Государственное бюджетное профессиональное образовательное учреждение города Москвы Колледж железнодорожного и городского транспорта

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования связана с необходимостью обеспечения информационной безопасности баз данных, как основного элемента структуры информационной системы на предприятии. Расширяя сферы применения информационных технологий в управлении деятельностью, компания идет на повышение рисков потери или порчи используемых данных.

Практика проходила в период с «06» апреля 2019 г. по «19» апреля 2019 г. в Государственном бюджетном профессиональном образовательном учреждении города Москвы «Колледж железнодорожного и городского транспорта» (ГБПОУ КЖГТ).

Цель прохождения практики состоит в закреплении и углублении знаний и умений, полученных в процессе изучения специализированных дисциплин и дисциплин общепрофессионального цикла, приобретении новых профессиональных навыков в соответствии с требованиями к уровню подготовки выпускника.

Достижение цели практики может быть реализовано путем решения следующего комплекса задач:

– освоение современных методик работы с информацией, включающие сбор, анализ и обработку научной и технической информации;

– изучение и овладение методиками работы в современных информационных системах, представленных в сфере работы организации прохождения практики;

– ознакомление со структурами и технологиями организации процесса управления на предприятиях и организациях;

– выполнение индивидуального задания по указанию руководителя практики.

Результатом прохождения практики стало решение указанных ниже задач:

– рассмотрены виды деятельности и функции ГБПОУ КЖГТ;

– рассмотрены техническое и программное обеспечение организации ГБПОУ КЖГТ;

– проведен обзор нормативно-правовой базы Российской Федерации в области технической защиты информации;

– изучен метод применения нечетких когнитивных карт для для анализа рисков информационной безопасности;

– смоделированы риски информационной безопасности на основе НКК для ГБПОУ КЖГТ.

Во время прохождения практики студентом были приобретены практические навыки на должности специалиста ИТ-отдела.

При написании отчета по практике использовались научные труды специалистов в сфере информационной безопасности: БирюковаА.А. [14], ПолтавцеваМ.А, Хабаров А.Р. [21] и Васильева В. И.[31].

1 Характеристика объекта практики

1.1 Основные сферы деятельности предприятия

В 2012 году Государственное бюджетное профессиональное образовательное учреждение города Москвы «Колледж железнодорожного и городского транспорта» получил свидетельство о сертификации образовательного учреждения, удостоверяющее, что уровень и качество подготовки, переподготовки и повышения квалификации специалистов отвечает требованиям для включения данного образовательного учреждения в реестр Торгово-промышленной палаты Российской Федерации[32].

В этом же году Департаментом по развитию предпринимательства и инновационной деятельности Правительства Москвы колледжу присвоен статус «Лидера инновационной экономики России 2012».

Стратегическими партнерами Колледжа железнодорожного и городского транспорта являются:

– ОАО «РЖД»;
– Московская и Октябрьская железные дороги;
– ГУП «Московский метрополитен»;
– ОАО «Федеральная пассажирская компания»;
– ОАО «ФПК» Московский филиал;
– ООО «Железнодорожный Сервис-Центр «Курс»;
– ГУП «Мосгортранс»;
– ГУП «Мослифт»;
– ОАО «МОСОТИС».

Основные направления обучения в колледже связаны с железнодорожным и городским транспортом и его обеспечением:

– «Техническая эксплуатация подвижного состава железных дорог»;
– «Организация перевозок и управление на железнодорожном транспорте»;
– «Сервис на транспорте (по видам транспорта)»;

– «Техническая эксплуатация и обслуживание электрического и электромеханического оборудования (по отраслям)»;

– «Эксплуатация транспортного электрооборудования и автоматики(по видам транспорта, за исключением водного)»;

– «Прикладная информатика (по отраслям)».

В процессе обучения студенты овладевают очень востребованными профессиями в железнодорожном и городском транспорте.

Структура управления колледжа предполагает выделение следующих направлений деятельности (рисунок 1.1):учебная работа, учебно-производственная работа, учебно-воспитательная работа.

В подчинении директора колледжа находятся первый заместитель и три заместителя, каждый из которых курирует соответствующее направление. При этом организация получает бюджетное финансирование, поэтому функционал ее обеспечивающих подразделений ограничивается исключительно хозяйственной деятельностью. Управление этим направлением передано первому заместителю директора, в подчинении которого находятся заведующий лабораторий и мастерских, а также отдел хозяйственного обеспечения, канцелярия и архив.

Руководителем организации является директор колледжа, который выполняет весь спектр обязанностей по управлению организацией и выработки стратегии ее развития. В должностные обязанности директора входит формирование планов по финансированию колледжа и формированию его организационной структуры. Заместитель директора по содержанию образования является руководителем учебного направления и в его подчинении находятся заведующие отделениями, в рамках которых работают специализированные кафедры. Вне иерархии организации работают цикловые комиссии по направлениям, состоящие из преподавателей различных кафедр и отделений.

Рисунок 1.1 – Организационная структура колледжа

В рамках этого же направления работает библиотека, заведующий которой подчиняется также заместителю директора по содержанию образования и отборочная комиссия, подготовительное отделение.

Обслуживание деятельности организации ведет учебно-производственное направление, которое включает не только управление хозяйственной частью, но и материально-техническое обеспечение лабораторий и мастерских, которые являются структурными подразделениями колледжа.

1.2 Оценка существующего обеспеченияИТ-процессов

Организация компьютерной сети в колледже ГБПОУ КЖГТпостроена с учетом выделения учебно-производственного направления, которое требует отдельного дополнительного уровня защиты данных о преподавателях и студентах, которые необходимы для формирования расписания и распределения нагрузки преподавателей. Сеть представлена следующими основными компонентами:

– серверы, обеспечивающие хранение и манипулирование основными данными, а также взаимодействие внутри сети;

– оборудование для проводного подключения отделов колледжа к сети интернет, а также внутрисетевой интеграции;

– оборудование для предоставления беспроводного доступа к сети для удаленных сотрудников от основных точек раздела доступа.

Общий сервер снабжен дополнительным оборудованием для хранения больших объемов данных и предназначен для управления данными о студентах, преподавателях, учебных планах и учебных программах. На сервере реализовано резервное копирование базы данных, поддерживающей работу с расписанием в рамках «1С: Автоматизированное составление расписания. Колледж».

Для этой системы реализована дополнительная защита и выделен сервер для хранения персональных данных преподавателей и учебных программ, доступ к серверу в колледже строго регламентирован. Работа многих лабораторий организована в специализированных помещениях и для их

заведующих организован удаленный доступ к сети интернет и локальной сети колледжа.Таблица 1.1отражает данные по применяемому компьютерному и сетевому оборудованию. Рисунок1.2 представляет схематичную модель технической архитектуры**.**

Таблица 1.1 – Техническое оснащение ГБПОУ КЖГТ

№ п/п	Обозначение	Наименование и техническая характеристика	Кол-во, шт.
1	Сервер	Сервер Двухпроцессорный TechHub BIGDATA1 2CPUs Xeon E5-2640 16GB RAM: – два процессора IntelXeon E5-2640 12 ядер 24 потока, 2.5-3.0 GHz LGA2011 – материнскаяплата Intel (Supermicro, Foxconn) – ОЗУ Samsung (Hynix, Micron, etc) 16GB DDR3 ECCREG – видеокарта встроенная – башенное охлаждение – тихое и эффективное – блок питания 700W 80+ – корпус на выбор: ChieftecGP-01B-OP, максимальное кол-во дисков в системе = 4 HDD + 2 SSD, или стоечный формата 4U (до 10 HDD)	2
2	19' шкаф с набором доп. элементов и крепежом	-	1 шт.
3	Рабочая станция (заведующих отделениями, преподавателей)	Intel Core i3-4130 (3.4 ГГц) / RAM 2 ГБ / HDD 500 ГБ / nVidia GeForce GTX 750, 1 ГБ / LAN	25
4	Рабочая станция (зав. хозяйственной частью, зам. директора)	Patriot S100 (N3150.2.500 mATX): Intel Celeron / N3150 (1.6-2.08 ГГц) / 2 Gb / 500 Гб / Intel® HD Graphics	4

Продолжение таблицы 1.1

№ п/п	Обозначение	Наименование и техническая характеристика	Кол-во, шт.
5	Монитор	Philips 220X1SW/00 glossywhite: ЖК (TFTTN) 22", широкоформатный, 1680x1050, 300 кд/м2, 2 мс, 160°/160°, DVI, VGA	12
6	Маршрутизатор	MikrotikRouterBOARD 951G-2HnD	5
7	Источник бесперебойного питания	ИБП EATON 5S 700 ВА	2
8	Роутер	MIKROTIK CRS125-24G-1S-2HnD-IN	2
9	Многофункциональ-ное устройство	МФУ HP LJ Pro M426fdn (F6W14A) ; A4	2
10	Внешнее хранилище данных	Western Digital 6TB 5400rpm 64MB Red WD60EFRX	1
11	Смартфоны сотрудников (заведующих лабораторий)	LenovoA316i 3GBlack Смартфон; MediaTekMT6572 1.3 ГГц / основная камера 2 Мп / Bluetooth 3.0 / Wi-Fi 802.11 b/g/n / 512 МБ оперативной памяти / 4 ГБ встроенной памяти + поддержка microSD	15
12	Межсетевой экран	Cisco SB RV110W Wireless N VPN Firewall (RV110W-E-G5-K9)	2

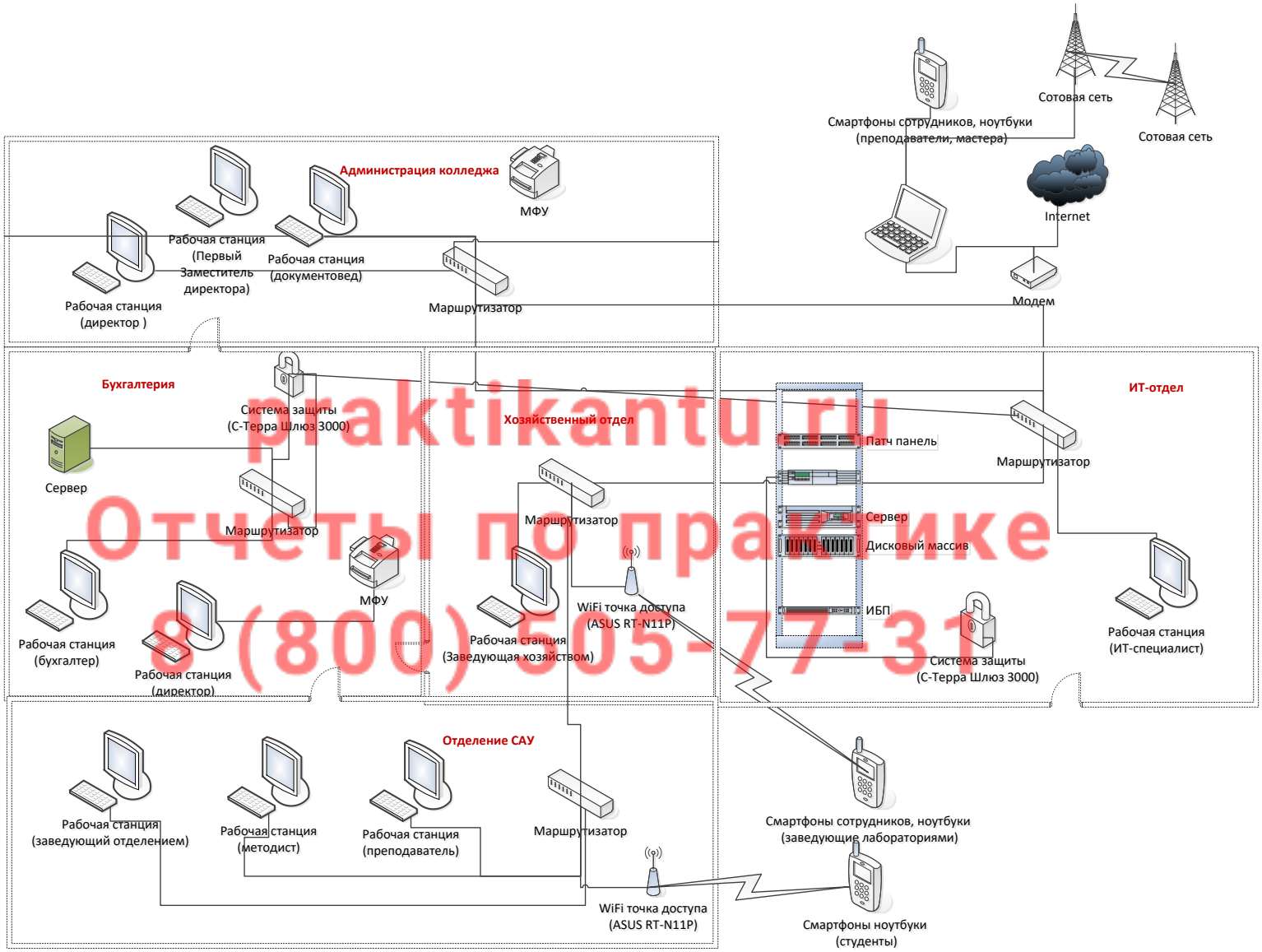

Рисунок1.2– Упрощенная техническая архитектура ГБПОУ КЖГТ (территория 1)

Автоматизация не коснулась всех сфер деятельности колледжа, однако составление расписания автоматизировано при помощи конфигурации «1С Автоматизированное составление расписания. Колледж» на платформе «1С: Предприятие 8.3», а бухгалтерия работает на базе конфигурации «1С: Бухгалтерия» (таблица 1.2).

Таблица 1.2 – Программное обеспечение ГБПОУ КЖГТ

Обозначение	Тип лицензии	Количество
MySQL 5.5	Открытое программное обеспечение	2 шт.
MSOfficePro 2010	Коробочная версия	35 шт.
1С Автоматизированное составление расписания. Колледж	Лицензия на сервер (платформа «1С: Предприятие 8.3») и 20 рабочих мест	1 шт.
1С: Бухгалтерия	Лицензия на 5 рабочих мест	1шт.
Windows7	Коробочная версия	35 шт.
Сервер nginx	Открытое программное обеспечение	1 экз.
Обработчик php 5.6.8	Открытое программное обеспечение	1 экз.

Сотрудники бухгалтерии используют конфигурацию «1С: Бухгалтерия» на базе той же платформы «1С: Предприятие 8.3». Заведующий хозяйственной частью для хранения данных о движимом имуществе использует файловый сервер. Данные по имуществу необходимы также заведующим лабораторий и мастерских, они получают доступ к данным по имуществу посредством локальной сети колледжа.

Сайт колледжа развернут на базе СУБД MySQL 5.5 и веб-сервера nginx, методисты, отвечающие за контент сайта колледжа, используют phpMyAdminдля манипулирования информацией на сайте**(**рисунок1.3**).**

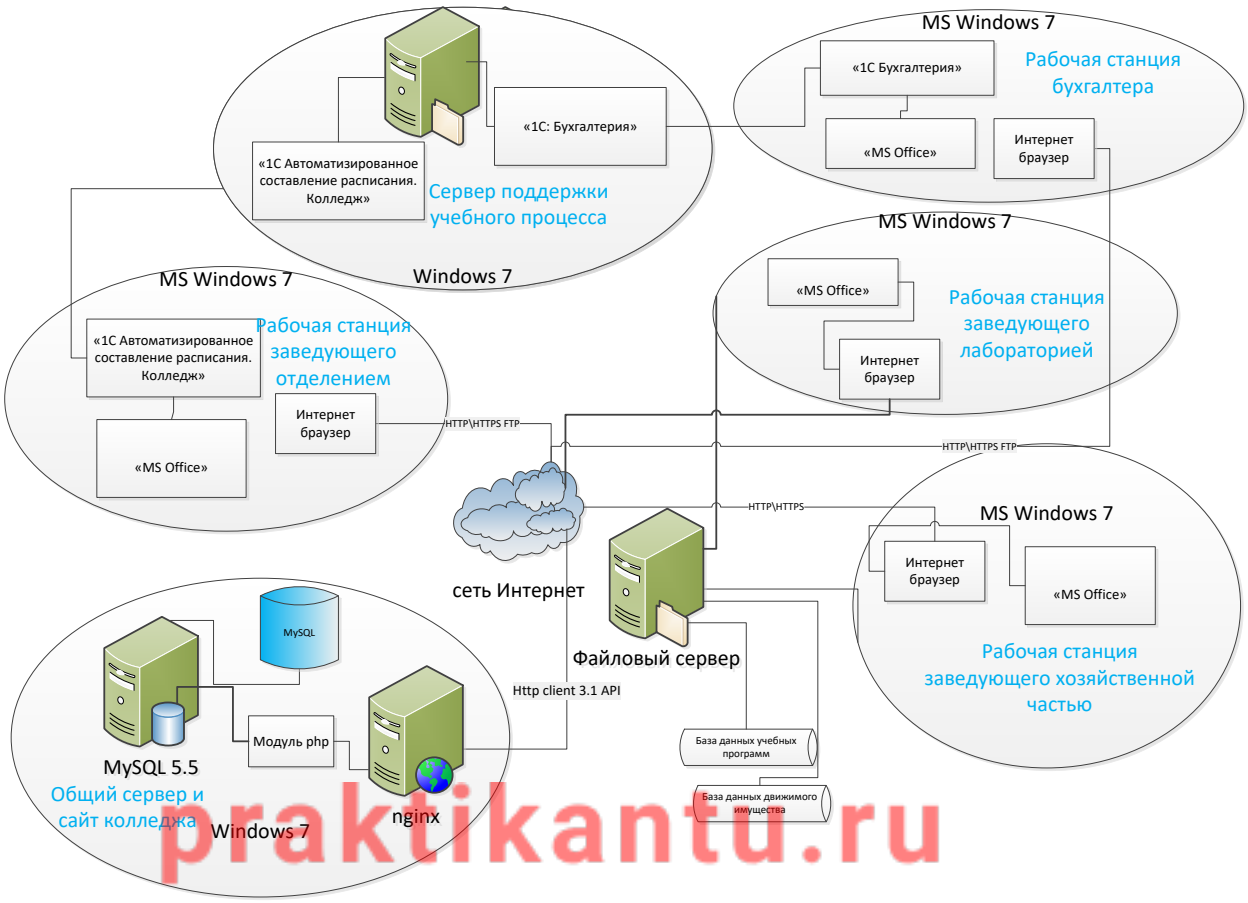

Рисунок1.3– Программная архитектура ГБПОУ КЖГТ (территория 1)

Для организации общего доступа к ресурсам локальной сети, а также для предоставления доступа к сети интернет для студентов и преподавателей организованы Wi-Fiточки доступа.

2 Проблемы обеспечения безопасности баз данных

2.1 Обзор нормативно-правовой базы Российской Федерации в области технической защиты информации

В 80-90 х годах в России начало формироваться коммерческое право, которое впоследствии было увязано с правом интеллектуальной собственности и патентным правом. Понятие «информационная безопасность также активно разрабатывалась в конце 20 века, в период активной автоматизации процессов производства в нашей стране. Автоматизированная система стала основных хранителем информационных ресурсов, что определило необходимость принятия мер по обеспечению их охраны.

Впервые термин «информационная безопасность» был закреплен в Федеральном законе «Об участии в международном информационном обмене» (ныне утратившем силу)[8], в котором говорилось, что под этим понятием следует понимать состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Следует выделить три основных направления обеспечения информационной безопасности Российской Федерации:

– защита информационных прав и свобод человека и гражданина;

– защита информационных ресурсов, в том числе и информации с ограниченным доступом, от неправомерного доступа;

– защита общества от вредной и недоброкачественной информации.

За последние годы в Российской Федерации проведена существенная работа по созданию и совершенствованию обеспечения ее информационной безопасности. Сформирована правовая основа обеспечения информационной безопасности. Приняты Закон Российской Федерации «О государственной тайне»[9], федеральные законы «Об информации, информационных технологиях и о защите информации» [10], «О персональных данных»[11], ряд других законов, ведется работа по их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Совокупность требований к безопасности определенных продуктов и систем ИТ определяется в соответствии с имеющимися и прогнозируемыми угрозами безопасности, установленной политики безопасности, а также с учетом условий их использования.

Разработка комплекса мер по обеспечению защиты информации входят в сферу ответственности подразделений по защите информации (служб безопасности) либо отдельных специалистов, которые назначаются руководством предприятия (учреждения) для осуществления таких работ. Разработка такого комплекса мер по защите информации может быть осуществлена также сторонними организациями, обладающими лицензиями на право проведения данного вида работ, выдаваемыми Гостехкомиссией России или ФСБ России.

С целью полноценного изучения понятия безопасность необходимым является изучение объектов безопасности. Данное определение является справедливым по отношению к гражданам (их прав и свобод), государству (территориальная целостность, суверенитет, конституционный строй), а также обществу (духовные и материальные ценности). Следовательно, деятельность по обеспечению безопасности осуществляется в соответствии с потенциальными и реальными угрозами (которые могут быть вызваны как внутренними, так и внешними источниками) по отношению к вышеназванным объектам.

В связи с бурным технологическим развитием и увеличением числа компьютерных преступлений появилась необходимость в обеспечении информационной безопасности (ИБ) в рамках правового поля. Основой правового обеспечения ИБ являются нормативные акты и указы, действующие в государстве, в соответствии с которыми происходит регламентирование обращения с информацией и данными, и ответственности в случае их нарушения. Ответственность за реализацию правового обеспечения ИБ возложена на государство. Организационными мерами по защите информации являются действия, которые способствуют регламентации функциональных

систем обработки данных, эксплуатации их ресурсов, деятельности сотрудников определенного предприятия и порядку взаимодействия с пользовательской системой.

При выполнении всего комплекса мер любые возможности реализации потенциальных угроз ИБ исключаются. Инженерно-техническое обеспечение ИБ включает в себя два направления – программную и аппаратно-программную защиту информации, а также физическую защиту элементов систем информации. В рамках первого направления могут быть использованы такие меры по защите информации, как антивирусные сканеры, системы аудита, системные и сетевые мониторы и т.д.

Второе направление заключается в использовании физических способов и методов защиты кабельных систем, систем энергоснабжения и данных, для реализации чего применяется дублирование. Можно с уверенностью говорить о том, что влияние понятия и видов безопасности, интегрируемых в системы жизнедеятельности, на жизнь общества в настоящий момент достаточно велико, или, другими словами, одним из определяющих условий гармоничного существования социума является защита.

На любом предприятии или значимом объекте при реализации политики безопасности ключевую роль играют технические методы защиты информации. Эти средства используются для поиска технических средств, направленных на кражу информации (часто устанавливаемых на территории объекта), для изоляции помещений на время проведения переговоров, либо иных важных совещаний (это делается с целью обезопасить технику, которая используется для обработки информации, и коммуникации).

Органом, уполномоченным в сфере технической защиты информации (кроме криптографической защиты), является Федеральная служба по техническому и экспортному контролю, ФСТЭК России, в спектр законов регламентирующих техническую защиту также входит федеральный закон «о техническом регулировании» [12].

Регламентация уровня ответственности за нарушение законодательства в области защиты информации возложена на соответствующие кодексы: уголовный, административный, налоговый, гражданский и др.

Вопросы лицензирования криптографической шифровальной деятельности регламентирует положение о лицензировании[], а также Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»определяет комплекс нормативных требований к защите персональных данных при обработке [13]

Особенности правового обеспечения технической защиты по документам ФСТЭК/Гостехкомиссии

– Положение «По аттестации объектов информатизации по требованиям безопасности информации»;

– РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;

– РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования по защите информации»;

– РД «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники»;

– РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

– РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

– РД «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации.

Классификация по уровню контроля отсутствия не декларированных возможностей» [23].

В настоящее время, разработан ряд методов по защите сведений. Одним из самых распространенных является метод создания препятствий, заключающийся в том, что злоумышленник сталкивается с «охранной программой» или комплексом защитных паролей. Также эффективным способом по обеспечению безопасности информационных систем является разграничение прав доступа к ней. Данное разграничение заключается в идентификации ресурсов, персонала и пользователей, проверка подлинности объекта или человека (в соответствии с установленным регламентом или образцом); ведении журнала всех обращений к защищаемым ресурсам; ответной реакции на попытки незаконных действий или несанкционированных проникновений в систему.

Разрабатываемая система касается следующихапсектов ИБ:

– защита информационных прав и свобод человека и гражданина;

– защита информационных ресурсов, в том числе и информации с ограниченным доступом, от неправомерного доступа;

Рассматривая поставленную в работе проблему по обеспечению защищенного взаимодействия преподавателя и студента можно говорить исключительно о проблеме защиты персональных данных, так как процесс и разработанная система не связаны не с хранением коммерческой, не тем более государственной тайной.

Соответственно вопрос защиты с точки зрения нормативно-правовых актов, которые регулируют способы защиты, определяется Федеральным законом «Об информации, информационных технологиях и о защите информации», а также Федеральным законом «О персональных данных».

Вопрос о защите информационных ресурсов, в том числе и информации с ограниченным доступом, от неправомерного доступа может стоять для системы только условно, либо в рамках принятого регламента учебным заведением.

Например, если в образовательном учреждении принято положение о домашних заданиях на правах рукописи, то они являются частной собственностью студента и требуют защиты от несанкционированного доступа, обычно такими свойствами обладают исключительно работы уровня курсовых и дипломных проектов, а также проекты научно-исследовательской деятельности.

Таким образом, с правой точки зрения наиболее актуальным является вопрос о защите персональных данных студента и необходимость защиты информации в разрезе защиты информационных прав и свобод человека и гражданина.

2.2 Применение нечетких когнитивных карт для анализа рисков информационной безопасности

Среди методов, направленностью которых является получение качественной оценки рисков, важное значение имеют методы когнитивного моделирования, основным назначением которых является исследование плохо формализуемых проблем и ситуаций за счет построения нечетких когнитивных карт (*Fuzzy Cognitive Maps, FCM*). Нечеткие когнитивные карты (НКК) были впервые предложены Б. Коско в 1986 г. в рамках его широко известной работы. В настоящее время произошло существенное расширение данного класса моделей, и в их состав входят обобщенные НКК, интервальные («серые») НКК, НКК в базисе «истина – ложь - неопределенность», продукционные НКК, реляционные НКК. Следует подробнее остановиться на сущности данной методики.

Нечеткие продукционные когнитивные карты (НПКК), либо нечеткие когнитивные карты, в основе которых лежат правила(*Rule Based Fuzzy Cognitive Maps*), были впервые предложены Х. Томе и Х. Карвалью в 1999 г. Они являются привлекательными для многих исследователей из-за своих, не подвергающихся сомнению, достоинств. Во-первых, они являются действительно нечеткими системами, которые дают возможность выполнить описание качественного поведения сложных систем, а

также их компонентов при помощи системы нечетких правил. Во-вторых, у них наблюдается значительная общность, допускается применение разных видов нечетких отношений (связей), в частности, обратных связей между входящими в их состав концептами. В третьих, данные карты позволяют учесть фактор времени, за счет чего существует возможность моделирования динамики плохо поддающихся формализации, сложных систем [19].

Под нечеткой продукционной когнитивной картой чаще всего понимается орграф (ориентированный граф), который задается парой множеств в соответствии с (2.1):

$$K = \{C, F\} \tag{2.1}$$

где $C = \{C_i\}, (i = 1,2,...,n)$является множеством вершин (узлов) орграфа, которые называются концептами; $F = \{F_{ij}\}, (i = 1,2,...,n)$является множеством дуг – отношений (связей) между концептами; n - количество концептов НПКК. Делается предположение, что переменную состояния X_i каждого концепта C_i следует рассматривать в качестве лингвистической переменной, которая принимает значение из определенного нечеткого терм-множества $\{T_{i1}, T_{i2},...,T_{im}\}$, термы (подмножества) которого $T_{ik}, (k = 1,2,...,m)$, задаются, в свою очередь, функциями принадлежности: $T_{i1} = \{(\mu_{ik}(X_i), X_i)\}, \mu_{ik} : X_i \to [0,1]$, где $X_i \in [0,1]$или $X_i \in [-1,1]$. Следует различать два вида концептов: уровни (*levels*), представляющие абсолютные значения состояния концепта в данный момент времени, и вариации (var*iations*), являющиеся изменениями состояния концепта по отношению к предыдущему моменту (отсчету) времени. Последнее представляет собой особую важность, так как дает возможность описать динамику поведения анализируемых систем. Чтобы определить взаимное влияние концептов $(C_i \to C_j)$, следует использовать ряд нечетких продукционных правил, которые позволяют осуществить представление условия (предпосылки) и заключение нечетких правил на базе нечетких множеств.

Рисунок 2.1 представляет пример задания нечетких правил для определения влияния концепта C_i на концепт C_j [16].

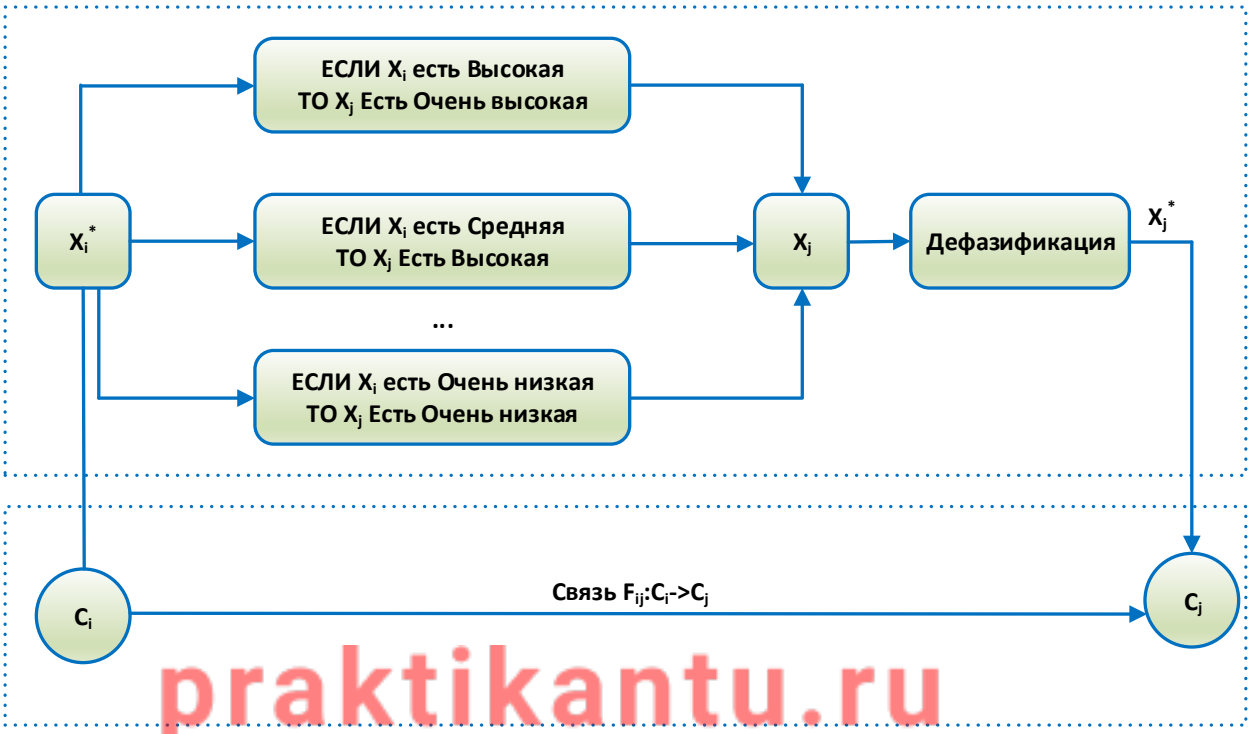

Рисунок 2.1 – Влияние концепта C_i на концепт C_j в НПКК (пример)

Делается предположение, что переменные X_i и X_j, которые характеризуют состояния концептов C_i и C_j, могут принимать значения, входящие в терм-множества{Очень высокая (VH), Высокая (H), средняя (M), Низкая (Z), Очень низкая (VL)}и задаваемые при помощи соответствующих функций принадлежности. Для того, чтобы осуществить реализацию процедуры нечеткого логического вывода (касательно определенного «четкого» значения входной переменной X_i^* и получения «четкого» значения переменной X_j^* на выходе), целесообразным является использование алгоритма Мамдани.

В данном случае особенность вычислительного процесса заключается в том, что выполняются последовательные преобразования (четкое значение $X_i^* \rightarrow$ фаззификация $\rightarrow$ нечеткий логический вывод $\rightarrow$ получение четкого множества для X_j^*) и так далее для каждой из следующих пар концептов $C_j \rightarrow C_{j+1} \rightarrow \ldots$ на пути следования к НПКК. Этап приведения к четкости

(деффазификации) выходной переменной X_j^* предполагает использование метода взвешенного среднего в соответствии с (2.2):

$$X_j^* = \frac{\sum_{l=1}^{m} a_l \cdot X_{jl}^0}{\sum_{l=1}^{m} a_l} \qquad (2.2)$$

где X_j^* является деффазифицированным значением переменной состояния концепта C_j; $X_{jl}^0, (l = 1,2,...,m)$ является центральными значениями термов (нечетких подмножеств) переменной X_j; a_l - является уровнем активности правила l, который находится в соответствии с конкретным значением входной переменной X_i^*; m является количеством термов (подмножеств) лингвистической переменной X_j (в данном конкретном примере $m = 5$).

В общем случае, если концепт C_j непосредственно зависит от k предшествующих концептов $C_i, C_{i+l},...,C_{i+k-1}$, то вид нечетких продукционных правил становится более сложным, например:

$П_1$: ЕСЛИ X_i есть ВЫСОКАЯ И X_{i+1} есть Высокая И… И X_{i+k-1} есть Высокая, то X_j есть Очень_высокая;

…

$П_N$: ЕСЛИ X_i естьОчень_низкая И X_{i+1} есть Очень_низкая И… И X_{i+k-1} есть Очень_низкая, то X_j есть Очень_низкая;

Реализация процедуры нечеткого логического вывода в данном случае реализована аналогично. Чтобы осуществить операцию логического И целесообразно использовать оператор MIN.

К основным недостаткам НПКК можно отнести резкий рост количества продукционных правил при увеличении количества концептов. Так, в рассматриваемом примере, для определения состояния одного концепта C_j (переменной X_j) при двух предшествующих взаимодействующих с ним концептах C_i, C_{i+1}, для описания которых используются, соответственно, переменные состояния X_i и X_{i+1}, получается $k = 2, m = 5$, а общее количество

правил, которые представлены выше, составляет $m^2 = 25$. Очевидно, что не все правила из данной совокупности будут активны (другими словами, $a_i \neq 0$)для определенных «четких» значений входов X_i^* и X_{i+1}^*, которые поступают с выходов концептов C_i, C_{i+1}. Кроме того, активизации подлежат только четыре правила, срабатывания остальных правил не происходит. Вместе с тем, проблема высокой размерности НПКК остается, что требует для ее решения применения специальных способов и методов.

2.3 Моделирование рисков информационной безопасности на основе НКК для ГБПОУ КЖГТ

Построение НКК проводится на основании методики, изложенной в работах Васильева В. И., Кудрявцевой Р. Т., Юдинцева В. А.[18]. Согласно этой методике для построения НКК для ГБПОУ КЖГТиспользуется следующая технология описания основных концептов:

C_G– множество целевых факторов, которые определяют меру достижения некоторого уровня ИБ;

C_U– множество дестабилизирующих факторов (угроз), которые могут оказать влияние на работу АСУ ТП;

C_S– множество информационных активов, которые могут подвергнуться нападению, так как являются наиболее «желанными» для злоумышленников;

C_I– множество базисных факторов (промежуточных концептов-индикаторов), определяющих направления достижения целевых факторов;

C_R– множество управляющих факторов, регулирующих меру воздействия на определенные связи угроз и активов.

Таблица 2.1 – Характеристики выбранных концептов и переменных состояния

№	Концепт	Наименование концепта	Переменная состояния x_i
1.	C_1^U	Кража данных и данных доступа	Среднее количество хищений / ед. вр.
2.	C_2^U	Разглашение данных и данных доступа	Среднее количество разглашений / ед. вр.

Продолжение таблицы 2.1

№	Концепт	Наименование концепта	Переменная состояния x_i
3.	$C3^U$	Фальсификацияданных	Среднее количество несанкционированных изменений / ед. вр.
4.	$C4^U$	Вирусы	Среднее количество вирусных атак /ед.вр.
5.	$C5^U$	Аппаратные сбои	Среднее количество аппаратных сбоев /ед. вр.
6.	$C6^U$	Программныесбои	Среднее количество программных сбоев /ед. вр.
7.	$C1^S$	База данных	Степень достоверности информации,содержащейся в БД, %
8.	$C2^S$	Сервер	Производительность сервера при обработке данных, %
9.	$C3^S$	АРМ сотрудников	Уровень готовности, %
9.	$C4^S$	Аппаратное обеспечение	Работоспособность оборудования, %
10.	$C5^S$	Сеть Ethernet	Отношение скорости работы сети к запланированной, %
11.	$C1^I$	Управление идентификацией и аутентификацией	Количество нарушений, ед.
12.	$C2^I$	Контроль использования и целостность системы	Количество нарушений, ед.
13.	$C3^I$	Конфиденциальность данных и ограничение на их поток	Отношение фактического потока к запланированному, %
14.	$C4^I$	Работоспособность и доступность ресурсов	Отношения числа работоспособных и доступных ресурсов к запланированным, %
15.	$C1^G$	Точность	Отношение достигаемого уровня точности к запланированному, %
16.	$C2^G$	Надежность	Отношение числа сбоев системы к запланированному, %
17.	$C3G$	Быстродействие	Отношения скорости работы системы к запланированной, %

При этом сами угрозы могут быть реализованы только при наличии соответствующего источника угроз. Для определения основных источников угроз и меры их воздействия на данный вид ИС ГБПОУ КЖГТ, применялась концепция, отражённая в работе Кирсанова С.В. [20].

Таблица 2.2 – Определение источников угроз ИС ГБПОУ КЖГТ[20]

Источник угроз	Описание вариантов
Внутренние антропогенные	Обеспечивающийперсонал
	Инженерно-технический персонал, заведующие лабораториями
	Пользователи ИСГБПОУ КЖГТ (преподаватели, методисты, педагоги)
	Администраторы (системные, сетевые), ответственный заобеспечение ИБ
	Руководители (заместители директора, территорий, заведующие отделений)
Внешние антропогенные	Посетители (студенты, родители, партнёры, аудиторы и др.)
	Обслуживающие организации
	Уволенные сотрудники, отчисленные студенты
	Внешние злоумышленники (конкуренты, криминал)
Внутренние техногенные	Количественная или качественная недостаточность компонентовИС ГБПОУ КЖГТ (аппаратные средства, программные средства,инженерно-технические средства)
Внешние техногенные	Внешний техногенный источник угроз (энергетические сети,инженерные сети, средства связи)
Стихийные	Стихийный источник угроз (наводнение, ураган, землетрясение,климатические явления)

Мера влияния соответствующей угрозы на конкретный целевой фактор определяется как сумма проходов по графу с учетом весов звеньев (2.3)

$$T = \sum_{i=1}^{n-1} W^i \qquad (2.3)$$

где $W^i = \|W_{ij}\|_{n \times n}$ представляет собой матрицу смежности НКК, заданную весами W_{ij}.

Опосредованный эффект от влияния фактора оценивается на основании (2.4):

$$T_k(C_i^U \to C_j^U) = \min\{W_{ij}\} \quad (2.4)$$

Тогда полный эффект определяется как максимальный уровень влияния (2.5), при выборе всех путем достижения целевого фактора по графу:

$$T(C_i^U \to C_j^U) = \max\{T_1, T_2, \ldots T_N\} \quad (2.5)$$

Оценка уровня риска целевого фактора относительно i-ой угрозы определяется на основании формулы (2.6):

$$R_{ij} = P_i \cdot T(C_i^U \to C_j^U) \cdot r_j \quad (2.6)$$

где через r_j определяется ценность j-го ресурса, а P_i дает оценку вероятности наступления i-ой угрозы.

Соответсвенно общий риск определяется как:

$$R = \sum_{i=1}^{m}\sum_{j=1}^{k} v_j \cdot R_{ij}, \quad (2.7)$$

где k определяет число целевых факторов, а m - число угроз, v_j - оценка, полученная экспертами по значимостицелевогофактора.

Рисунок 2.2 демонстрирует разработанную нечеткую когнитивную карту для ИСИС ГБПОУ КЖГТ.

Рисунок 2.2 – НКК для оценки информационных рисков ИС ГБПОУ КЖГТ

ЗАКЛЮЧЕНИЕ

Результатом прохождения практики стало изучение деятельности образовательного учреждения ГБПОУ КЖГТ, осуществляющей подготовку специалистов в сфере железнодорожного и городского транспорта.

Проведенный анализ технического обеспечения учреждения показал высокий уровень оснащенности специализированным компьютерным оборудованием, ориентированным в основном на работу IT-специалистов. Определенный уровень защищенности данных обеспечивается на аппаратном и программном уровня, реализованный межсетевыми экранами и другими средствами обеспечения защиты информации. Однако использование программных средств, обеспечивающих безопасность данных не на должном уровне. Достаточно часто возникают потери данных из-за отсутствия механизмов автоматизированной репликации данных и криптографической защиты данных.

Выяснено, что совокупность требований к безопасности определенных продуктов и систем ИТ определяется в соответствии с имеющимися и прогнозируемыми угрозами безопасности, установленной политики безопасности, а также с учетом условий их использования.

Разработка комплекса мер по обеспечению защиты информации входят в сферу ответственности подразделений по защите информации (служб безопасности) либо отдельных специалистов, которые назначаются руководством предприятия (учреждения) для осуществления таких работ. Разработка такого комплекса мер по защите информации может быть осуществлена также сторонними организациями, обладающими лицензиями на право проведения данного вида работ, выдаваемыми Гостехкомиссией России или ФСБ России.

Так как ГБПОУ КЖГТ является особой организацией, предоставляющей образовательные услуги, то для оценки рисков информационной безопасности решено было применить технологию нечетких когнитивных карт.

На основе анализа деятельности образовательного учреждения и используемых IT-ресурсов были выделены основные источники угроз информационной безопасности и построена нечеткая когнитивная карта для оценки рисков информационной безопасности для ГБПОУ КЖГТ.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ Р ИСО / МЭК 15408. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий URL: http:www.fstec.ru.

2. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения URL: http:www.fstec.ru.

3. COBIT 5. Information Security. URL: https://cobitonline.isaca.org/l2-main?professionalFocus=Information%20Security/

4. ISO/IEC 2700 URL: www.iso27001security.com/html/27005.html

5. NIST 800-37 URL: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России. 15.02.2008.

7. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895)//Электронный фонд нормативной и правовой документации// http://docs.cntd.ru.

8. Федеральный закон «Об участии в международном информационном обмене» от 04.07.1996 N 85-ФЗ.

9. Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне».

10. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ.

11. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ.

12. Федеральный закон «О техническом регулировании» №184-ФЗ от 27.12.02г. с изменениями и дополнениями).

13. Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» №1119 от 01.11.2012г.

14. Бирюков А. А. Информационная безопасность: защита и нападение. - М.: ДМК Пресс, 2017. – 474 с.

15. Васильев В. И., Вульфин А. М., ГузаировМ. Б. Анализи управление рисками информационной безопасности с использованием технологии когнитивного моделирования // Информационные технологии. – 2018. – №4. – С. 266-273.

16. Васильев В. И., Вульфин А. М., Гузаиров М. Б., Кириллова А. Д. Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт// Информационные технологии. – 2018. – №10. – С. 657-664.

17. Васильев В. И., Вульфин А. М., Кудрявцева Р. М. Анализ и управление рисками информационной безопасности с использованием технологии когнитивного моделирования // Доклады ТУСУР. – 2017. – №4.– С. 34-43.

18. Васильев В. И., Кудрявцева Р. Т., Юдинцев В. А. Автоматизация процесса оценки информационных рисков с использованием нечетких когнитивных карт // Вестник УГАТУ. – 2014. – №3 (64).– С. 23-28.

19. Градусов Д.А., Шутов А.В., АнцуповаД.П. Моделирование взаимовлияния целей и рисков проектов внедрения интегрированной системы управления предприятием на основе нечетких когнитивных карт // Экономический анализ: теория и практика. – 2013. – №37 (340). – С. 25-29.

20. Кирсанов С.В. Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли // Доклады ТУСУР. – № 2 (28). – С. 112-115.

21. ПолтавцеваМ.А, ХабаровА.Р. Безопасность баз данных: проблемы и перспективы // Программные продукты и системы. – 2016. – № 3. – С. 36-41.

22. Щеглов А.Ю. Компьютерная безопасность. Вопросы комплексирования. Системный подход к построению системы защиты информации от несанкционированного доступа. URL: http://www.itsec.ru/articles2/Inf_security/voprosy-kompleksirovaniya .

23. ФСТЭКРоссииURL: http://fstec.ru/litsenzionnaya-deyatelnost/tekhnicheskaya-zashchita-informatsii/.

24. Государственное бюджетное профессиональное образовательное учреждение города Москвы «Колледж железнодорожного и городского транспорта»URL: https://gk52.mskobr.ru/.