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 и управление службой информационной безопасности в образовательной организации

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

Проверка на объем заимствований:
84,9 % авторского текста
Работа рекомендована к защите
«08» 06 2022 г.
зав. кафедрой АТИТ и МОТД
_____ В.В. Руднев

Выполнила:
Студентка группы ОФ-209-210-2-1,
Осипова Дарья Владимировна
Научный руководитель:
Дмитриев Михаил Сергеевич
профессор каф.АТИТ и МОТД, д.т.н.

Челябинск, 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность

Современный уровень развития информационных технологий выдвигает на передний план новые требования к построению систем защиты информации и обеспечению информационной безопасности. В России на протяжении длительного времени понятие информационной безопасности отождествлялось с обеспечением конфиденциальности информации, а наибольшее распространение получило применение технических средств защиты. Сегодня информация, будучи нематериальной по своей природе, становится предметом товарно-денежных отношений и объектом нормативно-правового регулирования. Перед государственными и коммерческими предприятиями и организациями все острее встает проблема не только обеспечения надежной защиты информации от несанкционированного ознакомления и распространения, но и поддержки стабильного доступа к информации и возможности эффективной работы с ней. Более того, Доктрина информационной безопасности Российской Федерации провозглашает «соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею» одной из составляющих национальных интересов в информационной сфере.

Система информационной безопасности должна обеспечивать:

— конфиденциальность (защита информации от несанкционированного раскрытия или перехвата);

— целостность (достоверность и полноту информации и компьютерных программ);

— доступность (возможность получить пользователям информацию, в пределах своей компетенции).

С учетом зарубежного и отечественного опыта обеспечение информационной безопасности осуществляется по следующим направлениям:

— правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

— организационная защита – это регламентация производственной деятельности и отношений исполнителей на нормативно-правовой основе, исключить или ослабляющая нанесение ущерба;

— инженерно-техническая защита – это использование различных технических средств, которые предотвращают нанесение ущерба.

В связи с вышеизложенным сегодня при построении систем защиты информации все большее внимание уделяется установлению баланса между техническими средствами и законодательно-организационными мерами защиты. Преимущество получает комплексный подход к защите информации, который состоит в одновременном решении целого ряда разноплановых задач путем применения совокупности взаимосвязанных средств, методов и мероприятий.

Отечественная и зарубежная наука уделяет большое внимание информационной безопасности. Многие зарубежные социологи и политологи активно исследуют вопросы информационного противоборства и информационной безопасности. Среди наиболее известных трудов можно отметить работы Д.Альбертса, Г.С.Джоуэта, М.Либицки, Д.А.Мальтизи, Р.Д.Маклорина, Р.Л.Пфальцграффа, А.Шафрански, Р.Х.Шульца, А.Эделыптейна и других, где рассматриваются различные аспекты влияния информации на политические, экономические, военные и культурные процессы в современных международных отношениях.

Научное осмысление различных аспектов информационной безопасности активно проводились отечественными учеными: А.В.Возженниковым, Ю.Ф.Нуждиным, Е.Н.Пасхиным, Е.Е.Перчук, А.И.Поздняковым, Г.Г.Почепцовым, А.А.Прохожевым, С.П.Расторгуевым, А.А.Стрельцовым, Г.Л.Смоляным, Д.С.Черешкиным, А.С.Шийко, В.Н.Цыгичко и др.

Рассмотрению проблем защиты личности от вредного информационного воздействия в современном мире посвящены работы Г.В.Грачева, Ю.А.Ермакова, В.Е.Лепского, И.К.Мельника, И.Н.Панарина и других исследователей.

Различным аспектам правовой защиты интересов личности в информационной сфере общества посвящены работы В.А.Анниковой, А.А.Антопольского, А.Л.Балыбердина, И.Л.Бачило, М.С.Григорьева, В.И.Кирина, О.А.Колобова, В.А.Копылова, В.Н.Ясенева, В.Н.Лопатина, Д.В.Огородова, В.Д.Попова, Ю.Г.Просвирина, А.А.Фатьянова.

Техническим аспектам защиты информации в информационных системах и сетях посвящены работы В.А.Герасименко, С.Н.Гриняева, М.П.Зегжды, В.Н.Лопатина, В.А.Никитова, Е.И.Орлова, Г.И.Савина.

Различным аспектам проблемы защиты информации посвящены работы Д.А.Андрианова, Н.А.Брусницына, В.Н.Кузнецова, Е.Ю.Митрохина, С.З.Павленко, И.Н.Панарина, С.В.Рабовского, С.П.Расторгуева, А.В.Федорова, А.С.Шийко.

Анализ публикаций последних лет свидетельствует о необходимости выбора систем защиты информации, основанных на таком комплексном подходе, надежное функционирование которых невозможно без эффективного управления. Основные функции организации и управления службой информационной безопасности должны состоять в оценке степени критичности ситуации, связанной с нарушением информационной безопасности предприятия, организации процессов работы, оценке уровня риска нарушения информационной безопасности и в принятии решений относительно действий в данной ситуации.

Принятие решений в такой системе затруднено по ряду причин: не всегда возможно сформировать полное множество угроз информационной безопасности, количественно оценить степень критичности возникшей ситуации, построить прогноз ее развития. Другими словами, основная

проблема заключается в зачастую неполных и неопределенных исходных данных о состоянии системы защиты информации, возможных угрозах, дестабилизирующих факторах.

Таким образом, тема исследования, направленная на решение данной проблемы, является актуальной и определяет цели, задачи и основные направления исследования.

Объектом исследования является система защиты информации организации профессионального образования.

Предметом исследования является управление службой информационной безопасности образовательной организации.

Цель исследования заключается в анализе существующей системы организации и управления службой информационной безопасности образовательной организации и разработке мер по совершенствованию данной системы.

Гипотеза заключается в предположении о том, что внедрение рекомендаций по организации и управлению службой информационной безопасности позволит повысить эффективность функционирования указанной службы.

Для достижения поставленной цели необходимо решение следующих **задач**:

— раскрыть сущность и содержание организации управления информационной безопасностью;

— провести анализ объекта защиты ГБПОУ «Южно-Уральский государственный технический колледж», изучить структуру, информационные ресурсы и информационные потоки колледжа; выявить уязвимости в системе защиты информации.

— разработать рекомендации по организации и управлению службой информационной безопасности ГБПОУ «Южно-Уральский государственный технический колледж»;

— проверить предложенные рекомендации по управлению службой информационной безопасности ГБПОУ «Южно-Уральский государственный колледж» с помощью экспертной оценки.

Научная новизна проведенных исследований и полученных в ходе работы результатов заключается в демонстрации возможности изменения уже существующей системы обеспечения информационной безопасности образовательного процесса в образовательной организации среднего профессионального образования путем реализации комплексной программы мер.

Теоретическая значимость исследования определяется расширением научных знаний в области информационной безопасности образовательной организации.

Практическая значимость диссертации определяется тем, что ее результаты позволяют повысить степень защиты информации в образовательной организации путем использования предложенных рекомендаций по совершенствованию системы управления отделом информационной безопасности.

Методологическую основу исследования составили законодательные и нормативно-правовые документы РФ, разработки в области обеспечения информационной безопасности, методы и способы построения процессов управления информационной безопасностью в целях повышения информационной безопасности в организациях, системный анализ.

Теоретическую и информационную базу исследования составляют основные положения по информационной безопасности, системный подход к исследуемому объекту и предмету, в качестве информационных источников использованы аналитические и статистические материалы по информационной безопасности, материалы научных конференций, средств

массовой информации, отражающие аспекты информационной безопасности.

Структура магистерской диссертации: работа состоит из введения, двух глав, заключения, списка использованной литературы.

ГЛАВА 1. Теоретические основы организации и управления службой информационной безопасности в образовательной организации

1.1. Сущность и содержание службы информационной безопасности в образовательной организации

В организациях, использующих в своей деятельности сведения с ограниченным доступом, для разработки и проведения технических мероприятий по защите информации в соответствии с порядком, установленным Уставом (учредительным документом) организации, создаются соответствующие службы.

Служба защиты информации, как правило, является самостоятельным структурным подразделением, подчиненным непосредственно руководителю и заместителю по безопасности. При наличии в организации службы безопасности служба защиты информации входит в ее структуру.

В структурных подразделениях организации при необходимости могут создаваться части, группы службы защиты информации или назначаться приказом руководителя уполномоченные, на которых распространяются права и обязанности работников указанной службы.

Служба защиты информации относится к подразделениям, непосредственно участвующим в деятельности по выполнению работ с использованием сведений с ограниченным доступом.

Структура и штаты службы защиты информации определяются руководителем организации (предприятия) в зависимости от объема и

сложности работ по защите информации. Нормативной правовой базой для решения этой задачи является комплекс следующих актов:

— Федеральный закон РФ «О государственной тайне»;

— руководящие документы Гостехкомиссии при Президенте Российской Федерации («Защита от несанкционированного доступа к информации». «Классификация автоматизированных систем и требования по защите информации»);

— «Квалификационные характеристики должностей руководителей и специалистов, обеспечивающих защиту информации»;

— «Квалификационные характеристики работников режимно-секретных органов министерств, ведомств, учреждений, предприятий и организаций Российской Федерации»;

— «Концепция защиты СВТ и АС от НСД к информации».

Служба защиты информации комплектуется соответствующими работниками, отвечающими требованиям квалификационных характеристик на специалистов по комплексной защите информации.

Назначение и освобождение от должности руководителя службы защиты информации производятся руководителем организации с письменного согласия ведомственного отдела защиты информации. Там же до приема дел вновь назначенный руководитель и его заместитель должны пройти инструктаж. Руководитель службы защиты информации обязан организовывать и систематически проводить учебу работников службы и уполномоченных по защите информации в целях повышения деловой квалификации, уровня знаний и приобретения практических навыков по реализации, возложенных на службу защиты информации задач.

Целями системы защиты информации предприятия являются:

— предотвращение утечки, хищения, утраты, искажения, подделки информации;

— предотвращение угроз безопасности личности, предприятия, общества, государства;

— предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

— предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации как объекта собственности;

— защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

— сохранение, конфиденциальности документированной информации в соответствии с законодательством.

Для грамотного построения и эксплуатации системы защиты необходимо соблюсти следующие принципы ее применения:

— простота защиты;

— приемлемость защиты для пользователей;

— подконтрольность системы защиты;

— постоянный контроль за наиболее важной информацией;

— дробление конфиденциальной информации на составляющие элементы, доступ к которым имеют разные пользователи;

— минимизация привилегий по доступу к информации;

— установка ловушек для провоцирования несанкционированных действий;

— независимость системы управления для пользователей;

— устойчивость защиты во времени и при неблагоприятных обстоятельствах;

— глубина защиты, дублирование и перекрытие защиты;

— особая личная ответственность лиц, обеспечивающих безопасность информации;

— минимизация общих механизмов защиты.

Алгоритм создания системы защиты конфиденциальной информации таков:

1. Определение объектов защиты.
2. Выявление угроз и оценка их вероятности.
3. Оценка возможного ущерба.
4. Обзор применяемых мер защиты, определение их недостаточности.
5. Определение адекватных мер защиты.
6. Организационное, финансовое, юридическое и пр. виды обеспечения мер защиты.
7. Внедрение мер защиты.
8. Контроль.

Мониторинг и корректировка внедренных мер.

1. Начальник службы защиты информации приказом руководителя предприятия назначается во главе группы компетентных сотрудников, которые высказывают свои предложения по объему, уровню и способам обеспечения сохранности конфиденциальной информации.

2. Руководитель группы, обладая соответствующей квалификацией в этой области, с привлечением отдельных специалистов формирует предварительный список сведений, которые в дальнейшем войдут в «Перечень сведений, составляющих конфиденциальную информацию предприятия».

3. Руководитель группы на основе этого списка определяет и представляет на согласование необходимые к защите объекты (оборудование для обработки и обращения информации, программное обеспечение, коммуникации для передачи конфиденциальных данных,

носители информации, персонал, допущенный к работе с использованием коммерческой и иной тайны).

4. Анализируются существующие меры защиты соответствующих объектов, определяется степень их недостаточности, неэффективности, физического и морального износа.

5. Изучаются зафиксированные случаи попыток несанкционированного доступа к охраняемым информационным ресурсам и разглашения информации.

6. На основе опыта предприятия, а также используя метод моделирования ситуаций, группа специалистов выявляет возможные пути несанкционированных действий по уничтожению информации, ее копированию, модификации, искажению, использованию и т. п. Угрозы ранжируются по степени значимости и классифицируются по видам воздействия.

7. На основе собранных данных оценивается возможный ущерб предприятия от каждого вида угроз, который становится определяющим фактором для категорирования сведений в «Перечне» по степени важности, например – для служебного пользования, конфиденциально, строго конфиденциально.

8. Определяются сферы обращения каждого вида конфиденциальной информации: по носителям, по территории распространения, по допущенным пользователям. Для решения этой задачи группа привлекает руководителей структурных подразделений и изучает их пожелания.

9. Группа подготавливает введение указанных мер защиты.

Для обеспечения работоспособности разработанной системы защиты информации необходимо создать специальный отдел в составе организации, занимающийся данными вопросами – Службу защиты информации (СЗИ).

К задачам СЗИ относятся:

1. Своевременное выявление угроз защищаемой информации компании, причин и условий их возникновения и реализации.

2. Выявление и максимальное перекрытие потенциально возможных каналов и методов несанкционированного доступа к информации.

3. Отработка механизмов оперативного реагирования на угрозы, использование юридических, экономических, организационных, социально-психологических, инженерно-технических средств и методов выявления и нейтрализации источников угроз безопасности компании.

4. Организация специального делопроизводства, исключающего несанкционированное получение конфиденциальной информации.

Система методов управления информационной безопасности

Система методов управления информационной безопасности состоит из субъекта, объекта управления, прямой и обратной связи.

Субъектом управления службой безопасности выступают руководитель организации и начальник службы безопасности. Успешно выполнять свои задачи эти субъекты могут только в том случае, если компетенция каждого из них будет строго определена в правовых актах таким образом, чтобы не возникала почва для конфликтов. Если это сделано достаточно успешно, то можно говорить о сформированной управляющей подсистеме.

Объектом управления (управляемой подсистемой) в службе безопасности выступают ее отдельные сотрудники и подразделения. Объект управления соединен с субъектом управления каналами прямой и обратной связи (информационными каналами). По каналу прямой связи информация в виде управленческих решений поступает от субъекта управления к объекту, а по каналам обратной связи – в обратном направлении, сигнализируя о состоянии объекта управления, его реакции на управленческие воздействия.

Само управленческое воздействие, в свою очередь, реализуется в форме таких функций управления, как прогнозирование, планирование, организация, регулирование, мотивация и контроль. В системе управления все эти функции объединены в целостный процесс, хотя из методических соображений целесообразно рассматривать их отдельно. Рассмотрим вышеуказанные функции с учетом специфики деятельности службы безопасности.

Прогнозирование предполагает составление заключения (прогноза) о будущем событии, тенденции развития службы безопасности. Прогнозные оценки бывают оперативными (с упреждением не более одного месяца), краткосрочными (от 1 месяца до 1 года), среднесрочными (от 1 года до 5 лет). Составляются они как привлеченными со стороны специалистами, так и сотрудниками службы безопасности.

Планирование предполагает определение целей, задач службы безопасности на предстоящий период деятельности, средств и времени на их достижение. Наиболее распространенными в деятельности служб безопасности являются комплексные и специальные планы.

Функция организации состоит определении порядка и условий функционирования службы информационной безопасности. Это процесс объединения сил и средств для достижения поставленных целей. Такой процесс состоит из следующих элементов:

1. определение рациональных форм разделения труда;
2. распределение работ среди работников, групп работников;
3. разработка структуры органов управления;
4. регламентация функций, подфункций, работ, операций. Такую регламентацию следует проводить, начиная последовательно с функций и заканчивая операциями. Отражать их необходимо в Уставе;
5. подбор и расстановка кадров.

Воздействие руководителя на подчиненных несет характер административных, экономических, психологических и педагогических методов, средств и приемов.

Регулирование представляет собой «наладку» системы, приведение ее в нормальное рабочее состояние и необходимость в ней возникает в силу изменения внешних условий, либо из-за возникновения каких-то нарушений, «сбоев» в функционировании самой системы. Посредством этой функции достигается поддержание управляемых процессов в рамках, заданных программой, регламентом, планом.

Мотивация – это процесс побуждения сотрудников службы безопасности к деятельности для достижения целей самой службы и ее подразделений. Мотивация представляет собой совокупность сил, побуждающих сотрудника осуществлять деятельность с затратой определенных усилий, на определенном уровне старания и добросовестности, с определенной степенью настойчивости в направлении достижения определенных целей.

В основе любой теории мотивации лежат потребности человека, которые можно удовлетворить вознаграждениями. Причем выделяют внешние вознаграждения (заработная плата, премии и т.д.) и внутренние - чувство успеха при достижении цели, получаемое от самой работы.

Для практических целей достаточна типология с использованием трех типов мотивации:

I тип – сотрудники, ориентированные преимущественно на содержательность и общественную значимость труда;

II тип – преимущественно ориентированные на оплату труда и другие нетрудовые ценности;

III тип – сотрудники, у которых значимость разных ценностей сбалансирована.

Среди потребностей, которые обладают конкретными мотивационно-трудовыми значениями, можно выделить следующие:

— потребность в самоуважении (добросовестная трудовая деятельность независимо от контроля и оплаты труда ради положительного собственного мнения о себе как о человеке и работнике);

— потребность в самоутверждении (высокие количественные и качественные показатели в труде ради одобрения и авторитета, похвалы, положительное отношение со стороны коллектива и руководства);

— потребность в признании (направленность трудового поведения на доказательство своей профессиональной пригодности и способностей);

— потребность в самовыражении (высокие показатели в работе на основе творческого отношения к ней);

— потребность в активности (трудовая деятельность как самоцель, стремление к поддержанию через активность здоровья и самочувствия, целостности личности);

— потребность в стабильности (восприятие работы как способа поддержания существующего образа жизни, достигнутого достатка);

— потребность в общении (установка на трудовую деятельность вообще и частные фрагменты работы как условия и повод для человеческих контактов и знакомств; хорошая работа как основа и тема общения).

Перечисленные моральные потребности как мотивы к труду не могут заменить собой материальные планы и ожидания. Вот почему руководители службы безопасности должны использовать в своей деятельности все формы материального и морального стимулирования своих подчиненных, добиваясь высокой мотивации их труда.

Контроль состоит в процессе соизмерения (сопоставления) фактически достигнутых результатов с запланированными. Эффективная система контроля должна соответствовать следующим требованиям:

— контроль должен быть всеобъемлющим;

— контроль следует сосредоточить на результате;

— система контроля должна быть простой;

— контроль не может быть ни целенаправленным, ни нейтральным;

— контроль должен быть постоянным.

Отличительный признак управленческой деятельности по руководству людьми в том, что цели предприятия достигаются путем организации сложенной работы персонала. Субъектом управленческой деятельности является руководитель предприятия. Объектом – персонал, трудовая деятельность персонала, и отношения людей в организации.

Цель управленческой деятельности – обеспечение эффективности труда персонала. Эффективность труда сотрудников определяется результатом, выраженном в экономических и социальных показателях организации. Содержание экономических показателей функционирования организации зависит от ее назначения и сферы производства, например количество и качество выпускаемой и реализуемой продукции, производительность труда, сумма полученного дохода и т.д.

Социальными показателями являются: уровень образования, квалификации и профессионального мастерства сотрудников, состояние их здоровья, размер зарплаты, состояние трудовой дисциплины, текучесть кадров, условия труда быта и отдыха.

Средствами управленческой деятельности являются: устная речь, письменная речь, нормативные документы, средства стимулирования труда, технические средства передачи информации.

Деятельность руководителя носит сложный и интенсивный характер: постановка целей и задач, распределение заданий, инструктаж, проведение бесед, совещаний, переговоров, подготовка и принятие решений, контроль трудовой дисциплины, проверка выполнения заданий, мотивация труда, разрешение конфликтных ситуации.

Средствами управленческой деятельности являются: устная речь, письменная речь, нормативные документы, средства стимулирования труда, технические средства передачи информации.

Деятельность руководителя носит сложный и интенсивный характер: постановка целей и задач, распределение заданий, инструктаж проведение бесед, совещаний, переговоров, подготовка и принятие решений, контроль трудовой дисциплины, проверка выполнения заданий, мотивация труда, разрешение конфликтных ситуации.

Большая часть этих действий – управляющие действия – прямая связь, руководитель должен получать и обратную связь: поступление информации о результатах труда персонала. На основе этого руководитель разрабатывает новые управленческие решения и воздействия. Для осуществления обратной связи необходим систематический контроль работы персонала, сбор и обработка информации об основных показателях деятельности коллектива.

Одним из основных показателей организаторской деятельности является состояние коллектива и каждого работника.

При умелой и качественной организации труда коллектив развивается и улучшается его социальная структура, социально-психологический климат, самочувствие, настроение, возрастает трудовая активность людей.

Достичь подобного результата возможно, применив подходящие методы управления.

Методы управления – это способы осуществления управленческих воздействий на персонал для достижения целей управления организацией.

Различают: экономические, административно-правовые и социально-психологические методы управления, которые отличаются способами и результативностью воздействия на персонал.

Экономические методы управления – это система приемов и способов воздействия на исполнителей с помощью конкретного соизмерения затрат и результатов.

В качестве основных методов управления здесь выступает система заработной платы и премирования, которая должна быть максимально связана с результатами деятельности исполнителя. Оплату труда целесообразно связать с результатами его деятельности в сфере ответственности или с результатами деятельности всей фирмы.

Экономические методы управления базируются на действии экономических механизмов мотивации и стимулирования активной производственной деятельности.

К экономическим методам управления, применяемым на уровне страны, относятся:

— налоговая система страны;

— кредитно-финансовый механизм.

К экономическим методам, которые применяются на уровне организации, фирмы, учреждения и т.п., относятся:

— система заработной платы и других форм материального поощрения работников;

— система ответственности с соответствующим применением вознаграждений и санкций за качество и эффективность работы;

— система стимулирования инновационной деятельности, направленной на повышение эффективности деятельности данной организации и повышение качества ее продукции.

Социальными показателями являются:

— уровень образования, квалификации и профессионального мастерства сотрудников;

— состояние их здоровья;

— размер зарплаты;

— состояние трудовой дисциплины;

— текучесть кадров;

— условия труда быта и отдыха.

Для успешного выполнения этой политики необходимо реализовать стратегию безопасности предприятия, под которой понимается совокупность наиболее значимых решений, направленных на обеспечение приемлемого уровня безопасности функционирования образовательной организации.

Необходимо комплексное и системное применение методов управления службой защиты информации.

Политика безопасности предприятия – это общие ориентиры для действий и принятия решений, которые облегчают достижение целей. Таким образом для установления этих общих ориентиров необходимо первоначально сформулировать цели обеспечения безопасности предприятия (общая цель нами уже определена ранее). Такими целями могут быть:

— укрепление дисциплины труда и повышение его производительности;

— защита законных прав и интересов предприятия;

— укрепление интеллектуального потенциала предприятия;

— сохранение и приумножение собственности;

— повышение конкурентоспособности производимой продукции;

— максимально полное информационное обеспечение деятельности предприятия и повышение его эффективности;

— ориентация на мировые стандарты и лидерство в разработке и освоении новой технологии и выпускаемой продукции;

— выполнение производственных программ;

— оказание содействия управленческим структурам в достижении целей предприятия;

— недопущение зависимости от случайных и недобросовестных деловых партнеров.

С учетом вышеизложенного можно определить следующие общие ориентиры для действий и принятия решений, которые облегчают достижение этих целей:

— сохранение и наращивание ресурсного потенциала;

— проведение комплекса превентивных мероприятий по повышению уровня защищенности собственности и персонала предприятия;

— включение в деятельность по обеспечению безопасности предприятия всех его сотрудников;

— профессионализм и специализация персонала предприятия;

— приоритетность несиловых методов предотвращения и нейтрализации угроз.

Выделяются следующие типы стратегий безопасности:

— ориентированные на устранение существующих или предотвращение возникновения возможных угроз;

— нацеленные на предотвращение воздействия существующих или возможных угроз на предмет безопасности;

— направленные на восстановление (компенсацию) наносимого ущерба.

Первые два типа стратегий предусматривают такую деятельность по обеспечению безопасности, в результате которой не происходит угрозы либо создается заслон ее влиянию. В третьем случае ущерб допускается (возникает), однако он компенсируется действиями, которые предусматривает соответствующая стратегия. Совершенно очевидно, что стратегии третьего типа могут разрабатываться и реализовываться применительно к ситуациям, где ущерб восполним, либо тогда, когда нет возможности осуществить какую-либо программу реализации стратегий первого или второго типа.

1.1. Угрозы информационной безопасности в образовательной организации

Информационная безопасность образовательного учреждения представляет собой комплекс мер различного характера, направленных на реализацию двух основных целей.

Первой целью является защита персональных данных и информационного пространства от несанкционированных вмешательств, хищения информации и изменения конфигурации системы со стороны третьих лиц.

Вторая цель ИБ – защита учащихся от любых видов пропаганды, рекламы, запрещенной законом информации.

Информационная безопасность в современной образовательной среде в соответствии с действующим законодательством предусматривает защиту сведений и данных, относящихся к следующим трем группам:

— персональные данные и сведения, которые имеют отношения к учащимся, преподавательскому составу, персоналу организации, оцифрованные архивные документы;

— обучающие программы, базы данных, библиотеки, другая структурированная информация, применяемая для обеспечения учебного процесса;

— защищенная законом интеллектуальная собственность.

Действия злоумышленников могут привести к хищению указанных данных. Также при несанкционированном вмешательстве возможны внесения изменений и уничтожение хранилищ знаний, программных кодов, оцифрованных книг и пособий, используемых в образовательном процессе.

Спецификой обеспечения информационной безопасности в образовании является состав характерных угроз. К ним относится не только возможность хищения или повреждения данных хакерами, но также деятельность обучающихся. Подростки могут сознательно или ненамеренно повредит оборудование или заразить систему вредоносными программами.

Угрозам намеренного или ненамеренного воздействия могут подвергаться следующие группы объектов:

— компьютерное и другое оборудование образовательной организации, в отношении которого возможны воздействия вредоносного ПО, физические и другие воздействия;

— программное обеспечение, применяемое в учебном процессе или для работы системы;

— данные, которые хранятся на жестких дисках или портативных носителях;

— подростки, которые могут подвергаться стороннему информационному воздействию;

— персонал, поддерживающий работу ИТ-системы.

Угрозы информационной безопасности образовательного учреждения могут носить непреднамеренный и преднамеренный характер. К угрозам первого типа относятся:

— аварии и чрезвычайные ситуации – затопление, отключение электроэнергии и т. д.;

— программные сбои;

— ошибки работников;

— поломки оборудования;

— сбои систем связи.

Особенностью непреднамеренных угроз является их временное воздействие. В большинстве случаев результаты их реализации

предсказуемы, достаточно эффективно и быстро устраняются подготовленным персоналом.

Намного более опасными являются угрозы информационной безопасности намеренного характера. Обычно результаты их реализации невозможно предвидеть. Намеренные угрозы могут исходить от учащихся, персонала организации, конкуренты, хакеры. Лицо, осуществляющее преднамеренное воздействие на компьютерные системы или программное обеспечение, должно быть достаточно компетентным в их работе. Наиболее уязвимыми являются сети с удаленным в пространстве расположением компонентов. Злоумышленники могут достаточно легко нарушать связи между такими удаленными компонентами, что полностью выводит систему из строя.

Существенную угрозу представляет хищение интеллектуальной собственности и нарушение авторских прав. Также внешние атаки на компьютерные сети образовательной организации могут предприниматься для воздействия на сознание детей. Наиболее серьезная угроза – возможность вовлечения детей в криминальную или террористическую деятельность.

Для хищения данных, создания нарушений в работе информационной системы и для других действий требуется несанкционированный доступ. Различают следующие виды несанкционированного доступа:

Человеческий. Предусматривает хищение сведений методом их отправки по электронной почте или копирования на портативные носители, внесение вручную изменений в базы данных при наличии физического доступа к серверу.

Аппаратный. Применение специального оборудования для хищения данных или внесения изменений в систему. В том числе может применяться оборудование для перехвата электромагнитных сигналов.

Программный. Применение специального программного обеспечения для перехвата данных, копирования паролей, дешифровки и перенаправления трафика, внесения изменений в функционирование другого софта и т. д.

Выводы по первой главе

Служба защиты информации является самостоятельным структурным подразделением, подчиненным непосредственно руководителю и заместителю по безопасности. При наличии в организации службы безопасности служба защиты информации входит в ее структуру.

Назначение и освобождение от должности руководителя службы защиты информации производятся руководителем организации с письменного согласия ведомственного отдела защиты информации. Там

же до приема дел вновь назначенный руководитель и его заместитель должны пройти инструктаж. Руководитель службы защиты информации обязан организовывать и систематически проводить учебу работников службы и уполномоченных по защите информации в целях повышения деловой квалификации, уровня знаний и приобретения практических навыков по реализации, возложенных на службу защиты информации задач.

При умелой и качественной организации труда коллектив развивается и улучшается его социальная структура, социально-психологический климат, самочувствие, настроение, возрастает трудовая активность людей.

Достичь результата возможно, применив методы управления, они бывают: экономические, административно-правовые и социально-психологические методы управления, которые отличаются способами и результативностью воздействия на персонал.

Само управленческое воздействие, в свою очередь, реализуется в форме таких функций управления, как прогнозирование, планирование, организация, регулирование, мотивация и контроль.

Информацию, которую необходимо защищать в образовательной организации, условно можно разделить на несколько классов:

— персональные данные студентов, педагогического состава и персонала;

— исследования, научные работы и интеллектуальная собственность организации;

— информация образовательного учреждения, обеспечивающая образовательный процесс.

Создание службы информационной безопасности в образовательной организации и грамотное управление ей необходимы для защиты от существующих угроз безопасности, которые характерны для образовательных организаций.

Образовательная организация чаще всего подвержена угрозам преднамеренного характера, которые могут быть реализованы как внутри, так и вне организации. Преднамеренные угрозы являются более опасными так как результаты их реализации невозможно предвидеть. Чаще всего они могут исходить от любого субъекта учебного процесса (студент, сотрудник, обслуживающий персонал), но иногда от сторонних субъектов (конкуренты, хакеры).

Вышеперечисленные угрозы встречаются чаще всего в образовательных организациях и являются потенциально опасными, принося существенный материальный и нематериальный ущерб для организации в целом.

ГЛАВА 2. Организация и управление службой информационной безопасности в ГБПОУ «Южно-Уральский Государственный Технический Колледж»

2.1. Характеристика объекта ГБПОУ «ЮУрГТК»

Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный технический колледж»

(ГБПОУ «ЮУрГТК») главный корпус располагается по адресу 454007, г. Челябинск, ул. Горького, 15.

ГБПОУ Южно-Уральский государственный технический колледж создан в 1940 г. как строительный техникум при заводе металлоконструкций им. С. Орджоникидзе в городе Верхняя Салда. В 1941 г. техникум переезжает в г. Челябинск. После многочисленных переименований 7 сентября 2010 г. создается новое учебное заведение – Южно-Уральский государственный технический колледж (ЮУрГТК) в результате реорганизации Челябинского монтажного колледжа, Челябинского политехнического техникума и Челябинского машиностроительного техникума.

ЮУрГТК имеет следующую структуру 4 корпуса: Монтажный комплекс (корпус № 1-2) – ул. Горького, 15 и ул. Грибоедова, 45, Машиностроительный комплекс – ул. Марченко, 33, Политехнический комплекс – ул. Гагарина, 7.

Колледж реализует основные программы профессионального обучения (программы профессиональной подготовки по профессиям рабочих, должностных служащих, программы переподготовки рабочих, служащих, программы повышения квалификации рабочих, служащих).

Колледж сохраняет традицию подготовки специалистов технического профиля, причем доля технических специальностей неуклонно растет.

Колледж осуществляет подготовку по 5 направлениям: подготовка специалистов для строительной отрасли, для предприятий машиностроения, подготовка специалистов связи, специалистов в области информационных технологий, специалистов в сфере землеустройства

В ЮУрГТК существуют следующие отделения:

— архитектурно-строительное,

— экономики и инфраструктуры,

— электромонтажное,

— информационных технологий и сервиса,

— машиностроительное,

— заочное.

ФГБОУ «Южно-Уральский государственный технический колледж» осуществляет свою деятельность на основании следующих документов:

1. Федеральные закон «Об образовании в Российской Федерации» от 29.12.2012 г., № 273.

2. Приказ от 14.06.2013 № 464 «Об утверждении порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования»,

3. Приказ от 18.04.2012 № 291 «Об утверждении положения о практике студентов, осваивающих образовательные программы среднего профессионального образования»,

4. Приказ Министерства образования и науки Российской Федерации от 16.08.2013 г. № 968 «Об утверждении порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования»,

5. Лицензия на право осуществления образовательной деятельности № 11440 от 19.05.2015 г.,

6. Устав ГБПОУ ЮУрГТК – определяет общие положения, основные направления деятельности колледжа, структуру и компетенции органов управления учреждения, содержит сведения о финансовой и хозяйственной деятельности учреждения, порядок реорганизации и ликвидации учреждения.

7. Федеральные государственные образовательные стандарты (ФГОС) по направлениям подготовки.

8. Локальные нормативные акты.

9. Образовательные программы.

10. Учебные планы.

11. Календарные учебные графики.

12. Программы учебных дисциплин и профессиональных модулей.

Колледж обладает достаточной учебно-материальной базой для качественного осуществления образовательного процесса: общее количество объектов недвижимости – 56, общая площадь –59596 кв.м.

Для обеспечения учебного процесса рабочие станции подключены к сети Интернет. Создана корпоративная сеть на основе оптоволокна. Для решения производственных и учебных задач в колледже организована локальная сеть на одновременную работу 650 компьютеров. Все персональные компьютеры оснащены лицензионным программным обеспечением, подключены к локальной сети и имеют доступ в сеть Интернет, через защищенное соединение. В каждом комплексе имеется своя локальная сеть (100/1000 Мбит/с), охватывающая учебные корпуса и общежития. В комплексах все компьютеры подключены к сети Интернет со скоростью доступа до 100 Мбит/с.

Колледж обладает достаточной учебно-материальной базой для качественного осуществления образовательного процесса.

Учебные лаборатории оснащены учебно-лабораторными стендами и другим лабораторным оборудованием, обеспечивающим выполнение лабораторных работ и практических занятий, предусмотренных основными профессиональными образовательным программами. Специальные технические средства обучения коллективного и индивидуального пользования для инвалидов и лиц с ОВЗ имеются. Применяется электронное обучение с применением дистанционного образования система moodle, dom.sustec.ru, e. lanbook.ru

Ведущую роль в обеспечении образовательного процесса источниками учебной информации играет библиотека колледжа. В структуре библиотеки монтажного комплекса есть автоматизированная зона для самостоятельной работы студентов. Все рабочие места библиотекарей автоматизированы. Библиотека оснащена принтерами,

сканерами, копировальной техникой. В библиотеках всех комплексов внедрена автоматизированная информационно-библиотечной система 1С библиотека, которая позволила решить задачу сплошной компьютеризации библиотек, начиная от ввода библиографической записи в электронный каталог до использования технологии электронной книговыдачи.

Учебно-производственные мастерские и полигоны оснащены необходимым учебно-производственным оборудованием, вспомогательным оборудованием, инструментом и расходными материалами, необходимыми для организации и проведения учебных практик студентов, в том числе и для получения квалификации по рабочей профессии. Преподавателями ЮУрГТК разработано более 2000 электронных образовательных курсов, размещенных в системе дистанционного обучения колледжа dom.sustec.ru.

При входе в систему дистанционного обучения пользователь авторизуется, используя логин и пароль, применяемый для работы в сети колледжа. Инструкция для студентов по работе в СДО размещена в курсе «Работа студентов на платформе».

Система управления ГБПОУ «ЮУрГТК», обеспечивающая реализацию образовательных программ, являющихся основной целью деятельности учреждения, отвечает требованиям действующего законодательства Российской Федерации и Челябинской области. Организационная структура управления ГБПОУ «ЮУрГТК» (рисунок 1).

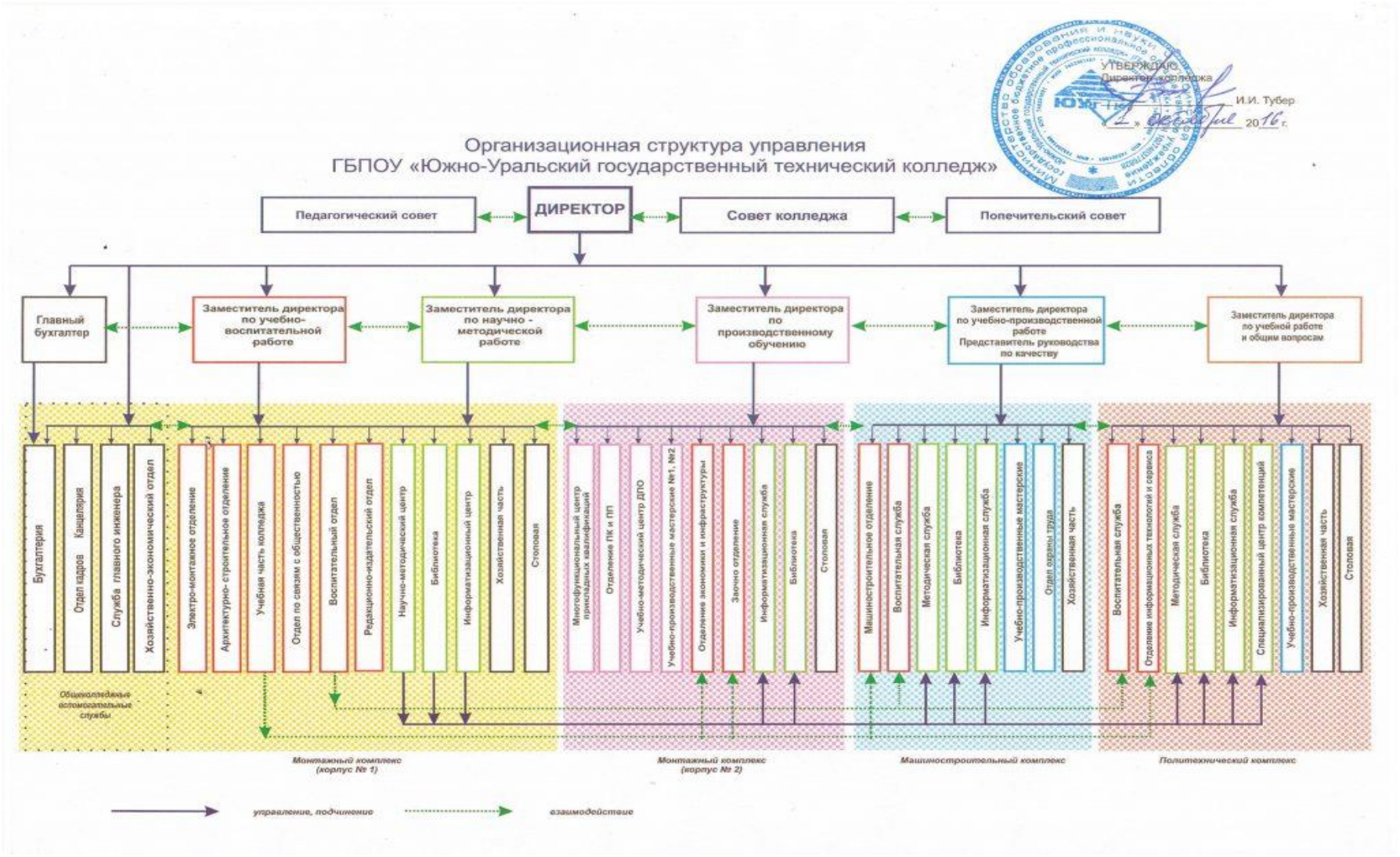

Рисунок 1 – Организационная структура управления ГБПОУ «ЮУрГТК»

В ГБПОУ «ЮУрГТК» используются следующие меры по защите информации.

Все сотрудники и педагогический состав работают по трудовому договору, который включает себя приложение по сохранению персональных данных.

Вход в здание осуществляется по пропускам через пункт охраны. Получение ключей от помещений осуществляется через регистрацию получения ключа в журнале регистрации получения и сдачи ключей от помещений на вахте после предъявления пропуска в здание.

Все помещения оборудованы системами противопожарной сигнализации.

Осуществляется идентификация и аутентификация пользователей. Существует разграничение прав доступа. Доступ в информационные системы (ИС) колледжа разрешен только зарегистрированным пользователям. Каждому пользователю настроены соответствующие его должности права доступа на различные объекты ИС. Перечень объектов и субъектов доступа определяется на основе прав, которые определены для каждого пользователя ИС. Защита доступа к ресурсам осуществляется при помощи пароля.

Информационная система колледжа содержит огромное количество информационных ресурсов, зафиксированных на материальных носителях, которые, в свою очередь, являются основным объектом защиты.

Перечень конфиденциальной информации (включая персональные данные):

1) *сведения о компаниях-клиентах*:

— протоколы переговоров;

— технические задания;

— результаты тестирования сотрудников;

— состав обучающих программ;

— результаты обучения сотрудников;

— персональные данные сотрудников компаний-клиентов (фамилия, имя, отчество сотрудника, год, месяц, дата рождения, личный электронный адрес, внутренний телефон в компании, личный мобильный телефон, сведения об пройденных обучающих программах, сведения о предпочтениях в области обучения, сведения о предыдущем месте работы, результаты тестирования в процессе обучения);

2) *сведения об управлении компанией*:

планы развития;

управленческие решения;

3) *конфиденциальные договоры с клиентами*;

4) *данные об уровне заработной платы сотрудников*;

5) *персональные данные сотрудников и обучающихся*:

— фамилия, имя, отчество сотрудника;

— год, месяц, дата рождения;

— место рождения;

— место регистрации;

— место проживания;

— паспортные данные;

— семейное положение;

— образование;

— уровень дохода;

— сведения о предыдущем месте работы;

— сведения о состоянии здоровья;

6) *стоимость обучающих программ*;

7) *бухгалтерская отчетность*;

8) *налоговая отчетность.*

Организационные и технические меры защиты.

1. Идентификация и аутентификация субъектов и объектов доступа осуществляется встроенными средствами MS Windows. Защита

обратной связи при вводе информации, используемой для аутентификации, осуществляется при помощи сокрытия ее посредством специальных символов.

2. Управление доступом субъектов к объектам доступа. Пользователи и администраторы ИС имеют различные обязанности и наделены разными правами.

3. Обеспечение целостности информационной системы и информации.

4. Контроль установки обновлений программного обеспечения (ПО) – установка обновлений ПО осуществляется в соответствии с утвержденным расписанием.

В качестве антивирусного программного обеспечения используется программный продукт Kaspersky Security.

Ограничение прав пользователей на просмотр, редактирование и ввод данных в информационную систему – ограничение прав пользователей информационной системы осуществляется при помощи встроенных средств ПО.

Контроль над ошибочными действиями пользователей при осуществлении операций ввода, редактирования, удаления или передачи конфиденциальной информации осуществляется сотрудниками в ручном режиме.

1. Защита от несанкционированного физического доступа к средствам обработки информации и средствам обеспечения функционирования информационной системы осуществляется посредством пропускного режима в здания и доступа к ключам от кабинетов посредством предъявления пропуска и регистрации получения ключа в журнале регистрации получения и сдачи ключей от помещений.

2. Защита от внешних воздействий (воздействий окружающей среды и иных внешних факторов) осуществляется посредством

применения систем пожарной сигнализации и источников бесперебойного питания.

Информацию, которую необходимо защищать в образовательной организации, условно можно разделить на несколько классов:

— персональные данные студентов, педагогического состава и персонала;

— исследования, научные работы и интеллектуальная собственность организации;

— информация образовательного учреждения, обеспечивающая образовательный процесс.

Эти данные могут попасть в поле зрения злоумышленников и стать целью атак. Статистика показывает, что мошеннические действия направлены не только на хищение личной информации, но и на вмешательство в финансовую сферу организации. Последствия таких проникновений могут варьироваться от хищения научных исследований до изменения работы всей структуры.

Однако не все угрозы могут исходить извне. Сами студенты также могут стать источником ряда проблем. Случайно или намеренно от действий учащихся могут быть повреждены компьютерные системы или целые массивы данных.

Основные угрозы.

Облачная безопасность. Сегодня образовательные организации используют облачные платформы для связи со студентами, чтобы упростить распространение учебных ресурсов. В этом случае значительная часть персональных, финансовых и операционных данных хранятся не на сервере организации, а на стороннем ресурсе. Кроме того, все устройства «Интернета вещей», используемые в сочетании с облачными технологиями, еще больше расширяют карту угроз.

Распределенный отказ в обслуживании (DDoS). DDoS-атаки наносят вред сети, отправляя в систему драматический поток запросов.

Использование брандмауэров, антивирусного и другого специализированного программного обеспечения может помочь свести к минимуму вероятность DDoS-атаки. Тестирование на проникновение поможет выявить пробелы в этом направлении.

Вредоносное программное обеспечение (ПО). Программы-вымогатели, вирусы, троянцы и рекламное ПО относятся к категории вредоносных программ. Целесообразно потребовать и проверить, чтобы студенты установили на свои устройства новейшее антивирусное программное обеспечение до подключения к университетской сети. Вредоносное ПО может привести к остановке операций, а также к вымогательству или мошенничеству со стороны злоумышленников.

Фишинг. Фишинговые электронные письма печально известны из-за своей способности преодолевать эшелонированную систему защиты. Сложность борьбы с ними в учебных заведениях возникает, когда злоумышленники подделывают реальные адреса электронной почты. Студенты и преподаватели переходят по вредоносным ссылкам и позволяют злоумышленнику получить доступ для всей системы. Повышение осведомленности сотрудников и учащихся служит одним из лучших способов защиты от фишинга наряду с использованием специального программного обеспечения, которое может идентифицировать мошеннические электронные письма или предупреждать пользователей о том, что письмо подозрительное.

2.2. Организация управления службой информационной безопасности в ГБПОУ «ЮУрГТК»

В силу специфики деятельности образовательной организации ГБПОУ «ЮУрГТК» была определена наступательная стратегия по информационной безопасности из-за больших объёмов обрабатываемой конфиденциальной информации и размера организации. Отделом бухгалтерии была проведена оценка информации. Стоимость ущерба от потери информации составляет около 3 млн. рублей.

Ниже приведены профильные наработки, которые позволяют обеспечить систему защиты персональных данных.

В качестве *административно-организационных мер* управления информационной безопасностью следует разработать, методические пособия и инструкций, которые будут регламентировать работу с персональными данными. Кроме пособий и инструкций будут включены дополнения в должностные инструкции преподавателей и всего административного персонала, с помощью которых руководство организации сможет контролировать весь процесс работы с информацией.

Нормативно-правовой способ обеспечения информационной безопасности направлен на то, чтобы предотвращать агрессивное воздействие сторонней информации на разум подростка. Ключевым инструментом для обеспечения такого рода защиты будет «Национальная стратегия действий в интересах детей».

— конфиденциальная информация;

— персональные данные;

— коммерческая и служебная тайна.

Для обеспечения всех вышеупомянутых интересов студентов и преподавателей необходимо разработать методику, обеспечивающую

защиту данных. При составлении такого рода документа необходимо руководствоваться основными законодательными актами Российской Федерации, а именно Трудовым кодексом, Гражданским кодексом, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и действующими стандартами.

Морально-этические средства обеспечения информационной безопасности. В сфере обеспечения информационной безопасности в образовательной организации важны вопросы морали и этики. Центральным документом является Федеральный закон от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации», который позволяет оградить несовершеннолетних от пропаганды, незаконной, нетактичной и аморальной информации. Такая система мер предусматривает тщательный контроль посещений определенного рода интернет-страниц, площадок и ресурсов.

Для создания нравственного микроклимата в образовательном учреждении необходимо создать ряд правил и внедрить специализированные программы, которые будут собирать опасные источники и сайты.

К физическим мерам относятся мероприятия по проверке физических лиц на предмет наличия запрещенных предметов можно отнести организацию доступа к тем или иным информационным ресурсам, а также обеспечение доступа к информации путем установления надежных паролей и регулярной их замены.

Технические меры. Существуют специализированные программные продукты, цель которых заключается в выявлении и борьбе со всевозможными угрозами безопасности. К таким программам можно отнести DLP-системы и SIEM-системы. С помощью этих инструментов можно обеспечить комплексную защиту данных от преднамеренного вмешательства. Однако, в связи с недостаточным финансированием,

данное решение является дорогостоящим программным обеспечением. В этом случае общая рекомендация заключается в использовании, лицензированных антивирусов. Но необходимо помнить, что этого недостаточно.

Необходимо контролировать электронную почту сотрудников и учащихся и устанавливать специальные спам-фильтры. Для профилактики руководство может полностью ограничить доступ к данным, которые находятся на жестких дисках компьютеров. В дополнение, образовательное учреждение может установить программное обеспечение, которое будет не допускать посещение сайтов с определенным контентом, например, пропагандистские и экстремистские сайты.

Проведя анализ СЗИ колледжа, можно выделить основные направления совершенствования существующей СЗИ:

В рамках подсистемы организационной безопасности необходимо: усилить защиту информационных объектов; усилить режим допуска на объект; организовать систему допуска к конфиденциальной информации., ограничить доступ сотрудников отдела в интернет.

В рамках правовых мер необходимо: добавить документ, в котором прописан допуск сотрудников организации к той или иной конфиденциальной информации.

В рамках подсистемы компьютерной безопасности необходимо: систематически внедрить антивирусное обеспечение на автоматизированные рабочие места; внедрить систему защиты от несанкционированного доступа на автоматизированные рабочие места; внедрить систему защиты от несанкционированного доступа в локально-вычислительную сеть, реализующую систему идентификации и аутентификации.

В рамках подсистемы физической защиты предложено усилить контроль допуска в образовательную организацию.

Синергия этих мер позволит защитить компьютерные системы организации не только от намеренных действий злоумышленников, но и от случайных действий обучающихся.

Для обеспечения работоспособности разработанной системы защиты информации необходимо создать специальный отдел в составе организации, занимающийся данными вопросами – Службу защиты информации (СЗИ).

Начальник СЗИ является новой штатной единицей. На эту должность необходимо взять профессионала и специалиста в области защиты информации, а также хорошо знающего юридическую сторону этой проблемы, имеющего опыт руководства и координации работы подобных служб.

Требования:

— высшее профессиональное образование;

— стаж работы в области защиты информации не менее 5 лет;

— хорошее знание законодательных актов в этой области и принципов планирования защиты.

Руководитель СЗИ должен выполнять следующие функции:

— вырабатывать политику обеспечения защиты информации и обеспечивать ее реализацию;

— отвечать за функционирование СЗИ и обеспечение защиты конфиденциальной информации;

— осуществлять планирование и непосредственное руководство работой СЗИ;

— нести персональную ответственность за выполнение службой возложенных на нее задач, за неукоснительное исполнение подчиненными своих должностных обязанностей и правил внутреннего трудового распорядка;

— принимать личное участие в проведении наиболее сложных мероприятий по обеспечению защиты информации в компании;

— разрабатывать планы действий в чрезвычайных ситуациях;

— проводить регулярную учебу с подчиненными;

— руководить проведением служебных расследований;

— организовывать взаимодействие СЗИ с другими подразделениями;

— разрабатывать инструкции по работе с коммерческой тайной для персонала, допущенного к работе с документами, ее содержащую;

— организовывать разработку рекомендаций по совершенствованию функционирования СЗИ;

— осуществлять руководство отделом охраны;

— кроме того, выполнять функции юриста: разрабатывать, вести и обновлять основополагающие документы с целью закрепления в них требований обеспечения безопасности и защиты конфиденциальной информации.

Для работы СЗИ необходимо подготовить ряд нормативных документов:

— положение о СЗИ;

— инструкцию по безопасности конфиденциальной информации;

— перечень сведений составляющих конфиденциальную информацию;

— инструкцию по работе с конфиденциальной информацией;

— должностные инструкции сотрудников СЗИ;

— инструкцию по обеспечению пропускного режима в компании;

— памятку работнику о сохранении конфиденциальной информации.

Для обеспечения полноценной организационной и правовой защиты информации необходимо разработать пакет документов, включающий в себя:

— положение о конфиденциальной информации организации;

— перечень документов предприятия, содержащих конфиденциальную информацию;

— инструкция по защите конфиденциальной информации в информационной системе предприятия;

— предложения по внесению изменений в устав организации;

— предложения по внесению изменений в трудовой договор, контракт с руководителем и коллективный договор;

— соглашение о неразглашении персональных данных сотрудником;

— обязательство сотрудника о неразглашении конфиденциальной информации предприятия при увольнении;

— предложения о внесении изменений в правила внутреннего распорядка предприятия (в части регламентации мер физической защиты информации и вопросов режима);

— предложения о внесении изменений в должностное (штатное) расписание предприятия (штат службы защиты информации);

— предложения о внесении дополнений в должностные инструкции всему персоналу;

— ведомость ознакомления сотрудников с положением о конфиденциальной информации и инструкцией по защите конфиденциальной информации в ИС организации;

— план проведения занятий с персоналом по сохранению и неразглашению конфиденциальной информации.

Эти документы играют важную роль в обеспечении безопасности организации.

2.3. Экспертная оценка эффективности организации и управления службы информационной безопасности в ГБПОУ «ЮУрГТК»

Для оценки эффективности внедрения новшеств в систему информационной безопасности была использована экспертно-табличная методика оценки эффективности. Экспертами выступили сотрудники службы информационной безопасности ГБПОУ «ЮУГК», ответственные за различные аспекты обеспечения информационной безопасности колледжа.

Была проведена оценка следующих подсистем СЗИ:

1. подсистема административно-организационных мер защиты информации;
2. подсистема правовой защиты информации;
3. подсистема компьютерной безопасности;
4. подсистема физической защиты информации;

Для каждой из перечисленных подсистем будут определены целесообразные мероприятия по защите информации и на основе экспертных оценок проставлена оценка по вероятностной шкале, представленная в таблице 2.

0 - вероятность защиты информации равна нулю;

1 - вероятность защиты информации достигаема;

2 - вероятность защиты информации достигаема;

3 - вероятность защиты информации достигаема;

4 - вероятность защиты информации достигаема;

5 - вероятность защиты информации достигаема;

4,5 - 5 - требуемый уровень защиты, исходя из принятой стратегии по информационной безопасности.

Таблица 2 – Экспертная оценка эффективности подсистем СЗИ

Подсистемы СЗИ и меры по защиты информации	Экспертные оценки эффективности (вероятность защиты информации) первого эксперта	Экспертные оценки эффективности (вероятность защиты информации) второго эксперта	Экспертные оценки эффективности (вероятность защиты информации) третьего эксперта	Средняя итоговая оценка
Подсистема административно-организационных мер защиты информации	5	4	5	4,5
Подсистема правовой защиты информации	4	5	5	4,5
Подсистема компьютерной безопасности	5	5	5	5
Подсистема физической защиты информации	4	4	5	4,5
Всего:	-	-	-	4,5

По результатам таблицы 2 было построено обобщённое графическое представление полученных результатов эффективности СЗИ ГБПОУ «ЮУрГТК» (рисунок 2).

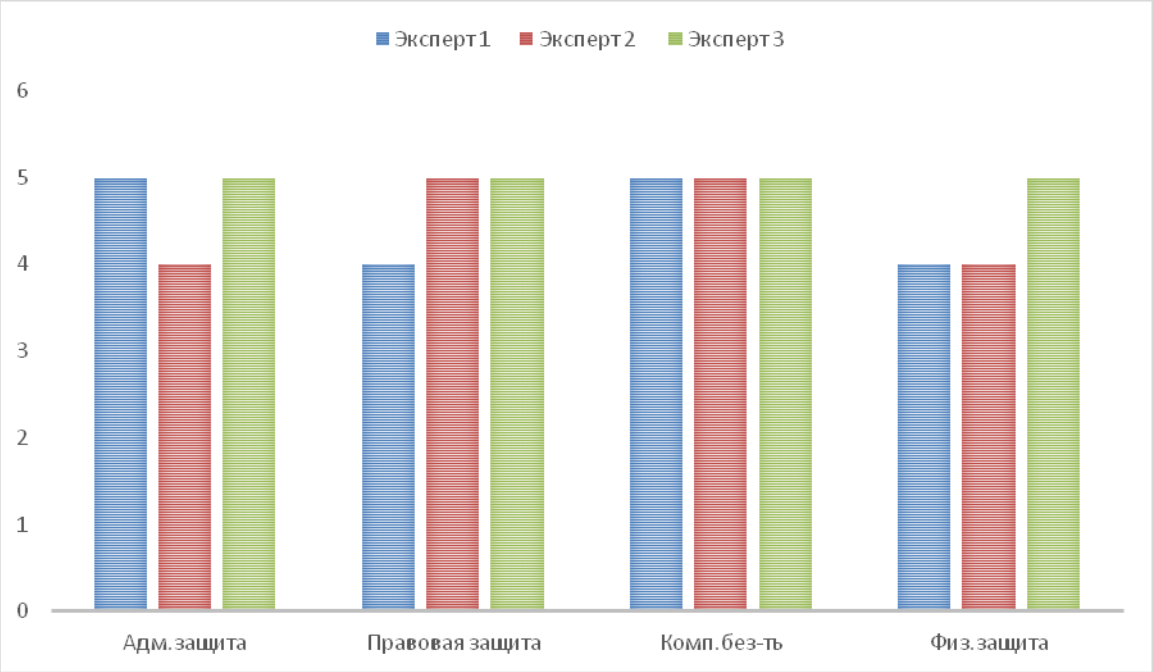

Рисунок 2 – Функциональная эффективность предложенных СЗИ ГБПОУ «ЮУрГТК»

Таким образом можно увидеть, что предложенные новшества в систему информационной безопасности ГБПОУ «ЮУрГТК» достигают требуемого уровня защиты, что подтверждено экспертной оценкой.

Выводы по второй главе

Во второй главе были выявлены существующие недочеты и предложены мероприятия по совершенствованию организации управления службой информационной безопасности колледжа.

В ходе исследования также удалось выяснить, что на данный момент в ГБПОУ «ЮУрГТК» отсутствует служба управления информационной безопасности как самостоятельное подразделение и всей работой занимаются системные администраторы.

Для обеспечения работоспособности разработанной системы защиты информации необходимо создать специальный отдел в составе организации, занимающийся данными вопросами – Службу защиты информации (СЗИ) и назначить ответственное лицо – начальника отдела. Начальник СЗИ должен являться профессионал в области защиты информации с высшим образованием и опытом работы в сфере защиты информации от 5 лет.

В ряд профильных наработок, которые позволят обеспечить систему защиты персональных данных, вошли: организационные методы, нормативно-правовые, морально-этические, физические и технические меры.

Основные направления совершенствования существующей СЗИ:

В рамках правовых мер необходимо: добавить документ, в котором прописан допуск сотрудников организации к той или иной конфиденциальной информации.

В рамках подсистемы компьютерной безопасности необходимо: систематически внедрить антивирусное обеспечение на автоматизированные рабочие места; внедрить систему защиты от несанкционированного доступа на автоматизированные рабочие места; внедрить систему защиты от несанкционированного доступа в локально-

вычислительную сеть, реализующую систему идентификации и аутентификации.

В рамках подсистемы физической защиты предложено усилить контроль допуска в образовательную организацию.

Была проведена оценка эффективности предложенных мероприятий. Для оценки эффективности внедрения новшеств в систему информационной безопасности была использована экспертно-табличная методика оценки эффективности. Экспертами выступили привлеченные специалисты службы информационной безопасности ГБПОУ «ЮУГК», ответственные за различные аспекты обеспечения информационной безопасности колледжа.

Следует отметить, что нет идеальной системы, которая будет обеспечивать защиту на 100 %, но предложенные новшества при внесении в систему информационной безопасности ГБПОУ «ЮУрГТК» достигают требуемого уровня защиты, что подтверждено экспертной оценкой.

ЗАКЛЮЧЕНИЕ

Из проведенной работы становится очевидно, что обеспечение информационной безопасности является комплексной задачей. Комплексная система защиты информации должна быть непрерывной, это обусловлено тем, что информационная среда является сложным многоплановым механизмом, в котором действуют такие компоненты, как электронное оборудование, программное обеспечение, персонал.

Информатизация общества несет в себе не только позитивные перемены, но и создает проблемы информационной безопасности, главные из которых – возникновение информационных войн и кибертерроризма. Эти проблемы носят глобальный характер, но вследствие геополитической и экономической ситуации приобретают особую остроту для России.

Для решения проблемы обеспечения информационной безопасности необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.

Данная работы направлена на изучение информационной безопасности в образовательной организации с учетом специфики деятельности, организационно-правовой формы, существующей и функционирующей системы организации управления службой информационной безопасности и прочих факторов.

В ходе выполнения магистерской диссертации, была раскрыта гипотеза исследования, заключавшаяся в предположении о повышении эффективности системы обеспечения информационной безопасности

образовательной организации при внедрении рекомендаций по ее совершенствованию.

В рамках этой гипотезы были решены поставленные задачи:

1. раскрыта сущность и содержание системы организации и управления информационной безопасностью в образовательной организации;
2. изучен объекта защиты ГБПОУ «Южно-Уральский государственный технический колледж», изучена структура, информационные ресурсы и информационные потоки колледжа; выявлены уязвимости в системе защиты информации.
3. разработаны рекомендации по организации и управлению службой информационной безопасности ГБПОУ «Южно-Уральский государственный технический колледж»;
4. проведена экспертная оценка предложенных рекомендаций по организации и управлению службой информационной безопасности колледжа ГБПОУ «Южно-Уральский государственный технический колледж».

В первой главе исследования проанализированы раскрыта сущность и содержание системы организации и управления информационной безопасностью в образовательной организации.

Во второй главе отражены результаты реализации эффективных методов организации и управления службой информационной безопасности ГБПОУ «ЮУрГТК».

Для оценки эффективности внедрения новшеств в систему информационной безопасности была использована экспертно-табличная методика оценки эффективности. Проведенное исследование подтвердило выдвинутую гипотезу.

Практическая значимость результатов, полученных в данной магистерской диссертации, заключаются в том, что они могут

использоваться в качестве базы исследовательской, аналитической и проектной деятельности авторов, изучающих тему методов управления информационной безопасности

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Александрова, А.В. Информационная безопасность и конституционные права личности/ А. В. Александрова, Е. И. Образумов // Наука.
2. Бабаш, А.В. Актуальные вопросы защиты информации: монография / А.В. Бабаш, — М.: РИОР: ИНФРА-М, 2017. — 111 ч
3. Бабаш, А.В. Информационная безопасность: Лабораторный практикум [Текст] / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.
4. Базелюк, Н. Г. Методы управления информационной безопасностью в организации/ Н. Г. Базелюк, А. В. Степанов // Евразийский союз ученых. – 2015. – № 4-13(13). – С. 65-67
5. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие [Текст] / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.
6. Баранова, Е.К. Основы информационной безопасности: учебник [Текст] / Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2019. — 202 с.
7. Белим, С.В. Проблемы построения политики безопасности при объединении информационных систем/ С. В. Белим, С. Ю. Белим // Математические структуры и моделирование. — 2018. — № 3. - С. 126-131
8. Белов, Е.Б. Основы информационной безопасности: учебное пособие для вузов/ Е.Б.Белов, В.П.Лось, Р.В.Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2016. – 544 с.

9. Белякова, Е.Г. Информационная культура и информационная безопасность школьников/ Е. Г. Белякова, Э. В. Загвязинская, А. И. Березенцева // Образование и наука. — 2017. — № 8. — С. 147-162.

10. Бондарев, В.В. Введение в информационную безопасность автоматизированных систем: учеб. пособие/ В.В. Бондарев. — Москва: Издательство МГТУ им. Н. Э. Баумана, 2016. — 250 с.

11. Габышева Н.В. Образовательный менеджмент: понятие и сущность // Материалы Всероссийской научно-практической конференции «Наука и социум». 2018. №7-1.

12. Гафнер, В. В. Информационная безопасность: учебное пособие/ В.В. Гафнер. - Рн/Д: Феникс, 2017. - 324 с.

13. Гельруд, Я.Д. Управление безопасностью подготовки кадров к работе с информационными и коммуникационными технологиями в информационном обществе/ Я.Д. Гельруд, С.А. Богатенков // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. — 2016. — № 3. — С. 40-51.

14. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие/ Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. - 64 с.

15. Государственная дума Федерального собрания Российской Федерации седьмого созыва Комитет по образованию и науке решение от 20 февраля 2018 года N 40-5 Развитие информатизации системы образования. Совершенствование законодательства в области электронного обучения и дистанционных образовательных технологий [Электронный ресурс]: URL: https://docs.cntd.ru/document/556985932 (дата обращения: 30.05.2022)

16. Грачева, Е.А. Информационная безопасность/ Е. А. Грачева // The Newman in Foreign Policy. — 2020. — № 54 (98) Vol. 3. — С. 57-59.

17. Гришина Н.В. Основы информационной безопасности предприятия: учебное пособие/ Н.В. Гришина. - Инфра-М., 2019. – 216 с.

18. Гультяева, Т. А. Основы информационной безопасности: учебное пособие/ Т. А. Гультяева. — Новосибирск: НГТУ, 2018. — 79 с.

19. Гущин, А. Н. Личностно-ориентированные информационные системы: учебное пособие / А. Н. Гущин. — Санкт-Петербург: БГТУ «Военмех» им. Д.Ф. Устинова, 2012. — 120 с.

20. Жарникова, Ю. С. Угрозы информационной безопасности образовательного учреждения / Ю. С. Жарникова. — Текст: непосредственный // Молодой ученый. — 2017. — № 11.2 (145.2). — С. 60-63. — URL: https://moluch.ru/archive/145/40613/ (дата обращения: 30.05.2022)

21. Жидко, Е.А. Информационная безопасность предприятия как необходимый фактор организации управления безопасностью труда / Е.А. Жидко, В.С. Муштенко // Научный вестник Воронежского государственного архитектурно-строительного университета. Серия: Высокие технологии. Экология. — 2014. — № 1. — С. 223-228.

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

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

24. Ильченко, Л.М. Расчет рисков информационной безопасности телекоммуникационного предприятия/ Л.М. Ильченко, Е.К. Брагина, И.Э. Егоров, С.И. Зайцев // Открытое образование, 2018. – С. 61-70.

25. Информационная безопасность образовательных учреждений [Электронный ресурс]: URL: https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdenij/ (дата обращения 13.03.2022)

26. Информационная безопасность: учебное пособие. — Пермь: ПГГПУ, 2018. — 87 с. — ISBN 978-5-85219-007-9. — Текст:

электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/129509 (дата обращения: 27.06.2022). — Режим доступа: для авториз. пользователей.

27. Ищейнов В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учебное пособие/ В. Я. Ищейнов, М. В. Мецатунян. — 2-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 216 с.

28. Ищейнов В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учебное пособие для студентов высших учебных заведений, обучающихся по специальностям «Организация и технология защиты информации» и «Комплексная защита объектов информатизации» / В. Я. Ищейнов, М. В. Мецатунян. — 2-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2017.

29. Киреева, Н. В. Аудит информационной безопасности: методические указания/ Н. В. Киреева, И. С. Поздняк, О. А. Караулова. — Самара: ПГУТИ, 2019. — 21 с.

30. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления: монография / И.С. Клименко. — Москва: ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/1137902 (дата обращения: 23.05.2022). – Режим доступа: по подписке.

31. Коджешау, М.А. Технологии и алгоритмы информационной безопасности / М.А. Коджешау // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. — 2017. — № 2. — С. 129-135.

32. Конкин, Ю. В. Основы информационной безопасности: учебное пособие/ Ю. В. Конкин, Ю. М. Кузьмин, В. Н. Пржегорлинский. — Рязань: РГРТУ, 2021. — 96 с.

33. Конституция Российской Федерации [Электронный ресурс]: (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2021) URL: http://www.consultant.ru/ (дата обращения 23.11.2021)

34. Крыжановский, А. В. Информационная безопасность: методические указания / А. В. Крыжановский, И. С. Поздняк. — Самара: ПГУТИ, 2018. — 38 с.

35. Леонтьев, А. С. Защита информации: учебное пособие / А. С. Леонтьев. — Москва: РТУ МИРЭА, 2021. — 79 с.

36. Логинова, А.О. Обзор нормативно-правовых источников и практик управления инцидентами информационной безопасности/ А. О. Логинова // Вестник СибГУТИ. — 2021. — № 1. — С. 50-59.

37. Лучинкина, А.И. Информационно-психологическая безопасность образовательной среды / А.И. Лучинкина // Научное мнение. — 2018. — № 1. — С. 73-78.

38. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации/ А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.

39. Маслова, М.А. Анализ и определение рисков информационной безопасности / М. А. Маслова // Научный результат. Информационные технологии. — 2019. — № 1. — С. 31-37. — ISSN 2518-1092.

40. Метод оценки экономической эффективности подразделения по защите информации [Электронный ресурс]: URL: https://lib.itsec.ru/articles2/Oborandteh/metod-ocenki-ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii (дата обращения 23.11.2020)

41. Минин, А.Я. Информационная безопасность в образовании/ А.Я. Минин // Наука и школа. — 2017. — № 1. — С. 29-36.

42. Моргунов, А. В. Информационная безопасность: учебно-методическое пособие/ А. В. Моргунов. — Новосибирск: НГТУ, 2019. — 83 с.

43. Мотивирование сотрудников на общую безопасность компании [Электронный ресурс]: URL: http://www.s-director.ru/magazine/magdocs/view/96.html# (дата обращения: 12.05.2021) — Текст : электронный.

44. Мызникова, Т. А. Основы информационной безопасности: учебное пособие / Т. А. Мызникова. — Омск: ОмГУПС, 2017. — 82 с.

45. Нестеров, С. А. Основы информационной безопасности: учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург: Лань, 2019. — 324 с. — ISBN 978-5-8114-4067-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/114688 (дата обращения: 15.05.2021). — Режим доступа: для авторизованных пользователей

46. Нормативное обеспечение эксплуатации средств защиты информации: учебное пособие/ А. В. Красов, И. И. Лившиц, Д. В. Юркин [и др.]. — Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 67 с.

47. Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс]: Указ Президента РФ от 05.12.2016 № 646 // URL: http://base.garant.ru/71556224/ (дата обращения 23.11.2020)

48. Обеспечение информационной безопасности организации [Электронный ресурс]: URL: https://iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/ (дата обращения 13.03.2022). – Текст: электронный

49. Петренко, В.И. Защита персональных данных в информационных системах. Практикум. Учебное пособие для вузов [Текст] / В.И. Петренко, И.В. Мандрица. - Лань Спб, 2020. – 108 с.

50. Поздняк, И. С. Управление информационной безопасностью: методические указания/ И. С. Поздняк, И. С. Макаров. — Самара: ПГУТИ, 2019. — 43 с.

51. Поздняк, И. С. Экспертные системы оценки информационной безопасности: методические указания/ И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара: ПГУТИ, 2019. — 23 с.

52. Поликарпов, А. В. Социально-философские аспекты проблемы информационной безопасности России: дис. ... канд. философ. наук. - М., 2000.- Режим доступа: https://www.dissercat.com/content/sotsialno-filosofskie-aspekty-problemy-informatsionnoi-bezopasnosti-rossii

53. Полякова А.А. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для академического бакалавриата и магистратуры: для студентов высших учебных заведений, обучающихся по юридическим направлениям и специальностям/ под ред. Т. А. Поляковой, А. А. Стрельцова. — Москва: Юрайт, 2017. — 324 с.

54. Постановление Правительства Российской Федерации № 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» URL: http://base.garant.ru/70252506/ (дата обращения 23.11.2020)

55. Постановление Правительства Российской Федерации № 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» URL: http://base.garant.ru/70252506/ (дата обращения 23.11.2020)

56. Привалов, А.Н. Методологические подходы к организации безопасной информационно-образовательной среды вуза/ А. Н. Привалов, Ю. И. Богатырева, В. А. Романов // Образование и наука. — 2017. — № 4. — С. 169-183.

57. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты». URL: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-

materialy/471-informatsionnoe-pismo-fstek-rossii-2 (дата обращения 23.11.2021)

58. Прокудин, Дмитрий Евгеньевич. Информационные технологии в образовании и их роль в формировании техногенной культуры: диссертация ... доктора философских наук: 24.00.01 / Прокудин Дмитрий Евгеньевич; [Место защиты: Санкт-Петербургский государственный университет]. - Санкт-Петербург, 2012. - 336 с.

59. Пугин, В. В. Защита информации в компьютерных информационных системах: учебное пособие/ В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара: ПГУТИ, 2018. — 119 с.

60. Резниченко, М.Г. Профессиональная успешность специалистов в сфере информационной безопасности/ М. Г. Резниченко, Е. А. Помельникова // Вестник Самарского университета. История, педагогика, филология. — 2019. — № 3. — С. 82-88.

61. Риск-модели информационной безопасности: учебное пособие / А. А. Корниенко, С. В. Корниенко, А. П. Глухов, М. Л. Глухарев. — Санкт-Петербург: ПГУПС, 2021. — 79 с.

62. Рыскулова Е.В. Проблема обеспечения информационной безопасности образовательных организаций в теории и практике педагогики / Е.В. Рыскулова // Вестник совета молодых ученых и специалистов Челябинской области. – 2020. Т. 2, № 4 (31). – с. 69-72

63. Санжаров, А.С. Методы оценки исследований информационной безопасности и компьютерных угроз / А.С. Санжаров, Ж.Т. Баранова // Известия Кыргызского государственного технического университета им. И.Раззакова. — 2018. — № 46. — С. 296-301.

64. Секлетова, Н. Н. Анализ рынка информационных систем и технологий: учебное пособие / Н. Н. Секлетова, А. С. Тучкова, О. И. Захарова. — Самара: ПГУТИ, 2018. — 215 с.

65. Серова А.Г. Анализ эффективности системы управления информационной безопасностью государственного учреждения. Экономика и управление. 2017;(6):71-74.

66. Скулябина, О. В. Системный анализ в информационной безопасности: учебное пособие/ О. В. Скулябина, С. Ю. Страхов. — Санкт-Петербург: БГТУ «Военмех» им. Д.Ф. Устинова, 2021. — 50 с.

67. Соколова, А.А. Информационно-образовательная среда и безопасность современной личности / А. А. Соколова, С. Н. Соколова, О. В. Пчелина // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. — 2020. — № 2. — С. 89-93.

68. Угрозы информации https://siblec.ru/telekommunikatsii/osnovy-informatsionnoj-bezopasnosti-v-telekommunikatsiyakh/10-ugrozy-informatsii

69. Управление информационной безопасностью в мире http://lib.itsec.ru/articles2/research/upravlenie-informacionnoi-bezopasnostu-v-mire Обеспечение информационной безопасности организации [Электронный ресурс]: URL: https://iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/ (дата обращения 13.03.2022). – Текст: электронный

70. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» URL: http://base.garant.ru/12148555/ (дата обращения 23.11.2020)

71. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». – Москва: Легион, 2022. – 144 с.

72. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» – Москва: Омега-Л, 2022. – 96 с.

73. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне». – Москва: Гросс-Медиа, 2022. – 16 с.

74. Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации». – Москва: Норматика, 2022. – 144 с.

75. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. — Москва: ФОРУМ: ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст: электронный. - URL: https://znanium.com/catalog/product/1189327 (дата обращения: 18.05.2021). – Режим доступа: по подписке

76. Шахворостов, Г.И. Актуальные направления совершенствования административного управления системой обеспечения информационной безопасности субъекта российской федерации: проблемы и предложения / Г. И. Шахворостов, А. И. Кустов, В. С. Самсонов, М. А. Жданов // Регион: системы, экономика, управление. — 2022. — № 1. — С. 28-35.

77. Ярочкин, В. Безопасность информационных систем/ В. Ярочкин. - М.: Ось-89, 2016. - 320 с.