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

Организация единого информационного пространства образовательной организации в условиях обеспечения информационной безопасности

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:
88,97% авторского текста

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

Выполнил:
Студент группы ЗФ-309-210-2-1
Горелкина Людмила Анатольевна

Научный руководитель:
к.п.н., доцент
Гафарова Е.А.

Челябинск
2023

Аннотация

на магистерскую диссертацию

Горелкиной Людмилы Анатольевны

Тема магистерской диссертации «Организация единого информационного пространства образовательной организации в условиях обеспечения информационной безопасности на примере ГАПОУ СМПК»

Магистерская диссертация содержит 129 страниц, 15таблиц, 5 рисунков, 96 источников литературы.

Ключевые слова: Информация, единое информационное пространство, информационная безопасность, анализ риска, информационные технологии.

Объектом исследования является Единое Информационное Пространство Государственного автономного образовательного учреждения среднего профессионального образования Стерлитамакский многопрофильный профессиональный колледж - ГАПОУ СМПК.

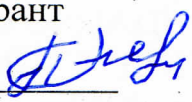
Цель магистерской диссертации - анализ методов и инструментов совершенствования системы информационной безопасности и разработке рекомендации по повышению информационной безопасности Единого Информационного Пространства образовательной организации профессионального образования ГАПОУ СМПК – Стерлитамакский педагогический колледж.

В процессе исследования изучены теоретические аспекты: единое информационное пространство образовательной организации, политика информационной безопасности, выявлены угрозы, уязвимости и риски в системе защиты информации образовательного учреждения. Определены требования к информационной безопасности в образовательной организации. Приведено описание стандартов управления информационной безопасностью, Методики

ФСТЭК России, определения актуальных угроз безопасности, рассмотрен рынок Российского программного обеспечения.

В результате проведённого исследования было проанализировано состояние единого информационного пространства образовательной организации, определена актуальность политики безопасности, разработаны рекомендации по совершенствованию системы информационной безопасности единого информационного пространства образовательного учреждения, проведена оценка риска информационных активов ГАПОУ СМПК.

Магистрант Горелкина Людмила Анатольевна



(ФИО) подпись

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Впервые в истории человечества поколения идей и технологий сменяются быстрее, чем поколения людей. Новейшие технологии с колоссальной скоростью внедряются во все сферы жизнедеятельности человека. Информация заняла уверенное место в нашей жизни, и стала в один ряд с экономическими, природными ресурсами, получив название информационных ресурсов. Всему этому способствовала глобальная информатизация общества, ознаменовавшаяся переходом от индустриального общества к информационному.

Человек при этом оказался на пороге новой информационной эры, где на первый план вышло не производство материальных благ, а производство информации с умением извлечь пользу из неё, определив информацию как один из значимых факторов успеха, весомого мотива и регулятора поведения человека в достижении цели, способствуя, при этом, формированию нового информационного общества и его значимого компонента – единого информационного пространства.

Всё это повлекло за собой изменение мышления, приводя к осознанию необходимости изменений во всех сферах жизнедеятельности человека, выводя на передний план информационные ресурсы, как ресурсы настоящего и будущего, предусматривая необходимость обязательного владения информационными технологиями, что в современном мире приравнивается к таким базовым качествам, как умения читать и писать. При этом информационные технологии открывают перед человеком практически безграничные возможности, в том числе и в решении вопросов профессиональной деятельности, но воспользоваться таковыми возможностями может только человек владеющий знаниями, и умеющий их применять.

Данные тенденции получили свой отклик, в первую очередь, в образовании, так как именно образование, являясь одним из глобальных производителей и потребителей информации, призвано сформировать человека, владеющего необходимыми и знаниями, и умениями, отвечающего требованиям современного времени, человека, по воле современных тенденций, вовлечённого в освоение некой новой для себя сферы информационной деятельности с использованием информации, как фундаментально нового источника развития.

При классической образовательной системе данные тенденции не могли получить реализацию развития в полной мере. В связи с этим, потребовалась модернизация всей системы образования, но никак не уничтожение её, а именно вывод такой системы образования на более высокий уровень, проявившись в информатизации образования и подтвердив в дальнейшем правильность выбранного пути, так же и того, что это был шаг не дань моде, а жизненная необходимость в условиях современности.

Особо значимым направлением информатизации образования, с исторической точки зрения, явилась управляемая информатизация образования, характеризующаяся организованностью процесса при поддержке материальными ресурсами, с обоснованными концепциями и программами. Так концептуальными принципами, обеспечивающими реализацию процесса информатизации образования, являются:

-принцип системности;

- принцип непрерывности;

- принцип междисциплинарной интеграции.

Основополагающей же задачей, при этом выступает задача формирования единого информационного пространства

образовательного учреждения, где информация является основой основ.

Таким образом, в самом общем виде данный аспект можно представить как систему, в которой задействованы и на информационном уровне связаны между собой все участники конкретной образовательной структуры, а в частности - совокупность информационных баз и банков данных, функционирующих на основе единых принципов и обеспечивающих информационное взаимодействие всех структурных подразделений образовательной организации в интересах деятельности образовательного учреждения, а также удовлетворения информационных потребностей всех её членов.

Отследить же успешность процесса информатизации образования можно по следующим тенденциям:

- сформированности системы непрерывного образования, т.е. «Образования через всю жизнь»;

- организации Единого Информационного Образовательного Пространства ОО;

- активности внедрения новых средств и методов обучения, ориентированных на использование новых информационных технологий;

- взаимодополняемости традиционного образования с нетрадиционным компьютерным;

- функционированием системы опережающего образования.

При этом очевидность процессов устаревания и обновления знаний, неизбежность изменений, способствуют прогрессивным преобразованиям. Образовательным организациям невозможно остаться в стороне от процесса информатизации. Так, система непрерывного образования, т.е. «Образование через всю жизнь» получила естественный, но интенсивный характер развития.

Организация и совершенствование образовательного пространства способствует получению и совершенствованию участниками прогрессивных, и знаний, и умений, одновременно с этим предопределяя и общую организацию единого пространства образовательной организации, с непременным прицелом внимания именно информационного порядка, с овладением новейшими информационными технологиями, так как активное внедрение оных в образование позволяет сделать ощутимый шаг в заданном направлении.

Так же необходимо понимать, что единое информационное пространство образовательной организации периодически продолжает структурироваться (выстраивается) её членами (субъектами создающими, перерабатывающими, использующими информацию), определённым образом под их собственные образовательные потребности, используя аппаратные и программные средства, в тот же момент, с учётом актуальных задач и требований текущего дня.

Основные требования сегодня можно сформулировать следующим образом:

- создание комфортных условий для всех задействованных участников;

- повышение эффективности их деятельности посредством автоматизации.

Значимость при этом организации единого информационного пространства образовательного учреждения, определяется, во-первых, главной целью внедрения информационных технологий, а во-вторых - способом решения поставленных задач в образовании, становясь неким ключом преодоления проблем взаимодействия всех участников образовательного процесса любой степени сложности. Следовательно, нужно быть готовым к тому, что организация единого

информационного пространства образовательного учреждения - это неизбежный, но довольно непростой процесс, поэтапный и непрерывный, сводящийся не к простому обеспечению образовательной организации новейшей техникой, а к созданию системы, в которой будут задействованы и на информационном уровне связаны все участники образовательного учреждения.

Все эти тенденции нашли своё отражение в государственной политике Российской Федерации и политике Республики Башкортостан в области информатизации образования. Так, Правительство РФ приняло Концепцию региональной информатизации 29.02.2014, в которой указало, что *«в сфере образования региональная информатизация осуществляется с учетом государственной программы Российской Федерации «Развитие образования»* на 2013-2020 годы, утвержденной постановлением Правительства Российской Федерации от 15 апреля 2014 года N 295 «Об утверждении государственной программы Российской Федерации «Развитие образования» на 2013-2020 годы», и Указа Президента Российской Федерации от 7 мая 2012 года N 599 «О мерах по реализации государственной политики в области образования и науки» и имеет целью развитие инфраструктуры и организационно-экономических механизмов, обеспечивающих равную доступность услуг дошкольного, общего и дополнительного образования, модернизацию образовательных программ, в том числе за счет использования информационных технологий в учебном процессе, повышение эффективности управления на всех уровнях образовательной системы Российской Федерации [66].

На уровне Правительства Республики Башкортостан был принят ряд постановлений и распоряжений, а именно Постановление Правительства Республики Башкортостан от 21 февраля 2013 года № 54 «О государственной программе "Развитие образования в

Республике Башкортостан"»; Постановление Правительства Республики Башкортостан от 31 октября 2016 года № 463 «Об утверждении государственной программы "Доступная среда в Республике Башкортостан"»; Распоряжение Правительства Республики Башкортостан от 28 декабря 2017 года № 1355-р «Об утверждении Плана мероприятий («дорожная карта») по реализации приоритетного проекта «Образование» по направлению «Подготовка высококвалифицированных специалистов и рабочих кадров с учетом современных стандартов и передовых технологий» в Республике Башкортостан».

Учитывая неизбежность процесса организации ЕИП образовательной организации, становится понятно, что чем раньше информационное пространство воплотиться в жизнь образовательной организации, тем более востребовано он будет в дальнейшем, и определит успех внедрения информационных технологий на всех его уровнях.

Взаимодополняемость традиционной системы образования новой компьютерной проявляется в востребованности новых знаний и умений, мотивацией, повышением качества управления, расширением спектра стратегий обучения. При этом у каждой образовательной организации корпоративная индивидуальность, а также коллектив, владеющий информационными технологиями, обладающий информационной культурой и располагающий своей системой информационной безопасности, так как именно информационная безопасность выступит условием продуктивной жизнедеятельности образовательного учреждения в целом.

Существенная особенность трактуется как объединение образовательной и административной деятельности учреждения, и отрадно заметить, на данный момент такое объединение достаточно гармоничное и продуктивное, и это, в современных условиях,

особенно в ситуации длительного локдауна в разгар пандемии COVID-19, а также санкций, введённых Западом в связи конфликтом России и Украины наиболее верное решение.

Успешность функционирования образовательной организации определяется тем, насколько эффективно в учреждении поставлен процесс сбора, обмена, анализа и защиты информации. Анализ необходим, так как важно установить пригодность, адекватность, результативность рассматриваемого объекта, при достижении установленных целей, что регламентировано ГОСТ Р ИСО/ МЭК 27005-2010 [31].

Информационная безопасность (далее – ИБ) образовательной организации, являясь приоритетной задачей, требующей к себе максимум внимания, получит реальную соизмеримую реализацию, ведь отсутствие современной, правильно выстроенной системы обеспечения безопасности в организации, может привести к потере важной информации. Потеря информации, в свою очередь, сопряжена с рисками больших издержек материального характера, потерей личных и персональных данных сотрудников организации, обучающихся, их родителей (законных представителей), ущербом для имиджа, что особо заостряет такой вопрос для образовательной организации и заставляет уделять ему максимум внимания.

«Информационная безопасность — это…защита информации и поддерживающей её инфраструктуры, от воздействий, с помощью совокупности программных, аппаратно-программных средств и методов, а также организационных мер, с целью недопущения причинения вреда владельцам этой информации или поддерживающей её инфраструктуре», - утверждают В.Ю.Статьев и В.А.Тиньков [89]. Воздействия могут носить разноплановый характер, от случайного до преднамеренного, естественного или искусственного.

В отечественной и зарубежной литературе в настоящее время немалое внимание уделяется проблемам информационной безопасности. Более подробно во второй половине XX века эта проблема была рассмотрена в работах: М.С. Вершинина, К. В. Ветрова, С. Э. Зуева, В. Д. Попова, А. И. Ракитова.

Особый вклад в исследование информационной безопасности в различных сферах общества, культуры, науки и техники, внесли такие ученые иисследователи, как А. Б. Агапов, А.С. Алексеев, И.Л. Бачило, А.В., Горский, Г.Н. Горшенков, И. С. Даниленко, Н. В. Данилов, С.А. Дятлов и другие. В работах этих ученых сформулированы концептуальные положения о сущности и содержании категорий информационной безопасности, исследованы их взаимосвязи, обоснованы приемы и способы исследования информационной безопасности и различных составляющих системного подхода.

На сегодняшний день существует широкий круг систем хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности хранения информации имеет особое значение. К таким информационным системам можно отнести, например, юридические системы безопасного документооборота, банковские системы, для которых обеспечение защиты информации является приоритетным. Это стало актуальным и для образовательной организации.

В настоящее время, несмотря на большое количество работ по вышеуказанной проблематике, следует отметить, что ее теоретическая изученность явно недостаточна, практические методики по формированию оптимального механизма информационной безопасности в образовательных организациях требуют постоянной актуализации.

Серьёзность подхода организации к защите своих

информационных активов отражается в политике информационной безопасности образовательной организации, при этом каждая организация должна осознавать необходимость поддержания соответствующего режима безопасности и выделения на эти цели достаточно необходимых ресурсов.

В современных условиях, при выходе на передний план угроз разнопланового характера для образовательного учреждения, последствия могут оказаться несоизмеримыми касательно наносимого ущерба, особенно в отношении: сотрудников и студентов, при вовлечении их в криминал и терроризм.

Таким образом, потребность в оптимальной системе информационной безопасности, в сложившихся современных экономических и политических условиях, а также проработка вопросов использования более совершенных методов обеспечения информационной безопасности в образовательных учреждениях определили тему, объект, предмет, цель и основные задачи исследования.

Цель исследования заключается в анализе методов и инструментов совершенствования системы информационной безопасности и разработке на этой основе рекомендаций по повышению информационной безопасности единого информационного пространства (далее – ЕИП) образовательной организации профессионального образования.

Объектом исследования является единое информационное пространство образовательной организации среднего профессионального образования.

Предметом исследования является система информационной безопасности образовательной организации среднего профессионального образования.

Гипотеза исследования состоит в предположении о том, что при условии модернизации системы информационной безопасности функционирование единого информационного пространства образовательной организации будет более эффективным.

Реализация поставленной цели в магистерской диссертации потребовала постановки и последовательного решения следующих взаимосвязанных **задач**:

1) Изучить понятийный аппарат и общие принципы информатизации образования, а также методы и средства обеспечения информационной безопасности ЕИП образовательной организации.
2) Проанализировать состояние системы информационной безопасности образовательной организации – ГАПОУ Стерлитамакский многопрофильный профессиональный колледж (далее - ГАПОУ СМПК).
3) Сформулировать, рекомендации по совершенствованию системы информационной безопасности колледжа и организации ЕИП ГАПОУ СМПК.

Теоретико-методологическую базу исследования составили законодательные и нормативно-правовые документы РФ и Республики Башкортостан, основные положения и разработки в области обеспечения информационной безопасности, методы и способы построения процессов управления информационной безопасностью в целях повышения ИБ в организациях, системный подход к исследуемому объекту и предмету, системный анализ, в качестве информационных источников использованы аналитические и статистические материалы по информационной безопасности, материалы научных конференций, средств массовой информации, отражающие аспекты информационной безопасности.

Положения, выносимые на защиту:

1. Процесс информатизации образования предполагает расширение объёма требований обеспечения информационной безопасности образовательной организации и актуализирует необходимость совершенствования информационной безопасности единого информационного пространства образовательного учреждения.
2. Анализ рисков информационной безопасности позволяет совершенствовать единое информационное пространство образовательной организации и обеспечивает возможность формирования стратегии развития ЕИП.

Научная новизна исследования состоит в комплексном решении **актуальной задачи**, состоящей в совершенствовании системы обеспечения информационной безопасности организации профессионального образования, в условиях сложившейся экономической и политической обстановки, позволяющей повысить уровень устойчивого функционирования ЕИП в условиях информационной безопасности.

Теоретическая значимость магистерской работы заключается в том, что результаты исследовательской части и выводы могут быть использованы для теоретических обобщений и дальнейшего более глубокого изучения темы.

Практическая значимость заключается в разработке рекомендаций по обеспечению ИБ для эффективного функционирования ЕИП в ГАПОУ СМПК.

Методы исследования

В ходе исследования применялись положения и закономерности информационного и системного подходов, анализ, синтез, индукция и дедукция.

База исследования: Государственное автономное профессиональное образовательное учреждение Стерлитамакский

многопрофильный профессиональный колледж.

Апробация исследования: результаты исследования были представлены на международной научно – практической конференции «Фундаментальные и прикладные научные исследования: Актуальные вопросы, достижения и инновации», 2022г.; международной научно – практической конференции «Научное обозрение: Актуальные вопросы теории и практики», 2022г.; XVI международной научно – практической конференции « Актуальные вопросы современной науки и образования», 2022г.; всероссийской научно – практической конференции «Национальная безопасность и молодёжная политика: Киберсоциализация и трансформация ценностей в VUCA-Мире» 2021г.

Структура магистерской диссертации: введение, три главы, выводы по главам, заключение, список использованных источников.

ГЛАВА 1 ПРОЦЕСС КОМПЛЕКСНОЙ ИНФОРМАТИЗАЦИИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1 Понятийный аппарат и общие принципы информатизации образования

Цифровизация в условиях современности – это наша реальность. Совершенно новая реальность, которая меняет не только технологии, но и взаимоотношения людей. Одни из нас вошли в это новое, другие непосредственно родились в нашем новом, воспринимая всё обыденной реальностью. Отмахнуться или отстраниться от происходящего не получится. Это наша жизнь. Жизнь во взаимодействии с информацией. Информация в современном мире привела нас к пониманию информации, как особого ценного ресурса. Высочайшая потребность в котором (информационная потребность) ставит таковую в один ряд с исторически востребованными ресурсами, энергетики, финансов, сырья.

«…Информационная потребность – это потребность, возникающая, когда цель, стоящая перед пользователем в процессе его профессиональной деятельности либо в его социально-бытовой практике, не может быть достигнута без привлечения дополнительной информации (дополнительных сведений)», - говорил Р.Тейлор. Агапов А.Б., конкретизируя уточнял, что «… информационные ресурсы при этом являются совокупностью данных, которые представляют реальную ценность. К ним можно отнести тексты, файлы с данными, сведения…».[2, с.5]

Современность нас заставляет идти в ногу со временем. Жить и работать в новом информационном мире, коммуникатировать, используя информационные ресурсы, применяя новейшие

технологии, заставляя нас становиться полноценными членами современного общества. Необходимо научиться гармонично функционировать в реальности самим и обучить этому других. Полноценное использование информационных ресурсов невозможно без применения соответствующих современных технологий. Поэтому внедрение, собственно новейших технологий, а именно информационных, во все сферы деятельности человека, происходит с колоссальной скоростью.

Впервые термин «информационные технологии» в России получил своё освещение в работе В. М. Глушкова, определяя информационные технологии как процессы, связанные с переработкой информации. А в монографии Б. С. Гершунского, даётся определение понятия информационных технологий: «… как совокупности средств и методов, с помощью которых осуществляется процесс переработки информации». [24, с.17]

При этом широкомасштабное применение таковых средств и методов, во все сферы жизнедеятельности человека, происходит довольно активно, а в некоторых случаях и агрессивно, получив название информатизации общества, заключая в своей основе такой значимый компонент, как единое информационное пространство.

Единое информационное пространство представляет собой совокупность баз и банков данных, технологий их ведения и использования, информационно – телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей [84, с. 21].

Однозначного научного определения понятия «единое информационное пространство» до сих пор не предложено, хотя словосочетание «информационное пространство» применяется

достаточно широко в разных смысловых интерпретациях. По мнению А. Калининой: «.. информационное пространство целесообразно определять как вид пространства, выделенный на основе признания эндогенности информационного фактора производства, включающий отношения хозяйствующих субъектов по поводу, как этого фактора, так и соответствующих условий, ресурсов и продуктов их деятельности».

Информационное пространство рассматривается как конструкция, выступающая в различных формах: физическое пространство, виртуальное пространство, иерархические системы пространства.

Организация единого информационного пространства организации – это весомая задача, требующая пристального внимания и проработки. Избежать данного процесса в обществе, не представляется возможным. Так как, по мнению Колина К., можно сегодня вполне обоснованно говорить о возникновении новой глобальной проблемы развития цивилизации - проблемы человека в изменяющемся мире [44, с. 11-14].

Реалии таковы, что наше общество перешагнуло рубеж индустриализации, оказавшись в новой для себя цифровой действительности. Где на первый план вышли не производство материальных благ, а производство информации с умением извлечь пользу из неё. Изменения повлекли за собой перемены в нашем сознании, сфокусировав понимание на необходимости и неизбежности изменений во всех сферах нашей жизни.

Человеческий фактор, несомненно, оказывает своё влияние. И получив изначально одну и ту же информацию, каждый из нас воспринимает её, преобразует и применяет совершенно по-разному. И здесь уже те, кто смогли правильно распорядиться информацией, окажутся «на голову» успешнее тех, кто оказались недостаточно умеющими и знающими. Всё это с подвигает каждого из нас получать

новые знания и умения, отвечающие требованиям нового времени, новой информационной эпохи.

Соответствующего рода тенденциозность нашла свой отклик в первую очередь в образовании. Потому что именно образование, призвано повысить уровень и знаний, и умений, и степень развития культуры соответственно, а в современных условиях, информационной культуры. То есть сформировать человека, отвечающего запросам новой эпохи, заинтересованного в освоении нового информационного пространства.

Следовательно образование не может остаться в стороне от всех тех процессов, что происходят в современном обществе. [45, с.110]. А информатизация общества – это некий толчок к запуску процесса информатизации образования, то есть активного внедрения информационных технологий в образование. [46, с.23]. Всё это открывает новые возможности, которыми необходимо суметь воспользоваться.

Учёные дают разные определения понятию «Информатизация образования». Так в Российской педагогической энциклопедии под редакцией Панова В. Г. даётся следующее определение. Информатизация образования в широком смысле – это комплекс социально-педагогических преобразований, связанных с насыщением образовательных систем информационной продукцией, средствами и технологией; в узком – внедрение в учреждения системы образования информационных средств, основанных на микропроцессорной технике, а также информационной продукции и педагогических технологий, базирующихся на этих средствах (компьютеризация обучения). [80, с.375].

А Ершов А.П. информатизацию образования определяет следующим образом. Информатизация образования – это стратегическая необходимость, характеризующаяся как комплекс

мер, направленный на обеспечение полного использования достоверного, исчерпывающего и своевременного знания во всех общественно значимых видах человеческой деятельности. [36, с.82]

Однозначно то, что информатизация образования – это неизбежный и стратегически важный процесс включающий в себя комплекс преобразований всей системы образования с точки зрения основополагающей составляющей – информации, как ресурса и фундаментального источника развития. И без реформирования, модернизации здесь просто не обойтись. Определив при этом содержание образования, его стратегическую целевую ориентацию [43, с.11].

Необходимо сделать акцент именно на стратегическом реформирование системы образования, а не уничтожение такового, что даст возможность вывести традиционную систему образования на более высокий значимый уровень. И информатизация образования в этом случае выступит именно тем вектором целенаправленной деятельности и обязательным условием, приводящих нас к качественно новому желаемому результату.

Хотя необходимо учесть, что это довольно сложный процесс, имеющий в своей направленности, ориентированность на разработку методов и средств реализации основных воспитательных и образовательных педагогических целей, с помощью использования современных достижений компьютерной техники. А также формирование нормативно-правовой базы по внедрению информационных технологий в деятельность образовательной организации. Административно-организационной деятельности для оптимизации использования информационных ресурсов.

Определённо и то, что информатизация образования преследует конкретные цели и задачи, производя корректировку таковых со временем и их дополнение. Так на сегодняшнем этапе

информатизации образования целью ставится: подготовка обучающихся к активной социальной и профессиональной жизни в сложившимся информационном обществе.

Реализуется же информатизация образования по двум основным исторически сформированным направлениям:

- управляемому
- неуправляемому.

Управляемое направление информатизации образования характеризуется организованностью процесса и поддержанием такового материальными ресурсами. Фундаментальной основой при этом выступают обоснованные общепризнанные концепции и программы.

Неуправляемая информатизация образования реализуется «снизу», т. е. по инициативе работников системы образования и охватывает наиболее актуальные сферы образовательной деятельности, и предметные области. Но она чревата хаотичностью, в отличие от управляемой информатизации

Выделяют следующие концептуальные принципы, обеспечивающие реализацию процесса информатизации образования. Это: - принцип системности, принцип непрерывности, принцип междисциплинарной интеграции.

Так в соответствии с принципом системности цель процесса информатизации образования заключается в изменении системных свойств сферы образования с целью повышения её восприимчивости к инновациям и предоставлении возможностей активного целенаправленного использования мировой информационной магистрали, новых возможностей влиять на свою образовательную, научную, профессиональную траекторию.

В соответствии с принципом непрерывности процесс информатизации представляет собой целенаправленное

использование методов и средств информационных технологий на всех уровнях и этапах подготовки.

По принципу междисциплинарной интеграции информационные технологии выступают механизмом оптимизации структуры моделей знаний и системы дисциплин, преобразуя всю систему подготовки в теоретическое, технологическое и методическое средство построения моделей профессиональной деятельности.

Существуют и свои трудности в реализации информатизации в системе образования, сводящиеся к формированию постоянной потребности применения компьютера, а также к необходимости непрерывного повышения информационной компетентности всех задействованных участников. Хотя это должно стать временным явлением, в силу осознания естественной необходимости потребности применения новейших технических средств и технологий.

Успешность же процесса информатизации можно отследить по следующим тенденциям:

- сформированности системы непрерывного образования, т. е. «Образования через всю жизнь»;
- организации ЕИП ОО;
- активности внедрения новых средств и методов обучения, ориентированных на использование новых информационных технологий;
- взаимодополняемости традиционного образования нетрадиционным компьютерным;
- функционированием системы опережающего образования.

При всей очевидности преимуществ информатизации образования имеются и существенные недостатки. Которые проявляются в ограниченности живого общения, некорректности работы с информацией, а также с возможностями развития

патологических зависимостей от таковой, с соответствующим снижением физического и психического здоровья.

Поэтому перед системой образования возникают поистине гигантские задачи, решить которые в рамках только традиционного образования, или только компьютерного не представляется возможным. И лишь векторное развитие по пути гармоничного взаимодополнения их дают возможность, в конечном итоге, нам приблизится к возможности формирования человека новой эпохи, отвечающего всем её требованиям, стремящегося к новым горизонтам. Помочь в этом призвана информатизация и она неизбежна, и необратима. Идя по пути успешного внедрения и овладения новейшими информационными технологиями всех участников. [94, с.34]. Всё это должно стать естественной потребностью для каждого, как разумеющееся умение, применяемое во взаимоотношениях с учётом нового времени.

Определить успех внедрения и овладения можно, как бы лакмусируя, образованное при этом единое информационное пространство образовательной организации, где каждый участник заинтересован прогрессом данных тенденций. Логическая важность организации единого информационного пространства в условиях ИБ представлена в приложении 1. на рисунке 5. Так изменяя себя, изменяется всё вокруг с изменениями взаимоотношений. При этом педагоги всё чаще выступают в роли консультантов, а обучающиеся в роли активных исследователей, администрация же в роли грамотных и рациональных управленцев.

Бесспорным при этом остаётся не просто повышение уровня образованности каждого участника, а формирование новых взглядов, нового образа мышления, нового типа интеллекта, в условиях новой информационной эпохи. Совершенно новой взаимосвязанности всех участников образовательной организации. Реализуя данную

тенденцию непрерывностью образования, системностью и интеграцией. Ведь только так возможно идти в ногу с непрерывными технологическими инновациями, позволяющими при этом ощущать реальную значимость процесса информатизации образования [92, с.28].

Процесс информатизации образования требует ориентация управленческой деятельности администрации образовательного учреждения на новые веянья времени, необходимо встать на «новые рельсы» самим и поставить на них остальных членов организации.

Процесс информатизации при этом, можно рассмотреть с помощью этапов управления информатизацией образовательного учреждения:

I этап — организационный. Его задача: выработка единого понимания, методологического подхода к процессу управления информатизацией и организации внедрения информационно-коммуникационных технологий в образовательный процесс (разработка локальных актов, разработка организационной структуры информационного центра, должностных инструкций специалистов информационного центра образовательного учреждения).

II этап — диагностический. Задача: анализ состояния информатизации образовательного процесса в общеобразовательном учреждении (анализ управления информатизацией; состояния преподавания информатики, внедрения ИКТ в предметные уроки; методического и научно-методического сопровождения информатизации образовательного процесса, информационно-коммуникационной компетентности педагогов и администрации; программно-аппаратного обеспечения информатизации образовательного процесса и др).

III этап — аналитико-прогностический. Задача: выработка рекомендаций для участников образовательного процесса по

направлениям информатизации образовательного процесса по результатам диагностики и проведенного анализа.

IV этап — технологический (обоснованная деятельность субъектов образовательного процесса в режиме управленческого мониторинга и контроля). Задача: трансформация содержания, методов и организационных форм учебной работы, связанных с информатизацией образовательного процесса в соответствии с рекомендациями, создание учреждения с высокой информационно-коммуникационной компетентностью участников образовательного процесса.

1.2 Единое информационное пространство образовательной организации (на примеры базы исследования - Государственного автономного профессионального образовательного учреждения Стерлитамакский многопрофильный профессиональный колледж).

Государственное автономное профессиональное образовательное учреждение Стерлитамакский многопрофильный профессиональный колледж (сокращенное – ГАПОУ СМПК, далее - колледж), расположен по адресу: Республика Башкортостан, г. Стерлитамак, ул. Николаева 124. Создан путем изменения типа существующего государственного учреждения среднего профессионального образования Стерлитамакский педагогический колледж в соответствии с распоряжением Правительства Республики Башкортостан № 1689-р от 22 декабря 2011года и распоряжением правительства РБ от 21 апреля 2015 года № 393-р. Свою историю колледж ведёт от Стерлитамакского педагогического училища, открытого в 1991 году на базе временных педагогических классов по

подготовке воспитателей детских садов, которые функционировали с 1979 года.

Учреждение является юридическим лицом. Лицензия Серия 02Л 01 № 0004985, от «28» сентября 2015г., рег.№ 3252 Свидетельство о государственной аккредитации, рег.№ 2559, от 09 июня 2021г., Серия 02А03№ 0000215.

Органами управления ГАПОУ СМПК являются: Директор, Наблюдательный совет, Общее собрание(конференция) работников и обучающихся колледжа, Совет колледжа, Педагогический совет, Попечительский совет, предусмотренные уставом колледжа. Управление осуществляется в соответствии с законодательством, Уставом, действующей сертифицированной системой менеджмента качества колледжа и строится на принципах сочетания единоначалия и коллегиальности. Директор колледжа осуществляет текущее руководство деятельностью образовательной организации. Назначается Учредителем. Подотчетен в своей деятельности Учредителю (Министерству образования Республики Башкортостан) и Наблюдательному совету (рис.1)

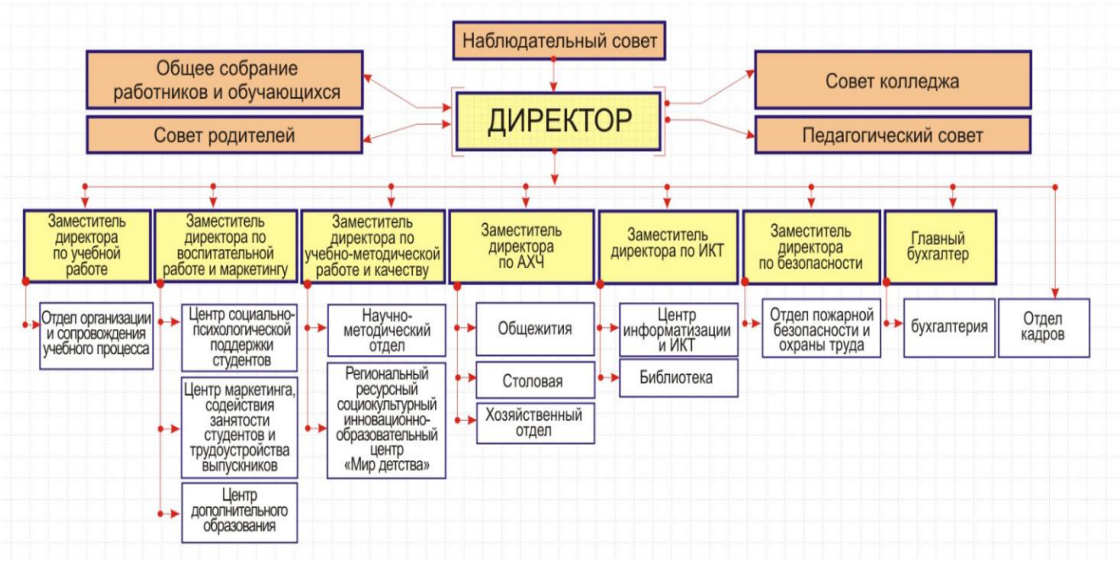


Рисунок 1. Структура управления ГАПОУ СМПК

ГАПОУ СМПК самостоятельно формирует свою структуру, в которой имеет:

- Отдел организации и сопровождения учебного процесса,
- Центр маркетинга, содействия занятости студентов,
- Центр дополнительного образования,
- Научно-методический отдел,
- Региональный ресурсный центр «Мир детства»,
- Центр информатизации и ИКТ,
- учебные кабинеты, мастерские, учебный полигон, библиотека, пресс-центр и др.

Предметом деятельности является реализация основных профессиональных образовательных программ среднего профессионального образования - программ подготовки квалифицированных рабочих, служащих, программ подготовки специалистов среднего звена, а также программы дополнительного образования, включающего в себя такие подвиды, как дополнительное образование детей и взрослых и дополнительное профессиональное образование, что в полной мере обеспечивает условия для непрерывного образования.

С целью реализации автономных прав, определяющих степень самостоятельности колледжа в осуществлении образовательной, научной, административной, финансово – экономической деятельности, в колледже принимаются локальные нормативные акты, соответствующие действующему законодательству и Уставу колледжа (Приёма обучающихся; Режима занятий; Формы, периодичности и порядка текущего контроля успеваемости; Промежуточной аттестации; Порядка и основания перевода, отчисления и восстановления обучающихся; и др.).

Колледж является многоуровневым образовательным учреждением среднего профессионального образования, реализующим в соответствии с лицензией программы подготовки специалистов среднего звена и программы подготовки

квалифицированных рабочих, служащих по следующим специальностям и профессиям: 44.02.01 Дошкольное образование, 44.02.02 Преподавание в начальных классах, 44.02.03 Педагогика дополнительного образования, 44.02.04 Специальное дошкольное образование, 44.02.05 Коррекционная педагогика в начальном образовании, 54.01.20 Графический дизайнер, 42.02.01 Реклама, 46.02.01 Документационное обеспечение управления и архивоведение, 54.02.01 Дизайн (по отраслям), 46.01.03 Делопроизводитель, 09.01.01 Наладчик аппаратного и программного обеспечения, 09.01.02 Наладчик компьютерных сетей, 09.01.03 Мастер по обработке цифровой информации, 09.02.06 Сетевое и системное администрирование, 09.02.07 Информационные системы и программирование, 11.02.15 Инфокоммуникационные сети и системы связи 39.02.01 Социальная работа, 40.02.01 Право и организация социального обеспечения, 40.02.02 Правоохранительная деятельность, 40.02.03 Право и судебное администрирование, .

В колледже реализуется «Программа развития ГАПОУ СМПК на 2019-2022 г.г.», содержание которой конкретизировано в Единых планах работы ГАПОУ СМПК на 2020-2021 и 2021- 2022 уч.г. Оперативное управление и контроль результатов осуществляется в процессе еженедельных совещаний.

Качество условий реализации профессиональных образовательных программ обеспечивается в соответствии с требованиями ФГОС, примерных программ, требованиями работодателей и стандартов Ворлдскиллс.

Приоритетными направлениями развития колледжа являются:

- инновационное развитие колледжа на основе проектной деятельности;
- развитие системы управления колледжем на основе бизнес-планирования и действующей системы менеджмента качества;

– обновление содержания обучения и совершенствования механизмов контроля его качества в соответствии с требованиями ФГОС;
– расширение спектра профессиональных образовательных программ различных уровней и направлений подготовки;
– научно-методическая оснащенность образовательных программ;
– развитие информатизации образования, освоение новых интерактивных технологий, развитие СМАРТ-образования как одного из условий обеспечения доступности образовательных услуг для всех слоев населения;
– участие в конкурсах, грантах в сфере образования;
- усиление социальной направленности и повышение качества воспитательной деятельности в профессиональной подготовке.

По итогам участия в двух Нацпроектах «Образование» создана современная информационно-технологическая база, которая дополнительно модернизирована благодаря объявления 2022 года в Республике Башкортостан «Годом модернизации профессионального образования, достойных условий труда и трудовых династий».

Процесс же информатизации Государственного автономного профессионального образовательного учреждения Стерлитамакский многопрофильный профессиональный колледж берёт своё начало с 2002 года, ознаменовавшегося открытием в колледже отделения «Информатика». Начиная с 2005 года - создания «Центра информационных технологий», процесс организации единого информационного пространства набирает свои темпы. Значительно активизируясь к 2011 году - открытием отделения «Прикладная информатика в дизайне», «Компьютерные сети» в 2012 году и «Сети связи и системы коммутаций» в 2016 году.

На каждом этапе информатизации выделялись приоритетные направления, ставились цели и задачи, от решения которых зависел очередной результат этапа информатизации.

Современный этап информатизации характеризуется системным подходом к процессу, включающему следующие компоненты:

- анализ на основе диагностики образовательных проблем информационных потребностей субъектов образовательного процесса;

-прогнозирование - определение предполагаемого результата управленческих действий;

- принятие управленческих решений;

-планирование - разработка плана мероприятий информатизации, определение ее этапов;

- контроль – осуществляется на каждом этапе определения промежуточных результатов.

В колледже функционируют 5 учебных корпусов, 2 общежития. В учебных корпусах для организации учебного процесса используются:

- 77 учебных кабинетов из них:

-18 компьютерных;

- 3 мобильных класса;

- 49 учебных кабинетов оборудованы интерактивными досками/ интерактивными панелями;

- Полигон администрирования сетевых операционных систем;

- 14 мастерских

В колледже имеются объекты социально-бытового обеспечения:

- Читальный зал на 25 посадочных мест (автоматизированы с выходом в Интернет;

- 2 спортивных зала;

- Актовый зал на 254 посадочных места (оборудован мультимедиа);

- Тренажёрный зал;

- Столовая на 260 посадочных мест;
- Буфет;
- Медпункт;
- Дискозал оборудован мультимедийным оборудованием.

Модернизация колледжа 2022г.г. способствовала обеспечению достаточного количество компьютеров (552 компьютера), объединённых в локальную сеть. Позволяющую связывать рабочее место директора со всеми структурными подразделениями колледжа, рабочими местами преподавателей и студентов, а также организовать сетевое взаимодействие между ними.

В колледже так же был приобретен необходимый комплект лицензионного программного обеспечения, например, MSDN Academic Alliance, MS Office (лицензий 200), Касперский Business Space Security (лицензий 200), пакеты прикладных программ (ABBYY FineReader, CorelDRAW Graphics Suite X5, Autodesk, Adobe Master Collection, Link для онлайн-взаимодействия и дистанционного обучения, MATLAB, Simulink, Stateflow). Таким образом, созданы все условия для организации образовательного процесса в соответствии с требованиями ФГОС СПО, а также для обеспечения возможности дистанционного обучения преподавателей колледжа по программам переподготовки, повышения квалификации, стажировки на рабочем месте.

В колледже оборудована серверная, в которой размещается 5 серверов:

-сервер для доступа и распределения интернет – трафика среди пользователей;

- сервер для хранения Интернет-ресурсов;

- сервер контроля и авторизации учётных записей пользователей;

- сервер для хранения единой базы данных колледжа и иных информационных ресурсов общего доступа;

- сервер официального сайта колледжа.

Функционирующая на базе сервера локальная сеть, объединяет все перечисленные выше кабинеты и помещения. Колледж имеет доступ в Интернет по выделенному каналу связи со скоростью 100 Мбит/с, выход на который можно осуществить с любого компьютера колледжа.

В 2011 году было приобретено программное обеспечение «1С». Установлено и настроено серверное программное обеспечение «1С: Предприятие 8.2». На его базе установлена конфигурация «1С: Колледж». На базе «1С: Колледж» настроен раздел «Приемная комиссия»: разработан шаблон анкеты абитуриента, сформированы отчеты «Ход приемной комиссии», «Источник получение информации о колледже», «Анализ предоставленных документов», «Формирование экзаменационной ведомости», «Формирование рейтинга абитуриентов». В разделе «Учебная часть» автоматизирована выдача справок об обучении студентов. На базе конфигурации «1С: Колледж» настроен также раздел «Кадровый учет»: автоматизирован учет переработок и отгулов сотрудников.

С целью заполнения электронной базы «1С: Колледж» была проведена серия обучающих семинаров для классных руководителей всех групп колледжа и работников приемной комиссии. Проведено обучение с работниками учебной части для автоматизации учета движения контингента.

На базе DataBase- сервера созданы базы данных: «Тьюторы», «Обмен», «Группы», «Правовые акты», «ПЦК», которые позволяют вести оперативный обмен информацией между администрацией колледжа, преподавателями, преподавателями и обучающимися.

Система оперативного обмена информацией на сервере (\\server-files) «Группы» даёт возможность преподавателям собирать весь учебный материал к урокам и сохранять практические, самостоятельные, лабораторные работы студентов.

На базе ПЦК создан фонд учебно-методической документации по всем специальностям обучения, реализуемых в колледже, доступной по локальной сети колледжа преподавателям и обучающимся. Все учебно–методические материалы, публикуемые на сервере преподавателями колледжа, лицензируются методическим кабинетом колледжа.

Для обеспечения безопасных условий доступа в сети Интернет в колледже установлены Антивирус Касперского Business Space Security и облачный сервис интернет-фильтрации SkyDNS. Интернет – безопасность организуется через использование исключительно Интернет-ресурсов, включённых в «белые списки».

Для оперативного обмена с Региональными органами исполнительной власти установлен электронный документооборот СЭД « ДЕЛО».

С 2009 года существует официальный сайт колледжа, его адрес: www/mirsmpc.ru. Разработан на основе Joomla 3,5, расположен на собственном Web-сервере, построенном на операционной системе Ubuntu Server. Администрирование сайта осуществляется в соответствии со статьёй 29 Федерального закона № 273 от 29.12.2012г. «Об образовании в Российской Федерации» и Постановления Правительства РФ №1802 от 20 октября 2021г. «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации». Структура сайта приведена в соответствие с Приказом Рособрнадзора от 14.08.2020г. № 831.

В колледже в целях обеспечения реализации образовательных программ функционирует библиотека, обеспечивающая доступ к профессиональным базам данных, образовательным ресурсам, информационным справочникам и поисковым системам. Фонд библиотеки постоянно обновляется.

В соответствии с договором ЭБС с ООО «Знаниум» колледж имеет доступ к электронно-библиотечной системе (ЭБС) ZNANIUM.com на 1000 пользователей. Содержимое приобретённой ЭБС соответствует требованиям обеспеченности обучающихся колледжа доступом к электронным научным и образовательным ресурсам. Что позволяет им самостоятельно приобретать и обновлять знания, педагогам часть рутинной работы переложить на технику. Всё это способствует повышению эффективности труда и тех и других, а также доступности образования. [66].

1.3 Перспективы развития единого информационного пространства образовательной организации - ГАПОУ СМПК

Двигаясь по пути эволюции, образовательная организация переступила рубеж оценки воздействия ИКТ в сфере образования, перейдя от оценки, направленной на определение доступности ИКТ (соотношение количества обучающихся и компьютеров, доступность широкополосного Интернета, доступности новых технологий в административной деятельности) к оценке, определяющей воздействие ИКТ на учение и обучение, продуктивность администрирования. Методики оценки должны быть связаны с результатами обучения и стратегией обучения. Разработка, применение и совершенствование таких систем оценки является одним из приоритетных направлений развития образования. [71]

В этой связи эффективность использования ИКТ понимается как преобразование работы колледжа на основе ИКТ и выражается в качественных изменениях единого информационного пространства, направленных на достижение нового качества образования, в возможности решать более широкий круг образовательных задач, расширении спектра предоставляемых колледжем образовательных услуг, а также совершенствование административного взаимодействия и управления.

Как показывает опыт голландских педагогов, использование ИКТ в образовательных целях имеет больше шансов на успех, если четыре основных элемента - видение, опыт, учебно-методические материалы и ИКТ инфраструктура - находятся в равновесии. Поэтому система оценки должна позволять определять баланс в развитии основных аспектов и компонентов ЕИП. Это важно для оптимизации управления, адресности использования ресурсов.

Таким образом, для успешного управления система оценки качества ЕИП должна:

- определять воздействие ИКТ на учение и обучение, быть связанной с результатами обучения и стратегией обучения. Оценивать тем самым эффективность использования ИКТ;
- позволять отслеживать качественные изменения в ИП на основе ИКТ (иметь качественные дескрипторы показателей);
- позволять определять баланс в развитии основных аспектов ИП (шкала многомерной оценки). [6, с. 54–69]

Разработка и реализация мер по повышению качества подготовки кадров осуществляется по направлениям: заключение договоров на подготовку кадров и трудоустройство выпускников, на организацию производственной практики, на оказание помощи в пополнении учебно-методической и материально-технической базы, на проведение учебных семинаров и иных мероприятий колледжем

совместно с работодателями. С работодателями в целях организации и проведения производственной практики обучающихся был заключен 131 договор. В соответствии с заключенными договорами на производственную практику было направлено 765 студентов колледжа

Центром маркетинга, профориентации и трудоустройства выпускников. Создан электронный банк данных выпускников колледжа в соответствии с рекомендациями Координационно-аналитического центра, содействия трудоустройству выпускников учреждений профессионального образования. Согласована возможность адаптации электронной базы колледжа к программному обеспечению «1С» с поставщиками программного продукта ООО «РАН Софт». Результатом такой работы являются стабильные показатели трудоустройства выпускников по специальности – 72–75%.

Стратегия развития образования XXI века ориентирована на подготовку специалистов, принципом которых должно стать «обучение через всю жизнь» на основе мобильного инфокоммуникационного взаимодействия в открытом информационно-образовательном пространстве. Платформой их подготовки сегодня является новая инфокоммуникационная парадигма обучения как закономерный объективный процесс. Механизмами перехода на новую парадигму обучения являются e-learning (электронное обучение) и Smart Education (умное образование). Технологизация учебного процесса на основе интеграции информационно-коммуникационных и педагогических технологий становится необходимым условием массового качественного образования. В Республике Башкортостан именно смарт-образование, базирующееся на электронном обучении, было выбрано в качестве приоритетного направления развития.

Введение федеральных государственных образовательных стандартов в систему профессионального обучения в IT-сфере, требующих соответствия качества подготовки современным требованиям работодателей, предполагает повышение интерактивности и индивидуализации обучения, которые достигаются путем применения в современном образовательном процессе электронного обучения и дистанционных образовательных технологий на основе концепции Smart-образования.

Долгосрочная целевая программа «Развитие образования в Республике Башкортостан» и разработанная на её основе Концепция системы электронного образования в Республике Башкортостан на 2015-2020 годы отмечают, что стратегическими задачами современной системы образования являются совершенствование и развитие информационно-технологической базы образовательных организаций, повышение информационных компетенций работников образования, внедрение современных методов обучения на базе ИКТ, а также определяют направления и основные мероприятия внедрения единой системы электронного образования в образовательных организациях республики.

Президент Республики Башкортостан Р. Ф Хабиров подчеркнул, что «…2022 год стал в Республике годом модернизации профессионального образования с акцентом на повышение качества подготовки молодого специалиста, системное взаимодействие с потенциальными работодателями».

Таким образом, подготовка высококвалифицированных кадров, обладающих и знаниями и умениями, отвечающих запросам потенциальных работодателей, является приоритетной задачей в дальнейших перспективах развития образовательного учреждения.

Следуя вектору, определённого заданного пути, блестяще проведя VII Открытый Региональный чемпионат «Молодые

профессионалы (WorldSkills Russia), колледж планирует продолжать работу дальше в области развития и модернизации профессионального образования, применения и совершенствования системы оценки, оптимизации управления.

Актуальность решения проблемы развития профессионального образования посредством применения интеллектуальных SMART-технологий обозначилась в идеи создания на базе Стерлитамакского многопрофильного колледжа Смарт-Центра подготовки IT-специалистов для отраслей экономики Республики Башкортостан, что также отвечает задачам, поставленным перед образованием в подготовке кадров. Так Смарт-Центр выступает материально-технической, методической и кадровой базой для организации сетевой формы реализации образовательных программ подготовки конкурентоспособных IT-специалистов в регионе.

Смарт-Центр способствует созданию в колледже собственной интегрированной интеллектуальной виртуальной среды обучения, в том числе с использованием устройств категории SMART: оборудование обучающими смарт- комплектами, смарт-столами, 3D документ-камерами, on-line дистанционными практиками, тренажерами, учебными полигонами, виртуальными лабораториями и др. Эта интегрированная среда обучения значительно расширяется за счет производственного оборудования, предоставляемого базовой кафедрой, созданной на предприятии, являющимся базой практики (ОАО «Уфанет), которая преследует политику стабилизации развития системы опережающего образования.

Колледж осуществляет подготовку специалистов по специальностям в соответствии с требованиями работодателей. Механизмом взаимодействия с работодателями является функционирование базовых кафедр, обеспечивающих качество реализации практикоориентированных профессиональных

образовательных программ на договорной основе. Вовлечение предприятий-работодателей в процесс методического и экспертного сотрудничества ведется на договорной основе, а также путем заключения соглашений о сотрудничестве и совместной деятельности. В договорах и соглашениях предусматриваются взаимные обязательства сторон, где оговаривается степень вовлечения работодателей в процесс разработки и реализации профессиональных образовательных программ:

- предоставление студентам ГАПОУ СМПК места прохождения практики в соответствии с программой практики;
- осуществление подбора непосредственных руководителей практики от организаций из числа постоянно работающих в них квалифицированных специалистов и условия для их работы, обеспечение необходимого уровня профессиональной, методической помощи студентам специальностей и профессий;
- предоставление студентам-практикантам возможность пользоваться имеющейся методической литературой, документацией, наглядными материалами, техническими средствами обучения, производственным оборудованием;
- оценка качества работы практикантов, составление характеристик с отражением в них степени и качества выполнения программы практики и индивидуальных заданий;
- оказание консультационно-экспертных услуг по разработке содержания контрольно- оценочных средств;
- участие в качестве независимых экспертов при проведении Государственной итоговой аттестации и экзаменов квалификационных по профессиональным модулям;
- организация стажировки преподавателей.

Таким образом, студентам и преподавателям предоставляются современные производственные условия формирования и развития

профессиональных компетенций на предприятиях такой отрасли экономики как информационно-коммуникационные технологии.

Создание современной интегрированной интеллектуальной виртуальной среды обучения в Смарт-Центре подготовки IT-специалистов способствует комплексной модернизации всех образовательных процессов, а также методов и технологий, используемых в этих процессах. Концепция Smart в образовательном разрезе влечет за собой появление таких технологий, как умная доска, умные экраны, доступ в Интернет из любой точки. Каждая из этих технологий позволяет по-новому построить процесс разработки контента, его доставки и актуализации. Обучение становится возможным не только в образовательной организации, но и дома и в любом месте: общественных местах, таких как музеи или кафе.

Основным же элементом, связывающим образовательный процесс, становится активный образовательный контент, на базе которого создаются единые репозитории, позволяющие снять временные и пространственные рамки. Становится возможным развивать такие компетенции, как аналитические, навыки решения комплексных проблем, инновационность – способность к развитию новых идей и их внедрению, навыки межкультурных коммуникаций.

Смарт-Центр подготовки IT-специалистов для отраслей экономики Республики Башкортостан обеспечивает возможность применения дистанционных образовательных технологий и электронного обучения в учебном процессе в электронной информационно-образовательной среде колледжа. Предполагается расширение участников образовательного процесса для всех профессиональных образовательных организаций, осуществляющих подготовку IT-специалистов и желающих влиться в смарт-образование.

При использовании электронного обучения и дистанционных образовательных технологий колледжем обеспечивается открытый доступ всех участников образовательного процесса к информационным ресурсам через официальный сайт www.mirsmpc.ru.

При реализации образовательных программ с применением дистанционных образовательных технологий и электронного обучения частично или в полном объеме независимо от мест нахождения обучающихся, колледжем обеспечивается доступ обучающихся к электронным информационным ресурсам, электронным образовательным ресурсам через образовательный портал ГАПОУ СМПК http://www.mirsmpc.ru/moodle (далее – портал), созданный на базе системы управления обучением и образовательным контентом Moodle.

При реализации образовательных программ колледжем обеспечивается доступ к электронно-библиотечной системе (ЭБС) http://znanium.com/ научно-издательского центра ИНФРА-М – коллекции электронных версий изданий (книг, журналов, статей и пр.), сгруппированных по тематическим и целевым признакам.

При создании Смарт-Центра подготовки IT-специалистов для отраслей экономики Республики Башкортостан посредством развития электронной информационно-образовательной среды колледжа осуществляется решение следующих задач смарт-образования:

- развитие технологической инфраструктуры колледжа за счет повышения уровня интеллектуальности устройств, формирующих окружающую среду для специалистов IT-отрасли экономики Республики Башкортостан;
- изменение платформ, используемых для передачи знаний и широкого использования SMART-устройств, внедрение и использование платформ мобильных устройств и облачных технологий;

– создание активного образовательного контента;
– создание единых репозиториев на базе активного образовательного контента;
– внедрение информационных систем сопровождения образовательных процессов, обеспеченных защитой согласно требованиям действующего законодательства;
– подготовка кадров в сфере электронного образования и для IT-отрасли экономики Республики Башкортостан;
– круглосуточная техническая возможность доступа для каждого участника учебного процесса к информационным образовательным ресурсам колледжа;
– хранение, обновление и систематизация информационных образовательных ресурсов;
– своевременная доставка учебных и методических материалов;
– организация и управление индивидуальной работы обучающегося;
– организация групповой работы обучающихся;
– организация самостоятельной работы и самоконтроля обучающихся;
– непрерывный мониторинг, учет и анализ работы обучающихся;
– непрерывный мониторинг работы преподавателей со стороны администрации;
– обратная связь, упорядоченное взаимодействие в синхронном (on-line) и асинхронном режиме связи (off-line);
– поддержка обучающихся (техническая, педагогическая, ресурсная);
– поддержка педагогического персонала (техническая, педагогическая, ресурсная);
– проведение контрольных мероприятий;
– процедура оценки качества освоения образовательных программ.

Изменяются и условия работы преподаватель в сфере «умного» образования, Smart Education позволяющие преподавателю не тратить

лишнее время на разработку курса: он может воспользоваться уже существующим контентом, комбинировать его, а также дорабатывать.

Колледж предполагает также использовать современные Интернет технологии и возможности дистанционного обучения для формирования виртуальных профессиональных сообществ преподавателей, общения, обсуждения проблем, решения общих задач, обмена опытом, информацией и т.д. Внедрение электронного обучения и дистанционных образовательных технологий требует от преподавателей колледжа и ИКТ-службы колледжа использования новых инструментов и методов обучения, построения новых моделей обучения, обеспечения безопасности.

Правовой основой для системного внедрения смарт-образования являются: Федеральная целевая программа развития образования на 2011-2015 годы (Утверждена Постановлением Правительства Российской Федерации от 7 февраля 2011г. № 61), Долгосрочная целевая программа «Развитие образования Республики Башкортостан» на 2013-2017 годы (Постановление Правительства Республики Башкортостан от 21 февраля 2013 г. № 54 с изменениями на 1 февраля 2022 года).и другие нормативно правовые акты [71]

Таким образом, Смарт-Центр подготовки IT-специалистов для отраслей экономики Республики Башкортостан способствует обеспечению доступности, современности и качеству условий реализации профессиональных программ на основе базовой кафедры как эффективной формы сотрудничества образовательных организаций и IT-предприятий. Возможность использования материально-технической, методической и кадровой базы Смарт-Центра другими профессиональными образовательными организациями региона в рамках сетевой формы реализации образовательных программ подготовки IT-специалистов добавляет значимости для развития кадрового потенциала

высокотехнологичных производств и тех отраслей экономики и социальной сферы, которые поддерживаются приоритетными национальными проектами.

В этих условиях оценка качества ИП в структуре управления образовательными системами становится действенным инструментом, позволяющим быть основой для стратегического планирования, определять эффективность реализации государственных программ, направленных на развитие системы образования, стать основой мониторинга качества, служить основой регламентации образовательной деятельности, частью общественно-профессиональной аккредитации, инструментом определения потребностей в подготовке и повышении квалификации педагогических работников.

Всё это позволяет утверждать о вышеперечисленных возможностях использования предложенной системы оценки качества ЕИП для развития колледжа, в управлении образовательными системами в целом и следовать по намеченному курсу далее.

Выводы по 1 главе.

Очевидность характерных процессов устаревания и обновления знаний на сегодня стали настолько стремительны, что осознание необходимости изменений, подвигает нас к активному приобретению новых знаний не одномоментного действия, а на протяжении всей жизни. Образовательным же учреждениям невозможно остаться в стороне, по-своему исторически определённому предназначению, способствуя, в свою очередь, актуальным изменениям, носящим управляемый поэтапный характер и обеспечивая создание новой сферы деятельности для всех участников образовательного процесса, определяемой как единое информационное пространство образовательной организации.

При этом понимание того, что единое информационное пространство образовательной организации продолжает структурироваться (выстраивается) её членами (субъектами создающими, перерабатывающими, использующими информацию), определённым образом, под их собственные потребности, используя аппаратные и программные средства, в тот же момент, учитывая актуальные задачи и требования, способствует продуктивности деятельности учреждения.

Основные задачи дальнейшей модернизации и совершенствования ЕИП таковы:

- создание комфортных условий для всех участников образовательного процесса;

- повышение эффективности деятельности посредством автоматизации.

На примере колледжа ГАПОУ СМПК мы отследили процесс информатизации образовательного учреждения, совершающийся в течении 20 лет, выделили эффективность, ставя акцент на незаконченности процесса информатизации для учреждения и перспективах дальнейшего его развития, обозначенных политикой Российской Федерации и политикой Республики Башкортостан в области образования, сводящихся к:

- качеству подготовки высококвалифицированных кадров

- взаимодействию с потенциальными работодателями

- развитию единой системы электронного образования

- продолжению активного внедрения новейших технологий и методов обучения;

-дальнейшей разработки, применения и совершенствования систем оценки, определяющих воздействие ИКТ на учение и обучение

- совершенствованию систем взаимодействия и администрирования

- безопасности человека в информационном пространстве.

Векторное направление развития колледжа определено, по которому и планируется дальнейшее последовательное движение.

ГЛАВА 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И НЕОБХОДИМОСТЬ СОВЕРШЕНСТВОВАНИЯ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1. Требования информационной безопасности для современной образовательной организации и меры защиты информации.

В педагогической литературе понятия информационной безопасности не содержится, но изучив основные подходы в научной литературе к определению информационной безопасности М. А. Борисова, В. Ю. Статьева, В.А. Тинькова, можно дать определение данного термина и в педагогическом аспекте [89], а именно:

Безопасность — это состояние защищённости от угроз, а иначе полное их отсутствие. Информация же представляет собой какие-либо сведения, следовательно, информационная безопасность — это состояние защищённости от угроз сведений, которыми располагает организация, в частности, образовательное учреждение. Угроза же — это потенциальные или реальные действия, приводящие к моральному или материальному ущербу, отсюда вытекает, необходимость принятия действий, или, точнее сказать, противодействий, соответствующего порядка защиты, в каждой конкретно взятой организации образования. По отношению к имеющейся в ней информации, представляющей для организации информационные ресурсы и поддерживающей инфраструктуры, поэтому реализация таковых действий должны осуществляться в интересах самой организации, её информационных ресурсов, а также всех её членов в общем и каждой отдельно взятой личности, в частности.

К тому же их векторное обращение должно соответствовать выявлению и своевременному пресечению угроз информационного порядка, по отношению к информации, имеющейся в распоряжении образовательной организации, и поддерживающей инфраструктуре, как потенциального, так и реального характера. Важность данного аспекта непозволительно недооценивать. Ведь игнорирование подобного рода… нарушений, основных качественных характеристик(свойств) информации …заключающихся в конфиденциальности, целостности, доступности, ведёт в итоге, к незаконному овладению охраняемыми сведениями…[15] . Проявляясь преднамеренностью либо случайностью действий, а также активностью или же пассивностью таковых, тем самым усугубляя положение дел защиты данных. Приоритетно имея в своей основе человеческий фактор, как внешнего, так и возможно внутреннего влияния. Приводя, рано или поздно, к нарушению процесса сбора и обмена информацией в организации. Напрямую отражаясь, при этом, на функционировании ЕИП ОО. Что чревато потерей качества, результативности и имиджа для образовательного учреждения.

Особо трагично обстоят дела, в условиях преднамеренности угроз, так как в большинстве случаев они не могут быть предвидены, а последствия их влияния будут несоизмеримы для учреждения, особенно касательно сотрудников и студентов, при вовлечении их в криминал, терроризм и морально психологического воздействия на них.

К тому же производство и потребление информации, с соответствующим сбором и обменом таковой, приобрело в образовательной организации огромную скорость, благодаря информатизации образования и овладения информационными технологиями. Одним из высокоценных видов информации, которым

располагает образовательная организация, можно назвать персональные данные всех задействованных участников образовательных взаимоотношений. При этом сегодня это неотъемлемая часть деятельности учреждения и представить этот процесс вне ИБ просто не представляется возможным.

Персональные данные должны быть защищены, в соответствии с требованиями Федерального закона 152-ФЗ ст.19 от 27 июля 2006года «О персональных данных», от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и иных неправомерных действий [67], поэтому, пресечение угрозы безопасности информации, т.е. потенциальной возможности нарушения основных качественных характеристик (свойств) информации при её обработке техническими средствами: конфиденциальности, целостности, доступности и совершенствование ЕИП организации – это наиважнейшая задача, от решения которой зависит благополучие в полном смысле этого слова.

Безопасность должна осуществляться комплексно на всех уровнях и всеми законом доступными средствами.

Из всего вышесказанного вытекают выводы следующего порядка, определяющие требования информационной безопасности для образовательной организации:

-Информационная безопасность – это одно из главных условий организации единого информационного пространства и качественного функционирования образовательной организации.

-ИБ должна иметь свою собственную своеобразную специфику, присущую образовательному учреждению, отвечающую его потребностям, поддерживаемую в нём на высоком современном уровне.

- ИБ в образовательной организации должна осуществляться в соответствии с нормативно правовой документацией.

Требования ИБ для образовательной организации сводятся к обеспечению:

- защиты от угроз, регламентируемые законами и инструкциями, как федерального значения, так и разработанными в соответствии с ними, и утверждёнными в образовательном учреждении с учётом специфики, и особенностей эксплуатации информационных систем организации и действующей нормативно правовой базой учреждения.

-современности системы безопасности;

-построения и курирования системы ИБ высококвалифицированными специалистами, имеющими соответствующую квалификацию и опыт работы;

- проведения анализа состояния информационных активов и систем хранения, обработки информации образовательной организации.

Другими словами, современные условия, трактуют информационную безопасность образовательной организации, как обязательный компонент многопланового процесса защиты, осуществляющегося посредством политики ИБ образовательного учреждения, осуществляемой на 5 уровнях:

- нормативно-правовой;
- административно-организационный;
- технический;
- морально-этический;
- физический.

Рассмотрим подробнее меры защиты, предпринимаемые на каждом из этих уровней.

Нормативно-правовой способ защиты

Основным документом, определяющим степень угроз и меры обеспечения информационной безопасности обучающихся в образовательной организации, является «Национальная стратегия действий в интересах детей». Она предусматривает приоритет мер, направленных на защиту сознания ребенка от информационного воздействия агрессивного характера. Меры по защите информационных систем и баз данных имеют второй уровень приоритетности.

Законодательством определяются данные, которые должны быть защищены от несанкционированного доступа третьих лиц. К числу таких сведений относятся:

- персональные данные;
- конфиденциальные сведения;
- служебная, профессиональная, коммерческая тайна.

Порядок обеспечения безопасности персональных данных регламентируется Трудовым кодексом, Гражданским кодексом, Федеральным законом «Об информации» и другими актами. Конкретные меры по защите данных, используемое для этого аппаратное и методическое обеспечение определяются законами и профильными ГОСТами.

Меры административно-организационного характера

Система административно-организационных мер строится на базе внутренних регламентов и правил организации, которыми регламентируется порядок обращения с информацией и ее носителями. В том числе должны быть разработаны:

- должностные инструкции;
- внутренние методики по ИБ;
- перечни не подлежащих передаче данных;

- регламент взаимодействия с уполномоченными государственными органами по запросам о предоставлении информации и т. д.

Разработанными методиками должен определяться порядок доступа учеников в интернет во время занятий в компьютерных классах, меры по предотвращению доступа детей к определенным ресурсам, предотвращение использования ими своих носителей информации и т. д.

Технические меры

Технические меры защиты предусматривают использование специализированного программного обеспечения. В том числе в образовательных организациях рекомендуется использовать DLP и SIEM-системы, которые эффективно обнаруживают угрозы ИБ и обеспечивают борьбу с ними. При невозможности использования подобных систем по причине бюджетных ограничений применяются рекомендованные и разрешенные антивирусы и другие виды специального софта.

Применяемое для технической защиты программное обеспечение должно обеспечивать контроль электронной почты, которой пользуются ученики или персонал образовательной организации. Также могут устанавливаться ограничения на копирование данных с жестких дисков компьютеров. Обязательно рекомендуется использование контент-фильтра, с помощью которого ограничивается доступ детей к определенным ресурсам в интернете.

Морально-этические средства обеспечения информационной безопасности

Система морально-этических ценностей имеет особое значение в сфере образования. Она служит основой для выработки комплекса мер, направленных на защиту детей и подростков от информации этически некорректного, травмирующего,

противозаконного характера. Защита детей от пропаганды основывается на законе «О защите прав ребенка». Этим актом определяются права детей на защиту от информации, которая может стать причиной моральной травмы.

В рамках мер по обеспечению ИБ создаются перечни источников (программ, документов и т. д.) способных травмировать детскую психику. В результате принимаемых мер должен предотвращаться доступ таких источников на территорию образовательного учреждения.

Физические меры

Ответственность за реализацию мер защиты компьютерной сети и носителей информации физического характера несет непосредственно руководитель образовательной организации и ее IT-персонал. Не допускается перекладывание этих мер на наемные охранные структуры.

К числу физических мер относятся:

- реализация пропускной системы для доступа в помещения, в которых находятся носители данных;
- создание системы контроля и управления доступом;
- определение уровней допуска;
- создание правил обязательного регулярного копирования критически важных данных на жесткие диски ПК, не подключенных к интернету.

Также среди физических мер можно назвать правила по созданию паролей и их периодической замене.

2.2. Состояние информационной безопасности в колледже ГАПОУ СМПК.

Стерлитамакский многофункциональный колледж, являясь

образовательным учреждением, располагает следующими информационными ресурсами:

Информация, относящаяся к коммерческой тайне:

- личные дела работников и обучающихся
- личные карты работников;
- трудовые договора;
- договоры со студентами;
- договоры с поставщиками и арендаторами;
- заработная плата;
- содержание регистров бухгалтерского учета и внутренней бухгалтерской документации;
- прочие разработки и документы для внутреннего пользования.

Открытая информация:

- информация на web-сайте www.mirsmpc.ru,
- коллективный договор;
- учредительный документ;
- устав;
- перечень образовательных программ;
- буклеты; консультации, информационные листы и т.п.…

Все информационные ресурсы колледжа, в соответствии с законом РФ (ФЗ № 149- ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г.), подлежат защите, посредством обеспечения информационной безопасности таковых.

Политика информационной безопасности колледжа предусматривает меры 5 уровневой системы защиты.

I уровень – Нормативно-правовой.

Включает в себя нормативно-правовую документацию, регулирующую вопросы информационной безопасности в учреждении:

– Конституция РФ;

– Гражданский кодекс РФ ст.139;

- Уголовный кодекс гл.28 ст.272, 273, 274, 138, 183;

– Федеральный закон Российской Федерации от 27 июля 2006 г. № 152- ФЗ «О персональных данных» в действующей редакции.

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

– Постановление Правительства Российской Федерации от 1 ноября 2012года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

II уровень*:* Административно - организационный. В соответствии со II уровнем мер защиты информационных активов в колледже чётко обозначены и расписаны алгоритмы действий.

1.Пользование информационными ресурсами в колледже, регламентируется в соответствии с Федеральным законом «Об образовании в Российской Федерации» от 29 декабря 2012 г. № 273-ФЗ;

2.Доступ педагогических работников и обучающихся к информационным ресурсам обеспечивается в целях качественного осуществления образовательной и иной деятельности, предусмотренной Уставом колледжа и образовательных программ и т. д. Осуществляется системным администратором.

3.Доступ к информационно-телекоммуникационным сетям (сети

Интернет), педагогических работников в колледже, осуществляется с персональных компьютеров (ноутбукови т. п.), подключенных к сети Интернет. Для доступа к информационно- телекоммуникационным сетям в колледже педагогическому работнику предоставляются идентификационные данные (логин и пароль / учётная запись). Предоставление доступа осуществляется системным администратором.

4.Также осуществляется доступ к базам данных, учебным и методическим материалам, материально-техническим средствам, дающим возможность обеспечения образовательной и административной деятельности педагогических работников в колледже, с учётом администрирования и разграничения прав доступа.

5. Курирует информационную безопасность ИБ учреждения подразделение ИКТ- ЦИТ (центр информационно коммуникационных технологий).

Работа ЦИТ (центра) регламентируется нормативно – правовыми законами, локальными актами организации и должностными инструкциями.

6. Организован контроль, соблюдение времени режима труда и пребывания сотрудников колледжа на территории организации;

7.Организована работа с документами и документированной информацией, т. е. ведется учет, исполнение, возврат, хранение носителей конфиденциальной информации.

Административно-организационные меры являются весомым звеном в создании надежного механизма защиты информационных активов для образовательной организации. Так как правильно выстроенная, продуктивно организованная деятельность, всех её участников, в соответствии с нормативно правовыми аспектами, обеспечит для таковых, комфортное, продуктивное взаимодействие.

А также положит начало формулировки всей политики информационной безопасности организации в целом.

В качестве недостатков данного уровня защиты можно указать следующее:

Соблюдение административно-организационных мер соответственно требований политики безопасности образовательной организации, пользователями колледжа иногда игнорируются, пренебрегаются и нарушаются, что проявляется в не регулярном изменении своих паролей, повторяемости и похожести их.

Хотя периодичность инструктажей, наказания/поощрения пользователей проводится. Тем не менее данный факт говорит о недостаточности таковых, либо о неэффективности, что в итоге ведет к небрежности сотрудников, выражаясь в недостаточном знании правил защиты конфиденциальной информации, непониманием необходимости тщательного их выполнения административными работниками, педагогами и студентами, проявляясь в частоте блокировки системы из-за неправильности и некорректности введенных данных.

Следовательно, на административном уровне политика информационной безопасности нуждается в корректировке.

III уровень: Технический.

Этот уровень предусматривает программно-технические меры защиты.

Программно-технические меры защиты информации — это совокупность аппаратных и программных средств и мероприятий по их использованию в интересах защиты конфиденциальности, целостности, доступности информации.

Программно-технические меры защиты реализуются в соответствии с политикой информационной безопасности образовательной организации. С этой целью в колледже установлены:

SHDSL-модем с возможностью работать в режиме маршрутизатор для закрытия сети от проникновения извне. SHDSL модем ZyXEL предназначен для создания корпоративной сети, в основе которой лежит скоростное двунаправленное соединение по медным проводам. Используется для объединения двух офисов по одной или по двум медным парам в режиме «точка-точка» с организацией симметричного скоростного полнодуплексного соединения. Модем имеет возможность работать в режиме моста или маршрутизатора. Встроена система обнаружения и предотвращения вторжений, аномалий активности в сети IDS (Intrusion Detection System).

Антивирусная система Kaspersky Security для защиты от компьютерных вирусов. Производится обновление баз и сканирование рабочих станций. Антивирусная защита имеет комплексный характер — устанавливается на компьютеры пользователей, а также в качестве системы мониторинга и контроля обновлений на сервера.

Обеспечивает безопасность основных свойств информации и осуществляет выявление и устранение вредоносных программ. Kaspersky Security является одним из самых качественных антивирусных программ, обеспечивающих базовую защиту ПК.

Для защиты в облаке имеется SkyDNS. Проверяет входит ли запрашиваемый ресурс в запрещённую категорию или нет.

Локальная сеть колледжа объединяет структурные подразделения колледжа с рабочими местами преподавателей и студентов, представлено программным обеспечением – LMS Moodle, способствующего расширению возможности дистанционного обучения, для обеспечения индивидуальных маршрутов обучающихся.

Как и любая другая сеть она имеет протоколы передачи данных или сетевые протоколы.

Корпоративная сеть колледжа построена на принципах протоколов TCP/IP.

Сетевой протокол — это четко определенный набор правил и соглашенийдля взаимодействия одинаковых уровней сети.

Протоколы TCP/IP - набор широко используемых в Интернете сетевых протоколов, поддерживающий связь между объединенными сетями, состоящими из компьютеров различной архитектуры и с разными операционными системами. Протокол TCP/IP включает в себя стандарты для связи между компьютерами и соглашения о соединении сетей и правилах маршрутизация сообщений. Собственно этот протокол состоит из двух протоколов:

- TCP (Transmission Control Protocol) – протокол, отвечающий за формирование и отправку пакетов.
- IP (Internet Protocol) – маршрутизируемый протокол семейства TCP/IP, отвечающий за IP-адресацию, маршрутизацию, а также за разбиение насегменты и повторную сборку пакетов IP.

Для защиты корпоративной сети используется:

Межсетевой экран, брандмауэр – это разные названия одного и того инструмента, обозначающего локальное или функционально распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и/или выходящей из автоматизированной системы. Так межсетевой экран служит контрольным пунктом на границе двух сетей. Эта граница лежит между внутренней сетью организации и внешней сетью - сетью Интернет. А также установлен для разграничения внутренних подсетей корпоративной сети организации. Наличие межсетевого экрана в колледже обусловлено хранением и обработкой ПДн, что обязательно по закону и сертифицировано ФСТЭК. Недостатком данного уровня защиты **является не выполнение обновлений**

операционной системы MS Windows и использующегося ПО, негативным образом отражаясь на безопасности функционирования образовательной организации, при этом активизируя риски несанкционированного доступа к хранящейся на ПК информации, в том числе ПДН и её повреждению из-за ошибок в ПО.

Необходимы меры по минимизации данного рода рисков, которые позволят, своевременно закрыть, ставшие известными уязвимости в программном обеспечении и избежать появления вирусов, а также не стать жертвой хакерских атак.

IV уровень: Морально-этические средства обеспечения информационной безопасности.

Морально-этические средства обеспечения информационной безопасности призваны сохранить как базы данных, с имеющейся в ней конфиденциальной информацией, так и гарантировать невозможность проникновения в учебные заведения любой пропаганды, как безобидной, так и агрессивной, способной нанести непоправимый урон детской психике. Так в колледже действует механизм - правило «Белого списка», когда нежелательная информация запрещена по умолчанию. Проводятся регулярные инструктажи, беседы, консультации, воспитательные мероприятия, как среди студентов, так и сотрудников колледжа, способствующие формированию морально-этических качеств, и нравственно-выраженных поведенческих действий, по отношению к вопросу информационной этики.

V уровень: Физические меры.

Физическая защита объекта – это способ обеспечения безопасности, посредством комплекса организационных мероприятий, технических и инженерных средств, а также действий подразделений сил обеспечения безопасности (охраны) объекта, направленных на предотвращение несанкционированных и

нерегламентированных действий, которые могут создать угрозу безопасности, приводя к нежелательным последствиям.

Охрану ГАПОУ СМПК осуществляет охранное предприятие ООО ЧОП «Дружина». Контроль физического доступа в помещения реализуется посредством системы СКУД. Настройка СКУД, с учётом разрешённых уровней доступа групп сотрудников и студентов, а также времени суток, произведена согласно техническому заданию. На входе имеются турникет и заграждения. Пропускная оборудована тревожными кнопками. В случае отключения электропитания предусмотрено автоматическое переключение на резервные источники питания. По периметру с наружи и внутри зданий организованно видеонаблюдение, с выводом на дисплей. Есть видеоархив с буфером хранения. Организована достаточная освещённость объекта. Присутствует система ручного биометрического учёта о посещении. Двери оборудованы замками, в том числе кодоблокирующими. Серверная расположена в отделе «Информационных технологий», физический доступ имеют только сотрудники ЦИТ.

Недостатком данного уровня защиты можно назвать отсутствие системы контроля доступа сотрудников к чужим рабочим местам.

Обследовав систему обеспечения ИБ в колледже, можно сделать следующие выводы:

- Существующая система обеспечения информационной безопасности в колледже несовершенна и имеет уязвимости, которые представляются следующего порядка:

1)Сотрудники

2)Технические средства

Следовательно, для выбора рентабельного пакета решений необходимо провести мероприятия по анализу рисков ИБ ЕИП колледжа с акцентом на правомерность.

В связи с этим требуется обозначение вектора совершенствования системы информационной безопасности ЕИП образовательной организации колледж с одновременным пересмотром политики ИБ образовательного учреждения.

2.3. Анализ рисков информационной безопасности образовательного учреждения – ГАПОУ СМПК

Действенным мероприятием, предполагающим получение реального состояния ИБ ЕИП образовательной организации, может выступить анализ рисков информационной безопасности образовательного учреждения. Позволяющий управлять информационными рисками, в достижении ИБ и возможности сформировать стратегию развития системы обеспечения ИБ колледжа, при этом определяя функциональность системы в целом. Производя идентификацию информационных активов учреждения, с учётом угроз безопасности, влияющих на эти активы, в соответствии с перечнем угроз представленных в банке данных ФСТЭК России, и связанных с ними уязвимостей, оценивая риски в соответствии с приоритетами.

При этом необходимо понимать, что достижение абсолютной безопасности, в принципе не представляется возможным, так как всегда остаётся присутствие остаточного риска. Следовательно, «…следует понимать информационную безопасность … как приемлемый уровень риска…»- утверждает Козлов О.А. доктор пед.наук, профессор Институт управления образованием Российской академии образования(«Информационная безопасность как условие деятельности образовательных организаций»[48]. Приемлемый риск при этом является неснижаемой характеристикой. И к тому же, риск всегда будет определяться, как потенциальная возможность воздействия определённой угрозой на уязвимости с целью

причинения ущерба.

Но так как в реальности уровень рисков может быть разным (и неприемлемым, и чрезмерным), поэтому принятие во внимание реальных и потенциальных угроз и рисков необходим. Не забывая об уязвимостях, как о наиболее слабых местах защиты (параметрах информационного объекта), которые могут быть использованы нарушителем для реализации угроз.

Так конкретными определёнными угрозами для информационных активов колледжа, можно назвать угрозы конфиденциальности, угрозы целостности, угрозы доступности.

Угрозы конфиденциальности:

- злоупотребления полномочиями;
- делегирование неиспользуемых полномочий;
- установка нелицензированного ПО;
- открытие портов.

Угрозы целостности информации:

- ввод неверных данных;
- несанкционированная модификация информации;
- кража информации;
- дублирование данных;
- потеря информации на жёстких носителях;
- угрозы целостности баз данных;
- угрозы целостности программных механизмов работы организации;

Угрозы доступности информации:

- разрушение (уничтожение) информации: вирусом, повреждение оборудования.

Соответствие между угрозами и рисками предопределено

Риски для информационной системы ГАПОУ СМПК «Система электронного документооборота СЭД «Дело» представлены в Таб.1

Таблица 1- Классификационная таблица информационных рисков

Информационная система	Информационный риск	По механизму воздействия	По характеру угрозы	По основному аспекту ИБ	По источнику воздействия
Система электронного документооборота СЭД «Дело»	Механическое повреждение устройств	Сбои и отказ технических средств	Технические	РНД	Внутренний
	Ошибки при вводе/выводе/передачи информации через ПК	Ошибки специалистов	Технические, организационные	РНД, РНЦ	Внутренний
	Ошибки при работе с носителями информации	Ошибки специалистов, сбои и отказ программных средств	Технические, организационные	РНД, РНЦ	Внутренний
	Непреднамеренное разглашение конфиденциальной информации	Ошибки специалистов	Организационные, технические	РНК	Внутренний, внешний
	Хищение информации, шпионаж	Нарушение авторских прав, несанкционированный доступ, шпионские программы	Организационные, технические	РНК	Внешний, внутренний
	Ошибки при эксплуатации программных средств	Ошибки специалистов, сбои и отказ программных средств	Технические, организационные	РНД, РНЦ, РНК	Внутренний
	Неправильные действия со средствами защиты информации	Ошибки специалистов, сбои и отказ программных средств	Технические, организационные	РНД, РНЦ	Внутренний
	Отказ системы ввода, вывода, чтения, запись информации	Сбои и отказ технических средств, сбои и отказ программных средств	Технические	РНД	Внутренний

Продолжение таблицы 1

	Умышленное внесение изменений в режимы работы устройств	Несанкционированный доступ, вредоносное ПО, шпионские программы	Организационные, технические	РНЦ	Внутренний
	Нарушение работоспособности каналов передачи данных, поломки сетевого оборудования	Сбои и отказы сетевого оборудования	Технические	РНД	Внутренний
	Блокировка системы защиты	Несанкционированный доступ, ошибки специалистов, вредоносное ПО, шпионские программы	Технические	РНД, РНЦ	Внешний, внутренний
	Аварии в системе электропитания, водоснабжения, отопления	Сбои и отказы технических средств	Технические	РНД	Внутренний

Уменьшить риски возможно уменьшив или устранив действия угроз. А это достигается путём воздействия на уязвимости системы. Поэтому каждая уязвимость должна быть учтена и оценена специалистом.

Единой стандартизированной методики анализа и оценки рисков ИБ для образовательной организации в настоящее время нет.

Существуют многочисленные методики, методы, алгоритмы, описанные в государственных и международных стандартах, анализа ИБ. И любая организация, преследуя цель управления информационными рисками, может выбрать для себя наиболее приемлемый вариант. Рассмотрим некоторые из них.

ГОСТ Р ИСО/МЭК 27005-2010 из серии стандартов ISO/IEC 27000 пришёл на смену устаревшему ISO13335. Законодательно действующий. Предназначен для применения в любых организациях, независимо от их типа, размера и характера бизнеса [31]. Разработан

в 2005 году и продолжается его модификация. Актуальна его версия 2010 года [31].

Методика ФСТЭК

Законодательно утверждённая. Данная методика разработана в 2008 году на основании Федерального закона от 27 июля 2006 года № 152-ФЗ « О персональных данных» и положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённого постановлением Правительства РФ от 17 ноября 2007 года № 781. Предназначена для использования при проведении работ по обеспечению безопасности персональных данных при их обработке в автоматизированных информационных системах персональных данных ИСПДн.

Метод МАРИОН(MARION)

Метод МАРИОН изобретён во Франции, соответствует стандарту ISO-SC27-WG1.[61]. Метод является стандартом де-факто по определению компьютерных рисков.

Алгоритм анализа информационных рисков ГРИФ

Самые известные в мире алгоритмы полного анализа информационных рисков – это британский CRAMM и американский RiskWatch, в России – это ГРИФ. В нём применяется метод классических видов угроз безопасности, основанном на целом комплексе параметров, которые определяются защищённостью исследуемого объекта. Представляет скорее научный интерес, чем практический.

Все известные в мире подходы решения вопроса анализа информационных рисков, хоть и отличаются друг от друга: одни в основе своей имеют качественную определяющую («Низкий», «Средний», «Высокий»), другие количественную – числовую составляющую, а третьи оперируют и теми и другими величинами,

тем не менее преследуют, в конечном итоге, единую цель - оценку риска.

Для нас в данной работе играет роль: правомерность выбранных методов и средств и факт оценки системы в целом. Поэтому в качестве базового стандарта для проведения анализа оценки рисков ИБ образовательной организации ГАПОУ Стерлитамакский Многопрофильный Педагогический Колледж, воспользуемся стандартом ГОСТ Р ИСО/МЭК 27005–2010, предусматривающим матричную систему оценки и методикой ФСТЭК России - для определения актуальности угроз.

Последовательность действий анализа риска ИБ ЕИП ОО будет содержать:

1) анализ риска, предполагающему: определение систем, подлежащих анализу риска, идентификацию соответствующих им активов, идентификацию угроз, идентификацию уязвимостей

2) измерение риска

3) оценивание риска.

Для наглядности обратимся к рисунку 2. На котором представлен процесс оценки рисков информационной безопасности [11].

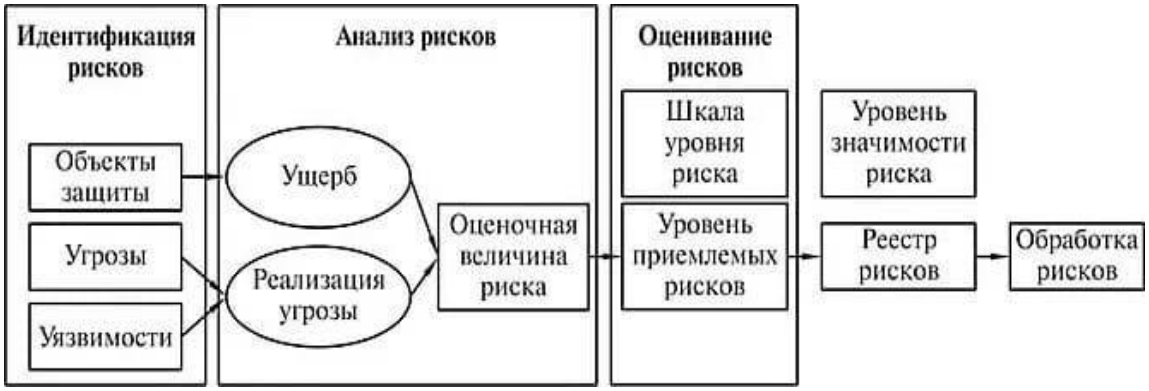


Рис.2. - Процесс оценки рисков информационной безопасности

Учитывая вышесказанное, алгоритм наших действий будет следующим:

- во-первых необходимо обозначить системы и их содержание;
- определить и описать активы систем;
- определить их ценность;
- описать угрозы;
- степень вероятности угроз;
- идентифицировать уязвимости;
- определить уровень угроз и уязвимостей;
- произвести оценку ценности для степени вероятности и возможных последствий рисков;
- вывести итоговый балл для актива;
- заключительным этапом будет: подсчёт всех итоговых баллов актива системы, для получения единого балла системы.

Полученный итоговый балл системы будет использоваться для проведения различай между системами и определения той системы, защите которой необходимо отдать предпочтение. Чем выше балл, тем больше внимания необходимо уделить информационной безопасности данной системы.

На основе полученных результатов станет возможным составить рекомендации.

I. Идентификация активов

В таблице 2 представлен перечень информационных систем подлежащих аудиту информационной безопасности ГАПОУ Стерлитамакский Многопрофильный Профессиональный Колледж. Так как именно эти системы наиболее соприкасаются с данными, подлежащими защите. В соответствии с мнением экспертов. С ними соотносятся одноимённые активы, в соответствии с перечнем содержания.

Оценка ценности активов была определена экспертным путём, с точки зрения стоимости его замены, восстановления или приобретения из опросов ведущих специалистов владельцев

информации по единой числовой шкале от 0 до 4. Перечень информационных систем обрабатывающих ПДН представлены в таблице 2.

Таблица 2 - Перечень информационных систем обрабатывающих ПДН

Оценка ценности актива	Наименование информационной системы	Описание информационной системы	Перечень содержания информационной системы
2	«1 С: Колледж» на технологической платформе «1 С: Предприятие 8.2 » Включена в Реестр российского ПО	Программный продукт, представляющий собой комплексное решение для управления деятельностью учреждений начального и среднего профессионального образования. Охватывающий все уровни управленческой деятельности основных подразделений колледжа и интегрируется с типовыми решениями фирмы «1С»для бухгалтерии и отдела кадров	-Паспортные данные студента - Паспортные данные родителей (представителей) - СНИЛС студента -СНИЛС законных представителей - Данные аттестата студента - Контактный телефон - Электронная почта - Достижения - Группа здоровья - Специальность - Приказы о зачислении/ отчислении/академических отпусках - Паспортные данные сотрудников ОО -СНИЛС сотрудников ОО - ИНН сотрудников ОО - Контактный телефон сотрудников ОО - Стаж работы сотрудников ОО - Расписание занятий - Успеваемость студентов

Продолжение таблицы 2

4	Региональная АИС «Сетевой город Образование»	Автоматизированная информационная система «Сетевой город. Образование», модуль «Профессиональная образовательная организация» Модуль для профессиональных образовательных организаций АИС ПОО позволяет решать административные задачи профессиональных образовательных организаций и проводить мониторинг текущего учебного процесса	- Паспортные данные студента - Паспортные данные родителей (законных представителей) - СНИЛС студента - СНИЛС родителей (законных представителей) - Данные аттестата - Контактный телефон - Электронная почта - Достижения -Группа здоровья - Специальность -Приказы о зачислении /отчислении/академических отпусках -Паспортные данные сотрудников ОО - СНИЛС сотрудников ОО - ИНН сотрудников ОО - Контактный телефон сотрудников ОО - Стаж работы сотрудников ОО - Образовательные программы - Рабочие программы -Расписание занятий -Успеваемость студентов -КТП

Продолжение таблицы 2

1	ФИС ГИА и Приёма В соответствии с требованиями Рособрнадзора от 04.07.2019 № 04–70	Федеральная информационная система обеспечения проведения единого государственного экзамена и приёма граждан в образовательные учреждения среднего профессионального образования и образовательные учреждения высшего образования	- Паспортные данные студента - Данные аттестата -Направление подготовки - Специальность - Приказ о зачислении
2	Официальный Сайт образовательной организации В соответствии с требованиями Роспотребнадзора	Разработан на основе Joomla 3,5, расположен на собственном Web-сервере, построенном на операционной системе Ubuntu Server, адрес:www/mirsmpc.ru.	- Все документы об образовательной организации - ФИО преподавателей - ФОТО преподавателей - Биография Преподавателей - Фото мероприятий и массовые Фото студентов
3	Система электронного документооборота СЭД «ДЕЛО» Включена в Реестр российского ПО	Многофункциональная программа для работы с любым видом документаций, позволяющая: -редактировать, -хранить файлы, -контролировать объёмы выполненной работы сотрудниками организации. -поддерживает смешанный	- Все документы об образовательной организации -ФИО сотрудников, паспортные данные, СНИЛС, ИНН, должность, подразделение, телефон - ФИО студентов, паспортные данные, СНИЛС, ИНН, телефон -Офисные документы, договора, отчёты -Корреспонденция -Электронные письма

Продолжение таблицы 2

		документооборот (бумажный и электронный), -может функционировать, как в локальной, так и в сети Интернет.	

II.Идентификация угроз

Идентификация угроз представлена в таблице 3. Она была произведена в соответствии с выявленными областями уязвимостей и активами подверженными угрозам.

Буквами будем обозначать:

A- ошибки персонала (случайный вред)

D- преднамеренные действия

Таблица 3 - Идентификация угроз ИБ

Выявленные области уязвимостей	Соответствующие виды угроз	Степень воздействия	Источники угрозы	Активы подверженные угрозам
Персонал	Ненадлежащее использование ресурсов	средняя	D, A	все
Нормативно-методическая база	Перехват, изменение информации	высокая	D	ПДн, служебная, прочая информация
Помещения и оборудование	Несанкционированный доступ	средняя	D	ПДн, служебная, прочая информация

Продолжение таблицы 3

Системы связи	Несанкционированное проникновение к средствам связи	высокая	D	ПДн, служебная, прочая информация, Коммутатор, модем, кабеля передачи данных ЛВС
ПО и ОС	Отказ в обслуживание, НСД	средняя	D, A	ОС, ПО,

2. На основании вышесказанного произвели выбор угроз для каждого информационного актива колледжа, из общего перечня угроз безопасности информации, содержащейся в банке данных угроз безопасности информации ФСТЭК России. Приложение 5.

Все расчёты угроз производились в соответствии с методикой ФСТЭК.

Частота (вероятность)реализации угроз и исходный уровень защищённости систем определялся экспертным путём.

Уровень угрозы вычислялся по формуле: $Y = (Y_1 + Y_2)/20$. Приложение 5 Таблица 14

Уровень угрозы – это коэффициент реализуемости угрозы.

Y- коэффициент реализуемости угрозы

Y_1 – исходный уровень защищённости системы

0 – для высокого уровня исходной защищённости системы

5 – для среднего уровня исходной защищённости системы

10 – для низкого уровня исходной защищённости системы

0 – если не менее 70% характеристик системы соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу «высокий»)

5 – если не выполняются условия по отнесению к высокому уровню

исходной защищённости, но не менее 70% соответствуют уровню не ниже «средний» (берется отношение суммы положительных решений к общему количеству решений)

10 – если не выполняются условия по отнесению к «высокому» и «среднему» уровням исходной защищённости

Y_2 - частота (вероятность) реализации угрозы.

0 – маловероятная угроза

2 – низкая вероятность угрозы

5 – средняя вероятность угрозы

10 – высокая вероятность угрозы

Малая вероятность угрозы (0) – отсутствуют объективные предпосылки для осуществления угрозы

Низкая вероятность угрозы (2) – объективные предпосылки для осуществления угрозы существуют, но принятые меры существенно затрудняют её реализацию

Средняя вероятность угрозы (5) – объективные предпосылки для осуществления угрозы существуют, но принятые меры обеспечения безопасности недостаточны

Высокая вероятность угрозы (10) - объективные предпосылки для осуществления угрозы существуют, но меры обеспечения безопасности не приняты.

По итогам уровень угрозы определяется следующей шкалой:

если $0 \leq Y \leq 0{,}3$, то возможность реализации угрозы признается низкой

если $0{,}3 < Y \leq 0{,}6$, то возможность реализации угрозы признается средней

если $0{,}6 < Y \leq 0{,}8$, то возможность реализации угрозы признается высокой

если $Y > 0{,}8$, то возможность реализации угрозы признается очень высокой

3. Далее производим оценку значения вероятности угроз, исходя из комбинации степени вероятности возникновения угрозы и простоты исполнения уязвимости.

Для этого необходимо первоочерёдно произвести идентификацию уязвимостей.

III.Идентификация уязвимостей

Аудит информационных активов колледжа позволил выявить уязвимости ИБ в следующих областях:

- сотрудники;
- нормативно – методическая база;
- помещение и оборудование;
- системы связи;
- ПС и ОС.

Сотрудники: может привести ко множествам угроз вследствие невнимательности, неквалифицированности, болтливости, желания отомстить (коллеге, руководству), наличия вредных привычек.

Например: Плохое управление паролями.

Нормативно – методическая база: Несовершенства в области разработки нормативно- методических документов, регламентов, актов и т. д.

Помещение и оборудование: Возможности реализации различных угроз, связанных с отсутствием системы контроля доступа к чужим рабочим местам.

Пример: НСД, неисправность оборудования.

Программные средства и операционные системы: Множество уязвимостей, обусловленных неправильным использованием программно-аппаратного обеспечения.

Данный процесс представлен на рис.3.

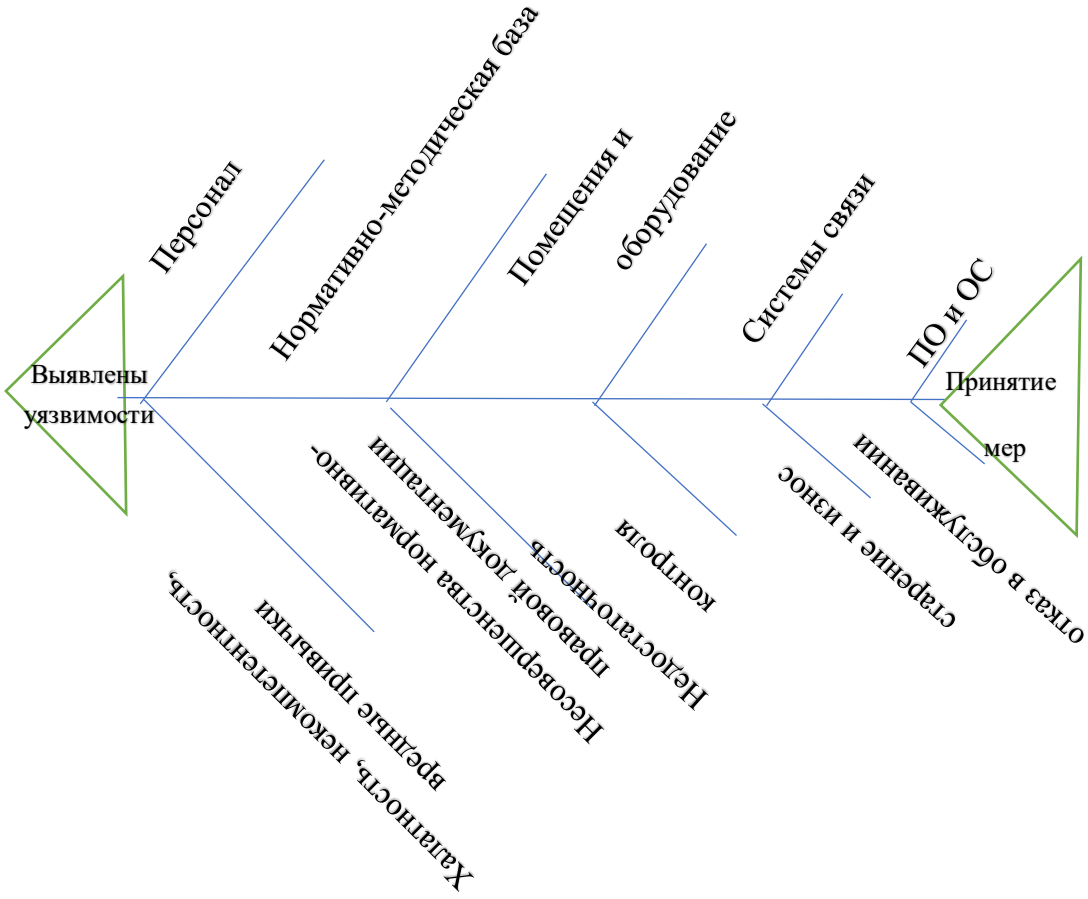


Рис.3. – Идентификация уязвимостей ИБ ГАПОУ СМПК

Уровень уязвимости определяет возможность получения доступа к системе и простоты её использования. Производится экспертным путём по шкале:

Высокий уровень уязвимости – уязвимость позволяет получить полный

контроль над критичной системой (приложением, компонентом IT-инфраструктуры) запускать произвольный код. Средства для

использования уязвимости доступны.

Средний уровень уязвимости - уязвимость позволяет получить полный контроль над критичной системой (приложением, компонентом IT-инфраструктуры) запускать произвольный код. Средства для использования уязвимости пока не доступны.

Низкий уровень уязвимости – уязвимость позволяет получить не критичную информацию. Уязвимость обнаружена в системе, не содержащей критичную информацию

Далее, воспользовавшись Приложением 5 Таблицей 12 «Оценки ценности для степени вероятности и возможных последствий рисков», произвели оценку значения вероятности угроз, исходя из комбинации степени вероятности возникновения угрозы и простоты исполнения уязвимости. Приложение 5. Таблице 11.

После чего по Таблице 13 «Определение меры риска (Ценность актива и значения степени вероятности)» Приложение 5. присвоили балл активу/угрозе

После чего произвели выбор актуальных угроз безопасности ПДн, в соответствии с правилом отнесения угрозы безопасности ПДн к актуальной, приведёнными в таблице 4.

Таблица 4 - Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальна	неактуальна	актуальна
Средняя	неактуальна	актуальна	актуальна
Высокая	актуальна	актуальна	актуальна
Очень высокая	актуальна	актуальна	актуальна

По итогам выполнили оценку рисков информационной безопасности по активам и соответствующим им угрозам. Представленная в Таблице 5.

IV Оценка рисков

Оценка рисков ИБ по активам и соответствующим им угрозам представлена в Таблице 5.

Таблица 5 - Оценка рисков ИБ по активам и соответствующим им угрозам

Актив	Ценность актива	Угрозы	Уровень угрозы	Уровень уязвимости	Значение степени вероятности	Мера риска	Актуальность угрозы	Итоговый бал для актива
«1С Колледж»	2	Угроза неправомерного ознакомления с защищаемой информацией	В	С	3	5	а	82

Продолжение таблицы 5

		Угроза внедрения вредоносного кода через рекламу, сервисы и контент	С	С	2	4	а	
		Угроза внедрения кода или данных	В	Н	2	4	а	
		Угроза использования информации идентификации/аутентификации, заданной по умолчанию	В	Н	2	4	а	
		Угроза несанкционированного удаления защищаемой информации	В	С	3	5	а	
		Угроза несанкционированного копирования защищаемой информации	В	С	3	5	а	
		Угроза использования уязвимых версий программного обеспечения	В	В	4	6	а	
		Угроза заражения компьютера при посещении неблагонадёжных сайтов	С	С	2	4	а	
		Угроза перехвата одноразовых паролей в режиме реального времени	С	Н	1	3	н/а	
		Угроза утраты носителей информации	С	С	2	4	а	
		Угроза перехвата данных, передаваемых по вычислительной сети	В	С	3	5	а	
		Угроза несанкционированной модификации защищаемой информации	В	С	3	5	а	
		Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	С	Н	1	3	н/а	

Продолжение таблицы 5

		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Н	Н	0	2	н/а	
		Угроза изменения компонентов системы	С	С	2	4	а	
		Угроза перехвата вводимой и выводимой на периферийные устройства информации	С	Н	1	3	н/а	
		Угроза форматирования носителей информации	В	С	3	5	а	
		Угроза исследования механизмов работы программы	С	Н	1	3	н/а	
		Угроза восстановления аутентификационной информации	В	Н	2	4	а	
		Угроза преодоления физической защиты	С	С	2	4	а	
ФИС ГИА и Приёма	1	Угроза неправомерного ознакомления с защищаемой информацией	В	С	3	4	а	64
		Угроза несанкционированной модификации защищаемой информации	В	С	3	4	а	
		Угроза внедрения кода или данных	С	С	2	3	а	
		Угроза использования информации идентификации/аутентификации, заданной по умолчанию	С	С	2	3	а	

Продолжение таблицы 5

		Угроза исследования механизмов работы программы	С	Н	1	2	н/а	
		Угроза перехвата одноразовых паролей в режиме реального времени	С	Н	1	2	н/а	
		Угроза использования уязвимых версий программного обеспечения	В	В	4	5	а	
		Угроза заражения компьютера при посещении неблагонадёжных сайтов	С	С	2	3	а	
		Угроза восстановления аутентификационной информации	С	С	2	3	а	
		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Н	Н	0	1	н/а	
		Угроза перехвата вводимой и выводимой на периферийные устройства информации	С	Н	1	2	н/а	
		Угроза перехвата данных, передаваемых по вычислительной сети	В	С	3	4	а	
		Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	С	Н	1	2	н/а	
		Угроза утраты носителей информации	С	С	2	3		
		Угроза форматирования носителей информации	В	С	3	4		
		Угроза внедрения вредоносного кода через рекламу, сервисы и контент	С	С	2	3	а	

Продолжение таблицы 5

		Угроза преодоления физической защиты	В	С	3	4	а	
		Угроза изменения компонентов системы	В	С	3	4	а	
		Угроза несанкционированного копирования защищаемой информации	В	С	3	4	а	
		Угроза несанкционированного удаления защищаемой информации	В	С	3	4	а	
Региональная АИС «Сетевой город Образование»		Угроза несанкционированного удаления защищаемой информации	В	С	3	6	а	103
		Угроза неправомерного ознакомления с защищаемой информацией	В	С	3	6	а	
		Угроза исследования механизмов работы программы	С	Н	1	4	н/а	
		Угроза утраты носителей информации	С	С	2	5	а	
		Угроза заражения компьютера при посещении неблагонадёжных сайтов	С	С	2	5	а	
		Угроза несанкционированной модификации защищаемой информации	В	С	3	6	а	
		Угроза использования уязвимых версий программного обеспечения	В	В	4	7	а	
		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Н	Н	0	3	н/а	

Продолжение таблицы 5

		Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	С	Н	1	4	н/а	
		Угроза перехвата вводимой и выводимой на периферийные устройства информации	С	Н	1	4	н/а	
		Угроза внедрения кода или данных	С	С	2	5	а	
		Угроза форматирования носителей информации	В	С	3	6	а	
		Угроза несанкционированного копирования защищаемой информации	В	С	3	6	а	
		Угроза перехвата одноразовых паролей в режиме реального времени	С	Н	1	4	н/а	
		Угроза использования информации идентификации/ аутентификации, заданной по умолчанию	С	С	2	5	а	
		Угроза перехвата данных, передаваемых по вычислительной сети	В	С	3	6	а	
		Угроза изменения компонентов системы	В	Н	2	5	а	
		Угроза преодоления физической защиты	В	С	3	6	а	
		Угроза восстановления аутентификационной информации	С	С	2	5	а	
		Угроза внедрения вредоносного кода через рекламу, сервисы и контент	С	С	2	5	а	

Продолжение таблицы 5

СЭД «ДЕЛО» Электронный документооборот	4	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	В	Н	2	6	а	123
		Угроза несанкционированного удаления защищаемой информации	В	С	3	7	а	
		Угроза исследования механизмов работы программы	С	Н	1	5	н/а	
		Угроза несанкционированного копирования защищаемой информации	В	С	3	7	а	
		Угроза заражения компьютера при посещении неблагонадёжных сайтов	В	Н	2	6	а	
		Угроза использования уязвимых версий программного обеспечения	В	В	4	8	а	
		Угроза несанкционированной модификации защищаемой информации	В	С	3	7	а	
		Угроза внедрения кода или данных	В	Н	2	6	а	
		Угроза перехвата вводимой и выводимой на периферийные устройства информации	С	Н	1	5	н/а	
		Угроза перехвата данных, передаваемых по вычислительной сети	В	С	3	7	а	
		Угроза перехвата одноразовых паролей в режиме реального времени	С	Н	1	5	н/а	

Продолжение таблицы 5

		Угроза утраты носителей информации	В	Н	2	6	а	
		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Н	Н	0	4	н/а	
		Угроза изменения компонентов системы	В	Н	2	6	а	
		Угроза форматирования носителей информации	В	С	3	7	а	
		Угроза восстановления аутентификационной информации	В	Н	2	6	а	
		Угроза преодоления физической защиты	В	С	3	7	а	
		Угроза использования информации идентификации/аутентификации, задаваемой по умолчанию	В	Н	2	6	а	
		Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	С	Н	1	5	н/а	
		Угроза неправомерного ознакомления с защищаемой информацией	В	С	3	7	а	

Продолжение таблицы 5

Сайт		Угроза неправомерного ознакомления с защищаемой информацией	В	С	3	5	а	
		Угроза несанкционированного удаления защищаемой информации	В	С	3	5	а	
		Угроза использования уязвимых версий программного обеспечения	В	В	4	6	а	
		Угроза несанкционированной модификации защищаемой информации	В	С	3	5	а	
		Угроза перехвата вводимой и выводимой на периферийные устройства информации	С	Н	1	3	н/а	
		Угроза заражения компьютера при посещении неблагонадёжных сайтов	С	С	2	4	а	
		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Н	Н	0	2	н/а	
		Угроза перехвата данных, передаваемых по вычислительной сети	В	С	3	5	а	
		Угроза утраты носителей информации	С	С	2	4	а	
		Угроза несанкционированного копирования защищаемой информации	В	С	3	5	а	
		Угроза использования информации идентификации/аутентификации заданной по умолчанию	С	С	2	4	а	

Продолжение таблицы 5

		Угроза исследования механизмов работы программы	Н	С	1	3	н/а	
		Угроза восстановления аутентификационной информации	С	С	2	4	а	
		Угроза форматирования носителей информации	В	С	3	5	а	
		Угроза хищения средств хранения, обработки и(или) ввода/вывода/передачи информации	С	Н	1	3	н/а	
		Угроза преодоления физической защиты	С	С	2	4	а	
		Угроза изменения компонентов системы	В	Н	2	4	а	
		Угроза внедрения вредоносного кода через рекламу, сервисы и контент	С	С	2	4	а	
		Угроза перехвата одноразовых паролей в режиме реального времени	С	Н	1	3	н/а	
		Угроза внедрения кода или данных	С	С	2	4	а	

На основании проведённых расчётов можем информационные активы расставить в соответствии с приоритетами.

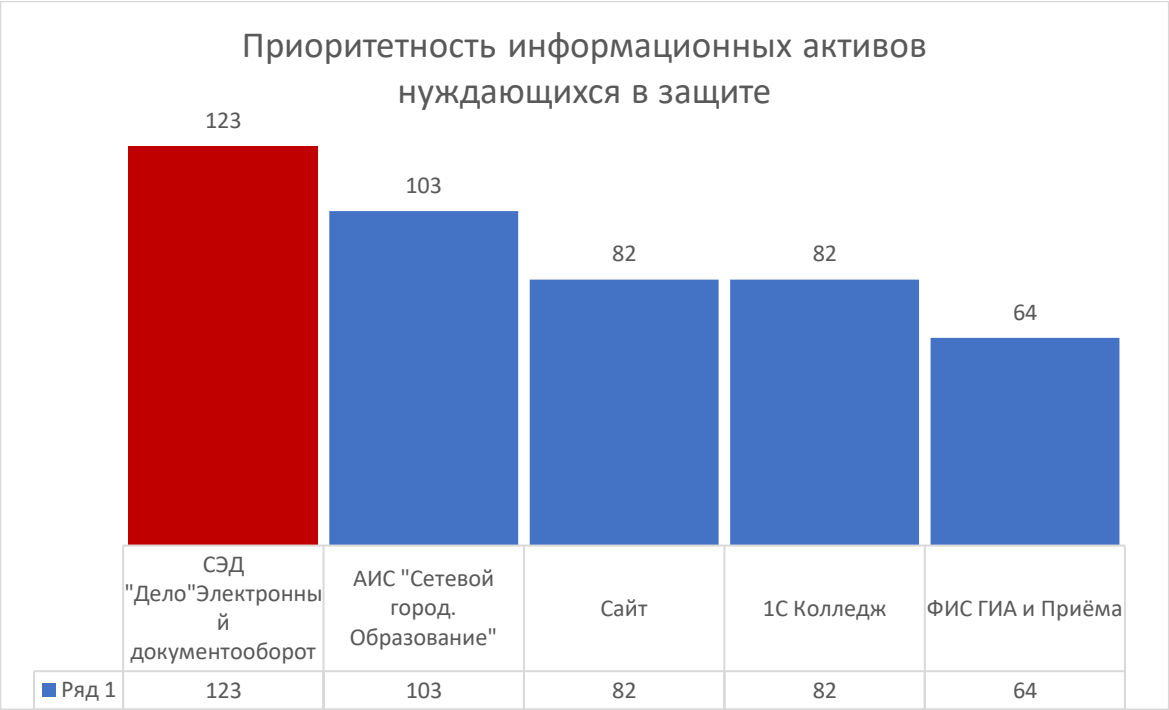


Рис. 4. – Приоритетность информационных активов нуждающихся в защите

V. Оценивание риска

Оценивание риска производится согласно критериям стандарта ГОСТ Р ИСО/МЭК-27005–2010

0–2 – низкий риск

3–5 – средний риск

6–8 – высокий риск

Представлено в Приложении 5; Таблица 16.

Дополнительно произведём оценивание риска относительно выявленных угроз.

Обратимся к шкале критериев оценивания рисков:

Границы критериев риска относительно выявленных угроз:

[0; 2x+ x/2] – низкий риск

[3x- x/2; 5x +x/2] – средний риск

[6x – x/2; 8x] – высокий риск

X – количество выявленных угроз

В нашем случае x= 20

0–50 – риски являются низкими (Н)

50–110 – риски являются средними (С)

110–160– риски являются высокими (В)

Окончательный шаг представляет собой подсчёт всех итоговых баллов активов системы, чтобы получить итоговый балл систем. Эта цифра может использоваться для проведения различай между системами. Для расставления приоритетов защиты систем.

Таблица 6 - Оценивание риска

№п/п	Информационный актив	Оценивание Риска	
		Итоговый балл	Критерии риска
1.	СЭД «ДЕЛО» Электронный документооборот	123	высокий
2.	Региональная АИС «Сетевой город Образование»	103	средний
3.	«1С Колледж»	82	средний
4.	Сайт	82	средний
5.	ФИС ГИА и Приёма	64	средний

Соответствующим одноимённым информационным системам, располагающим данными активами, с высокой степенью риска требуется планирование и корректирующие действия, направленные на снижение риска.

Таковой системой по итогам аудита информационной безопасности ГАПОУ СМПК является СЭД «Дело» Электронный документооборот. Так как система имеет высокий риск, что является неприемлемым и надлежит в первую очередь, принять меры по устранению или уменьшению риска.

Информационным системам со средним уровнем риска также необходимы меры одноимённого характера по устранению или ослаблению риска.

Для систем же с низким уровнем риска следует решить, нужны ли корректирующие действия вообще, или можно принять риск.
Координирующие действия должны в себя включать меры направленные на совершенствование системы информационной безопасности образовательного учреждения.

2.4. Необходимость совершенствования системы информационной безопасности ЕИП (на примере ГАПОУ СМПК колледж)

Система информационной безопасности колледжа призвана обеспечить безопасность ЕИП организации, при этом нейтрализуя уязвимости данного информационного пространства, что в итоге, будет обеспечено посредством развития, преобразования, совершенствования инструментов воздействия на уязвимости. Неизменность же системы ИБ организации, а именно её инструментов воздействия и преобразования, невзирая на не безупречность таковой в колледже, приведёт к последствиям непредсказуемого, а под час нежелательного характера по отношению к информационному пространству образовательной организации в целом, и к информационным активам учреждения, в частности, и таким наиболее ценным, как ПДн, конфиденциальные сведения, служебная, профессиональная, коммерческая тайна.

Поэтому не выполнение обновлений операционной системы MS

Windows и использующегося ПО, способствует возникновению рисков для образовательного учреждения и актуализации угроз: угроз несанкционированного доступа к информации и ПДН и угроз повреждения информации и ПДН из-за ошибок ПО, посредством уязвимостей – сотрудников и технических средств. Это первый шаг на пути к кризису. Поэтому без промедления необходимо сделать следующий шаг, а зацикливание образовательной организации на достаточно привычных для всех нас западных разработках ОС, ПО…, эти риски только усиливает и активизирует, что чревато колоссальными потерями.

Следующий шаг- шаг неотложных действий, позволит выйти из сложившейся ситуации с наименьшими потерями для образовательной организации, переосмыслить алгоритм действия каждого из нас, как непосредственного участника информационных отношений, акцентируя наше внимание на обеспечении целостности, доступности и конфиденциальности информации. Тем более, что для этого имеются все предпосылки, ориентируя нас на импортозамещение. В этом случае стоит обратить свой взгляд на российские разработки в IT-области.

При ориентировке на импортонезависимость и импортозамещение, ставя вопрос о реальной возможности российского IT-рынка нелишним будет подчеркнуть, что на российском IT-рынке достаточно давно существуют крупные производители отечественного ПО, продукты которых зарекомендовали себя и используются как на внутреннем, так и на внешнем рынках. Например, это продукты таких компаний как: 1С, «Яндекс», Dr. Web, «Консультант Плюс», «Гарант», «ИнфоТеКС» и другие. Тем не менее образовательные организации не спешат отказываться от привычных, зарубежных продуктов попросту игнорируя реалии. Конечно, отказаться в одночасье от массовых

продуктов такой компании как Microsoft - ОС Windows или офисный пакет Office сложно, но тем не менее стоит задуматься и принять во внимание.

Альтернативой могут выступить такие ОС: «Астра Линукс», «Альт Образование», РедОС, разработанные на основе свободно распространяемого ПО с открытым исходным кодом.

«Альт Образование» создано на основе операционной системы Linux. Подходит для образовательных учреждений всех уровней, включая в себя всё необходимое для ежедневной работы, серверные компоненты, позволяющие развернуть облачное хранилище документов, систему электронного обучения, проводить тестирование, удалённо управлять компьютерами в защищённой среде.

«Астра Линукс» подходит для использования в уже имеющейся IT-инфраструктуре организации любого масштаба, обеспечивая бесперебойную работу с данными любой степени конфиденциальности.

Ред ОС – Российская операционная система общего назначения для серверов и рабочих станций на базе ядра Linux, являющаяся составным продуктом, построенным на базе решений с открытым исходным кодом и собственных разработок компании РедСОФТ. Ориентирована в первую очередь на пользователя, с упором на удобство в использовании.

На любую российскую ОС можно установить российский офисный пакет «МойОфис» или «Р7-Офис», и использовать облачный вариант офисного пакета, в том числе и для совместного редактирования документов.

Для видео-конференц-связи можно воспользоваться «Сферум», «Яндекс.Телемост», «Videomost» и другими, без проблем работающими на российских ОС.

Специализированное программное обеспечение – это профессиональные программы, например дизайнерское ПО представлено компаниями: «АСКОН», «АССОЛЬ»,»Нанософт», имеющие в своей основе широкий функционал для решения самых разных задач. Эти программы называют «монструозными» - умеющие всё и даже больше.

Сориентироваться в выборе отечественных IT- продуктов, поможет каталог цифрового образовательного контента, рекомендованного Министерством просвещения, а также каталог образовательных программ и инициатив российских компаний, представленный на площадке комитета по информатизации образования Ассоциации разработчиков программных продуктов «Отечественный софт». В котором собрано более 40 предложений, в том числе льготные условия на лицензии, программы сотрудничества, информация по учебно-методическим материалам, программам повышения квалификации и переподготовки.

Так на сегодня быть осведомлённым самому и дать возможность свободно владеть и ориентироваться в перспективных продуктах отечественного IT-рынка студентам, позволит колледжу подготовить высококлассных специалистов, освоивших не один продукт, а несколько, в том числе – российские и свободно распространяемые, что немаловажно, а скорее весомо в реалиях современного мира и востребовано на рынке труда.

Одновременно с этим необходимы действия по формированию компетенций сотрудников, морально-этических качеств и поведенческих норм студентов в отношении информационной этики. Знания же при этом и фокусировка на инструментах совершенствования и стабилизации системы ИБ ЕИП ОО первоочерёдны и не исчерпываются одним решением. Следовательно, для выбора рентабельного пакета решений необходимо провести

мероприятия по анализу ИБ ЕИП колледжа с акцентом на правомерность.

Выводы по 2 главе

Эффективность функционирования образовательной организации в условиях современности не представляется вразрез с информационной безопасностью и это становится приоритетным направлением эффективного функционирования ЕИП образовательного учреждения. При этом информационная безопасность должна отвечать требованиям современности, профессионализма, своевременности, быстрого реагирования, защиты информации, при поддержании её статуса функциональности. Эти требования дополняются и адаптируются, в зависимости от сложности поставленных целей и с учётом действительности.

Так во второй главе магистерской диссертации было проанализировано состояние информационной безопасности в образовательной организации ГАПОУ СМПК(колледж), подчёркнуты достоинства и недостатки, обозначены угрозы и определены векторные направления совершенствования ИБ ЕИП образовательного учреждения. Был поэтапно описан выполненный анализ рисков ИБ ЕИП образовательной организации ГАПОУ СМПК в соответствии со стандартом ГОСТ Р ИСО/МЭК 27005–2010 и методикой ФСТЭК России. Заключающийся в определение информационных активов образовательного учреждения, их оценке, выявление соответствующих им угроз и уязвимостей, с последующей их количественной и качественной оценкой. Оценка угроз производилась по методике ФСТЭК, правилу определения

актуальных угроз. Оценка рисков произведена согласно заданным критериям, позволившая фиксировать приоритетность рисков, с выявлением наиболее важных систем для ИБ ЕИП ОО. В результате был составлен отчёт. Сделан обзор российского IT-рынка. Намечены шаги по совершенствованию ИБ ЕИП образовательной организации.

ГЛАВА 3 РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО СОВЕРШЕНСТВОВАНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ГАПОУ СМПК

3.1. Рекомендации по совершенствованию системы информационной безопасности ЕИП.

Темпы информатизации образования и внедрения новых информационных технологий значительно опережают темпы разработки рекомендательной и нормативно – правовой базы руководящих документов. Следовательно разработка и последующее внедрение их в актуальную политику информационной безопасности образовательного учреждения имеет свою перспективность, являясь тем необходимым шагом на пути к безопасности учреждения.

От понимания организацией значимости данного аспекта зависит её успешное завтра.

Учитывая данный факт, на основании проведённого анализа рисков информационной безопасности ЕИП ГАПОУ СМПК было признано приоритетно нуждающейся системой в корректировки со стороны информационной безопасности информационная система «Сед Дело. Электронный документооборот». В результате несанкционированного доступа, ошибок ПО, в результате не обновлений Ос и ПО, не обновления паролей, вследствие чего возможны – повреждения информации: утрата, утечка, повреждение, разглашение информации. Нуждаемость информационных систем представлена в Приложении 5 Таблице 15. На основании всего выше

сказанного было выполнено соотнесение угроз и необходимых защитных мер, направленных для их нейтрализации, в соответствии с базовыми мерами защиты информации ФСТЭК России. Данные представлены в таблице 7.

Таблица 7 - Соотнесение угроз и необходимых защитных мер направленных для их нейтрализации

ИАФ – Идентификация и аутентификация субъектов доступа и объектов доступа

УПД – Управление доступом субъектов доступа к объектам доступа

ОПС – Ограничение программной среды

ЗНИ – Защита машинных носителей информации

РСБ – Регистрация событий безопасности

АВЗ – Антивирусная защита

АНЗ – Контроль(анализ)защищённости информации

ОЦЛ – Обеспечение целостности информационной системы и информации

ЗТС – Защита технических средств

ЗИС – Защита информационной системы, её средств, систем связи и передачи данных

Тип угрозы	Виды угроз	Содержание мер по обеспечению безопасности
А	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	АВЗ.1 Реализация антивирусной защиты АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
А	Угроза несанкционированного удаления защищаемой информации	ИАФ.1. Идентификация и аутентификация пользователей, являющихся работниками оператора УПД.1. Управление (заведение, активация, блокирование, уничтожение) учётными записями пользователей, в том числе внешних пользователей УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа

Продолжение таблицы 7

		УПД.4Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы УПД.5Назначение минимально необходимых прав и привилегий пользователям , администраторам и лицам, обеспечивающим функционирование информационной системы УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени информационного бездействия(неактивности) пользователя или по его запросу УПД.11 Разрешение (запрет)действий пользователей, разрешённых до идентификации и аутентификации УПД.13 Реализация защищённого удалённого доступа субъектов доступа через внешние информационно-телекоммуникационные сети УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) ЗНИ.2 Управление доступом к машинным носителям информации ЗНИ.8Уничтожение (стирание) на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения АНЗ.5 Контроль правил генерации и смены

Продолжение таблицы 7

		паролей пользователей, заведения и удаления учётных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствами защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
н/а	Угроза исследования механизмов работы программы	Не требует дополнительных мер
А	Угроза несанкционированного копирования защищаемой информации	ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы УПД.10

Продолжение таблицы 7

		Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационнотелекоммуникационные сети УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) ЗНИ.2 Управление доступом к машинным носителям информации ЗНИ.8 Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них РСБ.7
		Защита информации о событиях

Продолжение таблицы 7

		безопасности АН3.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей АН3.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации АН3.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
А	Угроза заражения компьютера при посещении неблагонадёжных сайтов	АВ3.1 Реализация антивирусной защиты АВ3.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

Продолжение таблицы 7

А	Угроза использования уязвимых версий программного обеспечения	ОПС.3 Установка(инсталляция) только разрешённого к использованию ПО и (или) его компонентов АНЗ.1 Выявление , анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации ОЦЛ.3 Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
А	Угроза несанкционированной модификации защищаемой информации	ИАФ.1. Идентификация и аутентификация пользователей, являющихся работниками оператора УПД.1. Управление (заведение, активация, блокирование, уничтожение) учётными записями пользователей, в том числе внешних пользователей УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа УПД.4Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы УПД.5Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы УПД.10 Блокирование сеанса доступа в

Продолжение таблицы 7

		информационную систему после установленного времени информационного бездействия(неактивности) пользователя или по его запросу УПД.11 Разрешение (запрет)действий пользователей, разрешённых до идентификации и аутентификации УПД.13 Реализация защищённого удалённого доступа субъектов доступа через внешние информационно-телекоммуникационные сети УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) ЗНИ.2 Управление доступом к машинным носителям информации ЗНИ.8Уничтожение (стирание) на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

Продолжение таблицы 7

		АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствами защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
А	Угроза внедрения кода или данных	УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные

Продолжение таблицы 7

		системы) ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них РСБ.6 Генерирование временных меток и (или) синхронизация системного времени в информационной системе АВЗ.1 Реализация антивирусной защиты АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ
		(вирусов) АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информацииЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и

Продолжение таблицы 7

		сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
Н/А	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Не требует дополнительных мер
А	Угроза перехвата данных, передаваемых по вычислительной сети	УПД.3Управление информационными потоками между устройствами, сегментами ИС, а также между информационными системами ЗИС.3 Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при её передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
Н/А	Угроза перехвата одноразовых паролей в режиме реального времени	Не требует дополнительных мер
А	Угроза утраты носителей информации	ЗНИ.1 Учет машинных носителей информации
Н/А	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Не требует дополнительных мер
А	Угроза изменения компонентов системы	ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих

Продолжение таблицы 7

		регистрации РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них АНЗ.4 Контроль состава технических средств, программного обеспечения и средств защиты информации ОЦЛ.3 Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
А	Угроза форматирования носителей информации	УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование

Продолжение таблицы 7

		информационной системы УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
A	Угроза восстановления аутентификационной информации	ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации ИАФ.5 Защита обратной связи при вводе аутентификационной информации УПД.6 Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий

Продолжение таблицы 7

		безопасности и реагирование на них АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе
А	Угроза преодоления физической защиты	ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
А	Угроза использования информации идентификации/аутентификации, задаваемой по умолчанию	ИАФ.4. Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации АНЗ.5. Контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе

Продолжение таблицы 7

Н/А	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Не требует дополнительных мер
А	Угроза неправомерного ознакомления с защищаемой информацией	ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационнотелекоммуникационные сети УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) ЗНИ.2 Управление доступом к

Продолжение таблицы 7

		машинным носителям информации ЗНИ.8 Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них РСБ.7 Защита информации о событиях безопасности АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в

Продолжение таблицы 7

		информационной системе ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

На основании вышеизложенного были сформулированы рекомендации.

Рекомендательные меры совершенствования информационной безопасности ЕИП образовательной организации ГАПОУ СМПК

1.Обеспечить полноту нормативно-правовой базы.

- Неукоснительное соблюдение Федерального закона Российской Федерации от 27 июля 2006 года № 149- ФЗ «Об информации,

информационных технологиях и о защите информации», предписывающего:

- Защиту информации от несанкционированного доступа, уничтожения, модификации, блокирования, копирования, фальсификации, распространения, а также от других несанкционированных действий в отношении таковой информации
- Соблюдение конфиденциальности информации ограниченного доступа
- Реализацию права на доступ к информации
- Функционирование организации в соответствии со стандартами по защите информации:

ГОСТ Р ИСО/МЭК 27005–2010 и методика ФСТЭК России

- Исполнение локальных актов образовательной организации, вытекающих из правовых основ регулирования

2.Повысить квалификацию и осведомлённость(ознакомление) сотрудников по вопросам информационной безопасности

3. Обеспечить ответственность за сохранность конфиденциальной информации

4. Реализовать разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы с назначением минимально необходимых прав и привилегий

5. Производить уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)

6. Использовать программное обеспечение, включённое в Реестр российского ПО

7. Обеспечить возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций

8. Организовать контролируемую зону, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования

9. Производить определение событий безопасности, подлежащих регистрации, и сроков их хранения, с определением состава и содержания информации о событиях безопасности, подлежащих регистрации

10. Совершенствовать политику информационной безопасности в соответствии с усложнением целей и задач образовательной организации.

3.2. Оценка эффективности мероприятий по совершенствованию информационной безопасности в образовательной организации ГАПОУ СМПК

Эффективность обеспечения информационной безопасности в образовательной организации будет низкой при отсутствии целенаправленных действий по управлению информационными рисками, направленными на причинение ущерба ЕИП образовательной организации.

Для повышения уровня информационной безопасности ЕИП образовательного учреждения необходимо проведение чётко выверенных мероприятий анализа рисков ИБ организации. Ведь ответственный подход к безопасности в образовательной организации – это необходимость в условиях современной информационной

действительности. А экономическое обоснование мер предоставит дополнительные возможности, позволяющие избежать непредсказуемых ресурсных затрат образовательному учреждению. Оценка экономических затрат мер совершенствования информационной безопасности колледжа представлена в таблице 8.

Таблица 8 - Оценка экономических затрат по внедрению операционной системы «Альт Образование» и полнофункционального набора приложений «Мой Офис»

№п/п	Наименование товаров и услуг	Цена, ₽	Количество	Стоимость, ₽
1.	Обследование информационных систем(аудит документов, анкетирование сотрудников, обследование помещений, сети и компьютеров) с подготовкой соответствующей документации	50000	1	50000
	Консультация			бесплатно
Итого:				50000
2.	Установка «Мой Офис» /лицензия на 3 года/	1140	на все компьютеры	1140
3.	Альт Сервер 10 - на 1 год/бессрочная	3000 / 7500	5	15000 / 37500
	Альт Образование 10 - 1 год/ бессрочная	1200 /3000	60	72000 / 180000
	Сертификат на сопровождение стандартный/ на 1 год/	24000	на все /60	24000

Продолжение таблицы 8

	Организационно-технические мероприятия по проверке соответствия требованиям по безопасности информации с выдачей «***Аттестата соответствия***»/на 3 года/	8000	-	8000
	Альт Образование 10 - 1 год/ бессрочная	1200 /3000	552	662400/1656000
Итого:			60	120140 / 250640
Итого:			552	710540/1726640

Следует отметить, что внедрение операционной системы «Альт Образование» и полнофункционального набора приложений «Мой Офис» затратно для образовательной организации, но штрафные санкции, применяемые при выявлении нарушений в области информационной безопасности несоизмеримо выше и применяются не только по отношению к образовательной организации, но и к руководителю, как юридическому лицу, а также подразделению или должностному лицу, допустившему подобные нарушения.

Так выявление нарушений в области информационной безопасности для образовательной организации, грозят ответственностью, предусмотренной статьями закона об административной, гражданской, уголовной, дисциплинарной ответственности, применяемые для организации, руководителя организации - юридического лица, подразделения или виновного работника. Серьёзность последствий определяется законом. Анализ нормативно-правовых требований согласно законам РФ для юридического лица представлено в Таблице 9.

Таблица 9 - Анализ нормативно-правовых требований согласно законам РФ для юридического лица

Статья	Тип нарушения	Штраф юр.лица тыс.₽
Уголовная ответственность		
Статья 137.1(2) УК РФ	Нарушение неприкосновенности частной жизни Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия, или в публичном выступлении…средствах массовой информации	150 - 350 Либо лишение свободы до 4 лет
Статья 140 УК РФ	Отказ в предоставлении гражданину информации	До 200
Статья 272 УК РФ	Неправомерный доступ к компьютерной информации наказываются штрафом, обязательными работами, исправительными работами, принудительными работами, лишением права занимать определенные должности или заниматься определенной деятельностью, арестом, лишением свободы.	До 200 либо ограниением свободы до 2лет
Административная ответственность		
Статья 5.39 КоАП	Отказ в предоставлении информации	5тыс.₽-10тыс.₽
Статья 13.11.1 КоАП	Обработка данных в случаях, не предусмотренных законодательством	60-100 За повторное 100-300
Статья 13.11.7 КоАП	Невыполнение оператором, являющимся государственным или муниципальным органом, обязанности по обезличиванию ПДн…	30 тыс.₽ -6мл.₽
Статья 13.11.2 КоАП	Обработка ПДн без письменного согласиясубъекта	100-300 За повторное 300-500 до 18мл.₽ Организациям 15- 75
Статья 13.12 КоАП	Нарушение правил защиты информации	20-25
Статья 13.12.2 КоАП	Использование не сертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации(за исключением информации, составляющей гос.тайну)	20-30
Статья13.13.1 КоАП	Незаконная деятельность в области защиты информации	10-20 С конфискацией средств защиты информации

Продолжение таблицы 9

Статья 13.14 КоАП	Разглашение информации с ограниченным доступом	100- 200
Статья 17.13.1 КоАП	Нарушения предусмотренные законодательством РФ о гос. Защите требований по обеспечению конфиденциальности сведений о защищаемых лицах и об их имуществе..	300- 500тыс.р. Или дисквалификация на 3 года
Статья19.4.4 КоАП	Неповиновение законному распоряжению должностного лица органа, осуществляющего надзор (контроль)	5-10 тыс.₽
Статья 19.4.1 КоАП	Воспрепятствование законной деятельности должностного лица органа государственного контроля (надзора), органа муниципального контроля	5-10 тыс.₽
Статья 19.5.1 КоАП	Невыполнение в срок законного предписания (постановления, представления, решения)органа (должностного лица), осуществляющего государственного надзор(контроль)… об устранении нарушений. Законодательства	200 тыс.₽ Или дисквалификация на срок до 3 лет
Статья 19.5.2 КоАП	Невыполнение в срок законного предписания решения органа уполномоченного экспертного контроля, его территориального органа	100-500тыс.р.
Статья 19.7 КоАП	Непредставление сведений (информации) влечет предупреждение, наложение административного штрафа на граждан, должностных лиц, юридических лиц, конфискацию несертифицированных/сертифицированных средств защиты информации, административное приостановление деятельности.	3 тыс.₽ - 5тыс.₽
Дисциплинарная ответственность		
Статья 90 ТК РФ	Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника	
Статья 192 ТК РФ	Дисциплинарные взыскания за совершение дисциплинарного проступка работодатель имеет право применить дисциплинарные взыскания: замечание, выговор, увольнение по соответствующим основаниям.	
Гражданско-правовая ответственность		
Статья 15 ГК РФ	Причинение лицу убытков в результате нарушения правил обработки его персональных данных	
Статья 151 ГКРФ	Компенсация морального вреда	

На основе выше сказанного можно произвести сопоставление предлагаемых затрат на модернизацию системы информационной безопасности и возможных рисках непроведения таких работ. Соответствующие данные представлены в таблице 10

Таблица 10 - Сопоставление предлагаемых затрат на модернизацию системы информационной безопасности и возможных рисках непроведения таких работ

Статья	Штрафные санкции для юр. Лица/за повторные нарушения	Штрафные санкции для должностного лица
Статья 272 УК РФ	До 200тыс.р. либо ограниением свободы до 2лет	200тыс.р.либо ограниением свободы до 2лет
Статья 13.11.7 КоАП	30 тыс.₽ /До 6мл.₽	3-6 тыс.р.
Статья 13.12 КоАП	20тыс.р/25тыс.р	1500-2500р
Статья 13.12.2 КоАП	20тыс.р./ 30тыс.р.	2500-3000р
Статья13.13.1 КоАП	10тыс.р./ 20тыс.р. С конфискацией средств защиты информации	2-3тыс.р.с С конфискацией средств защиты информации/без таковой
Статья 13.14 КоАП	100тыс.р./ 200тыс.р.	40-50 тыс.р., или дисквалификация на 3 г.
Статья 17.13.1 КоАП	300тыс.р/500тыс.р. Или дисквалификация на 3 года	500-1000р
Статья 19.5.1 КоАП	200тыс.₽/500 тыс.₽	50тыс.р.
Статья 19.5.2 КоАП	100тыс.₽/500 тыс.₽	10-50 тыс.р.
Итого:	980 тыс.₽/7975тыс.₽	373тыс.₽

Продолжение таблицы 10

Затраты на модернизацию системы информационной безопасности образовательной организации, (частичная;полная/бессрочная)	552 тыс.₽	710540₽/ 1726640р.

Выводы очевидны: Штрафные санкции уже только юридического лица превышают затраты на модернизацию системы информационной безопасности образовательной организации, с сертификацией на 1 год и приближаются к затратам на модернизацию системы информационной безопасности бессрочного плана. Тем самым подтверждая выгодность модернизации системы информационной безопасности для образовательного учреждения, становясь рентабельно оправданным действием в сложившихся современных условиях.

Тем более, что значительно возросли штрафные санкции и для должностных лиц, и организаций, что немаловажно на сегодняшний момент и определяет дополнительные расходы образовательной организации. Усугубляясь рисками репутационного характера как для организации в целом, так и для её руководителя, и должностных лиц в частности, нанося непоправимый ущерб имиджу таковых. На лицо, серьёзность темы и стимуляция ответственности, в объёме весомого аргумента в пользу совершенствования информационной безопасности единого информационного пространства образовательной организации, посредством внедрения операционной системы и полнофункционального набора приложений отечественного происхождения.

Выводы по 3 главе

В третьей главе было произведено соотнесение выявленных актуальных угроз информационной безопасности ЕИП образовательной организации и необходимых защитных мер, направленных на их нейтрализацию, в соответствии с базовыми мерами защиты информации ФСТЭК России. Предложены рекомендательные меры совершенствования информационной безопасности Единого Информационного Пространства образовательной организации ГАПОУ СМПК. Дана экономическая оценка эффективности мероприятий по совершенствованию информационной безопасности колледжа. В аспекте данной оценки рассмотрена экономическая обоснованность возможности внедрения операционной системы «Альт Образование» в формате импортозамещения, как наиболее удобной в работе и простой в установке операционной системы, ориентированной на повседневное использование при организации и проведении учебного процесса и административной деятельности учреждения среднего профессионального образования. И полнофункционального набора приложений «Мой Офис», предназначенного для решения повседневных задач пользователей.

Также проанализирована законом предусмотренная ответственность за нарушения в области информационной безопасности для юридического лица, организации и должностного лица, относительно: уголовной, административной, гражданской и дисциплинарной ответственности.

ЗАКЛЮЧЕНИЕ

Магистерское диссертационное исследование решает вопрос значимости организации единого информационного пространства образовательной организации в условиях информационной безопасности, ставя три основных задачи.

1.Решая первую задачу, нами был изучен понятийный аппарат и общие принципы информатизации образования. Изучены методы и средства обеспечения информационной безопасности единого информационного пространства образовательной организации. Позволив сделать выводы о:

- неизбежности, управляемости, поэтапности процесса информатизации образования,
- сочетании в себе принципов системности, непрерывности, междисциплинарной интеграции
- нацеливание на создание единого информационного пространства, структурируемого его членами под их собственные потребности
- информационной безопасности, как непременного условия функционирования единого информационного пространства образовательной организации, определяемого многоплановостью процесса защиты, посредством политики информационной безопасности образовательной организации предусматривающей пятиуровневую систему защиты, включающую в себя нормативно-правовые, административно-организационные, технические, морально-этические, физические меры и средства защиты. Основными из них являются: «Национальная стратегия действий в интересах детей», нормативно-правовые, локальные акты, инструкции, меры препятствия пропаганде среди обучающихся, средства физической защиты, специальное программное обеспечение и антивирусники.

2.Решая вторую задачу, нами было:

-проанализировано состояние образовательной организации Стерлитамакский многопрофильный профессиональный колледж с учётом информационной безопасности

-произведено описание единого информационного пространства образовательного учреждения колледж г. Стерлитамак

- выделены этапы организации единого информационного пространства образовательного учреждения

- обозначен вектор развития колледжа

- определены требования информационной безопасности для образовательных организаций

- выявлены уязвимости информационной безопасности организации

- рассмотрены методы, методики и алгоритмы анализа рисков информационной безопасности

- выполнен анализ рисков информационной безопасности колледжа в рамках соответствия ГОСТ Р ИСО/МЭК 27005-2010

-произведено выявление актуальных угроз в соответствии с методикой выявления актуальных угроз ФСТЭК России

- составлен отчёт анализа рисков информационной безопасности ГАПОУ СМПК,

- рассмотрен и описан российский IT-рынок программного обеспечения

Позволив сделать вывод о необходимости совершенствования информационной безопасности единого информационного пространства образовательной организации Стерлитамакский многопрофильный профессиональный колледж.

3.Решая третью задачу, нами были:

- соотнесены актуальные угрозы и защитные меры необходимые для их нейтрализации

- произведена оценка экономических затрат мер совершенствования

информационной безопасности колледжа.

- проанализированы нормативно-правовые требования предусмотренные законодательством РФ, определяющие ответственность за

нарушения в области информационной безопасности как для организации, так и руководителя организации и должностного лица или подразделения, допустивших данный вид нарушений

- сформулированы предложения по совершенствованию системы информационной безопасности колледжа и организации единого информационного пространства Стерлитамакский многопрофильный профессиональный колледж

Позволившие сделать вывод о том, что разработка и последующее внедрение рекомендаций в актуальную политику информационной безопасности образовательного учреждения имеет свою перспективность, являясь необходимым шагом на пути к безопасности учреждения.

Результаты исследования рекомендуется использовать в практической деятельности образовательных организаций СПО с целью совершенствования информационной безопасности организаций СПО.

Таким образом, цель магистерской работы достигнута, задачи выполнены в полном объёме, гипотеза подтверждена.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Аверченков В.И. Организационная защита информации: учеб. пособие / В.И. Аверченков, М.Ю. Рытов// Брянск: БГТУ, 2014. С.184.

2. Агапов А.Б. Основы Федерального Информационного Права России/ А.Б.Агапов//Экономика,2000, С.8-12

3. Ажмухамедов, И.М., Ханжина, Т.Б. Оценка экономической эффективности мер по обеспечению информационной безопасности / И.М. Ажмухамедов, Т.Б. Ханжина // Вестник АГТУ. Серия: «Экономика», 2011. №1. С.185-190.

4. Ажмухамедов И.М., Ханжина Т.Б. Определение оптимального комплекса мер по обеспечению информационной безопасности / И.М. Ажмухамедов, Т.Б. Ханжина // Мат. методы в технике и технологиях – ММТТ-24: сб. трудов XXII Междунар. науч. конф.: в 10 т. Т.9. Секция 13 / под общ. ред. В.С Балакирева. Саратов: Изд-во Саратовского гос. технического университета, 2011. 187с., С.73-75.

5. Андреева Н.В. Функциональная модель системы управления информационной безопасностью как средство внедрения стандартов линейки ISO/IEC 2700x (BS 7799)/ Н.В.Андреева // Научно-технический вестник информационных технологий, механики и оптики, 2007. № 39. С. 40–44.

6. Апатова Н.В., Королёв В.А., Пенькова И.В Цифровая экономика: информационные технологии и модели [Текст]:[монография] / Н.В. Апатова, В.А.Королёв, И.В.Пенькова// «Цифровая экономика» Вестник ФГАОУ КФУ имени В.И. Вернадского. Серия: «Цифровая экономика», 2018. С.305.

7. Асмолов А.Г. Российская школа и новые информационные технологии:

взгляд в следующее десятилетие / А.Г. Асмолов, А.Л. Семенов, А.Ю. Уваров / Изд-во «НексПринт», 2010. С.84.

8. А. Бабаш, Е. Баранова, Д. Ларин «Информационная безопасность. История защиты информации в России», СПб.: Питер, 2015

9. Банк данных угроз безопасности информации / ФСТЭК России // Threat List/ Список угроз, 2017. URL: http://bdu.fstec.ru/threat. Дата обращения: 04.12.21.

10. Банк данных угроз безопасности информации // Федеральная служба по техническому и экспортному контролю. URL: https://bdu.fstec. Ru. Дата обращения: 01.02.2022.

11. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности / Е.К. Баранова // Образовательные ресурсы и технологии, 2015. № 1 (9). С. 73-79. 74

12. Баранова Е.К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности / Е.К. Баранова // Управление риском, 2009. № 1(49). С. 15–26.

13. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации / Е.К. Баранова, А.В. Бабаш. – М.: ИНФРА-М_РИОР, 2014.

14.Бармен С. Разработка правил информационной безопасности. - М.: Издательский дом "Вильямс", 2002.

15. Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право.- Спб.: Изд-во «Юридический центр Пресс», 2001.

16.Биячуев Т.А. Безопасность корпоративных сетей. Учебное пособие / под ред. Л.Г.Осовецкого - СПб.: СПбГУ ИТМО, 2004.

17.Блэк У. Интернет: протоколы безопасности. Учебный курс. - СПб.: Питер, 2001.

18.Бождай А.С., Финогеев А.Г. Сетевые технологии. Часть 1: Учебное пособие. Пенза: Изд-во ПГУ, 2005.

19. Бойцев О. Многофакторный анализ рисков информационной безопасности. Подходы и методы / О. Бойцев. - URL: http://www.nestor.minsk.by/kg/2008/44/kg84403.html. Дата обращения: 01.02.2022.

20.Борисов, М. А. Основы организационно-правовой защиты информации / М. А. Борисов, О. А. Романов// Основы защиты информации. 2015. С. 248.

21. Велигура А. О выборе методики оценки рисков информационной безопасности / А. Велигура. – URL: http://itsec.ru/articles2/pravo/o_vybore_metodiki_ocenki_riskov_informac_bezop/. Дата обращения: 20.01.2022.

22. Виды и источники угроз информационной безопасности. – URL: http://infoprotect.net/note/vidyi_i_istochniki_ugroz_informacionnoy_bezopasnosti/ Дата обращения: 15.11.2021.

23. Вихорев С.В. Классификация угроз информационной безопасности / С.В. Вихров. - URL: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml/. Дата обращения: 22.11.2021. 16. Глушенко С.А. Применение системы Matlab для оценки рисков информационной безопасности организации // Бизнес-информатика. 2013. № 4 (26). С. 35–42.

24. Гершунский Б.С. Компьютеризация в сфере образования: Проблемы и перспективы[Текст] / Б.С.Гершунский // Педагогика, 1987. С.264.

25. Глушков В.М., Добров Г.М., Терещенко В.И. Беседы об управлении [Текст] / В.М.Глушков, Г.М.Добров, В.И.Терещенко // «Проблемы науки и технического прогресса»,1974. С.224.

26.ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. С. 9.

27.ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. – Введ. 2006-12-27. – М.: Изд-

во стандартов, 2006. С.7.
28.ГОСТ Р ИСО/МЭК 15408-2002. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий (КОБИТ). Части 1, 3-5.
29. ГОСТ 12.0.003-2015. Система стандартов безопасности труда. Опасные и вредные производственные факторы. Классификация. – Введ. 2015- 12-10. – М.: Межгосударственный совет по стандартизации, метрологии и сертификации, 2015. С 16.

30. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента 75 информационной безопасности требования. – Введ. 2008-02-01 – М.: ФСТЭК России, 2006.

31. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Взамен ГОСТ Р ИСО/МЭК ТО 13335-3-2007 и ГОСТ Р ИСО/ МЭК ТО 13335-4-2007; Введ. с 30.11.2010. Москва: Изд-во Стандартинформ, 2011.

32. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска; Введ. с 01.12.2012. Москва: Изд-во Стандартинформ; 2012.

33. Губарева О.Ю. Оценка рисков информационной безопасности в телекоммуникационных сетях. // Вестник Волжского университета им. В.Н. Татищева. 2013. № 2 (21). С. 76–81.

34.Доктрина информационной безопасности Российской Федерации, № Пр-1895 от 9 сентября 2000 г.
35.Домарев, В.В. Безопасность информационных технологий. Системный подход [Текст] / В.В. Домарев. – Киев: «ТИД», 2012. С. 912.
36.Ершов А.П. Информатизация: от компьютерной грамотности учащихся к информационной культуре общества. // Коммунист, 1988. №2. С.82-92.

37.Завгородний, В.И. Комплексная защита информации в компьютерных системах [Текст] / В.И. Завгородний // М.: «Логос», 2001.

38. Зегжда, Д.П. Основы безопасности информационных систем[Текст]: учеб. пособие для вузов / Д. П. Зегжда, А. М. Ивашко // М.: Горячая линия Телеком, 2000. С 452.

39. Иванов В. А., Соловьев В. М. О концепции формирования единого информационного пространства университетского комплекса. Инновационные методы и технологии в условиях новой образовательной парадигмы: Сб. науч. Тр. — Саратов: Изд-во Сарат. ун-та, 2008. С. 52–56.

40. Ильченко Л.М. Анализ системы менеджмента информационной

безопасности на базе стандарта ISO 27001:2013. // Материалы 5 научнопрактической конференции студентов, аспирантов и курсантов «IT вчера, сегодня, завтра». 2017. С. 51–61.

41. Ильченко Л.М. Расчет рисков информационной безопасности телекоммуникационного предприятия / Л.М. Ильченко, Е.К. Брагина, И.Э. Егоров, С.И. Зайцев // Открытое образование, 2018. №22. № 2.

42. Информационная безопасность образовательных учреждений. – URL: https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnayabezopasnost-obrazovatelnykh-uchrezhdenij/. Дата обращения: 01.12.2021.

43. Колин К.К. Вызовы XXI-го века и проблемы образования/ К.К.Колин // М., 2000. С 53.

44. Колин К.К. Человек и будущее: динамический вызов// Вестник высшей школы. - М., 1999. - № 10. - С.11-14

45. Колин К.К. Информатизация образования: новые приоритеты// Педагогика. - 2001. - № 6. - С.110-136

46. Колин К.К. Информатизация образования как фундаментальная проблема// Дистанционное образование. - 1998. - № 4. - С.22-28

47. Концепция обеспечения информационной безопасности предприятия [Электронный ресурс]. - Режим доступа: www.securitypolicy.ru. Дата обращения:12.07.2022.

48. Козлов О.А., Гузикова Л.А.2017г.Том 6 №22 Вопросы методики преподавания в вузе/О.А.Козлов,Л.А.Гузикова// 2017г.Том 6 №22

49. Королев В.Ю., Бенинг В.Е., Шоргин С.Я. Математические основы теории риска: учеб. пособие / В.Ю. Королев, В.Е. Бенинг, С.Я. Шоргин. - М.: ФИЗМАТЛИТ, 2011. С. 620.

50. Коротнев К. Методики управления рисками информационной безопасности и их оценки (часть 2) / К. Коротнев. – URL: https://safesurf.ru/specialists/article/5194/587935/. Дата обращения: 01.02.2022.

51. Красникова Т.В., Невежин В.П. Моделирование оценки при аудите безопасности информационных систем / Т.В. Красникова, В.П. Невежин // VII Международная студенческая электронная научная конференция «Студенческий научный форум 2015».

52. Кудрявцева Р.Т. Управление информационными рисками с использованием технологий когнитивного моделирования: автореф. дис. … канд. техн. наук./ Р.Т.Кудрявцева// Уфа, 2008. С. 17.

53. Куканова Н. Современные методы и средства анализа и управление рисками информационных систем компаний / Н. Куканова // www.dsec.ru, Digital Security. Дата обращения: 20.01.2022.

54. Левченко В.Н. Этапы анализа рисков / В.Н. Левченко. - URL: http://masters.donntu.org/2016/fknt/levchenko/library/article6.htm. Дата обращения: 12.01.2022.

55. Лютова И.И. Моделирование уровня приемлемого риска информационной безопасности // Вестник Адыгейского государственного университета. Серия 5: Экономика. 2014. №2 (141). URL: https://cyberleninka.ru/article/n/modelirovanie-urovnya-priemlemogo-riskainformatsionnoy-bezopasnosti. Дата обращения: 02.02.2019.
56. Малюк, А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. – М.: Горячая линияТелеком, 2012. С.148.
57. Медведовский И. Современные методы и средства анализа и контроля рисков информационных систем компаний / И. Медведовский //, www.dsec.ru, Digital Security. Дата обращения: 20.01.2019. 77
58. Международный стандарт ISO/IEC 27005:2008. Информационная технология – Методы защиты – Менеджмент рисков информационной безопасности BS ISO/IEC 27005:2008.
59. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков. – М.: Издательский центр «Академия», 2013. С.336.
60. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008.
61. Методики и программные продукты для оценки рисков. - URL: https://www.intuit.ru/studies/courses/531/387/lecture/8996?page=2/. Дата обращения: 01.02.2022.
62. Методы организации защиты информации: учебное пособие для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55 / Ю.Ю. Громов и др. – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2013. С. 80.
63. Методические рекомендации по обеспечению с помощью крипто средств безопасности персональных данных при их обработке информационных системах персональных данных с использованием средств автоматизации

[Электронный ресурс]: [Утверждены руководством 8 центра ФСБ России 21.02.2008 г. №149/54-144]. Режим доступа: www.consultant.ru. Дата обращения: 15.06.2021.

64. Милютина О.В. Особенности защиты информации в образовательном учреждении / О.В. Милютина // URL: http://www.fcoit.ru/internet_conference/information_security_training_process/features_information_security_in_an_educational_institution.php. Дата обращения: 15.12.2021.
65. О безопасности [Электронный ресурс]: [федеральный закон: от 05.03.1992 г. № 2446-I, в ред. от 25.12.1992 г. № 4235-I, от 24.12.1993 г. №2288, от 25.07.2002 г. № 116-ФЗ, от 07.03.2005 г. № 15-ФЗ]. - Режим доступа: www.consultant.ru. Дата обращения: 28.11.2021.
66. О мерах по реализации государственной политики в области образования и науки [Электронный ресурс]: [Указ Президента РФ от 07.05.2012г.№599]. - Режим доступа: www.consultant.ru. Дата обращения: 28.11.2021.
67. О персональных данных [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. № 152-ФЗ, в ред. от 04.06.2014 г. № 152-ФЗ]. - Режим доступа: www.consultant.ru. Дата обращения: 28.11.2018.
68. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. 78 №149-ФЗ, в ред. от 06.04.2011 г. № 149-ФЗ]. - Режим доступа: www.consultant.ru. Дата обращения: 28.11.2018.
69. Обеспечение информационной безопасности организации. URL: http://www.iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/. Дата обращения: 01.12.2018.
70. Организационное обеспечение информационной безопасности [Электронный ресурс]. Режим доступа: www.starik2222.narod.ru. Дата обращения: 22.11.2018.
71. Официальный сайт ГАПОУ СМПК / www.mirsmpc.ru //Дата обращения: 22.12.2018.

72. Оценка информационной безопасности в деятельности организаций. Способы оценки информационной безопасности. URL: http://www.pvsm.ru/informatsionnaya-bezopasnost/19741. Дата обращения: 05.12.2018.
73. Пащенко И.Н., Васильев В.И. Разработка требований к системе защиты информации в интеллектуальной сети Smart Grid на основе стандартов ISO/IEC 27001 и 27005 / И.Н. Пащенко, В.И.Васильев // Известия ЮФУ. Технические науки. 2013. № 12 (149). С. 117–126.
74. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В.// М.: Компания АйТи; ДМК Пресс, 2014.
75. Плетнев П.В., Белов В.М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса / П.В. Плетнев, В.М. Белов. URL: http://old.tusur.ru/filearchive/reports-magazine/2012-25-2/083.pdf. Дата обращения: 25.01.2019.
76. Полат Е.С., Бухаркина М.Ю., Моисеева М.В., Петров А.Е. Новые педагогические и информационные технологии в системе образования: Учеб. пособ. для студ. пед. вузов и системы повыш. квалиф. пед. кадров / Е. С. Полат, М. Ю. Бухаркина, М. В. Моисеева, А. Е. Петров // М.: Издательский центр «Академия», 2010.
77. Потапова, Н.М.Солдатова, И.А.Юдина , Современные тенденции в политике информатизации образования: Учеб. пособие / В.Ю.Потапова, Н.М.Солдатова, И.А.Юдина. // Владивосток: Изд-во ПИППКРО, 2008
78. Пугин В.В., Губарева О.Ю. Обзор методик анализа рисков информационной безопасности информационной системы предприятия / В.В. Пугин, О.Ю. Губарева. URL: https://rus.neicon.ru/xmlui/bitstream/handle/123456789/12956/9_st13.pdf?sequence=1. Дата обращения: 12.12.2018. 79
79. Ребко Э. М. Информационная образовательная среда учебного заведения как средство формирования информационной культуры студентов [Текст] /

Э. М. Ребко, А. П. Федорова // Молодой ученый. 2014. №1. С. 566-568.

80. Российская педагогическая энциклопедия: В 2 т. Т.1 (А-Л)/ Под ред. В.Г. Панова. // М., 1993
81. Симонович С., Евсеев Г. Эффективная работа: познай свойкомпьютера / С. Симонович, Г. Евсеев // СПб.: Питер, 2005.
82. Свободная энциклопедия Википедия [Электронный ресурс]. 2010. Режим доступа: http://ru.wikipedia.org. Дата доступа: 27.12.21.
83. Садердинов А.А. Информационная безопасность предприятия: учеб. пособие / А.А. Садердинов, В.А. Трайнев, А.А. Федулов. // М.: Дашков и К, 2013. С.336.
84. Сайт национального открытого университета ИНТУИТ [Электронный ресурс].- Режим доступа: https:www….Дата обращения 16.04.2022)
85. Симонов С. Технологии и инструментарий для управления рисками / С. Симонов // JetInfo, 2013. №2.
86. Система обеспечения информационной безопасности. URL: http://www.ec-leasing.ru/products/sistemy-obespechiniya-informacionnoibezopasnosti/. Дата обращения: 01.12.2018.
87. Средство оценки безопасности Microsoft Security Assessment Tool (MSAT). URL: http://technet.microsoft.com/ru-ru/security/cc185712.aspx. Дата обращения: 12.01.2019.
88. Стандарты информационной безопасности. URL: https://tvoi.biz/biznes/informatsionnaya-bezopasnost/prakticheskaya-polzastandartov-info.html. Дата обращения: 20.11.2018.
89. Статьев В.Ю.,Тиньков В.А. Информационная безопасность распределённых информационных систем// В. Ю. Статьев, В.А. Тиньков// Информационное общество,1997.№1. С.68-71.
90. Степанов Е.А. Информационная безопасность и защита информации: учеб. пособие / Е.А. Степанов, И.К. Корнеев // М.: ИНФРА – М, 2013. С. 304.
91. Тейлор Р. Способ задавать вопросы / Р. Тейлор // Amerikan Documentation – 1962.

92. Фролова Г.В.Образование и XXI-й век/ Г.В.Фролова // М.: Наука, 1999
93. Шарафутдинова А.Р., Пядышев В.С. Защита информации в образовательных учреждениях / А.Р. Шарафутдинова, В.С. Пядышева. URL: http://www.rusnauka.com/17_APSN_2013/Matemathics/2_140911.doc.htm. Дата обращения: 25.12.2018.
94. Ядов Г.Б. Информация и общество/ Г. Б. Ядов // Вокруг света, 2004г.
95. Ярочкин В. И. Информационная безопасность / В.И. Ярочкин // М. Академический проект, 2012. С.640.
96. Ярочкин В. И. Словарь терминов и определений по безопасности и защите информации / В.И. Ярочкин, Т.А. Ильещова // М.: «Ось-99», 2011. С. 48.

ПРИЛОЖЕНИЯ

Приложение 1

Логическая важность организации ЕИП образовательной организации в условиях информационной безопасности

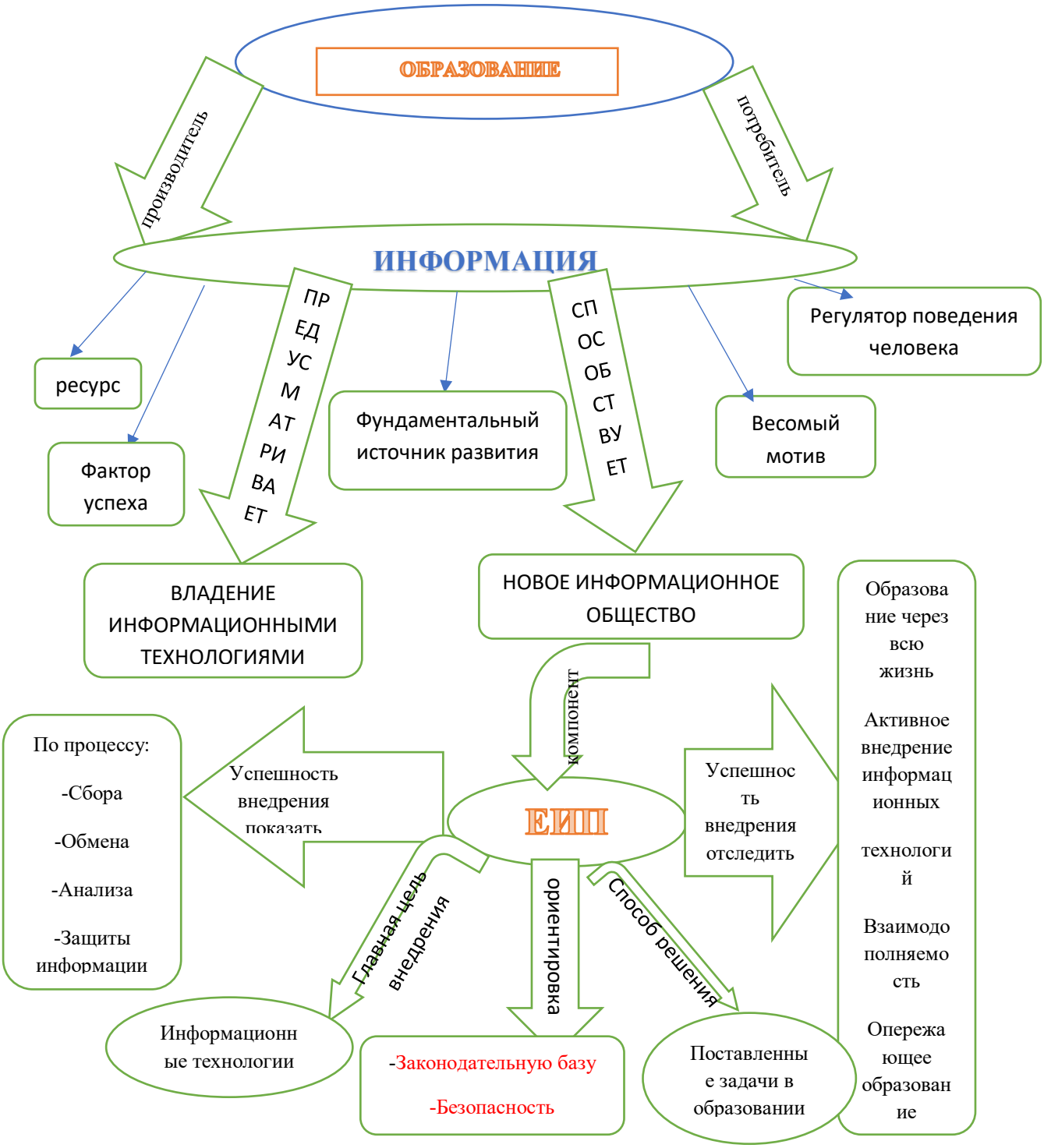
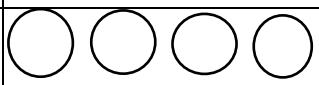
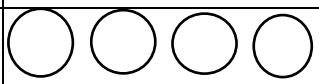
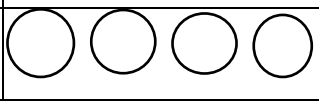


Рисунок 5. - Логическая важность организации ЕИП образовательной организации в условиях информационной безопасности

Приложение 2

Пример Анкеты для экспертов (руководящих специалистов отделов) ОО ГАПОУ СМПК «Оценка ценности активов».

№п/п	Наименование актива	Оценка ценности актива
1.	«1С Колледж»	
2.	ФИС ГИА и Приёма	
3.	Региональная АИС «Сетевой город Образование»	
4.	СЭД «ДЕЛО» Электронный документооборот	
5.	Сайт	

Приложение 3

Пример Анкеты для экспертов (руководящих специалистов отделов) ОО ГАПОУ СМПК (Источником риска является многофункциональная система СЭД «Дело» электронный документооборот.

Анкетирование проводится с целью определения влияния информационных рисков на деятельность образовательного учреждения. Анкета состоит из вопросов, ответы на которые, предполагается получить в ходе анкетирования специалистов.

Пример Анкеты

Вопрос	Вероятность	Сила влияния
Разработана ли в организации политика информационной безопасности, положения которой внедрены в существующую информационную систему	◯◯◯◯	◯◯◯◯
Принято ли в организации проводить регулярные совещания руководителей организации по вопросам информационной безопасности	◯◯◯◯	◯◯◯◯
Приняты ли в организации четкие обязанности и ответственность по защите	◯◯◯◯	◯◯◯◯

Продолжение «Пример Анкеты»

отдельных ресурсов к		
выполнению конкретных действий по обеспечению информационной безопасности		
Определены ли все основные информационные ресурсы и сервисы	◯◯◯◯	◯◯◯◯
Идентифицированы ли все основные информационные ресурсы и сервисы	◯◯◯◯	◯◯◯◯
Включена ли задача обеспечения информационной безопасности в служебные обязанности всех сотрудников на стадии приёма на работу	◯◯◯◯	◯◯◯◯
Проводятся ли периодические проверки того, что каждый сотрудник выполняет свои служебные обязанности	◯◯◯◯	◯◯◯◯
Какие правила физической безопасности соблюдаются для критичных информационных ресурсов	◯◯◯◯	◯◯◯◯

Продолжение «Пример Анкеты»

Осуществляется ли распределение обязанностей как средство снижения риска от случайных и преднамеренных угроз	◯◯◯◯	◯◯◯◯
Отражаются ли в политики контроля доступа правила и права каждой группы пользователей	◯◯◯◯	◯◯◯◯
Определена ли ответственность для всего персонала, вовлечённого в процесс обработки и ввода исходных данных	◯◯◯◯	◯◯◯◯
Соответствует ли законодательству порядок обращения с информацией о персональных данных сотрудников и студентов, родителей(законных представителей)	◯◯◯◯	◯◯◯◯
Угроза внедрения вредоносного кода через рекламу, сервисы и контент	◯◯◯◯	◯◯◯◯

Продолжение «Пример Анкеты»

Угроза несанкционированного удаления защищаемой информации	◯◯◯◯	◯◯◯◯
Угроза исследования механизмов работы программы	◯◯◯◯	◯◯◯◯
Угроза несанкционированного копирования защищаемой информации	◯◯◯◯	◯◯◯◯
Угроза заражения компьютера при посещении неблагонадёжных сайтов	◯◯◯◯	◯◯◯◯
Угроза использования уязвимых версий программного обеспечения	◯◯◯◯	◯◯◯◯
Угроза несанкционированной модификации защищаемой информации	◯◯◯◯	◯◯◯◯
Угроза внедрения кода или данных	◯◯◯◯	◯◯◯◯
Угроза перехвата вводимой и выводимой на периферийные устройства информации	◯◯◯◯	◯◯◯◯

Продолжение «Пример Анкеты»

Угроза перехвата данных, передаваемых по вычислительной сети	◯◯◯◯	◯◯◯◯
Угроза перехвата одноразовых паролей в режиме реального времени	◯◯◯◯	◯◯◯◯
Угроза утраты носителей информации	◯◯◯◯	◯◯◯◯
Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	◯◯◯◯	◯◯◯◯
Угроза изменения компонентов системы	◯◯◯◯	◯◯◯◯
Угроза форматирования носителей информации	◯◯◯◯	◯◯◯◯
Угроза восстановления аутентификационной информации	◯◯◯◯	◯◯◯◯
Угроза преодоления физической защиты	◯◯◯◯	◯◯◯◯

Продолжение «Пример Анкеты»

Угроза использования информации идентификации/аутентификации, задаваемой по умолчанию	◯◯◯◯	◯◯◯◯
Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	◯◯◯◯	◯◯◯◯
Угроза неправомерного ознакомления с защищаемой информацией	◯◯◯◯	◯◯◯◯

Приложение 4

Отчёт по аудиторскому обследованию ИТ-безопасности Государственного автономного образовательного учреждения Стерлитамакский многопрофильный профессиональный колледж (ГАПОУ СМПК г. Стерлитамак)

Оглавление

1. Физический контроль доступа в помещения, наблюдение за помещениями

Объект изучения	Текущее состояние	Оптимальная структура	Нарушения, замечания и угрозы	Меры по исправлению ситуации
Контроль физического доступа в помещения в рабочее и нерабочее время	Имеется СКУД- отдельная интеллектуальная система управления доступом	СКУД- отдельная интеллектуальная система управления доступом, базированная на собственном сервере, к которой по сети IP подключены контроллеры доступа каждого отдельного помещения: -Серверная -Кабинеты руководителей - Кабинеты изолированных отделов	- Все внутренние отдельные помещения физически защищены	-Система СКУД настроена согласно техническому заданию, с учётом разрешённых уровней доступа групп сотрудников и студентов, и времени суток -Фиксация группы доступа в регламенте ИТ-безопасности есть Дополнительные меры не требуются
Визуальный контроль перемещения сотрудников и студентов в помещении	- Камеры есть -запись событий камер есть - настроены ярлычки на прямой web-доступ к камерам	Выделенный сервер со специальным серверным ПО видеонаблюдения, имеющий функционал: - Наблюдение в режиме онлайн - Хранения и	Есть постоянный защищённый видеосервер	видеонаблюдение ведётся - есть необходимость в дополнительных камерах

Продолжение «Физический контроль доступа в помещения, наблюдение за помещениями»

		ротации записей с периодом месяц, частотой – ежедневно - Отправки оповещений при нарушении периметра либо другом заданном событии		
Система отчётности и оповещений о доступе и перемещении	- Есть видеоархив с буфером хранения - Есть система ручного биометрического учёта о посещении -Охранная компания ООО ЧОП «Дружина»	1.Должна присутствовать удобная система статистики сервера СКУД с отчётностью -Сотрудник -Время и дата - Действие (вошёл/вышел) - Помещение 2.Должна присутствовать удобная панель просмотра и работы с видеоархивом 3. Должна присутствовать система автоматического учёта рабочего времени на основе данных СКУД	Нет системы автоматического оповещения о нарушении физического периметра защиты	Внедрение системы оповещения контроля доступа согласно ТЗ

Продолжение «Физический контроль доступа в помещения, наблюдение за помещениями»

		4.Должна		
		присутствовать функция оповещения ответственного лица о нарушении периметра на основании данных СКУД и видеонаблюдения		

2.Аппаратное обеспечение информационной системы

Объект изучения	Текущее состояние	Оптимальная структура	Нарушения, замечания и угрозы	Меры по исправлению ситуации
Защищённость помещения и наличие специальных защитных монтажных изделий, в которых физически расположена серверная и коммутационная структура	- На объекте есть выделенное помещение для работы серверной и центральной коммутационной структуры - Помещение защищено	На объекте должно быть выделенное помещение с чётко ограниченном доступом сотрудникам согласно регламенту безопасности Или - На объекте должен быть защищённый серверный шкаф,	Нарушения не выявлены	Дополнительные меры не требуются

Продолжение «Аппаратное обеспечение информационной системы»

		ключи должны находиться у ответственного лица -Должны быть запрещены прямые консольные выводы (типа розеток питания, клавиатур, мониторов…) за пределы серверного шкафа либо полки - Серверная комната не должна использоваться в качестве склада и других вспомогательных ролей		
Наличие инвентаризационной системы учёта и привязки рабочих станций к конкретным пользователям системы	-Маркировка рабочих станций есть - Автоматическая система учёта оборудования есть -Карточки учёта ПК есть - имена рабочих станций есть (в соответствии с требованиями)	- Электронный либо бумажный каталог рабочих станций, серверов, телефонного и периферийного оборудования объекта с уникальными идентификаторами каждой единицы - Маркировка оборудования и поддержка её в актуальном состоянии	Нарушения не выявлены	Внедрение специальных программ инвентаризации компьютерной сети, построение интерактивной карты сети и мониторинга её состояния

3.Сетевое обеспечение информационной системы

Объект изучения	Текущее состояние	Оптимальная структура	Нарушения, замечания и угрозы	Меры по исправлению ситуации
Наличие общедоступных участков кабельной системы с возможностью неконтролируемого подключения спец устройств	- Сеть сделана по проекту специализированной компании - Проектная документация присутствует - Структурированная документация и схема сети - В сети присутствует защита ….	- Структура должна соответствовать стандартам построения кабельных сетей - Структура должна иметь разделённую физически пользовательскую область и демилитаризованные зоны с контролем обмена трафика между ними	Нарушения не выявлены	Дополнительные меры не требуются
Возможность подключения посторонних лиц по сети Wi-fi	- Шифрование WPA2 - Пароль сложный - криптостойкость пароля присутствует - В беспроводной сети присутствует	Сеть Wi-fi в центральном офисе должна быть отнесена в демилитаризованную зону с контролем и разделением обмена трафиком	Нарушения не выявлены	Дополнительные меры не требуются
	защита Беспроводная сеть вынесена в отдельный Vlan			

4.Системное программное обеспечение

Объект изучения	Текущее состояние	Нарушения, замечания и угрозы	Меры по исправлению ситуации
«1 С: Колледж» на технологической платформе «1 С: Предприятие 8.2 »	Продукт охватывает все уровни управленческой деятельности основных подразделений колледжа. Функционирует в соответствии с лицензионным соглашением	не выявлены	Дополнительные меры не требуются
ФИС ГИА и Приёма	Федеральная Информационная Система государственной итоговой аттестации В соответствии с Постановлением Правительства РФ №755 от 31.08.2013г.	не выявлены	Дополнительные меры не требуются
Региональная АИС «Сетевой город Образование»	Система полноценно обеспечивает работу колледжа в разных режимах(обычного, обычного с элементами дистанционного обучения, в режиме	Доступность сотрудников к рабочим местам коллег	Необходимы меры организационного и физического характера

Продолжение «Системное программное обеспечение»

	карантина, а также взаимодействие и управление.(Экспертное заключение 013/503-11-17)		
СЭД «ДЕЛО» Электронный документооборот	Система предназначена для управления электронными и бумажными документами, контроля за их прохождением и исполнением в структурных подразделениях организации.	не обновление ОС	Необходимы технические и организационные меры
Microsoft Office(лицензия 200)	Офисный пакет приложений для работы с различными типами документов(тексты, эл.таблицы, базы данных и др.) В соответствии с лицензией 200	не выявлено	рекомендовано Российское обеспечение
Kaspersky Business Space Security (лицензий 200),	Программа обнаружения компьютерных вирусов и их уничтожения	не выявлено	не требуется
Windows, Linux	Комплекс программ, распределяющих ресурсы компьютерной системы и организующих работу других программ	не обновление Windows	необходимы технические и организационные меры

Продолжение «Системное программное обеспечение»

Winrar, 7Zip	Программы упаковки файлов и группы файлов для уменьшения занимаемого места на диске. Лицензия.	не обнаружено	не требуется

5. Организационное обеспечение

Объект изучения	Текущее состояние	Оптимальная структура	Нарушения, замечания и угрозы	Меры по исправлению ситуации
Возможность доступа к включённой рабочей станции, периферийному оборудованию посторонним лицом либо другим пользователем при отсутствии сотрудника на рабочем месте(вышел по необходимости, на обед, на перекур…)	Рабочие станции выключаются по питанию при долгосрочном отсутствии сотрудника - При краткосрочном отсутствии сотрудника рабочие станции, рабочие столы и открытые документы остаются доступными Экраны не блокируются(за исключением некоторых лиц)	Доступ к операционной среде должен блокироваться вручную при уходе сотрудника с рабочего места либо автоматически по истечению 5 минут простоя операционной среды	Злоумышленник может свободно получить доступ к незащищённому рабочему месту, оставленному без присмотра	Внедрение политики безопасности рабочих мест при отсутствии сотрудника

Продолжение «Организационное обеспечение»

Пользовательская операционная система и интерфейс пользователя	-Рабочие станции пользователей представляют собой автономные ПК -Политика ограничения пользовательских прав и ресурсов рабочих мест есть -Ограничений рабочих столов и личных папок нет	ОС пользователей должна быть ограниченна только нужным функционалом. Уровень ограничения операционной среды (например, интерфейса Microsoft Windows) должен соответствовать группам доступа пользователей и быть закреплён в таблице регламента ИТ-безопасности - Время работы сотрудников в операционной среде должно технически регулироваться, иметь возможность блокировки доступа к ОС в зависимости от времени суток согласно таблице регламента ИТ-безопасности - Права пользователей на выполнение		Необходимы организационные меры защиты

Продолжение «Организационное обеспечение»

		операций в ОС, с периферийным оборудованием либо в спец ПО должны быть разделены по ролям, и зафиксированы в таблице регламента ИТ-безопасности Возможность изменения прав должна быть реализована только с помощью письменного запроса руководителя		

6.Нормативное обеспечение

Объект изучения	Текущее состояние	Оптимальная структура
Документы , регламентирующие права и обязанности сотрудников в ИТ-сфере компании	Системные документы есть	1.Работу и обеспечение системы безопасности должны регулировать центральный регламент ИТ- безопасности, в котором содержатся разделы по: -Правам и обязанностям сотрудников -Уровням и возможностям доступа к ресурсам - Физическая безопасность помещений и структуры -Безопасность рабочих мест
Документы регламентирующие уровни и	Системные документы есть	

Продолжение «Нормативное обеспечение»

возможности доступа к ресурсам		-Безопасность данных, уровни доступа к ним - Ответственность и санкции в случае нарушений 2. В системе должны присутствовать должностные правила по безопасности, оформленные на основе детализации пунктов регламента ИТ- безопасности Сотрудники должны быть ознакомлены под роспись. 3.В системе должны присутствовать инструкции и методики тех или иных действий сотрудников в случае возникновения ситуаций, предусмотренных регламентом ИТ- безопасности 4.В системе должны присутствовать плакаты, напоминания, предупреждения, оформленные в бумажном виде, чёткими крупными символами или картинками и размещённые в общественных помещениях и на рабочих местах пользователей
Документы регламентирующие уровни физической безопасности помещений и структуры	Системные документы есть	
Документы регламентирующие ИТ- безопасность рабочих мест	Системные документы есть	
Документы, регламентирующие безопасность данных, уровни доступа к ним	Системные документы есть	
Документы, обозначающие уровень ответственности и санкций в случае нарушений	Системные документы есть	

7. Корпоративные данные

Роли и ресурсы	Текущее состояние	Меры по исправлению ситуации
Файл-сервер и документы	Данные размещены на специальном удалённом сервере с ограниченным сетевым доступом	Дополнительные меры не требуются
Защита серверной структуры от информационных атак	- Антивирусная система присутствует, лицензионная -Обновления проводятся - Пароли сложные	Необходимо разработать план регламентных мероприятий серверной части Контроль актуальности обновлений осуществляет сетевой администратор с помощью автоматического мониторинга
Почтовая система	Осуществляется центральное администрирование	Соответствует
Дублирование и отказоустойчивость	Есть система резервного копирования, копии актуальные	Соответствует

8. Серверная IT-структура- сервера и их роли в системе организации

№ п/п	Сервер	Роли	Соответствие меры
1.	Сервер для доступа и распределения интернет – трафика среди пользователей	Доступ и распределение интернет – трафика	Соответствует Дополнительных мер не требуется
2.	Сервер для хранения Интернет-ресурсов	Хранение Интернет-ресурсов	Соответствует Дополнительных мер не требуется
3.	Сервер контроля и авторизации учётных записей пользователей	Контроль и авторизация	Соответствует Дополнительных мер не требуется
4.	Сервер для хранения единой базы данных колледжа и иных информационных ресурсов общего доступа	Хранение единой базы данных	Соответствует Дополнительных мер не требуется
5.	Сервер официального сайта колледжа	Хранение	Соответствует Дополнительных мер не требуется

9. Стратегические рекомендации

Исходя из результатов анализа ИБ ЕИП ГАПОУ СМПК можно видеть, что в колледже имеется:

- необходимый комплект лицензионного программного обеспечения

- оборудована серверная, в которой размещается 5 серверов

-функционирующая на базе сервера локальная сеть, объединяет все кабинеты и помещения

-колледж имеет доступ в Интернет по выделенному каналу связи со

скоростью 100 Мбит/с

-установлены Антивирус Касперского Business Space Security и облачный сервис интернет-фильтрации SkyDNS

- ПО лицензировано

- имеется официальный сайт колледжа

- имеется доступ к электронно-библиотечной системе (ЭБС) ZNANIUM.com

- для оперативного обмена с Региональными органами исполнительной

власти установлен электронный документооборот СЭД « ДЕЛО»

Анализ рисков выявил уязвимости в следующих областях:

- персонал,

- нормативно- методическая база,

-помещения и оборудование,

- программные средства и операционные системы

Для уменьшения и минимизации уязвимостей предлагаются следующие меры, которые будут сводиться к:

1) применению методов и средств;

2) мероприятий по снижению уязвимостей системы, а также препятствующих несанкционированному доступу, в результате чего возможны: утраты, утечки, повреждения, разглашения информации. На этой основе разработаны рекомендации следующего характера: Средства и методы защиты:

1. Неукоснительное соблюдение Федерального закона Российской Федерации от 27 июля 2006 года № 149- ФЗ « Об информации, информационных технологиях и о защите информации», предписывающего:

- Защиту информации от несанкционированного доступа, уничтожения, модификации, блокирования, копирования, фальсификации, распространения, а также от других несанкционированных действий в отношении таковой информации;
- Соблюдение конфиденциальности информации ограниченного доступа;
- Реализацию права на доступ к информации;

2.Функционирование организации в соответствии со стандартами по защите информации, носящими рекомендательный характер:

- ГОСТ Р 50922–2007 Защита информации. Термины и определения.
- ГОСТ Р 51275–2007 Защита информации. Объекты информатизации.
- ГОСТ Р 51624–2000 Защита информации. Автоматизированные системы в защищённом исполнении. Общие положения.
- ГОСТ Р 52863–2007. Защита информации. Автоматизированные системы в защищённом исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования.

3.Исполнение локальных актов образовательной организации, вытекающих из правовых основ регулирования

4.Провести инструктажи по теме ИБ среди сотрудников и студентов

5. Введение строгого учёта доступа сотрудников к информации ограниченного распространения;

6. Внедрить мониторинг инцидентов ИБ в инфраструктуре организации

7. Внедрить практику контроля действий администраторов

8. Пересмотреть и актуализировать меры направленные на управление информационными рисками

9.Усилить физические меры информационной безопасности

10. Использовать программное обеспечение включённого в Реестр российского ПО

Приложение 5

Таблица 11- Сводная таблица значения степени вероятности угроз и меры риска

Актив	Ценность актива	Угрозы	Уровень угрозы	Уровень уязвимости	Значение степени вероятности	Мера риска
«1С Колледж»	2	Угроза неправомерного ознакомления с защищаемой информацией	В	С	3	5
		Угроза внедрения вредоносного кода через рекламу, сервисы и контент	С	С	2	4
		Угроза внедрения кода или данных	В	Н	2	4
		Угроза использования информации идентификации/аутентификации, заданной по умолчанию	В	Н	2	4
		Угроза несанкционированного удаления защищаемой информации	В	С	3	5

Продолжение таблицы 11						
		Угроза несанкционированного копирования защищаемой информации	B	C	3	5
		Угроза использования уязвимых версий программного обеспечения	B	B	4	6
		Угроза заражения компьютера при посещении неблагонадёжных сайтов	C	C	2	4
		Угроза перехвата одноразовых паролей в режиме реального времени	C	H	1	3
		Угроза утраты носителей информации	C	C	2	4
		Угроза перехвата данных, передаваемых по вычислительной сети	B	C	3	5
		Угроза несанкционированной модификации защищаемой информации	B	C	3	5

Продолжение таблицы 11						
		Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	С	Н	1	3
		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Н	Н	0	2
		Угроза изменения компонентов системы	С	С	2	4
		Угроза перехвата вводимой и выводимой на периферийные устройства информации	С	Н	1	3
		Угроза форматирования носителей информации	В	С	3	5
		Угроза исследования механизмов работы программы	С	Н	1	3
		Угроза восстановления аутентификационной информации	В	Н	2	4

Продолжение таблицы 11

		Угроза преодоления физической защиты	C	C	2	4
ФИС ГИА и Приёма	1	Угроза неправомерного ознакомления с защищаемой информацией	B	C	3	4
		Угроза несанкционированной модификации защищаемой информации	B	C	3	4
		Угроза внедрения кода или данных	C	C	2	3
		Угроза использования информации идентификации/аутентификации, заданной по умолчанию	C	C	2	3
		Угроза исследования механизмов работы программы	C	H	1	2
		Угроза перехвата одноразовых паролей в режиме реального времени	C	H	1	2
		Угроза использования уязвимых версий программного	B	B	4	5

Продолжение таблицы 11

		Угроза заражения компьютера при посещении неблагонадёжных сайтов	С	С	2	3
		Угроза восстановления аутентификационной информации	С	С	2	3
		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Н	Н	0	1
		Угроза перехвата вводимой и выводимой на периферийные устройства информации	С	Н	1	2
		Угроза перехвата данных, передаваемых по вычислительной сети	В	С	3	4
		Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	С	Н	1	2
		Угроза утраты носителей информации	С	С	2	3

Продолжение таблицы 11

		Угроза форматирования носителей информации	B	C	3	4
		Угроза внедрения вредоносного кода через рекламу, сервисы и контент	C	C	2	3
		Угроза преодоления физической защиты	B	C	3	4
		Угроза изменения компонентов системы	B	C	3	4
		Угроза несанкционированного копирования защищаемой информации	B	C	3	4
		Угроза несанкционированного удаления защищаемой информации	B	C	3	4
Региональная АИС «Сетевой город Образование»	3	Угроза несанкционированного удаления защищаемой информации	B	C	3	6
		Угроза неправомерного ознакомления с защищаемой	B	C	3	6

Продолжение таблицы 11

		информацией				
		Угроза исследования механизмов работы программы	С	Н	1	4
		Угроза утраты носителей информации	С	С	2	5
		Угроза заражения компьютера при посещении неблагонадёжных сайтов	С	С	2	5
		Угроза несанкционированной модификации защищаемой информации	В	С	3	6
		Угроза использования уязвимых версий программного обеспечения	В	В	4	7
		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Н	Н	0	3
		Угроза хищения средств хранения, обработки и (или) ввода/вывода/пере	С	Н	1	4

Продолжение таблицы 11

		Угроза перехвата вводимой и выводимой на периферийные устройства информации	С	Н	1	4
		Угроза внедрения кода или данных	С	С	2	5
		Угроза форматирования носителей информации	В	С	3	6
		Угроза несанкционированного копирования защищаемой информации	В	С	3	6
		Угроза перехвата одноразовых паролей в режиме реального времени	С	Н	1	4
		Угроза использования информации идентификации/ аутентификации, заданной по умолчанию	С	С	2	5
		Угроза перехвата данных, передаваемых по вычислительной сети	В	С	3	6

Продолжение таблицы 11

		Угроза изменения компонентов системы	В	Н	2	5
		Угроза преодоления физической защиты	В	С	3	6
		Угроза восстановления аутентификационной информации	С	С	2	5
		Угроза внедрения вредоносного кода через рекламу, сервисы и контент	С	С	2	5
СЭД «ДЕЛО» Электронный документооборот	4	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	В	Н	2	6
		Угроза несанкционированного удаления защищаемой информации	В	С	3	7
		Угроза исследования механизмов работы программы	С	Н	1	5
		Угроза несанкционированного копирования защищаемой информации	В	С	3	7

Продолжение таблицы 11

		Угроза заражения компьютера при посещении неблагонадёжных сайтов	B	H	2	6
		Угроза использования уязвимых версий программного обеспечения	B	B	4	8
		Угроза несанкционированной модификации защищаемой информации	B	C	3	7
		Угроза внедрения кода или данных	B	H	2	6
		Угроза перехвата вводимой и выводимой на периферийные устройства информации	C	H	1	5
		Угроза перехвата данных, передаваемых по вычислительной сети	B	C	3	7
		Угроза перехвата одноразовых паролей в режиме реального времени	C	H	1	5
		Угроза утраты носителей информации	B	H	2	6

Продолжение таблицы 11

		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	H	H	0	4
		Угроза изменения компонентов системы	B	H	2	6
		Угроза форматирования носителей информации	B	C	3	7
		Угроза восстановления аутентификационной информации	B	H	2	6
		Угроза преодоления физической защиты	B	C	3	7
		Угроза использования информации идентификации/аутентификации, задаваемой по умолчанию	B	H	2	6
		Угроза хищения	C	H	1	5
		средств хранения,				

Продолжение таблицы 11

		обработки и (или) ввода/вывода/передачи информации				
		Угроза неправомерного ознакомления с защищаемой информацией	B	C	3	7
Сайт	2	Угроза неправомерного ознакомления с защищаемой информацией	B	C	3	5
		Угроза несанкционированного удаления защищаемой информации	B	C	3	5
		Угроза использования уязвимых версий программного обеспечения	B	B	4	6
		Угроза несанкционированной модификации защищаемой информации	B	C	3	5
		Угроза перехвата вводимой и выводимой на периферийные устройства информации	C	H	1	3

Продолжение таблицы 14

		Угроза заражения компьютера при посещении неблагонадёжных сайтов	С	С	2	4
		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Н	Н	0	2
		Угроза перехвата данных, передаваемых по вычислительной сети	В	С	3	5
		Угроза утраты носителей информации	С	С	2	4
		Угроза несанкционированного копирования защищаемой информации	В	С	3	5
		Угроза использования информации идентификации/аутентификации заданной по умолчанию	С	С	2	4
		Угроза исследования механизмов работы	Н	С	1	3

Продолжение таблицы 14

		Угроза восстановления аутентификационной информации	С	С	2	4
		Угроза форматирования носителей информации	В	С	3	5
		Угроза хищения средств хранения, обработки и(или) ввода/вывода/передачи информации	С	Н	1	3
		Угроза преодоления физической защиты	С	С	2	4
		Угроза изменения компонентов системы	В	Н	2	4
		Угроза внедрения вредоносного кода через рекламу, сервисы и контент	С	С	2	4
		Угроза перехвата одноразовых паролей в режиме реального времени	С	Н	1	3
		Угроза внедрения кода или данных	С	С	2	4

Таблица 12 - Оценка ценности для степени вероятности и возможных последствий рисков

Уровни угрозы	низкая			средняя			высокая		
Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Значение степени вероятности	0	1	2	1	2	3	2	3	4

Таблица 13 - Определение меры риска

Степень вероятности возникновения угрозы		Низкая			Средняя			Высокая		
Простота использования		Н	С	В	Н	С	В	Н	С	В
Ценность актива	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Таблица 14 - Таблица расчёта коэффициента реализуемости угроз для информационных активов ГАПОУ СМПК «1С Колледж»

Актив	Угроза	Коэффициент реализуемости угроз	
		$(Y_1 + Y_2)/20=Y$	Качественный наминал
«1С Колледж»	Угроза неправомерного ознакомления с защищаемой информацией	(5+10)/20= 0,75	В
	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	(5+5)/20= 0,5	С
	Угроза внедрения кода или данных	(5+10)/20=0,75	В
	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	(5+10)/20=0,75	В
	Угроза несанкционированного удаления защищаемой информации	(5+10)/20=0,75	В
	Угроза несанкционированного копирования защищаемой информации	(5+10)/20=0,75	В
	Угроза использования уязвимых версий программного обеспечения	(5+10)/20=0,75	В
	Угроза заражения компьютера при посещении неблагонадёжных сайтов	(5+2)/20=0,35	С
	Угроза перехвата одноразовых паролей в режиме реального времени	(5+5)/20=0,5	С
	Угроза утраты носителей информации	(5+2)/20=0,35	С

Продолжение таблицы 14

	Угроза перехвата данных, передаваемых по вычислительной сети	(5+10)/20=0,75	B
	Угроза несанкционированной модификации защищаемой информации	(5+10)/20=0,75	B
	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	(5+2)/20=0,35	C
	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	(5+0)/20=0,25	H
	Угроза изменения компонентов системы	(5+2)/20=0,35	C
	Угроза перехвата вводимой и выводимой на периферийные устройства информации	(5+5)/20=0,5	C
	Угроза форматирования носителей информации	(5+10)/20=0,75	B
	Угроза исследования механизмов работы программы	(5+5)/20=0,5	C
	Угроза восстановления аутентификационной информации	(5+10)/20=0,75	B
	Угроза преодоления физической защиты	(5+2)/20=0,35	C

Продолжение таблицы 14

ФИС ГИА и Приёма

Актив	Угроза	Коэффициент реализуемости угроз	
		(Y1 + Y2)/20=Y	Качественный наминал
ФИС ГИА и Приёма	Угроза неправомерного ознакомления с защищаемой информацией	(5+10)/20=0,75	В
	Угроза несанкционированной модификации защищаемой информации	(5+10)/20=0,75	В
	Угроза внедрения кода или данных	(5+2)/20= 0,35	С
	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	(5+5)/20= 0,5	С
	Угроза исследования механизмов работы программы	(5+2)/20= 0,35	С
	Угроза перехвата одноразовых паролей в режиме реального времени	(5+5)/20= 0,5	С
	Угроза использования уязвимых версий программного обеспечения	(5+10)/20=0,75	В
	Угроза заражения компьютера при посещении неблагонадёжных сайтов	(5+5)/20= 0,5	С
	Угроза восстановления аутентификационной информации	(5+5)/20= 0,5	С
	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	(5+ 0)/20= 0,25	Н

Продолжение таблицы14

	Угроза перехвата вводимой и выводимой на периферийные устройства информации	(5+5)/20= 0,5	C
	Угроза перехвата данных, передаваемых по вычислительной сети	(5+10)/20=0,75	B
	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	(5+2)/20= 0,35	C
	Угроза утраты носителей информации	(5+2)/20= 0,35	C
	Угроза форматирования носителей информации	(5+10)/20=0,75	B
	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	(5+5)/20= 0,5	C
		(5+10)/20=0,75	B
	Угроза изменения компонентов системы	(5+10)/20=0,75	B
	Угроза несанкционированного копирования защищаемой информации	(5+10)/20=0,75	B
	Угроза несанкционированного удаления защищаемой информации	(5+10)/20=0,75	B

Продолжение таблицы 14

Региональная АИС «Сетевой город Образование

Актив	Угроза	Коэффициент еализуемости угроз	
		(Y1 + Y2)/20=Y	Качественный наминал
Региональная АИС «Сетевой город Образование	Угроза несанкционированного удаления защищаемой информации	(5+10)/20= 0,75	В
	Угроза неправомерного ознакомления с защищаемой информацией	(5+10)/20= 0,75	В
	Угроза исследования механизмов работы программы	(5+2)/|20= 0,35	С
	Угроза утраты носителей информации	(5+5)/20= 0,5	С
	Угроза заражения компьютера при посещении неблагонадёжных сайтов	(5+5)/20= 0,5	С
	Угроза несанкционированной модификации защищаемой информации	(5+10)/20= 0,75	В
	Угроза использования уязвимых версий программного обеспечения	(5+10)/20= 0,75	В
	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	(5+0)/20= 0,25	Н
	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	(5+2)/20= 0,35	С

Продолжение таблицы 14

	Угроза перехвата вводимой и выводимой на периферийные устройства информации	(5+5)/20= 0,5	С
	Угроза внедрения кода или данных	(5+2)/20= 0,35	С
	Угроза форматирования носителей информации	(5+10)/20= 0,75	В
	Угроза несанкционированного копирования защищаемой информации	(5+10)/20= 0,75	В
	Угроза перехвата одноразовых паролей в режиме реального времени	(5+2)/20= 0,35	С
	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию	(5+5)/20= 0,5	С
	Угроза перехвата данных, передаваемых по вычислительной сети	(5+10)/20= 0,75	В
	Угроза изменения компонентов системы	(5+10)/20= 0,75	В
	Угроза преодоления физической защиты	(5+10)/20= 0,75	В
	Угроза восстановления аутентификационной информации	(5+2)/20= 0,35	С
	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	(5+2)/20= 0,35	С

Продолжение таблицы 14

СЭД «ДЕЛО» Электронный документооборот

Актив	Угроза	Коэффициент реализуемости угроз	
		(Y1 + Y2)/20=Y	Качественный наминал
СЭД «ДЕЛО» Электронный документооборот	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	(5+10)/20= 0,75	В
	Угроза несанкционированного удаления защищаемой информации	(5+10)/20= 0,75	В
	Угроза исследования механизмов работы программы	(5+0)/20= 0,25	С
	Угроза несанкционированного копирования защищаемой информации	(5+10)/20= 0,75	В
	Угроза заражения компьютера при посещении неблагонадёжных сайтов	(5+10)/20= 0,75	В
	Угроза использования уязвимых версий программного обеспечения	(5+10)/20= 0,75	В
	Угроза несанкционированной модификации защищаемой информации	(5+10)/20= 0,75	В
	Угроза внедрения кода или данных	(5+10)/20= 0,75	В
	Угроза перехвата вводимой и выводимой на периферийные устройства информации	(5+2)/20= 0,35	С
	Угроза перехвата данных, передаваемых по вычислительной сети	(5+10)/20= 0,75	В

Продолжение таблицы 14

	Угроза перехвата одноразовых паролей в режиме реального времени	(5+2)/20= 0,35	С
	Угроза утраты носителей информации	(5+10)/20= 0,75	В
	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	(5+0)/20= 0,25	Н
	Угроза изменения компонентов системы	(5+10)/20= 0,75	В
	Угроза форматирования носителей информации	(5+10)/20= 0,75	В
	Угроза восстановления аутентификационной информации	(5+10)/20= 0,75	В
	Угроза преодоления физической защиты	(5+10)/20= 0,75	В
	Угроза использования информации идентификации/аутентификации, задаваемой по умолчанию	(5+10)/20= 0,75	В
	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	(5+2)/20= 0,35	С
	Угроза неправомерного ознакомления с защищаемой информацией	(5+10)/20= 0,75	В

Продолжение таблицы 14

Сайт

Актив	Угроза	Коэффициент реализуемости угроз	
		(Y1 +Y2)/20=Y	Качественный наминал
Сайт	Угроза неправомерного ознакомления с защищаемой информацией	(5+10)/20= 0,75	В
	Угроза несанкционированного удаления защищаемой информации	(5+10)/20= 0,75	В
	Угроза использования уязвимых версий программного обеспечения	(5+10)/20= 0,75	В
	Угроза несанкционированной модификации защищаемой информации	(5+10)/20= 0,75	В
	Угроза перехвата вводимой и выводимой на периферийные устройства информации	(5+2)/20= 0,35	С
	Угроза заражения компьютера при посещении неблагонадёжных сайтов	(5+2)/20= 0,35	С
	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	(5+0)/20= 0,25	Н
	Угроза перехвата данных, передаваемых по вычислительной сети	(5+10)/20= 0,75	В
	Угроза утраты носителей информации	(5+2)/20= 0,35	С
	Угроза несанкционированного копирования защищаемой информации	(5+10)/20= 0,75	В

Продолжение таблицы 14

	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	(5+2)/20= 0,35	С
	Угроза исследования механизмов работы программы	(5+0)/20= 0,25	Н
	Угроза восстановления аутентификационной информации	(5+2)/20= 0,35	С
	Угроза форматирования носителей информации	(5+10)/20= 0,75	В
	Угроза хищения средств хранения, обработки и(или) ввода/вывода/передачи информации	(5+2)/20= 0,35	С
	Угроза преодоления физической защиты	(5+2)/20= 0,35	С
	Угроза изменения компонентов системы	(5+10)/20= 0,75	В
	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	(5+2)/20= 0,35	С
	Угроза перехвата одноразовых паролей в режиме реального времени	(5+2)/20= 0,35	С
	Угроза внедрения кода или данных	(5+2)/20= 0,35	С

Таблица 15 - Сводная таблица коэффициента реализуемости угроз для информационных систем ГАПОУ СМПК

№ п/п	Виды угроз	«1С Колледж»	ФИС ГИА и Приёма	Региональная АИС «Сетевой город Образование»	СЭД «ДЕЛО» Электронный документооборот	Сайт
1.	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	0,5	0,5	0,35	0,75	0,35
2.	Угроза несанкционированного удаления защищаемой информации	0,75	0,75	0,75	0,75	0,75
3.	Угроза исследования механизмов работы программы	0,5	0,35	0,35	0,25	0,25
4.	Угроза несанкционированного копирования защищаемой информации	0,75	0,75	0,75	0,75	0,75
5.	Угроза заражения компьютера при посещении неблагонадёжных сайтов	0,35	0,5	0,5	0,75	0,35
6.	Угроза использования уязвимых версий программного обеспечения	0,75	0,75	0,75	0,75	0,75
7.	Угроза несанкционированной модификации защищаемой информации	0,75	0,75	0,75	0,75	0,75
8.	Угроза внедрения кода или данных	0,75	0,35	0,35	0,75	0,35

Продолжение таблицы 15

9.	Угроза перехвата вводимой и выводимой на периферийные устройства информации	0,5	0,5	0,5	0,35	0,35
10.	Угроза перехвата данных, передаваемых по вычислительной сети	0,75	0,75	0,75	0,75	0,75
11.	Угроза перехвата одноразовых паролей в режиме реального времени	0,5	0,5	0,35	0,35	0,35
12.	Угроза утраты носителей информации	0,35	0,35	0,5	0,75	0,35
13.	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	0,25	0,25	0,25	0,25	0,25
14.	Угроза изменения компонентов системы	0,35	0,75	0,75	0,75	0,75
15.	Угроза форматирования носителей информации	0,75	0,75	0,75	0,75	075
16.	Угроза восстановления аутентификационной информации	0,75	0,5	0,35	0,75	0,35
17.	Угроза преодоления физической защиты	0,35	0,75	0,75	0,75	0,35
18.	Угроза использования информации идентификации/аутентификации, задаваемой по умолчанию	0,75	0,5	0,5	0,75	0,35
19.	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	0,35	0,35	0,35	0,35	0,35
20.	Угроза неправомерного ознакомления с защищаемой информацией	0,75	0,75	0,75	0,75	0,75

Таблица 16 - Оценка рисков ИБ согласно критериям стандарта

ГОСТ Р ИСО/МЭК-27005–2010

0–2 – низкий риск

3–5 – средний риск

6–8 – высокий риск

Актив	Угрозы	Мера риска	Оценка риска
«1С Колледж»	Угроза неправомерного ознакомления с защищаемой информацией	5	С
	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	4	С
	Угроза внедрения кода или данных	4	С
	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	4	С
	Угроза несанкционированного удаления защищаемой информации	5	С
	Угроза несанкционированного копирования защищаемой информации	5	С
	Угроза использования уязвимых версий программного обеспечения	6	В
	Угроза заражения компьютера при посещении неблагонадёжных сайтов	4	С
	Угроза перехвата одноразовых паролей в режиме реального времени	3	С

Продолжение таблицы 16

	Угроза утраты носителей информации	4	С
	Угроза перехвата данных, передаваемых по вычислительной сети	5	С
	Угроза несанкционированной модификации защищаемой информации	5	С
	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	3	С
	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	2	Н
	Угроза изменения компонентов системы	4	С
	Угроза перехвата вводимой и выводимой на периферийные устройства информации	3	С
	Угроза форматирования носителей информации	5	С
	Угроза исследования механизмов работы программы	3	С
	Угроза восстановления аутентификационной информации	4	С
	Угроза преодоления физической защиты	4	С
ФИС ГИА и Приёма	Угроза неправомерного ознакомления с защищаемой информацией	4	С
	Угроза несанкционированной модификации защищаемой информации	4	С
	Угроза внедрения кода или данных	3	С

Продолжение таблицы 16

	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	3	С
	Угроза исследования механизмов работы программы	2	Н
	Угроза перехвата одноразовых паролей в режиме реального времени	2	Н
	Угроза использования уязвимых версий программного обеспечения	5	С
	Угроза заражения компьютера при посещении неблагонадёжных сайтов	3	С
	Угроза восстановления аутентификационной информации	3	С
	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	1	Н
	Угроза перехвата вводимой и выводимой на периферийные устройства информации	2	Н
	Угроза перехвата данных, передаваемых по вычислительной сети	4	С
	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	2	Н
	Угроза утраты носителей информации	3	С
	Угроза форматирования носителей информации	4	С

Продолжение таблицы 16

	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	3	С
	Угроза преодоления физической защиты	4	С
	Угроза изменения компонентов системы	4	С
	Угроза несанкционированного копирования защищаемой информации	4	С
	Угроза несанкционированного удаления защищаемой информации	4	С
Региональная АИС «Сетевой город Образование»	Угроза несанкционированного удаления защищаемой информации	6	В
	Угроза неправомерного ознакомления с защищаемой информацией	6	В
	Угроза исследования механизмов работы программы	4	С
	Угроза утраты носителей информации	5	С
	Угроза заражения компьютера при посещении неблагонадёжных сайтов	5	С
	Угроза несанкционированной модификации защищаемой информации	6	В
	Угроза использования уязвимых версий программного обеспечения	7	В
	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	3	С
	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	4	С

Продолжение таблицы 16

	Угроза перехвата вводимой и выводимой на периферийные устройства информации	4	C
	Угроза внедрения кода или данных	5	C
	Угроза форматирования носителей информации	6	B
	Угроза несанкционированного копирования защищаемой информации	6	B
	Угроза перехвата одноразовых паролей в режиме реального времени	4	C
	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию	5	C
	Угроза перехвата данных, передаваемых по вычислительной сети	6	B
	Угроза изменения компонентов системы	5	C
	Угроза преодоления физической защиты	6	B
	Угроза восстановления аутентификационной информации	5	C
	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	5	C

Продолжение таблицы 16

СЭД «ДЕЛО» Электронный документооборот	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	6	В
	Угроза несанкционированного удаления защищаемой информации	7	В
	Угроза исследования механизмов работы программы	5	С
	Угроза несанкционированного копирования защищаемой информации	7	В
	Угроза заражения компьютера при посещении неблагонадёжных сайтов	6	В
	Угроза использования уязвимых версий программного обеспечения	8	В
	Угроза несанкционированной модификации защищаемой информации	7	В
	Угроза внедрения кода или данных	6	В
	Угроза перехвата вводимой и выводимой на периферийные устройства информации	5	С
	Угроза перехвата данных, передаваемых по вычислительной сети	7	В
	Угроза перехвата одноразовых паролей в режиме реального времени	5	С
	Угроза утраты носителей информации	6	В
	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	4	С
	Угроза изменения компонентов системы	6	В
	Угроза форматирования носителей информации	7	В

Продолжение таблицы 16

	Угроза восстановления аутентификационной информации	6	B
	Угроза преодоления физической защиты	7	B
	Угроза использования информации идентификации/аутентификации, задаваемой по умолчанию	6	B
	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	5	C
	Угроза неправомерного ознакомления с защищаемой информацией	7	B
Сайт	Угроза неправомерного ознакомления с защищаемой информацией	5	C
	Угроза несанкционированного удаления защищаемой информации	5	C
	Угроза использования уязвимых версий программного обеспечения	6	B
	Угроза несанкционированной модификации защищаемой информации	5	C
	Угроза перехвата вводимой и выводимой на периферийные устройства информации	3	C
	Угроза заражения компьютера при посещении неблагонадёжных сайтов	4	C
	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	2	H
	Угроза перехвата данных, передаваемых по вычислительной сети	5	C
	Угроза утраты носителей информации	4	C
	Угроза несанкционированного копирования защищаемой информации	5	C

Продолжение таблицы 16

	Угроза использования информации идентификации/аутентификации заданной по умолчанию	4	С
	Угроза исследования механизмов работы программы	3	С
	Угроза восстановления аутентификационной информации	4	С
	Угроза форматирования носителей информации	5	С
	Угроза хищения средств хранения, обработки и(или) ввода/вывода/передачи информации	3	С
	Угроза преодоления физической защиты	4	С
	Угроза изменения компонентов системы	4	С
	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	4	С
	Угроза перехвата одноразовых паролей в режиме реального времени	3	С
	Угроза внедрения кода или данных	4	С