросов теста:

– рассылка проверочных фишинговых писем с дальнейшим выявлением «попавшихся».

– просмотр журналов смены паролей на рабочих ПК.

– наблюдение за пользователями на предмет оставления рабочих компьютеров без присмотра, распространения личных паролей и т.п.

– контроль использования рабочих электронных почтовых ящиков.

В завершении проверочных мероприятий проводится подробный инструктаж по информационной безопасности не прошедших проверку пользователей, где на примерах рассматриваются возможные угрозы безопасности организации и способы борьбы с ними. А также обговариваются все возможные последствия несоблюдения основных требований по защите информации.

Все подобные мероприятия рекомендуется проводить не реже одного раза в год, а также при появлении новых пользователей информационной системы.

Безопасность информационной системы организации один из ключевых показателей стабильности ее работы, об этом стоит помнить всем, начиная от руководства и заканчивая рядовыми пользователями. Основной задачей руководства является донесение важности этого показателя, своевременное обнаружение слабых звеньев и устранение пробелов знаний персонала в этой области.