МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)
ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА ЭКОНОМИКИ, УПРАВЛЕНИЯ И ПРАВА

Противодействие угрозам информационной безопасности организации со стороны собственного персонала

Магистерская диссертация
по направлению 38.04.02 Менеджмент

Направленность программы магистратуры
«Управление человеческим капиталом»
Форма обучения заочная

Проверка на объем заимствований:
79,32 % авторского текста

Работа рекомендована к защите
«12» января 2020 г.
Зав. кафедрой Э, У и П
_____ Рябчук П. Г.

Выполнила:
Студентка группы ЗФ-309-147-2-1
Пронина Лилия Фаилевна

Научный руководитель:
к.п.н, доцент
Рябинина Екатерина Владимировна

Челябинск, 2020

Оглавление

Введение

Актуальность исследования. Современный этап развития общества характеризуется возрастающей ролью информационных взаимодействий. Массовая компьютеризация, внедрение и развитие новейших информационных технологий привели к прорыву в сферах образования, науки, бизнеса, промышленности и социальной жизни. В связи с этим, информация, создаваемая, потребляемая и хранимая в процессе функционирования всех сфер деятельности человека, является источником явной или скрытой угрозы для личности, общества или государства.

В системе приоритетов обеспечения условий для всесторонней самореализации личности, общества, государства особая роль сегодня отводится информационной безопасности как базовой предпосылке формирования материальных, интеллектуальных, технико-технологических ресурсов, необходимых для реализации потребностей и интересов людей.

Информационные ресурсы и информационные системы становятся основными защищаемыми элементами во всех сферах жизнедеятельности современных организаций. Вместе с этим, сегодня активно развиваются средства негативного воздействия на эти элементы, противодействие которым требует широких разноплановых исследований и разработок соответствующих определений, концепций, программ организации конкретных работ в области создания средств, методов и методик обеспечения информационной безопасности.

Непрерывное совершенствование системы обеспечения информационной безопасности становится приоритетной задачей предприятий, фирм и организаций в современном мире.

Персонал организации влияет на все аспекты жизнедеятельности организации, а также неразрывно связан с ее информационной и экономической безопасностью. Возрастание роли угроз информационной

безопасности со стороны собственного персонала в современных условиях обусловлено, с одной стороны, такими социальными тенденциями, как либерализация экономики и рынка труда; изменение сущности контроля за персоналом; повышение роли менеджмента персонала в управлении организацией; с другой стороны, в это время наблюдаются процессы усложнения труда, роли творчества и инноваций, предоставление работникам свободы и автономии в принятии решений, что приводит к ослаблению возможности жесткого контроля за персоналом. При этом надо иметь в виду, что утрата информации происходит в большинстве случаев не в результате преднамеренных действий, а из-за невнимательности и безответственности сотрудников организации.

Вышеприведенное свидетельствует о наличии серьезной проблемы, требующей исследования противодействия угрозам информационной безопасности организации со стороны собственного персонала. Она базируется на глубоком противоречии между запросами модернизируемого общества, потребностями менеджмента как науки и управленческой практики, с одной стороны, и реально существующим уровнем теоретико-методологической и практической разработанности информационной безопасности организации со стороны собственного персонала, с другой стороны.

На разрешение данного противоречия направлена разработка темы исследования: «**Противодействие угрозам информационной безопасности организации со стороны собственного персонала**».

Цель исследования: разработать и апробировать комплекс мероприятий по противодействию угрозам информационной безопасности организации со стороны собственного персонала на примере МОУ «Саргазинской СОШ».

Объектом исследования является информационная безопасность организации со стороны собственного персонала.

Предметом исследования является процесс противодействия угрозам информационной безопасности МОУ «Саргазинской СОШ» со стороны собственного персонала.

Гипотеза исследования: уровень информационной безопасности организации будет выше, если внедрить комплекс мероприятий, направленных на противодействие угрозам информационной безопасности организации со стороны собственного персонала, содержащий три основных блока: управленческий, методический и инженерно-технический.

Цель и гипотеза позволили определить следующие **задачи исследования:**

1. Раскрыть понятие информационной безопасности, дать характеристику основным угрозам и способам оценки информационной безопасности организации.

2. Определить меры, которые необходимо принять организации для нейтрализации и минимизации внутренних угроз конфиденциальной информации со стороны собственного персонала организации.

3. Проанализировать процесс обеспечения информационной безопасности МОУ «Саргазинской СОШ» от угроз со стороны собственного персонала и выявленные в нем недостатки.

4. Разработать и апробировать комплекс мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности МОУ «Саргазинской СОШ» со стороны собственного персонала.

5. Определить эффективность комплекса мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности МОУ «Саргазинской СОШ» со стороны собственного персонала.

Методологическую основу исследования составили законодательные и нормативно-правовые документы РФ, разработки в

области обеспечения информационной безопасности, методы и способы построения процессов управления информационной безопасностью и человеческими ресурсами организации.

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 и управлению персоналом, материалы научных конференций, средств массовой информации, отражающие аспекты информационной безопасности и управления персоналом организации.

Особый вклад в исследование информационной безопасности в различных сферах общества, культуры, науки и техники, внесли такие ученые и исследователи, как А. Р. Алавердов [3, 4, 5, 6], И. Л. Бачило [8], А. В. Волоткин [15], В.А. Галатенко [16], П. Н. Девянин [19], С. А. Клейменов [32], С. П. Расторгуев [41], М. И. Шубинский [57], и другие. В работах этих ученых сформулированы концептуальные положения о сущности и содержании категорий информационной безопасности, обоснованы приемы и способы исследования информационной безопасности, доказано влияние человеческого капитала на информационную безопасность организации, описаны процессы управления человеческими ресурсами организации в сфере информационной безопасности.

Для решения задач исследования применялся комплекс основных **методов исследования**: теоретических методов (анализ, синтез, классификация, систематизация, обобщение, моделирование); эмпирических методов, методов экспериментальной работы (наблюдение, тестирование, анкетирование и опрос, статистическая обработка опытных данных).

Решение поставленных задач осуществлялось в три этапа:

Первый этап (2017 год) включал в себя анализ научной, учебной, методической литературы и изучение опыта работы МОУ «Саргазинской СОШ» с целью выяснения состояния исследуемой проблемы в теории и практике. Были определены основы планируемого исследования: цель, объект, предмет, гипотеза и задачи исследования. Был разработан план проведения исследования и проведен анализ базы исследования.

На втором этапе исследования (2018 год), который проводился на базе МОУ «Саргазинской СОШ» был разработан комплекс мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности организации со стороны собственного персонала. Проводился анализ текущего состояния информационной безопасности базы исследования.

На третьем этапе исследования (2019 год) было осуществлено внедрение разработанного комплекса мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности организации со стороны собственного персонала. Апробация проводилась с целью проверки гипотезы исследования. Произведена оценка эффективности данного комплекса, сформулированы основные выводы и завершена работа по оформлению диссертации.

Научная новизна исследования состоит в решении актуальной задачи, состоящей в совершенствовании процесса противодействия угрозам информационной безопасности образовательной организации со стороны собственного персонала с применением комплекса мероприятий, включающего в себя управленческий, методический и инженерно-технический блоки.

На защиту выносятся следующие положения:

1. Для нейтрализации и минимизации внутренних угроз конфиденциальной информации со стороны собственного персонала организации необходимо принять следующие меры:

– управленческие мероприятия по защите информации (комплекс административных, ограничительных и контрольно-правовых мер);

– методические мероприятия (работа с кадрами: подбор персонала, инструктажи, обучение персонала по вопросам обеспечения защиты информации, воспитание бдительности сотрудников, повышение их квалификации);

– инженерно-технические мероприятия (кодирование информации, установка видеонаблюдения, ограничение прав доступа к электронным носителям, внедрение защитных программно-технических средств и т.п.).

2. Оценка текущего состояния информационной безопасности на основе системы показателей позволит оценить уровень информационной безопасности образовательной организации.

3. Для повышения текущего состояния уровня информационной безопасности организации необходимо внедрить разработанный комплекс мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности МОУ «Саргазинской СОШ» со стороны собственного персонала.

Теоретическая значимость данной магистерской диссертации состоит в том, что

1. Исследована проблема обеспечения информационной безопасности в образовательной организации на теоретико-методическом уровне, создающем прочную основу для его практического использования в условиях современного образования.

2. Дано определение информационной безопасности в образовательной организации, как защищенности информации образовательной организации от случайных или преднамеренных воздействий естественного или искусственного характера, способных

нанести ущерб самой образовательной организации или участникам образовательного процесса образовательной организации.

Практическая значимость состоит в возможности использования результатов, полученных в ходе исследования, в деятельности образовательных организаций при разработке комплекса мероприятий по противодействию угрозам информационной безопасности организации со стороны собственного персонала.

Апробация и внедрение результатов исследования осуществлялись посредством участия в научно-практических конференциях Международного и Всероссийского уровней**.**

Основное содержание исследования отражены в следующих публикациях:

1. К вопросу обеспечения информационной безопасности образовательной организации [Текст]: статья / Л. Ф. Пронина // Профессиональный проект: идеи, технологии, результаты: научный журнал. – Москва: Со–Действие, 2018 – № 2 (31). – 33-37 с. – ISSN: 2221-254X.

2. Информационная безопасность: угрозы конфиденциальной информации в образовательной организации [Текст]: статья / Л. Ф. Пронина // Алдамжаровские чтения: сборник материалов Международной научно-практической конференции, 5 декабря 2018 г. – Костанай: Костанайский социально-технический университет имени академика З. Алдамжар, 2018 – 68-71 с. – ISBN 978-601-7125-81-3.

3. Информационная безопасность в современной образовательной организации [Текст]: статья / Л. Ф. Пронина // Актуальные проблемы образования: позиция молодых: сборник научных трудов по материалам Всероссийской студенческой научно-практической конференции, 5-24 апреля 2019 г. Челябинск: ЗАО «Библиотека А. Миллера», – 2019 г. – 117-121 с. – ISBN: 978-5-93162-187-6.

В качестве **базы исследования** была выбрана образовательная организация Муниципальное общеобразовательное учреждение «Саргазинская средняя общеобразовательная школа», Челябинская область, Сосновский район, п. Саргазы, ул. Мира, 10.

Структура магистерской диссертации соответствует логике исследования и включает введение, две главы, заключение, библиографический список и приложение.

Глава **1. Теоретические основы проблемы обеспечения информационной безопасности организации**

1.1. Понятие и уровни обеспечения информационной безопасности организации в эпоху информационного общества

В настоящее время оперативно решать многие задачи современного общества невозможно без помощи информационных технологий. Постоянное увеличение количества информационных систем, обслуживающих мировое сообщество, внедрение во все сферы жизнедеятельности человека такого глобального изобретения, как Интернет, ставит перед обществом задачи обеспечения информационной безопасности. Несмотря на то, что с каждым годом усовершенствуются технологии защиты информации, уязвимость защиты не только не уменьшается, но и постоянно растет. Поэтому очевидна актуальность проблем, связанных с защитой потоков данных и информационной безопасностью их сбора, обработки и передачи.

Практически во всех мировых культурах безопасность понимается в первую очередь как ощущение защищенности от различного рода опасностей. По аналогии, С.П. Расторгуев дает определение информационной безопасности.

«Информационная безопасность страны» - это ощущение защищенности от применения определенного информационного воздействия как извне, так и внутри страны, направленного на причинение ущерба стране [41].

Профессор С.А. Клейменов под информационной безопасностью Российской Федерации предлагает понимать состояние защищенности национальных интересов РФ в информационной сфере, определяющееся совокупностью сбалансированных интересов личности, общества и государства [32].

Меры по обеспечению информационной безопасности осуществляются в разных сферах – политике, экономике, обороне, а также на различных уровнях – международном, государственном, организационном и личностном. Поэтому задачи информационной безопасности на уровне государства отличаются от задач, стоящих перед информационной безопасностью на уровне организации.

В. Бетелин и В. Галатенко дают определение информационной безопасностью на уровне организации:

Информационная безопасность – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры [16].

Валоткин А.В. и Маношкин А.П. в своей книге «Информационная безопасность» под информационной безопасностью (или безопасностью информационных технологий) подразумевают защищенность информации, обрабатываемой в информационно-вычислительной системе, от случайных или преднамеренных воздействий внутреннего или внешнего характера, чреватых нанесением ущерба владельцам информационных ресурсов или пользователем информации [15]. Из определения ясно, что информационная безопасность это не только защита информационных ресурсов от несанкционированного доступа посторонних лиц, но и обеспечение безопасности от случайных процессов (сбои, аварии, пожары и т.п.).

Мы не вполне согласны с таким определением, так как считаем, что цифровая информация и компьютерная техника является только частью информационной системы организации.

В целях дальнейшего исследования введем понятие информационной безопасности в образовательной организации.

В результате семантического анализа рассматриваемой дефиниции, автором предложено следующее ее определение:

Информационная безопасность в образовательной организации – это защищенность информации образовательной организации от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб самой образовательной организации или участникам образовательного процесса образовательной организации.

К настоящему времени достигнуты определенные результаты по теоретическому изучению и практической разработке проблемы информационной безопасности. Уже более 50 лет она находится в центре внимания специалистов. Заложены основы теории защиты информации. Разработаны разнообразные средства защиты информации и налажено их производство. Накоплен опыт практического решения задач защиты информации в различных системах. Разработана государственная система защиты информации. Проблема защиты информации имеет реальную основу для дальнейшего развития. Для этого необходимо обеспечить постоянный сбор и обработку статистической информации о функционировании существующих систем защиты, что можно достичь, создав организационные структуры, которые будут этим заниматься. Это крайне важно для совершенствования методологии проектирования систем защиты и развития теории защиты информации. Актуальной является задача развития научно-методологических основ защиты информации и информационной безопасности.

Информационная безопасность состоит в применении определенных методов и средств защиты от негативного влияния на составляющие какой-либо системы информации, как внутренней, так и внешней [2]. Актуальность этой проблемы заключается в том, что информация может оказывать колоссальное воздействие и на человека, и на технику, как положительное, так и отрицательное, в частности, вызывая у людей неправильное поведение, плохое настроение, а путем установки в

компьютере специальных закладок можно извне вывести из строя аппаратуру или прервать ее работу.

Информация становится уникальным и вечным ресурсом для человека. Ее уникальность только усиливается в современных условиях. На наш взгляд, основное назначение и важность информации для человека, общества, экономики состоит в ее использовании, обращении. При этом информация может выступать как: источник получения знаний и навыков; источник информирования о событиях и явлениях; средство формирования систем; ресурс при принятии решений; источник негативного влияния на общество и человека; объект интеллектуальной собственности; товар. Именно обращаясь, т.е. переходя от одного субъекта к другому в различных формах, информация приобретает ценность. Именно поэтому актуальность рассматриваемой нами проблемы информационной безопасности не вызывает сомнений.

Важно отметить, что с термином информационная безопасность тесно связаны некоторые другие понятия, которыми мы будет оперировать в следующих разделах исследования. Это, в частности, защита информации, информационные ресурсы, угроза (безопасности информации), источник угрозы информационной безопасности, информационная система, уязвимость (информационной системы), информационная деятельность и ряд других.

Информационные ресурсы (активы) – отдельные документы и отдельные массивы документов, документы и массивы документов, содержащихся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов) [32].

Под информационной деятельностью понимается деятельность, связанная с получением, использованием, распространением, передачей и хранением информации [18]. Результатом информационной деятельности является информационный продукт, который покупается и продается на рынке в виде информационных товаров и услуг.

Информационная система представляет собой формализованную модель ведения бизнеса на определенном предприятии или осуществления собственной деятельности в определенной организации [2]. С ее помощью отображаются все основные процессы, которые здесь происходят. Информационная система компании (или корпоративная информационная система) рассматривается как сложный мультимодельный объект проектирования и содержит следующие типовые элементы: сетевое, компьютерное, телекоммуникационное оборудование; программное обеспечение; методы защиты информации; служебные инструкции; кабельные внутренние и внешние сети.

Информационные риски представляют собой угрозу внешних и внутренних компьютерных атак на информационную систему организации, вследствие чего происходит кража, порча или подмена функционирующей в системе информации, в первую очередь конфиденциальной. На наш взгляд, более точным является следующее определение. Информационный риск - это вероятность получения убытков или ущерба в результате применения организации информационных технологий [9]. Таким образом, информационные риски связаны с созданием, передачей, хранением и использованием любой информации при помощи электронных носителей и других средств связи.

Информационная безопасность представляет собой сложную и многогранную проблему. Она должна обеспечиваться для всех экономических агентов и хозяйствующих субъектов, т.е. населения - основного носителя информации, предприятий и организаций, а также для государства в целом. Определим уровни обеспечения информационной безопасности, включающие в себя заинтересованные в информационной безопасности субъекты (рисунок 1).

Рисунок 1 - Уровни обеспечения информационной безопасности

С начала 2000-х гг. в информационной сфере наступил период активизации и, был принят целый ряд документов, таких как Окинавская хартия глобального информационного общества, итоговые документы Всемирной встречи на высшем уровне по вопросам информационного общества (2003 г. в Женеве и 2005 г. в Тунисе), а также Генеральной Ассамблеи ООН, ОБСЕ принят ряд резолюций в области обеспечения международной информационной безопасности, которые являются основополагающими политико-правовыми документами, направленными на ускорение формирования постиндустриальных тенденций в экономической, социально-политической и духовной сферах жизни общества.

Построение информационного общества в качестве глобальной задачи в новом тысячелетии провозгласила Декларация принципов от 12.12.2003, принятая на Всемирной встрече на высшем уровне в Женеве в 2003 г. по вопросам информационного общества. В Декларации подчеркнуто, что, строя информационное общество, необходимо обеспечить, повышать доверие и безопасность при использовании

информационных технологий и это является одним из ключевых принципов построения открытого для всех информационного общества.

Следуя этим принципам, на концептуально-политическом уровне принимаются документы, определяющие направления государственной политики информационной безопасности, формулируются цели и задачи, пути и средства их достижения. Примером такого документа служит Доктрина информационной безопасности РФ [20].

На законодательном уровне создается и поддерживается комплекс мер, направленных на правовое регулирование и обеспечение информационной безопасности, отражаемых в законах и других правовых актах (указы Президента, постановления Правительства и др.). Важнейшей задачей этого уровня выступает формирование механизма, позволяющего согласовать процесс разработки законов с прогрессом в области информационных технологий.

На нормативно-техническом уровне разрабатываются стандарты, руководящие материалы, методические материалы и другие документы, регламентирующие процессы разработки, внедрения и эксплуатации средств обеспечения информационной безопасности. Одной из главных задач этого уровня является приведение российских стандартов в соответствие с международным уровнем информационных технологий.

В России, как и во всем мире, существует законодательство, регулирующее вопросы информационной безопасности, а также защиты информации. Информационная безопасность является одной из составляющих национальной безопасности. Основным источником права в области национальной безопасности, составляющими правовую систему в Российской Федерации [22], являются прежде всего Конституция РФ, Федеральный закон «О безопасности», Стратегия национальной безопасности Российской Федерации (утверждена Указом президента РФ от 31.05.2015 №683), другие нормативные правовые акты Президента РФ, Правительства РФ, федеральных законов исполнительной власти, а также

международные договоры РФ, международные обычаи и общепризнанные принципы и нормы международного права (ст. 15 Конституции РФ), общие принципы права, принятые цивилизованными народами (п.1 ст. 38 Статуса Международного суда).

Одним из важнейших направлений государственного регулирования применения информационных технологий в нашей стране являются лицензирование и сертификация в области защиты информации [25]. Государственная система лицензирования деятельности в области защиты информации направлена на обеспечение допуска организаций к оказанию услуг по защите информации и контроля качества и эффективности этих услуг. Для получения лицензии организация должна удовлетворять определенным требованиям и условиям. Например, для обработки информации должны использоваться только сертифицированные автоматизированные системы, а также средства защиты. Деятельность должны осуществлять исключительно специалисты с высшим образованием по специальностям «Компьютерная безопасность» или «Информационная безопасность телекоммуникационных систем» и т.д. В 1994 г. было утверждено Положение о государственном лицензировании деятельности в области защиты информации.

Как и в других странах, ввоз и вывоз криптографической техники подлежит государственному контролю и регулированию. В частности, экспорт осуществляется только по лицензии Министерства внешних экономических связей РФ, которая выдается по решению ФАПСИ.

Правовая основа защиты информации на предприятиях в РФ базируется на следующих нормативных документах:

– Конституция Российской Федерации;

– Гражданский кодекс Российской Федерации;

– Трудовой кодекс Российской Федерации;

– Уголовный кодекс Российской Федерации;

– Доктрина информационной безопасности Российской Федерации;

– Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. №149-ФЗ;

– Закон РФ «О персональных данных» от 29.07.2006 г. №151-ФЗ;

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

– Постановление Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановление Правительства РФ от 15 августа 2006 г. №504 «О лицензировании деятельности по технической защите конфиденциальной информации»;

– Постановление Правительства РФ от 31 августа 2006 г. №532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»;

На уровне организации (рисунок 1) осуществляются конкретные меры по обеспечению информационной безопасности.

Состав и содержание в основном определяются особенностями конкретной организации. В основе подобных мер лежит политика информационной безопасности. Она представляет собой совокупность документированных управленческих решений, целью которых является обеспечение защиты информации и связанных с ней ресурсов. Она определяет стратегию, необходимое количество средств и ресурсов, выделяемых организацией на обеспечение должной информационной безопасности. Политика информационной безопасности формируется на основе проведения анализа существующих рисков, угрожающих информационной системе организации.

На программно-техническом уровне осуществляется защита оборудования, программных средств и информационных ресурсов [51]. Реализуется это при помощи сервисов безопасности: идентификация и аутентификация, разграничение доступа, протоколирование и аудит, шифрование, экранирование, обеспечение целостности, обеспечение доступности, обеспечение отказоустойчивости.

При всем существующем на сегодняшний день богатстве выбора программно-технических решений обеспечить информационную безопасность организации на этом уровне до сих пор остается непростой задачей.

На процедурном уровне (рисунок 1) определяются непосредственные меры по обеспечению информационной безопасности, осуществляемые людьми. К ним можно отнести управление персоналом, физическую защиту и планирование восстановительных работ (рисунок 2).

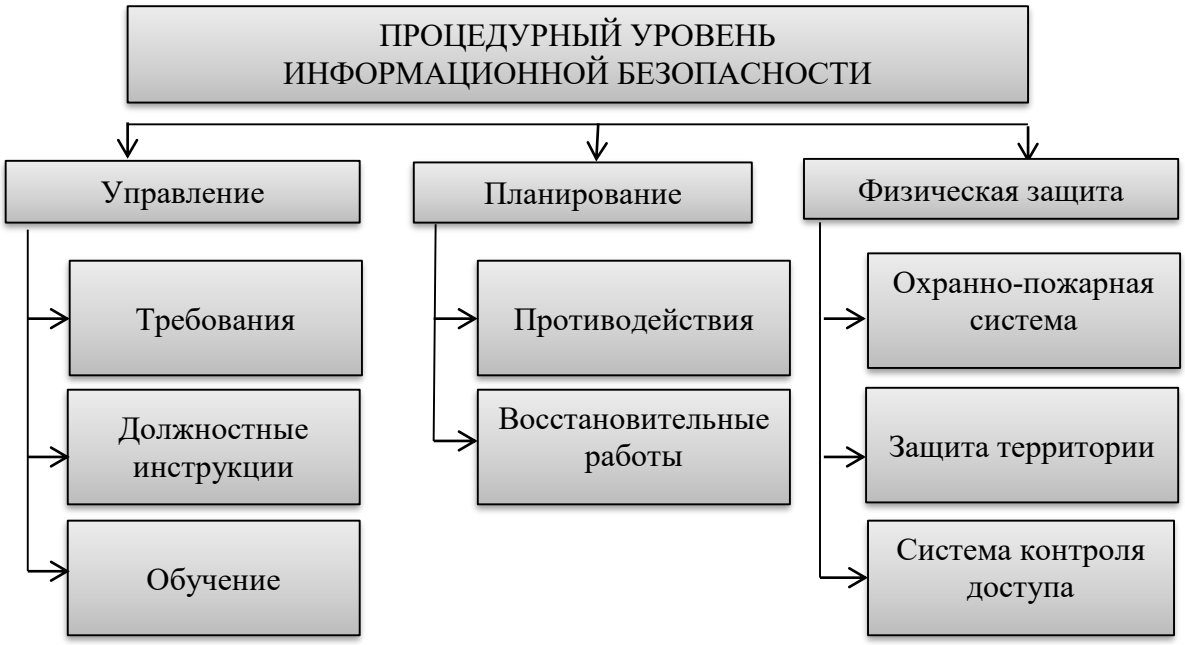

Рисунок 2 - Меры по обеспечению информационной безопасности на процедурном уровне

Управление персоналом начинается с приема нового сотрудника на работу и даже раньше, с составления описания должности и требований к

претендентам. Уже на данных этапах желательно подключить к работе специалиста по информационной безопасности для определения ролей и информационных привилегий, ассоциируемых с должностью. Должностные инструкции так же должны включать обязанности выполнения правил информационной безопасности, принятых в организации. Когда кандидат определен, он должен пройти обучение, его следует подробно ознакомить со служебными обязанностями, а также с нормами и процедурами информационной безопасности.

Планирование информационной безопасности должно предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима информационной безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные. Реакция на нарушения режима безопасности преследует три главные цели: локализация инцидента и уменьшение наносимого вреда; выявление нарушителя; предупреждение повторных нарушений. Поскольку, как показывает практика, выявить злоумышленника очень сложно [19], на наш взгляд, в первую очередь следует заботиться об уменьшении ущерба. Ни одна организация не застрахована от серьезных аварий, вызванных естественными причинами, действиями злоумышленника, халатностью или некомпетентностью. В то же время, у каждой организации есть функции, которые руководство считает критически важными, они должны выполняться несмотря ни на что. Планирование восстановительных работ позволяет подготовиться к авариям, уменьшить ущерб от них и сохранить способность к функционированию хотя бы в минимальном объеме.

Физическая защита позволяет контролировать и при необходимости ограничивать вход и выход сотрудников и посетителей. Контролироваться может все здание организации, а также отдельные помещения, например, те, где расположены серверы, коммуникационная аппаратура и т.п.

Изучив понятие информационной безопасности и уровни, на которых она должна быть обеспечена, мы пришли к выводу, что обеспечение информационной безопасности современных организаций является чрезвычайно острой проблемой. Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий по управлению информационной безопасностью, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного обеспечения. Указанные мероприятия должны обеспечить достижение целей информационной безопасности организации. К процедурному уровню относятся меры безопасности, реализуемые людьми. В отечественных организациях накоплен богатый опыт составления и реализации процедурных (организационных) мер, однако проблема состоит в том, что они пришли из докомпьютерного прошлого, и поэтому нуждаются в существенном пересмотре.

1.2 Основные угрозы и способы оценки текущего состояния информационной безопасности организации

Рассматривая вопросы информационной безопасности организации, можно говорить о наличии некоторых «желательных» состояний системы функционирования организации, через которые и описывается ее «защищенность» или «безопасность». Информационная безопасность является таким же свойством системы, как надежность или производительность, и в последнее время ей уделяется все большее внимание. Чтобы указать на причины выхода системы функционирования организации из безопасного состояния, вводятся понятия «угроза» и «уязвимость».

Угроза (информационной безопасности) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [13].

Источник угрозы информационной безопасности – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации. По типу источника угрозы делят на связанные и несвязанные с деятельностью человека. Примерами могут служить, соответственно, удаление пользователем файла с важной информацией и пожар в здании. Угрозы, связанные с деятельностью человека, разделяют на угрозы случайного и преднамеренного характера. В последнем случае источник угрозы называют нарушителем или злоумышленником.

Уязвимость (информационной системы) — свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации [53]. Например, угроза потери информации из-за сбоя в сети электропитания реализуется, если в организации не применяются источники бесперебойного питания или средства резервного электроснабжения (это является уязвимостью).

Если говорить об информационных ресурсах, то реализация угрозы может привести к таким последствиям, как получение информации людьми, которым она не предназначена, уничтожение или изменение информации, недоступность ресурсов для пользователей. Таким образом, мы подошли к определению трех основных угроз безопасности.

Угроза конфиденциальности (угроза раскрытия) — это угроза, в результате реализации которой конфиденциальная или секретная информация становится доступной лицу, группе лиц или какой-либо организации, которой она не предназначалась [53, 33]. Здесь надо пояснить разницу между секретной и конфиденциальной информацией. В отечественной литературе «секретной» обычно называют информацию,

относящуюся к разряду государственной тайны, а «конфиденциальной» — персональные данные, коммерческую тайну и т. п.

Угроза целостности — угроза, в результате реализации которой информация становится измененной или уничтоженной [33]. Необходимо отметить, что и в нормальном режиме работы организации данные могут изменяться и удаляться. Являются ли эти действия легальными или нет, должно определяться политикой безопасности. Политика безопасности — совокупность документированных правил, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

Угроза отказа в обслуживании (угроза доступности) — угроза, реализация которой приведет к отказу в обслуживании клиентов организации, несанкционированному использованию ресурсов злоумышленниками по своему усмотрению [53,33].

Ряд авторов [19, 29, 37] дополняют приведенную классификацию, вводя угрозу раскрытия параметров автоматизированной системы организации, включающей в себя подсистему защиты. Угроза считается реализованной, если злоумышленником в ходе нелегального исследования системы определены все ее уязвимости. Данную угрозу относят к разряду опосредованных: последствия ее реализации не причиняют какой-либо ущерб обрабатываемой информации, но дают возможность для реализации первичных (непосредственных) угроз.

Таким образом, информационная безопасность — это состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность. Защита информации может быть определена как деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Выделяются следующие направления защиты информации:

– правовая защита информации — защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением;

– техническая защита информации — защита информации, заключающаяся в обеспечении некриптографичсскими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

– криптографическая защита информации — защита информации с помощью ее криптографического преобразования;

– физическая защита информации — защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Защита информации осуществляется с использованием способов и средств защиты. Способ защиты информации — порядок и правила применения определенных принципов и средств защиты информации [42, 44]. Средство защиты информации – техническое, программное, программно-техническое средство, вещество или материал, предназначенные или используемые для защиты информации. Отдельно выделяют:

– средства контроля эффективности защиты информации,

– средства физической защиты информации,

– криптографические средства защиты информации.

Отметим, что следует различать понятия информационной безопасности и защиты информации. Часто в научной и учебной литературе эти два понятия отождествляются, что приводит к путанице.

Нам представляется необходимым их разграничить. Защита информации представляет собой комплекс мер по обеспечению информационной безопасности, т.е. это правовые, организационные, технические меры (способы, методы, средства, механизмы, действия) по предотвращению угроз информационной безопасности и устранению их последствий. К основным элементам защиты информации мы относим следующие: создание условий, ограничивающих распространение информации; предупреждение несанкционированного доступа к информации; предотвращение хищения, утечки, искажения, уничтожения, разглашения информации; обеспечение права собственника на владение и распоряжение информацией и т.д.

Задачи информационной безопасности состоят в том, чтобы обеспечить четыре основные характеристики информации, а именно: доступность, целостность, конфиденциальность и достоверность [42]. Под этими терминами принято понимать соответственно:

– способность систем представлять своевременный беспрепятственный доступ к информационным ресурсам субъектов, обладающих соответствующими правами;

– защиту от сбоев, ведущих к потере информации, защиту от несанкционированных изменений или уничтожения данных;

– ограниченный доступ к информации, предназначенной только для авторизированного пользователя;

– общую полноту и точность воспринимаемой информации.

Наиболее важным и сложным для реализации на практике аспектом информационной безопасности является обеспечение ее конфиденциальности [34]. Существуют три основные причины, приводящие к потере конфиденциальности информации: разглашение, утечка и несанкционированный доступ (рисунок 3).

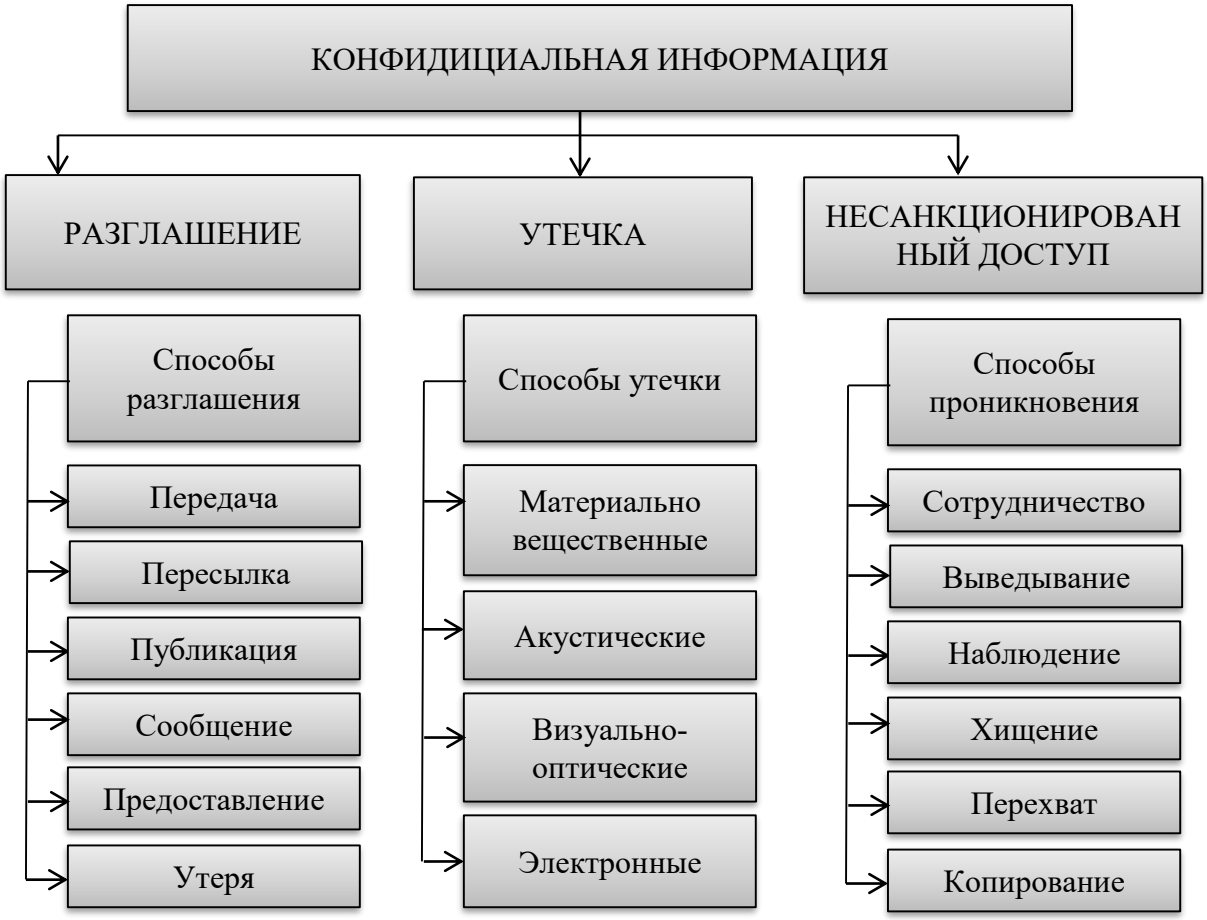

Рисунок 3 - Причины потери конфиденциальности информации

Под разглашением понимается событие, приведшее в результате преднамеренных или неумышленных действий к получению информации субъектами, не обладающими соответствующими правами [30, 34]. Разглашение может осуществляться различными способами. Это могут быть сообщение, передача, пересылка, публикация, утеря и т.п. Осуществляется разглашение формальными и неформальными средствами предоставления информации. К формальным каналам следует отнести переговоры, деловые встречи, совещания и т.п. Неформальными каналами служат личные встречи, переписка, выставки, конференции, средства массовой информации и т.п. Обычно, разглашение конфиденциальной информации происходит в результате некомпетентности сотрудников, невыполнения правил защиты секретных сведений.

Под утечкой мы понимаем неконтролируемый процесс передачи конфиденциальной информации за пределы предприятия или

определенного круга лиц [30, 34]. Реализация утечки конфиденциальной информации происходит при помощи технических каналов. Каналом утечки информации называется физический путь конфиденциальных сведений, используя который злоумышленник может получить доступ к охраняемым информационным ресурсам. Каналы утечки информации классифицируются по способу переноса информации на: материально-вещественные, акустические, визуально-оптические и электромагнитные.

Несанкционированным доступом называется преднамеренное действие, направленное на получение конфиденциальной информации лицом, не обладающим соответствующими правами доступа к ней [30, 34]. Осуществляется несанкционированный доступ при помощи различных методов, к которым относятся подкуп сотрудников, насильственное склонение к сотрудничеству, непосредственное проникновение на объект и др.

Также одной из задач информационной безопасности является обеспечение доступности информации [58, 59], поскольку информационные системы строятся и служат для предоставления различного рода информационных услуг (продуктов). Нарушение связи, отказ в доступе получения подобных услуг влекут за собой значительный ущерб заинтересованным субъектам. Ведущая роль доступности проявляется в системах управления в различных сферах деятельности организации.

Целостность информации как задача информационной безопасности подразделяется на статическую и динамическую. Под статической целостностью понимается неизменность информационных ресурсов, динамическая же относится к точному проведению сложных операций - транзакций. Обеспечение динамической целостности информации важно при проведении финансовых операций с целью обнаружения краж, дублирования и т.п. Нарушение целостности информации, т.е. ее

искажение, потеря, ошибки в различных областях человеческой деятельности могут привести к непредсказуемым результатам.

На сегодняшний день уже известны возможные угрозы информационной безопасности любой организации. К ним относятся: атаки хакеров с целью получения ценной конфиденциальной информации или причинения вреда деятельности организации; преднамеренные действия сотрудников; случайные действия сотрудников, в результате чего нарушается нормальное функционирование организации, или к информации получают доступ посторонние лица. По мнению экспертов, внутренние пользователи - сотрудники совершают 94% преступлений, 6% - совершается внешними пользователями. В ближайшие годы основные угрозы для информационной безопасности государственных организаций будут исходить от персонала, в том числе бывшего, а основными видами преступлений будут вирусы и несанкционированный доступ.

Желание иметь систему обеспечения информационной безопасности, адекватную целям информационной безопасности организации по обеспечению доступности, целостности и конфиденциальности информационных активов, приводит к стремлению совершенствовать систему обеспечения информационной безопасности. Совершенствование, улучшение системы обеспечения информационной безопасности возможно при условии знания состояний характеристик и параметров используемых защищаемых данных, процессов менеджмента, осознания информационной безопасности и понимания степени их соответствия требуемым результатам [31]. Понять эти аспекты системы обеспечения информационной безопасности можно только по результатам оценки текущего состояния информационной безопасности организации, полученной с помощью модели оценки информационной безопасности на основании свидетельств оценки, критериев оценки и с учетом контекста оценки.

Критерии оценки — это все то, что позволяет установить значения оценки для объекта оценки. В качестве критериев оценки информационной безопасности могут использоваться требования информационной безопасности, процедуры информационной безопасности, сочетание требований и процедур информационной безопасности, уровень инвестиций, затрат на информационную безопасность.

К свидетельствам оценки информационной безопасности относятся записи, изложение фактов или любая информация, которая имеет отношение к критериям оценки информационной безопасности и может быть проверена. Такими свидетельствами оценки информационной безопасности могут быть доказательства выполняемой и выполненной деятельности по обеспечению информационной безопасности в виде отчетных, нормативных, распорядительных документов, результатов опросов, наблюдений.

Контекст оценки информационной безопасности объединяет цели и назначение оценки информационной безопасности, вид оценки (независимая оценка, самооценка), объект и области оценки информационной безопасности, ограничения оценки и роли.

Модель оценки информационной безопасности определяет сферу оценки, отражающую контекст оценки информационной безопасности в рамках критерия оценки информационной безопасности, отображение и преобразование оценки в параметры объекта оценки, а также устанавливает показатели, обеспечивающие оценку информационной безопасности в сфере оценки.

В общем виде процесс проведения оценки текущего состояния информационной безопасности представлен основными компонентами процесса: контекст, свидетельства, критерии и модель оценки – необходимыми для реализации процесса оценки [1].

Оценка текущего состояния информационной безопасности заключается в выработке оценочного суждения относительно пригодности

(зрелости) процессов обеспечения информационной безопасности, адекватности используемых защитных мер или целесообразности (достаточности) инвестиций (затрат) для обеспечения необходимого уровня информационной безопасности на основе измерения и оценивания критических элементов (факторов) объекта оценки.

Наряду с важнейшим назначением оценки текущего состояния информационной безопасности – создание информационной потребности для совершенствования информационной безопасности, возможны и другие цели проведения оценки информационной безопасности, такие как:

– определение степени соответствия установленным критериям отдельных областей обеспечения информационной безопасности, процессов обеспечения информационной безопасности, защитных мер;

– выявление влияния критических элементов (факторов) и их сочетания на информационную безопасность организации;

– сравнение зрелости различных процессов обеспечения информационной безопасности и сравнение степени соответствия различных защитных мер установленным требованиям.

Результаты оценки текущего состояния информационной безопасности организации могут также использоваться заинтересованной стороной для сравнения уровня информационной безопасности организаций с одинаковым бизнесом и сопоставимым масштабом [1, 24].

В зависимости от выбранного для оценки текущего состояния информационной безопасности критерия способы оценки информационной безопасности организации разделяют на оценку по эталону, риск-ориентированную оценку и оценку по экономическим показателям [31, 1].

Способ оценки текущего состояния информационной безопасности по эталону сводится к сравнению деятельности и мер по обеспечению информационной безопасности организации с требованиями,

закрепленными в эталоне. По сути дела проводится оценка соответствия системы обеспечения информационной безопасности организации установленному эталону. Под оценкой соответствия информационной безопасности организации установленным критериям понимается деятельность, связанная с прямым или косвенным определением выполнения или невыполнения соответствующих требований информационной безопасности в организации. С помощью оценки соответствия информационной безопасности измеряется правильность реализации процессов системы обеспечения информационной безопасности организации и идентифицируются недостатки такой реализации.

В результате проведения оценки информационной безопасности должна быть сформирована оценка степени соответствия системы обеспечения информационной безопасности эталону, в качестве которого могут быть приняты (в совокупности и отдельно):

– требования законодательства Российской Федерации в области информационной безопасности;

– отраслевые требования по обеспечению информационной безопасности;

– требования нормативных, методических и организационно-распорядительных документов по обеспечению информационной безопасности;

– требования национальных и международных стандартов в области информационной безопасности.

Основные этапы оценки информационной безопасности по эталону включают выбор эталона и формирование на его основе критериев оценки информационной безопасности, сбор свидетельств оценки и измерение критических элементов (факторов) объекта оценки, формирование оценки информационной безопасности.

Риск-ориентированная оценка текущего состояния информационной безопасности организации представляет собой способ оценки, при котором рассматриваются риски информационной безопасности, возникающие в информационной сфере организации, и сопоставляются существующие риски информационной безопасности и принимаемые меры по их обработке. В результате должна быть сформирована оценка способности организации эффективно управлять рисками информационной безопасности для достижения своих целей.

Основные этапы риск-ориентированной оценки информационной безопасности включают идентификацию рисков информационной безопасности, определение адекватных процессов менеджмента рисков и ключевых индикаторов рисков информационной безопасности, формирование на их основе критериев оценки информационной безопасности, сбор свидетельств оценки и измерение риск-факторов, формирование оценки информационной безопасности.

Способ оценки текущего состояния информационной безопасности на основе экономических показателей оперирует понятными для бизнеса аргументами о необходимости обеспечения и совершенствования информационной безопасности. Для проведения оценки в качестве критериев эффективности системы обеспечения информационной безопасности используются система показателей, понятная именно для этой сферы бизнеса.

Под показателем понимается сумма прямых и косвенных затрат на внедрение, эксплуатацию и сопровождение системы обеспечения информационной безопасности. Под прямыми затратами понимаются все материальные затраты, такие как покупка оборудования и программного обеспечения, трудозатраты соответствующих категорий сотрудников. Косвенными являются все затраты на обслуживание системы обеспечения информационной безопасности, а также потери от произошедших инцидентов. Сбор и анализ статистики по структуре прямых и косвенных

затрат проводится, как правило, в течение года. Полученные данные оцениваются по ряду критериев с показателями аналогичных организаций отрасли.

Оценка на основе системы показателей позволяет оценить затраты на информационную безопасность и сравнить информационной безопасности организации с типовым профилем защиты, а также управлять затратами для достижения требуемого уровня защищенности.

Основные этапы оценки текущего состояния информационной безопасности на основе системы показателей включают сбор данных о текущем уровне информационной безопасности, анализ областей обеспечения информационной безопасности, выбор сравнимой модели системы показателей в качестве критерия оценки, сравнение показателей с критерием оценки, формирование оценки информационной безопасности.

Однако этот способ оценки требует создания общей информационной базы данных об эффективности системы обеспечения информационной безопасности организаций схожего бизнеса и постоянной поддержки базы данных в актуальном состоянии. Такое информационное взаимодействие организаций, как правило, не соответствует целям бизнеса. Поэтому оценка информационной безопасности на основе системы показателей практически не применяется. Но для оценки текущего состояния информационной безопасности образовательной организации, целью которой является осуществление образовательной деятельности по образовательным программам, по нашему мнению, подходит именно способ оценки эффективности системы обеспечения информационной безопасности на основе системы показателей. Так как целью образовательной организации не является прибыль, то показатели оценки текущего состояния информационной безопасности не целесообразно отражать в виде затрат, а необходимо представить в виде вопросов, ответы на которые дадут возможность определить оценку текущего состояния информационной безопасности.

Обобщая вышесказанное, можно сделать вывод, что для построения полноценной защиты конфиденциальной информации организации необходимо иметь полное представление обо всех реальных и потенциальных угрозах, которые могут иметь место. Существует три основные угрозы информационной безопасности: угроза конфиденциальности (угроза раскрытия), угроза целостности, угроза отказа в обслуживании (угроза доступности). Большая часть атак на информационную безопасность организации происходит изнутри. Любой пользователь системы является потенциальным злоумышленником, в силу того, что он способен нарушить конфиденциальность информации, допустив ошибку или сделав осознанный выбор. Состав всех внешних злоумышленников отличается. Как правило, это конкуренты, реже партнеры, иногда в качестве злоумышленников выступают клиенты. Организации, желающие обеспечивать доступность, целостность и конфиденциальность своих информационных активов, должны постоянно совершенствовать систему обеспечения своей информационной безопасности. Понять аспекты обеспечения информационной безопасности можно только по результатам оценки текущего состояния информационной безопасности организации.

1.3. Степень влияния персонала организации на информационную безопасность организации

Степень участия персонала в создании, эксплуатации и функционировании системы информационной безопасности организации относится к категории основополагающих проблем безопасности, так как сотрудники организации одновременно являются неотъемлемой частью системы информационной безопасности и основным источником угроз. Как мы уже отмечали ранее, согласно статистическим данным, большая часть нарушений информационной безопасности исходит от действующих

сотрудников организаций. Это не означает, что к сотрудникам организации нужно относиться как к потенциальным нарушителям, ведь согласно той же статистике, до 65% среди всех нарушений в области информационной безопасности происходит из-за непреднамеренных ошибок пользователей информационных систем, то есть в силу незнания, невнимательности и т.д.

Выделяют два основных принципа, которые лежат в основе работы с персоналом организации. Соблюдение данных принципов гарантирует поддержание минимального уровня информационной безопасности:

– принцип разделения обязанностей,

– принцип минимизации привилегий.

Первый принцип означает, что обязанности между сотрудниками организации должны быть распределены таким образом, чтобы один сотрудник не мог в одиночку нарушить важный для организации процесс. Это означает, что все критически важные процессы в организации необходимо разбить на этапы, которые выполняются разными сотрудниками [28]. Необходимо отметить, что в организации существуют такие должности, как «администратор локальной сети» или «бухгалтер», действия которых в сфере внутренней информационной системы организации практически неограниченны.

Следовательно, от действий указанного сотрудника, его профессионализма и опыта может зависеть функционирование всей организации, притом, что процесс делегирования возложенных на него обязанностей является одной из наиболее актуальных проблем в сфере информационной безопасности. Представленная ситуация является одним из немногих примеров, когда разделение обязанностей становится сложно осуществимым процессом.

Принцип минимизации привилегий обозначает, что круг полномочий сотрудника расширен в той мере, в которой это необходимо для

выполнения его обязанностей [28]. Это позволяет получить сразу несколько преимуществ.

Во-первых, так как обязанности и привилегии сотрудника строго определены, в случае нарушения информационной безопасности будет легче установить личность нарушителя.

Во-вторых, указанный принцип поможет спланировать работу сотрудника таким образом, чтобы сделать ее максимально безопасной для информационной среды организации. Например, введение запрета сотрудникам на выполнение определенных действий на рабочем компьютере.

В-третьих, использование данного принципа поможет уменьшить ущерб от непреднамеренных или умышленных действий сотрудника, способных причинить вред информационной среде организации.

Для более полного представления о влиянии персонала на информационную безопасность организации, целесообразно разделить работу с сотрудниками на три основных этапа [27]:

1. Этап подбора и работа с персоналом до приема в штат организации.

2. Работа с действующими сотрудниками организации.

3. Работа с увольняемыми и бывшими сотрудниками организации.

Рассмотрим более подробно представленные этапы и выделим из них основные моменты.

1 Этап. Подбор и работа с персоналом до приема в штат организации.

Этап подбора персонала представляется одним из самых важных при работе с персоналом. При правильной организации работы на данном этапе, в будущем можно избежать большого числа проблем не только в области безопасности, но также эффективного функционирования предприятия. Не допустив ошибок на этапе приема на работу, и выбрав среди претендентов ответственного и профессионального человека,

работодатель одновременно сможет решить множество сопутствующих задач.

Существуют различные методы работы с кандидатами при приеме в организацию. Первоочередным этапом, с которым сталкивается сотрудник при поступлении на работу, является процесс собеседования. Нужно отметить, что в организациях по-разному относятся к данному этапу. В большинстве организаций достаточно одного собеседования для того, чтобы быть зачисленным в штат. Данный показатель зависит, в первую очередь, от должности, на которую претендует кандидат, но также это может свидетельствовать о низком уровне информационной безопасности, так как решение о приеме на работу принимается за минимальное время, на основании одного собеседования и, что особенно важно, работодатель располагает очень ограниченным объемом информации о нанимаемом сотруднике. По такому принципу строят свою работу большинство предприятий, не ставящих проблематику безопасности в число приоритетных [12].

По нашему мнению, на данном этапе обязательно использование методик управления человеческими ресурсами, включающих в себя прохождение собеседования в несколько этапов и с различными специалистами организации, проведение тестирования, сбор и проверку информации о кандидате.

Отдельно необходимо отметить, что на этапе приема на работу необходима совместная скоординированная работа различных служб, отделов и подразделений предприятия по обсуждению кандидатуры претендента на должность, сбору сведений и вынесению окончательного решения.

2 Этап. Работа с действующими сотрудниками организации.

При успешном прохождении кандидатом этапа зачисления в сотрудники организации, работа с ним с позиции информационной безопасности не заканчивается, а только усиливается. Для обеспечения

нормальной работы с принятым сотрудником, служба безопасности должна обеспечить себе правовое пространство, в том числе, в случае возможного расследования нарушений.

Начало деятельности сотрудника на новом месте сопряжено, в первую очередь, с ознакомлением с внутренней документацией организации. К ней относятся должностные инструкции, трудовой договор, правила техники безопасности, правила и методические указания в области безопасности и т.д. Также необходимо ознакомление сотрудника с действующим законодательством в области информационной безопасности. Здесь следует выделить несколько основных моментов.

Во-первых, сотрудник будет осведомлен о своих правах и компетенции организационных служб по безопасности, что позволит предотвратить возможные конфликты на почве вмешательства в сферу личных интересов сотрудника. Также это позволит провести черту, разделяющую зоны вмешательства и определяющую до какой степени это вмешательство будет оправдано. Например, насколько оправдан просмотр сотрудниками службы безопасности истории посещений интернет сайтов, проводившегося с рабочего компьютера того или иного сотрудника? Решением этих и других задач будут заниматься сотрудники службы информационной безопасности.

Во-вторых, знание внутриорганизационной документации будет гарантией соблюдения законодательства самой организацией, так как сотрудники будут иметь представление о том, за какие действия они могут быть привлечены к ответственности. Необходимо чтобы сотрудник подписался под всеми изученными документами и не мог впоследствии сослаться на незнание. Если организация принимает особые меры по защите своей информации, то положения по конфиденциальности также следует включить в перечень подписываемых документов.

Сотрудник организации должен быть осведомлен о любых возможных вмешательствах в рабочий процесс со стороны службы

информационной безопасности. Например, отправляя электронные письма, он должен быть проинформирован о том, что сотрудники службы могут просматривать их содержание [10].

Во многих организациях при приеме на работу нового сотрудника для проверки его способности выполнять работу назначается испытательный срок, условия которого должны быть оговорены на этапе собеседования [14]. Прохождение испытательного срока является абсолютно законным требованием, предусмотренным в трудовом законодательстве [47], и позволяет организации без оформления документации и трудоустройства нового сотрудника проверить его личные и профессиональные качества.

На этапе испытательного срока для отдела или специалиста по информационной безопасности открывается дополнительная возможность проверить нового сотрудника на соответствие требованиям безопасности, провести более основательно работу, которая была проведена еще на этапе собеседования. Очевидно, что собеседование - процесс скоротечный, и оптимально оценить кандидата за столь короткое время можно не успеть, а время испытательного срока, которое, согласно законодательству, может длиться до трех месяцев, открывает широкие возможности для проверки кандидата не только в профессиональной области [46].

Таким образом, после прохождения испытательного срока решение по приему нового сотрудника будет принимать не только сотрудник отдела персонала, но и представители других служб, включая специалиста по информационной безопасности.

Какие этапы проверки по безопасности может пройти будущий сотрудник на испытательном сроке? Это могут быть те же процедуры, которые использовались на этапе собеседования: тестирование, проверка на психологическое соответствие занимаемой должности, готовность сотрудника нести законодательную ответственность за нарушения в области информационной безопасности [4]. Также сотрудники службы

безопасности смогут более детально проверить сведения, указанные кандидатом на этапе собеседования, связаться с предыдущими местами работы, потребовать предоставления рекомендательного письма [38]. Например, необходимо проверить знание основ компьютерной безопасности, а также безопасной работы с почтой и в сети интернет.

Нужно отметить, что нет необходимости применять жесткие требования к принимаемому сотруднику. Это может создать неблагоприятное впечатление о компании, стать предпосылкой к напряженности и психологическому дискомфорту, которые бы оказывали дополнительное давление на сотрудника, помимо адаптации на новом месте работы. В этом случае представляется целесообразным проводить обучение в области информационной безопасности для вновь прибывших сотрудников, ознакомить с уровнем требований, предъявляемых к сотрудникам организации в области безопасности.

Испытательный срок как этап совпадает по времени с началом периода адаптации нового сотрудника, но, как отмечается [54], при этом «не следует заниматься подменой понятий «адаптация» и «испытание работника». В период испытания нового сотрудника процесс его адаптации будет неизбежен. Вопрос только в том, будет ли иметь место помощь со стороны трудового коллектива и непосредственно самого руководителя, или как в большинстве случаев реализацию своего «Я» работник осуществит посредством самоадаптации.

Следующим важным этапом при работе с персоналом предприятия является организация процесса регулярного обучения мерам безопасности [38]. Это особенно актуально на этапе обновления оборудования, а также вследствие постоянного изменения информационной среды. Появление и распространение новых технических средств, программ, сервисов и служб несет в себе опасность возникновения новых рисков для информационной безопасности и каналов утечки данных. Службам безопасности предприятий необходимо своевременно реагировать на появление новых

угроз и вносить изменения во внутреннюю нормативную документацию, незамедлительно информировать об этом сотрудников. Для того чтобы сделать этот процесс наиболее эффективным, важным этапом представляется организация планового процесса обучения сотрудников основам безопасности.

Помимо обучения необходимо сформировать систему оперативного оповещения сотрудников о возможных угрозах и мероприятиях по защите от этих угроз [44]. Подобное оповещение целесообразно проводить на плановых собраниях, посвященных общим вопросам работы компании, либо осуществлять посредством рассылки по внутренней сети организации информации о возникновении новых угроз.

Следующим этапом работы с персоналом является проверка деятельности сотрудников. Этот процесс можно осуществлять выборочно, ориентируясь на отдельных сотрудников, либо массовая через определенный промежуток времени, в зависимости от особенностей деятельности организации. Результаты проверок необходимо фиксировать в специальном журнале, реестре учета или личном деле сотрудника. Таким образом, появляется определенный статистический материал для фиксации состояния информационной безопасности на предприятии. Из анализа полученных данных можно делать выводы о том, требуются ли мероприятия по улучшению информационной среды на предприятии, либо положение информационной безопасности можно считать удовлетворительным.

3 Этап. Работа с увольняемыми и бывшими сотрудниками организации.

Данный этап работы с персоналом представляется достаточно важным, но при этом сильно недооцененным со стороны руководства предприятий. С позиции информационной безопасности, здесь необходимо выделить несколько существенных моментов.

Как отмечают исследователи [4, 5, 6], «косвенным образом о желании сотрудника перейти на новое место работы может служить посещение соответствующих сайтов в интернете или рассылка резюме. Возможно, что с этого момента потребуется взять под контроль переписку с рабочего компьютера, а также технические операции (действия со сменными носителями информации, запоминающими устройствами и т.д.)».

Как крайняя мера, может рассматриваться возможность создания резервной копии хранящейся на рабочем компьютере сотрудника информации. Необходимо помнить, что сотрудник может поменять свои планы и остаться работать в компании, поэтому в большинстве случаев нет необходимости принимать явных мер безопасности.

Другая особенность работы с увольняемыми сотрудниками состоит в том, что по нормам действующего законодательства работник обязан уведомить руководство о своем решении покинуть организацию в двух недельный срок. В этот период рекомендуется начинать мероприятия по увольнению, сменить учетные записи пользователя, тем самым ограничив или отменив увольняемому сотруднику доступ к внутриорганизационной информации и базам данных. Приблизительный список мер может выглядеть следующим образом [4]:

– «проинформировать всех сотрудников о предстоящем увольнении и запретить передавать ему любую или какую-то конкретную информацию, имеющую отношение к работе;

– сделать резервную копию файлов пользователя;

– организовать передачу дел;

– постепенно, по мере передачи дел, сокращать права доступа к информации;

– по необходимости организовать сопровождение увольнения специалистом по информационной безопасности».

В том случае, если сотрудник подписывал обязательства о неразглашении конфиденциальной информации, необходимо напомнить ему об обязательстве их соблюдения, так как действия подобных соглашений распространяются на период после увольнения.

Итак, для организаций, которые заботятся о долгосрочных перспективах развития, важным является работа с собственным персоналом по обеспечению информационной безопасности. Обучение персонала это универсальное направление, составляющее кадровую безопасность организации, так как персонал способен как укреплять, так и разрушать систему информационной безопасности компании. Работники, осведомленные об ответственности за нарушение правил информационной безопасности намного более устойчивы к «соблазнам»: их сложно переманить в другую организацию, склонить к сотрудничеству с конкурентами, мошенничеству и злоупотреблению полномочиями.

Выводы по главе

В ходе выполнения первой главы, которая была посвящена теоретическим основам информационной безопасности, автор пришел к следующим выводам:

1. Целью информационной безопасности организации является полная защищенность информационных ресурсов, т.е. в любой момент времени, в любой обстановке и от любых угроз.

2. В ближайшие годы основные угрозы для информационной безопасности государственных организаций будут исходить от персонала, в том числе бывшего, а основными видами преступлений будут вирусы и несанкционированный доступ.

3. Для нейтрализации и минимизации внутренних угроз конфиденциальной информации со стороны собственного персонала организации необходимо принять следующие меры:

– управленческие мероприятия по защите информации (комплекс административных, ограничительных и контрольно-правовых мер);

– методические мероприятия (работа с кадрами: подбор персонала, инструктажи, обучение персонала по вопросам обеспечения защиты информации, воспитание бдительности сотрудников, повышение их квалификации);

– инженерно-технические мероприятия (кодирование информации, установка видеонаблюдения, ограничение прав доступа к электронным носителям, внедрение защитных программно-технических средств и т.п.).

4. Оценка текущего состояния информационной безопасности до и после усовершенствования системы обеспечения информационной безопасности на основе системы показателей позволит оценить уровень информационной безопасности организации. Показатели оценки текущего состояния информационной безопасности образовательной организации могут быть представлены в виде вопросов, ответы на которые дадут возможность определить оценку текущего состояния информационной безопасности.

Глава 2. Экспериментальная работа по апробации комплекса мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности со стороны собственного персонала в МОУ «Саргазинской СОШ»

2.1. Цели, задачи, этапы и организация экспериментальной работы

В первой главе исследования нами были рассмотрены теоретические аспекты проблемы противодействия угрозам информационной безопасности организации со стороны собственного персонала. Теоретический анализ проблемы позволил нам выдвинуть предположение, которое требует проверки в ходе экспериментальной работы. Так, мы предположили, что:

– уровень информационной безопасности организации будет выше, если внедрить комплекс мероприятий, направленных на противодействие угрозам информационной безопасности организации со стороны собственного персонала, содержащий три основных блока: управленческий, методический и инженерно-технический.

В соответствии с гипотезой и целью данного исследования нами сформулированы цель и задачи экспериментальной работы.

Цель экспериментальной работы заключается в апробации комплекса мероприятий, направленных на противодействие угрозам информационной безопасности организации со стороны собственного персонала.

На основе цели экспериментальной работы были определены следующие задачи:

1. Проанализировать текущее состояние информационной безопасности образовательной организации и выявить недостатки процесса противодействия угрозам информационной безопасности образовательной организации со стороны собственного персонала.

2. Разработать комплекс мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности образовательной организации со стороны собственного персонала.

3. Внедрить комплекс мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности образовательной организации со стороны собственного персонала.

4. Определить эффективность комплекса мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности образовательной организации со стороны собственного персонала.

Экспериментальная работа осуществлялась на базе Муниципального общеобразовательного учреждение «Саргазинской средней общеобразовательной школы» Челябинской области в период с 2017 по 2019 гг. В работе был задействован педагогический коллектив численностью 32 человека.

В ходе исследования были замерены уровни лояльности и удовлетворенности трудом сотрудников образовательной организации; исследована организационная структура образовательной организации; проверены знания основ информационной безопасности собственным персоналом образовательной организации; оценено текущее состояние информационной безопасности образовательной организации.

В соответствии с целью, предметом, гипотезой и задачами данного исследования экспериментальная работа проводилась в три этапа:

Первый этап – 2017 г. На данном этапе была организована работа в следующих направлениях: во-первых, мы исследовали образовательную организацию (виды деятельности, качественный состав персонала, организационная структура; используемые программно-технические средства и др.); во-вторых проанализировали общий уровень информационной безопасности и определили наиболее актуальные угрозы.

Основные методы исследования: наблюдение, тестирование, опрос, анализ документации, беседа.

Второй этап – 2018 г. Содержанием данного этапа явилось разработка комплекса мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности организации со стороны собственного персонала. На данном этапе важным было провести анализ текущего состояния информационной безопасности базы исследования до внедрения разработанного комплекса. Основными методами исследования на данном этапе послужили: наблюдение, беседа, экспертный анализ.

Третий этап – 2019 г. Этот этап мы посвятили внедрению комплекса мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности организации со стороны собственного персонала. После внедрения разработанного комплекса мы еще раз провели анализ текущего состояния информационной безопасности базы исследования. Было также проведено описание хода экспериментальной работы: обработка, анализ, обобщение результатов исследования, а также соотнесение их с целью, гипотезой и задачами экспериментальной работы; произведена оценка эффективности внедренного комплекса; сформулированы основные выводы и завершена работа по оформлению диссертации.

Приступим к описанию первого этапа экспериментальной работы.

Для разработки эффективного комплекса мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности со стороны собственного персонала организации необходимо обладать сведениями о видах деятельности организации, качественном составе персонала, используемых программно-технических средствах передачи данных, а также о финансовых возможностях организации.

Муниципальное общеобразовательное учреждение «Саргазинская средняя общеобразовательная школа» создано муниципальным

образованием Сосновский муниципальный район для выполнения работ, оказания услуг в целях обеспечения реализации предусмотренных законодательством Российской Федерации полномочий администрации Сосновского муниципального района в сфере образования [35].

В своей деятельности образовательная организация руководствуется Конституцией Российской Федерации, Федеральным законом от 29.12.2012 г. № 273-ФЗ "Об образовании в Российской Федерации", Федеральным законом от 12.01.1996 № 7-ФЗ "О некоммерческих организациях", другими федеральными законами, иными нормативными правовыми актами Российской Федерации, законами и иными нормативными правовыми актами Челябинской области, нормативными правовыми актами Администрации Сосновского муниципального района, распоряжениями Управления образования администрации Сосновского муниципального района и Уставом образовательной организации.

Образовательная организация осуществляет свою деятельность в соответствии с предметом и целями деятельности, определенными в соответствии с Федеральным законом № 273-ФЗ от 29.12.2012 г. «Об образовании в Российской Федерации», иными нормативными правовыми актами Российской Федерации, нормативными правовыми актами Челябинской области, нормативными правовыми актами Сосновского муниципального района и Уставом образовательной организации [35].

Государственная регламентация образовательной деятельности образовательная организация включает в себя:

– лицензирование образовательной деятельности,

– государственную аккредитацию образовательной деятельности,

– государственный контроль (надзор) в сфере образования.

Основной целью образовательной организации является осуществление образовательной деятельности по образовательной программе дошкольного образования и имеющим аккредитацию

образовательным программам начального общего, основного общего и среднего общего образования.

Основной задачей образовательной организации является всестороннее удовлетворение образовательных потребностей человека в интеллектуальном, духовно-нравственном, физическом совершенствовании.

Образовательная организация финансируется за счет средств бюджета Челябинской области и бюджета муниципального образования – Сосновский муниципальный район путем выделения субсидий на выполнение муниципального задания, а также иных источников.

Управление образовательной организации строится на основе сочетания принципов единоначалия и коллегиальности. Формами коллегиального управления образовательной организации являются: Педагогический совет, Общее собрание трудового коллектива, Совет школы.

Коллектив образовательной организации – 46 человек.

Технический персонал – 14 человек.

Педагогический коллектив – 32 человека:

– высшее образование – 23 человека, 75 %;

– среднее профессиональное образование – 9 человек, 25 %.

Квалификационные категории:

– высшая – 32 %;

– первая – 26 %.

Для оценки уровня лояльности сотрудников мы использовали методику, описанную в приложении 1 [52, 55]. Анкетирование показало (рисунок 4), что 85% сотрудников образовательной организации лояльны к своей организации, их устраивает практически все, они готовы жертвовать некоторыми собственными интересами ради успеха организации.

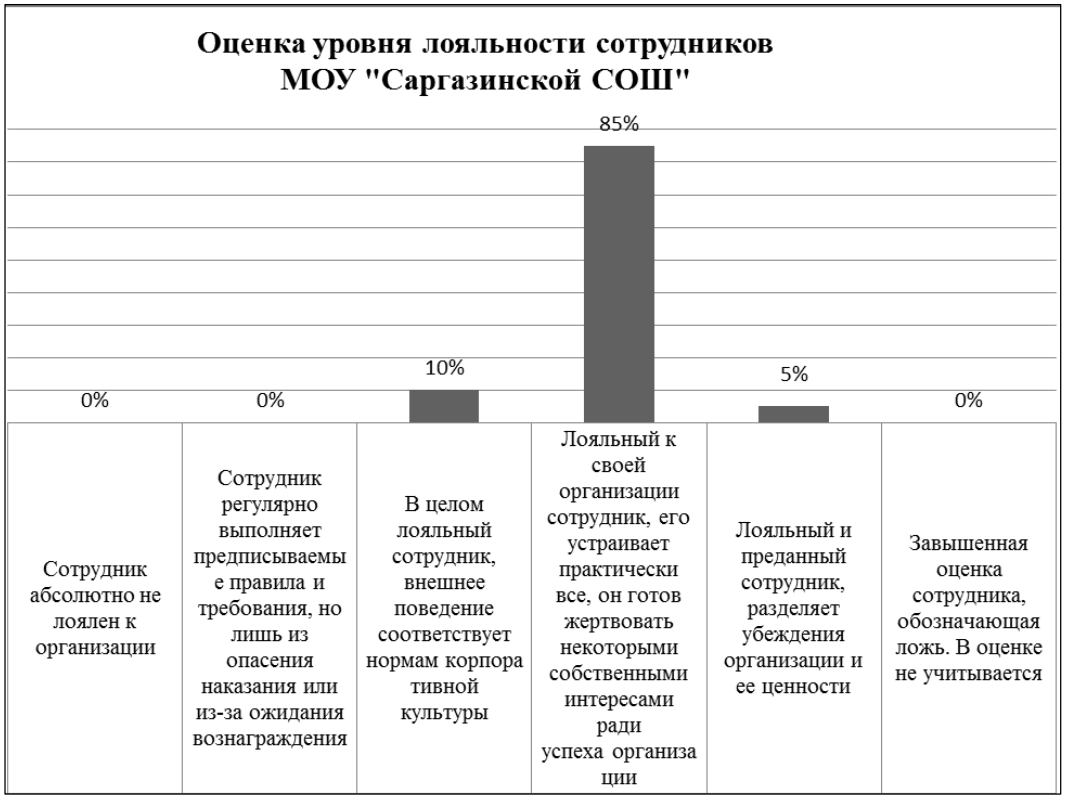

Рисунок 4 – Оценка уровня лояльности МОУ «Саргазинской СОШ»

Из диаграммы (рисунок 4) видно, что в организации нет нелояльных сотрудников, а также сотрудников выполняющих предписываемые правила и требования только из опасения наказания или из-за ожидания вознаграждения.

Исследуя мотивации сотрудников образовательной организации (приложение 2), мы увидели, что в ближайшие годы 90% сотрудников планирует остаться работать на прежних должностях, ни один работник не планирует сменить место работы. Материальное и моральное стимулирование, а так же трудовой настрой коллектива повышают трудовую активность сотрудников. Тогда как нововведения в организации у 60% испытуемых вызывают обратную реакцию и снижают трудовую активность. Самыми важными характеристиками работ для персонала образовательной организации оказались: благоприятный психологический климат, самостоятельность в выполнении работ, радость от работы, участие в развитии организации, благоприятные условия труда. Самыми важными для сотрудников видами поощрений стали: все виды доплат

(премии, льготы), бесплатное обучение и уважение со стороны руководства.

Удовлетворенность трудом является интегративным показателем, отражающим благополучие-неблагополучие положения в трудовом коллективе [48]. Показатель содержит оценки интереса к выполняемой работе, удовлетворенности взаимоотношениями с коллегами, руководством, уровня притязаний в профессиональной деятельности и т. д. Для оценки удовлетворенности персонала трудом мы использовали «Методику определения интегральной удовлетворенности трудом» А. В. Батаршева (приложение 3).

Результаты исследования показаны в таблице 1.

Таблица 1 - Удовлетворенность сотрудников МОУ «Саргазинской СОШ» своим трудом

Составляющие удовлетворенности	% от общей суммы баллов	Уровень удовлетворенности трудом
Интерес к работе	65%	Высокий
Удовлетворенность достижениями в работе	59%	Высокий
Удовлетворенность взаимоотношениями с коллегами	85%	Высокий
Удовлетворенность взаимоотношениями с руководством	80%	Высокий
Уровень притязаний в профессиональной деятельности	68%	Высокий
Предпочтение выполняемой работы заработку	57%	Высокий
Удовлетворенность условиями труда	73%	Высокий
Профессиональная ответственность	81%	Высокий
Общая удовлетворенность трудом	71%	Высокий

Можно сделать вывод, что в образовательной организации «высокий» уровень удовлетворенности трудом по всем составляющим. Общая удовлетворенность трудом составляет 71%, что соответствует «высокому» уровню.

Далее опишем результаты анализа использования средств передачи информации, полномочий сотрудников и их уровня доступа к информационным ресурсам. Это позволит получить наглядное

представление об общем уровне информационной безопасности и определить наиболее актуальные угрозы.

Пользование информационными ресурсами МОУ «Саргазинская СОШ» регламентируется в соответствии с Федеральным законом «Об образовании в Российской Федерации» от 29 декабря 2012 г. № 273-ФЗ.

Доступ педагогических работников к информационным ресурсам обеспечивается в целях качественного осуществления образовательной и иной деятельности, предусмотренной Уставом образовательной организации.

Доступ педагогических работников к информационно-телекоммуникационной сети Интернет в образовательной организации осуществляется с персональных компьютеров (ноутбуков и автоматизированных рабочих мест), подключенных к сети Интернет. Локальной сети в образовательной организации нет. Вопрос о ее «строительстве» закрыт Учредителем по причине дороговизны.

Нормативно–правовой уровень обеспечения информационной безопасности организации включает законы, постановления правительства и указы президента, нормативные акты и стандарты, которыми регламентируются правила использования и обработки информации ограниченного доступа.

Основными законодательными актами, регулирующими вопросы информационной безопасности образовательной организации, являются: Гражданский кодекс РФ ст.139; Уголовный кодекс гл.28 ст.272, 273, 274, 138, 183 [49]; Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в действующей редакции [50]; 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 2012 года № 1119 «Об утверждении требований к

защите персональных данных при их обработке в информационных системах персональных данных».

Информационная безопасность не выделена из общего понятия «безопасность образовательной организации». Локальных нормативных актов, затрагивающих вопросы информационной безопасности в образовательной организации не принято.

Организационные меры защиты информации в образовательной организации реализованы следующим образом:

– организован контроль, соблюдение временного режима труда и пребывания сотрудников на территории организации;

– организована работа с документами и документированной информацией, т.е. ведется учет, исполнение, возврат, хранение носителей конфиденциальной информации;

– администрирование автоматизированных систем с разграничением прав пользователей.

Политика безопасности автоматизированных информационных систем образовательной организации предписывает пользователям регулярно (не реже одного раза в год) изменять свои пароли, но не контролирует смену и непохожесть паролей.

Чтобы определить задействованных в обмене критической информацией сотрудников и угрозы информационной безопасности, которые могут возникнуть в связи с их деятельностью, представим графически организационную структуру образовательной организации (рисунок 5).

На вершине организационной структуры находится директор школы. Далее расположены бухгалтер, заместитель директора по хозяйственной части, заместитель директора по учебно-воспитательной работе, заместитель директора по воспитательной работе и заведующий структурным подразделением.

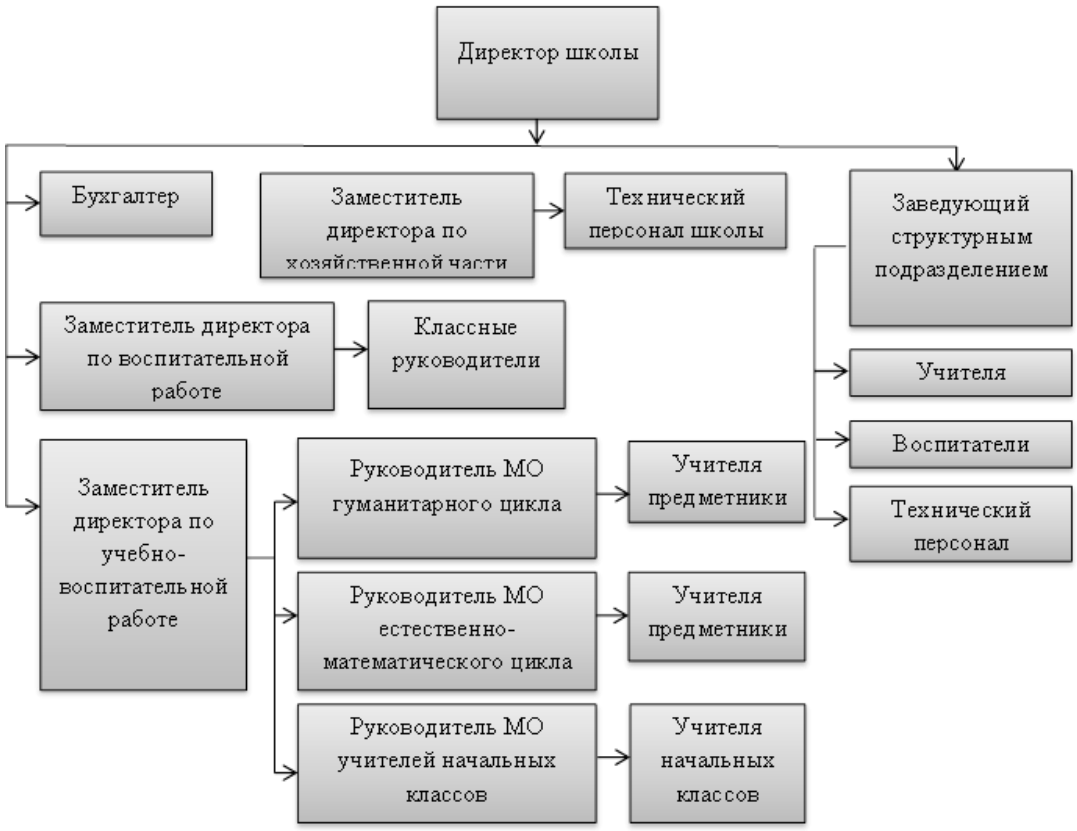

Рисунок 5 – Организационная структура МОУ «Саргазинской СОШ»

Под руководством заместителя директора по учебно-воспитательной работе работают руководители методических объединений и все учителя школы. Заместитель директора по воспитательной работе руководит работой классных руководителей. Структурным подразделением руководит заведующий, в его подчинении находятся учителя, воспитатели и технический персонал структурного подразделения. Под началом заместителя директора по хозяйственной части работает технический персонал школы. Из-за совмещения нескольких профессиональных ролей, например учитель и классный руководитель, наблюдается подчинение одного работника нескольким руководителям.

Проведя анализ структуры организации в аспекте информационной безопасности [54, 56], можно сделать вывод, что педагогический состав осуществляет между собой хаотическое информационное взаимодействие. Технический персонал образовательной организации в информационном

обмене конфиденциальной информации не участвует, но имеет к ней доступ.

Анализ организационной структуры дает нам общее и самое поверхностное представление об угрозах информационной безопасности. Для более комплексного понимания того, какие меры необходимо принять для противодействия угрозам информационной безопасности в организации, необходимо выявление критических видов информации и поддерживающей инфраструктуры.

Исследуемая образовательная организация содержит следующие информационные ресурсы [17, 36, 40]:

1. Информация, относящаяся к коммерческой тайне:

– заработная плата,

– договоры с сетевыми партнерами и поставщиками.

2. Защищаемая информация:

– личные дела работников и обучающихся,

– трудовые договора,

– личные карты работников,

– содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности,

– персональные данные работников и обучающихся,

– прочие разработки и документы для внутреннего пользования.

3. Открытая информация:

– информация на web-сайте http://mousargazinskay.ucoz.ru,

– учредительный документ,

– устав,

– перечень образовательных программ и т. д.

Ко всей информации образовательной организации без ограничений имеет доступ только директор школы. К информации, относящейся к коммерческой тайне, в образовательной организации имеют доступ только

два человека – это директор и бухгалтер. Личные дела сотрудников, трудовые договора и личные карты работников хранятся в кабинете директора, в специальном металлическом шкафу с замком. Личные дела обучающихся хранятся в приемной у директора в незащищенном шкафу. Перед входом в приемную директора установлена камера видеонаблюдения. Регистры бухгалтерского учета и внутренняя бухгалтерская отчетность хранится в кабинете бухгалтера на стеллажах. Перед входом в кабинет бухгалтера установлена камера видеонаблюдения. Доступ в кабинет бухгалтера имеет только бухгалтер.

К видам критической информации относится та информация, потеря которой способна оказать существенное воздействие на работоспособность организации. Критической информацией для МОУ «Саргазинской СОШ» можно отнести информацию первых двух групп: информацию, относящуюся к коммерческой тайне и защищаемую информацию. За разглашение, утечку или допущение несанкционированного доступа к данной информацию образовательную организацию привлекут к административной и/или уголовной ответственности, что повлечет с собой приостановление деятельности организации.

На программно-техническом уровне в образовательной организации осуществляется управление доступом в автоматизированных информационных системах путем деления информации по соответствующим должностям и полномочиям доступа к ней, т.е. спецификация и контроль действий пользователей над информационными ресурсами образовательной организации.

Программно-аппаратным средством защиты информации на автоматизированном рабочем месте сотрудника в образовательной организации является базовая защита операционной системы Windows и Антивирусная система Kaspersky Anti-Virus для защиты от компьютерных вирусов.

Мы исследовали персональные компьютеры образовательной организации. Автоматизированным рабочим местом в 50% случаев пользуется группа педагогов, при этом используется один пользователь операционной системы. Часто (87%) пароль для входа в систему хранится в общем доступе (на мониторе, под клавиатурой) или может передаваться в устной форме. Также производится нерегулярное обновление баз и сканирование рабочих станций на наличие вредоносного программного обеспечения. На 30% персональных компьютеров антивирусная система не установлена. Разграничение прав на автоматизированных рабочих местах отсутствуют на 98% персональных компьютеров, что ведет к беспорядочной установке нелицензионного программного обеспечения. Межсетевой экран используется на 20% персональных компьютеров организации.

Ни один сотрудник организации не проходил обучение основам информационной безопасности. Нами был составлен и проведен тест на знание основ информационной безопасности (приложение 4). В данный тест были включены вопросы теоретического и практического характера [26]. Результаты теста представлены на рисунке 6.

Рисунок 6 – Результаты теста на знание основ информационной безопасности

Результаты теста показали, что персонал образовательной организации обладает низким уровнем знания основ информационной безопасности: 63% опрошенных дали меньше 30% правильных ответов на вопросы теста. Тест также показал, что персонал образовательной организации часто нарушает основные правила информационной безопасности и не знает, что за это предусмотрено наказание. Более 80% правильных ответов дал только 1% опрошенных сотрудников.

Исходя из вышесказанного, можно сделать вывод, что главным источником угрозы информационной безопасности в МОУ «Саргазинской СОШ» является собственный персонал организации. Исследования проблем информационной безопасности образовательной организации указывают на то, что большая часть нарушений в области безопасности приходится на неумышленные действия персонала организации, которые наносят наибольший вред информационной среде организации. Причиной неумышленных действий персонала, приводящих к нарушению информационной безопасности, чаще всего становится незнание основных правил информационной безопасности.

2.2. Комплекс мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности МОУ «Саргазинской СОШ» со стороны собственного персонала

На втором этапе исследования автором разработан комплекс мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности МОУ «Саргазинской СОШ». Комплекс мероприятий (рисунок 7) содержит три блока: управленческий, методический и инженерно-технический. В первый блок входят мероприятия по противодействию угрозам информационной безопасности со стороны собственного персонала, которые рекомендованы к внедрению администрацией организации. Во втором блоке описаны мероприятия,

направленные непосредственно на собственный персонал организации. Третий блок охватывает мероприятия, способствующие минимизации угроз информационной безопасности со стороны персонала организации с помощью технических средств.

Цель данного комплекса: предложить мероприятия, способствующие развитию и совершенствованию информационной безопасности и эффективному противодействию угрозам информационной безопасности со стороны собственного персонала для МОУ «Саргазинской СОШ».

Из сформулированных целей вытекают следующие задачи:

- разработать управленческие мероприятия;
- разработать методические мероприятия;
- разработать инженерно-технические мероприятия.

Важно отметить, что значимость внедрения комплекса мероприятий по противодействию угрозам информационной безопасности со стороны собственного персонала для рассматриваемой организации является актуальной, так как организация осуществляет свою деятельность в информационной среде, и безопасность критической информации является основой работоспособности организации.

В нашем исследовании под информационной безопасностью образовательной организации мы будем понимать защищенность информации образовательной организации от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб самой образовательной организации или участникам образовательного процесса образовательной организации. В свою очередь защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности, а организация мероприятий - это комплекс мер, направленных на реализацию запланированных действий в решении данного вопроса.

Рисунок 7 - Комплекс мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности МОУ «Саргазинской СОШ» со стороны собственного персонала

Остановимся на каждом мероприятии более подробно.

Мероприятие 1. Разработка управленческих решений в сфере информационной безопасности.

Информационные ресурсы организации предоставляются для производственных целей. Их использование должно быть санкционировано руководством. Использование этих ресурсов для целей, не связанных с основной работой организации, или для несанкционированных целей без утверждения руководства и процедур учета следует рассматривать как незаконное использование информационных ресурсов. При выявлении таких случаев с помощью средств отслеживания действий или других средств, их следует довести до сведения соответствующего руководства для наложения дисциплинарных взысканий. Сотрудников организации следует предупредить, что они не имеют право доступа, кроме случаев, которые формально санкционированы и задокументированы. Список лиц с правом доступа к конфиденциальной документации должен быть максимально ограничен, а разрешение на ее использование должно выдаваться руководством организации и фиксироваться в соответствующих журналах.

Документы, содержащие информацию, относящуюся к коммерческой тайне и защищаемую информация необходимо хранить в защищенном месте для удовлетворения правовых требований, а также для поддержки основных производственных работ. Конфиденциальная документация должна храниться в надежных шкафах под замком. Содержащую конфиденциальную информацию документацию, создаваемую с помощью технических средств, следует хранить отдельно от других файлов и приложений. Для персонала следует определить процедуры доступа в спецхранилища.

Все помещения организации в зависимости от назначения и характера совершаемых в них актов, действий или операций необходимо разделить на несколько зон доступности (безопасности), которые

учитывают степень важности различных частей объекта с точки зрения возможного ущерба от криминальных угроз.

Обязательно к использованию в организации системы охранной и противопожарной сигнализации. Охранно-пожарная сигнализация организации должна быть предназначена для обнаружения проникновения в помещение человека, движения на объекте, целостности окон, стен, решеток, открытия дверей, или возникновения пожара в помещении и своевременно информировать об этом событии ответственных лиц, который, в свою очередь, принимают необходимые меры по ликвидации данного события. Персонал организации не должен иметь возможность отключить или повлиять на работу охранно-пожарной сигнализации. Так же обязательно к использованию в организации системы видео наблюдения, как постоянного визуального мониторинга и запись на магнитные или цифровые носители информации о ситуации на охраняемом объекте с централизованного поста. Она должна контролировать входы персонала на территорию организации, в здания, отдельные кабинеты. При необходимости система видеокамер может устанавливаться непосредственно во внутренних помещениях организации (аудиториях, классах, конференц-залах и т.п.), что позволяет вести наблюдение за происходящим.

Для всех программно-технических средств организации необходимо использовать источники бесперебойного питания. Система бесперебойного питания и резервных аккумуляторов должна обеспечивать работоспособность всех сигнализационных, видео, контрольных и компьютерных систем при пропадании напряжения в электрической сети. При работе на автоматизированном рабочем месте обязательно использовать систему идентификации пользователей. Обязательно к использованию только лицензионное программное обеспечение для нужд организации.

Использовать программно-аппаратные средства и оборудование организации необходимо исключительно в рабочих целях. Должен быть установлен запрет на использование программно-аппаратных средств и оборудования в личных и других целях.

Важным управленческим решение является закрепление во внутриорганизационной документации и трудовых договорах с сотрудниками постановления о том, что информация, созданная и хранящаяся на программно-аппаратных средствах организации, является собственностью данной организации, а также того, что сотрудник организации несет ответственность за сохранность своего пароля, при этом запрещается передача, запись на бумаге, хранение в сети и другие действия, в результате которых пароль может стать известным сторонним лицам, в том числе другим сотрудникам организации.

Для своевременного реагирования на нарушения информационной безопасности со стороны персонала в организации должны проводиться регулярные совещания руководства для разработки изменений политики безопасности, перераспределения обязанностей по обеспечению защиты и координации действий по поддержанию режима безопасности. В случае необходимости следует привлечь специалистов по вопросам защиты информации для консультаций. Необходимо вступать в контакты со специалистами других организаций, чтобы быть в курсе современных направлений и промышленных стандартов, а также, чтобы установить соответствующие деловые отношения для рассмотрения случаев нарушения защиты. Следует всячески поощрять комплексный подход к проблемам информационной безопасности, оказывать административную поддержку инициативам по обеспечению безопасности, а также организовывать совместную работу персонала организации для эффективного решения проблем.

Также необходимо управленческое решение о внесении дополнений во внутриорганизационные нормативные документы данных о том, что

сотрудники организации обязаны строго придерживаться законодательства Российской Федерации при эксплуатации программно-аппаратных средств и оборудования организации, обязаны соблюдать авторские права производителей программного обеспечения и условия использования программных лицензий, а также законодательство в области интеллектуальной собственности. Необходимо принятие управленческого решения о том, что каждый пользователь внутренней сети организации обладает теми привилегиями использования программно-аппаратных средств, которые необходимы для осуществления его деятельности. Необходимо определить привилегии и нормативно установить полномочия сотрудников при использовании информационных систем.

Важным является принятие управленческого решения о том, что все сотрудники организации обязаны проходить обучение основам информационной безопасности, установить соответствующие сроки, время и содержание обучающих программ.

Среди запрещающих мер, составляющих управленческие решения, можно выделить запрет на эксплуатацию программно-аппаратных средств и оборудования организации лицами, не являющимися сотрудниками организации. Нужно также отметить введение запретов на самостоятельную установку программного обеспечения на программно-аппаратные средства организации; на изменение, копирование, удаление и другие действия с информацией, хранящейся на автоматизированных рабочих местах других сотрудников организации; на использование программно-аппаратных средств организации в целях, противоречащих законодательству Российской Федерации. Также руководство организации должно оставлять за собой право проверки и анализа всех программно-аппаратных средств и оборудования организации.

Мероприятие 2. Осуществление контроля за доступом к данным и информационным системам.

Для обеспечения эффективного контроля за доступом к данным и информационным системам руководство должно реализовывать формальный процесс пересмотра прав доступа пользователей через регулярные промежутки времени. Такой процесс должен обеспечивать следующее:

– пересмотр полномочий доступа пользователей через регулярные промежутки времени (рекомендуется период в 6 месяцев);

– пересмотр разрешения на предоставление специальных привилегированных прав доступа через более короткие промежутки времени (рекомендуется период в 3 месяца);

– проверка предоставленных привилегий через регулярные промежутки времени, чтобы не допустить получения пользователями несанкционированных привилегий.

Контроль за работой персонала 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.

Субъектами контрольной деятельности в вопросах противодействия угрозам информационной безопасности образовательной организации являются все сотрудники организации.

Подконтрольным объектом может быть деятельность любого сотрудника организации, система профессиональной подготовки и переподготовки сотрудника. Выбор объекта контроля должен определяться его способностью влиять (положительно или отрицательно)

на информационную безопасность организации в целом. В рамках подконтрольного объекта очень важны его составные элементы, после определения которых можно непосредственно приступить к контролю. Так, в рамках проверки состояния защиты конфиденциальной информации конкретным сотрудником образовательной организации должны быть изучены:

– соблюдение сотрудником норм, правил хранения и охраны в помещениях, спецхранилищах, на рабочих местах носителей информации;

– соблюдение сотрудником порядка хранения и уничтожения конфиденциальной информации;

– соблюдение сотрудником требований порядка обращения с носителями конфиденциальной информации;

– соблюдение сотрудником правил и мер по предотвращению несанкционированного выноса носителей конфиденциальной информации за территорию организации.

Мероприятие 3. Обучение персонала МОУ «Саргазинской СОШ» основам информационной безопасности.

Чтобы программа обучения сотрудников была успешной, она должна быть полезной, уместной, интересной, она должна отвечать и нуждам организации в целом и нуждам каждого работника в отдельности.

Ориентационные семинары должны иметь своей целью обучение методам сохранности ценной информации. Сотрудники должны четко знать категории охраняемых сведений, возможные способы и методы проникновения к ним со стороны нарушителя, процедуры защиты конфиденциальной информации организации и правила работы с конфиденциальными документами.

Необходимо иметь систему повышения уровня технической грамотности и информированности пользователей в области информационной безопасности, а также переподготовки специалистов по

защите информации. Для этого необходимы регулярное проведение тренингов для персонала и контроль готовности новых сотрудников по применению правил информационной защиты, а также периодическая переподготовка специалистов организации в сфере информационной безопасности. Особенно важно проводить тренинги при изменении конфигурации информационной системы (внедрении новых технологий и прикладных автоматизированных систем, смены оборудования, операционной системы, ключевых приложений, принятии новых правил или инструкций и т.д.).

В процессе проведения обучения и повышения уровня технической грамотности и информированности пользователей необходимо ознакомить персонал с мерами ответственности за нарушение правил информационной безопасности организации. Этот раздел требует особого внимания. Зачастую организации забывают четко проработать моменты, связанные с наступлением той или иной ответственности в случае нарушения политики безопасности. В связи с этим, злоумышленники могут остаться безнаказанными даже в случае их обнаружения, выявления и доказательства умышленности их злонамеренных действий. В зависимости от наступивших последствий и юридического статуса нарушителя к нему могут быть применены дисциплинарные, административные или уголовные меры воздействия.

Мероприятие 4. Разработка рекомендаций для персонала МОУ «Саргазинской СОШ» в сфере информационной безопасности.

Крайне важным условием эффективного противодействия угрозам информационной безопасности организации является участие и помощь персонала организации.

Сотрудники организации должны ознакомиться с необходимыми сведениями о политике организации и принятых в ней процедурах, включая требования к информационной безопасности и другим средствам контроля, а также научиться правильно пользоваться информационными

ресурсами (например, знать процедуру входа в систему, уметь пользоваться пакетами программ).

Главной рекомендацией для персонала организации по противодействию угрозам информационной безопасности является внимательное изучение всех документов по вопросам обеспечения информационной безопасности, в которых должно быть четко и однозначно определены права, обязанности, уровни ответственности, система поощрения/наказания сотрудника. Каждый сотрудник должен безукоризненно соблюдать все процедуры организации по вопросам информационной безопасности. Например, обязаны посещать мероприятия по вопросам обеспечения информационной безопасности по плану-графику организации (проходить обучение, повышать квалификацию, участвовать в тренингах).

Каждый сотрудник является активным пользователем информационных ресурсов организации. Пользователи должны знать свои обязанности по обеспечению эффективного контроля доступа, особенно, что касается использования паролей и защиты пользовательского оборудования.

Пользователи должны следовать установленным процедурам поддержания режима безопасности при выборе и использовании паролей.

Пароли являются основным средством подтверждения полномочий доступа пользователей к компьютерным системам. Предлагаются следующие рекомендации по выбору и использованию паролей:

– хранить пароли в секрете;

– не записывать пароли на бумаге, если не представляется возможным ее хранение в защищенном месте;

– изменять пароли всякий раз, когда есть указания на возможную компрометацию систем или паролей;

– выбирать пароли, содержащие не менее шести символов;

– при выборе паролей не следует использовать: месяцы года, дни недели; фамилии, инициалы и регистрационные номера автомобилей; названия и идентификаторы организаций; номера телефонов или группы символов, состоящие из одних цифр; пользовательские идентификаторы и имена, а также идентификаторы групп и другие системные идентификаторы; более двух одинаковых символов, следующих друг за другом; группы символов, состоящие из одних букв;

– изменять пароли через регулярные промежутки времени (приблизительно через 30 суток) и избегать повторное или циклическое использование старых паролей;

– чаще изменять пароли для привилегированных системных ресурсов, например, пароли доступа к определенным системным утилитам;

– изменять временные пароли при первом входе в системы;

– не включать пароли в сценарии автоматического входа в системы, например в макросы или функциональные клавиши.

Если пользователям необходим доступ ко многим сервисам и платформам и от них требуется поддержание нескольких паролей, то им рекомендуется использовать один единственный надежный пароль для входа во все системы, которые обеспечивают минимальный уровень защиты для хранения паролей.

Пользователи должны обеспечить надлежащую защиту оборудования, оставленного без присмотра. Оборудование, установленное на рабочих местах пользователей, например, рабочие станции и файловые серверы, может потребовать специальной защиты от несанкционированного доступа в тех случаях, когда оно оставляется без присмотра на продолжительное время. Все пользователи должны знать требования к безопасности и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты. Предлагаются следующие рекомендации:

– завершить активные сеансы связи по окончанию работы, если их нельзя защитить посредством соответствующей блокировки;

– выйти из мэйнфреймов по окончании сеанса связи. Не ограничиваться только выключением персонального компьютера или терминала;

– защитить персонального компьютера или терминалы, которые не используются, с помощью блокировки с ключом или эквивалентного средства контроля, например, доступом по паролю.

Пользователи информационных сервисов обязаны регистрировать любые наблюдаемые или предполагаемые слабости в системе безопасности, либо угрозы системам или сервисам и сообщать о них. Пользователи должны незамедлительно доводить подобные инциденты до сведения своего непосредственного руководства, либо поставщиков соответствующих услуг. Пользователи не должны пытаться проверять предполагаемые слабости в системы защиты. Это нужно для защиты самих пользователей, поскольку их действия по тестированию слабости могут быть истолкованы как попытки несанкционированного использования системы.

Пользователям информационных сервисов необходимо регистрировать все случаи, когда функционирование программного обеспечения представляется им неправильным, т.е. не соответствующим спецификации; они должны сообщать об этом в местную службу технической поддержки информационных систем или непосредственно поставщику данных услуг.

Пользователю, подозревающему, что сбой вызван вредоносной программой, например, компьютерным вирусом, рекомендуется выполнить следующие действия:

1. Записать симптомы и все сообщения, появляющиеся на экране.

2. Прекратить работу на компьютере и, если возможно, отключить его.

3. Немедленно сообщить об инциденте в службу технической поддержки информационных систем. Если оборудование подлежит осмотру, то его необходимо отсоединить от сетей организации, прежде чем снова включить питание. Не использовать на других компьютерах носители информации, записанные на этом компьютере.

4. Ни при каких обстоятельствах пользователи не должны пытаться удалить подозрительное программное обеспечение. Восстановление программного обеспечения должны выполнять специалисты, имеющие соответствующие знания и опыт работы.

Противовирусные программные средства, разработанные поставщиком с хорошей репутацией, следует использовать следующим образом:

– программные средства обнаружения конкретных вирусов (которые должны регулярно обновляться и использоваться в соответствии с инструкциями поставщика) следует применять для проверки компьютеров и носителей информации на наличие известных вирусов либо как меру предосторожности, либо как повседневную процедуру;

– программные средства обнаружения изменений, внесенных в данные, должны быть по необходимости инсталлированы на компьютерах для выявления изменений в выполняемых программах;

– программные средства нейтрализации вирусов следует использовать с осторожностью и только в тех случаях, когда характеристики вирусов полностью изучены, а последствия от их нейтрализации предсказуемы.

– носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования.

Мероприятие 5. Использование системы управления доступом и разграничения полномочий сотрудников в использовании информации и информационных систем организации.

Для управления процессом предоставления прав доступа к персональным компьютерам и информационным системам организации требуются формальные процедуры. Эти процедуры должны включать в себя все стадии жизненного цикла управления доступом пользователей — от начальной регистрации новых пользователей до удаления учетных записей пользователей, которые больше не нуждаются в доступе к информационным сервисам. Особое внимание следует уделить необходимости управления процессом предоставления привилегированных прав доступа, которые позволяют пользователям обойти средства системного контроля.

Для управления доступом ко всем многопользовательским информационным системам должна существовать формальная процедура регистрации и удаления учетных записей пользователей.

Доступ к многопользовательским информационным системам необходимо контролировать посредством формального процесса регистрации пользователей, который должен, например:

– проверять, предоставлено ли пользователю разрешение на использование сервиса владельцем системы;

– проверять, достаточен ли уровень доступа к системе, предоставленного пользователю, для выполнения возложенных на него функций и не противоречит ли он политике безопасности, принятой в организации, например, не компрометирует ли он принцип разделения обязанностей;

– предоставлять пользователям их права доступа в письменном виде;

– потребовать от пользователей подписания обязательства, чтобы показать, что они понимают условия доступа;

– потребовать от поставщиков услуг, чтобы они не предоставляли доступ к системам до тех пор, пока не будут закончены процедуры определения полномочий;

– вести формальный учет всех зарегистрированных лиц, использующих систему;

– немедленно изымать права доступа у тех пользователей, которые сменили работу или покинули организацию;

– периодически проверять и удалять пользовательские идентификаторы и учетные записи, которые больше не требуются;

– проверять, не выданы ли пользовательские идентификаторы, которые больше не нужны, другим пользователям.

Предоставление и использование излишних системных привилегий зачастую оказывается одним из основных факторов, способствующих нарушению режима безопасности систем (уязвимость). Для многопользовательских систем, требующих защиты от несанкционированного доступа, предоставление привилегий необходимо контролировать посредством формального процесса определения полномочий следующим образом:

1. Идентифицировать привилегии, связанные с каждым программным продуктом, поддерживаемым системой, например, с операционной системой или системой управления базой данных, а также категории сотрудников, которым их необходимо предоставить.

2. Предоставить привилегии отдельным лицам только в случае крайней необходимости и в зависимости от ситуации, т.е. только когда они нужны для выполнения ими своих функций.

3. Реализовать процесс определения полномочий и вести учет всех предоставленных привилегий. Не следует предоставлять привилегии до окончания процесса определения полномочий.

4. Содействовать разработке и использованию системных программ, чтобы избежать необходимость предоставления привилегий пользователям.

5. Пользователи, которым предоставлены большие привилегии для специальных целей, должны использовать другой пользовательский идентификатор для обычной работы.

В настоящее время пароли являются основным средством подтверждения полномочий доступа пользователей к компьютерным системам. Назначение паролей необходимо контролировать посредством формального процесса управления, требования к которому должны быть следующими:

1. Потребовать от пользователей подписания обязательства по хранению персональных паролей и паролей рабочих групп в секрете.

2. В тех случаях, когда пользователи должны сами выбирать свои пароли, выдать им надежные временные пароли, которые они обязаны немедленно сменить на надежный персональный пароль. Временные пароли также выдаются, когда пользователи забывают свои пароли. Временные пароли должны выдаваться только после положительной идентификации пользователя.

3. Передавать временные пароли пользователям надежным способом. Следует избегать передачу паролей через посредников или посредством незащищенных (незашифрованных) сообщений электронной почты. Пользователи должны подтвердить получение паролей.

Мероприятие 6. Разработка мер, направленных на программно-технические средства МОУ «Саргазинской СОШ».

Необходимо периодически проводить процедуры шифрования конфиденциальной информации, находящейся в электронном виде, по мере ее поступления.

Необходимо постоянно использовать межсетевой экран, обязательно использовать средств фильтрации входящих и исходящих почтовых

сообщений организации и использовать системы защиты от спама почтового сервера организации.

Необходимо обязательно использовать обновляемое антивирусное программное обеспечение на всех серверах и рабочих станциях организации. Для предотвращения и выявления случаев внедрения вредоносного программного обеспечения требуется принятие надлежащих мер предосторожности. Необходимо реализовать меры по обнаружению и предотвращению проникновения вирусов в системы и процедуры информирования персонала об их вреде. Сотрудникам необходимо разъяснить, что предотвращение вирусов лучше, чем ликвидация от их проникновения. В основе защиты от вирусов должны лежать знания и понимание правил безопасности, надлежащие средства управления доступом к системам и следующие конкретные меры:

1. Организация должна определить формальную политику, требующую соблюдение условий лицензий на использование программного обеспечения и запрещающую использование несанкционированных программ.

2. Необходимо проводить регулярную проверку программ и данных в системах, поддерживающих критически важные производственные процессы. Наличие случайных файлов и несанкционированных исправлений должно быть расследовано с помощью формальных процедур.

3. Необходимо определить управленческие процедуры и обязанности по уведомлению о случаях поражения систем компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения.

4. Следует составить надлежащие планы обеспечения бесперебойной работы организации для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных, программ и их восстановления.

2.3. Оценка эффективности комплекса мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности организации

Противодействие угрозам информационной безопасности организации со стороны собственного персонала это, по сути, процесс минимизации рисков, связанных с возможным негативным воздействием собственного персонала организации на ее информационную безопасность.

Политике информационной безопасности организации должны соответствовать как сама информационная среда организации, так и каждый ее элемент. Персонал организации - это ключевой элемент информационной среды организации, который может оказать и/или оказывает негативное влияние на информационную безопасность организации.

Для эффективного противодействия угрозам информационной безопасности со стороны собственного персонала организации необходимо принимать меры. Особенно остро в принятии таких мер нуждаются образовательные организации. Наличие конфиденциальной информации на бумажных и электронных носителях, а так же множества персональных компьютеров с доступом к информационным системам требует ответственного подхода к обеспечению информационной безопасности.

В рамках данной работы был проанализирован процесс противодействия угрозам информационной безопасности МОУ «Саргазинской СОШ» со стороны собственного персонала. На основании анализа выявлены проблемные места и предприняты меры по совершенствованию системы информационной безопасности школы.

На третьем этапе исследования был внедрен комплекс мероприятий по противодействию угрозам информационной безопасности организации со стороны собственного персонала (рисунок 7).

Управленческий блок

Мероприятие 1. Разработка управленческих решений в сфере информационной безопасности.

Мероприятие 2. Осуществление контроля за доступом к данным и информационным системам.

Методический блок

Мероприятие 3. Обучение персонала МОУ «Саргазинской СОШ» основам информационной безопасности

Мероприятие 4. Разработка рекомендаций для персонала МОУ «Саргазинской СОШ» в сфере информационной безопасности.

Инженерно-технический блок

Мероприятие 5. Использование системы управления доступом и разграничения полномочий сотрудников в использовании информации и информационных систем организации.

Мероприятие 6. Разработка мер, направленных на программно-технические средства МОУ «Саргазинской СОШ».

В рамках мероприятия 1 были приняты следующие управленческие решения:

1. Конфиденциальная документация помещена в надежный шкаф под замок. Для документации, созданной с помощью технических средств, создано отдельное защищенное хранилище. Для персонала определены процедуры доступа в спецхранилища: назначен ответственный за доступ к конфиденциальной информации, заведен журнал учета.

2. Все помещения организации в зависимости от назначения и характера совершаемых в них актов, действий или операций разделены на несколько зон доступности (безопасности), которые учитывают степень важности различных частей объекта с точки зрения возможного ущерба от криминальных угроз.

3. Установлено 6 дополнительных камер видеонаблюдения в «слепые» зоны организации.

4. Заключен договор обслуживания технических средств образовательной организации со специализированной сторонней организацией.

5. В повестку совещаний руководства организации внесены вопросы по разработке изменений политики безопасности, перераспределения обязанностей по обеспечению защиты и координации действий по поддержанию режима безопасности.

6. В методическую работу школы включены вопросы по обучению сотрудников организации основам информационной безопасности.

В рамках мероприятия 2 было решено:

1. Пересмотр полномочий доступа пользователей к информационным системам организации осуществлять через каждые 6 месяцев.

2. Пересмотр разрешения на предоставление специальных привилегированных прав доступа осуществлять через каждые 3 месяца.

3. В систему контроля образовательной организации включить контроль:

– за соблюдением сотрудником норм, правил хранения и охраны в помещениях, спецхранилищах, на рабочих местах носителей информации;

– за соблюдением сотрудником порядка хранения и уничтожения конфиденциальной информации;

– за соблюдением сотрудником требований порядка обращения с носителями конфиденциальной информации;

– за соблюдением сотрудником правил и мер по предотвращению несанкционированного выноса носителей конфиденциальной информации за территорию организации.

В рамках мероприятия 3 в планы работы методических объединений школы были внесены мероприятия по обучению персонала МОУ «Саргазинской СОШ» основам информационной безопасности.

В течение 2018 и 2019 годов на семинарах были изучены следующие темы:

1. Понятие информационной безопасности. Основные составляющие. Важность и сложность проблемы информационной безопасности.

2. Наиболее распространенные угрозы информационной безопасности.

3. Уровни информационной безопасности.

4. Идентификация и аутентификация, управление доступом.

5. Экранирование, анализ защищенности.

6. Обеспечение высокой доступности.

Нами был повторно проведен тест на знание основ информационной безопасности (приложение 4). Результаты теста (рисунок 8) показали, что уровень знания основ информационной безопасности повысился.

Рисунок 8 – Результаты первого и повторного тестов на знание основ информационной безопасности

Второй тест на знание основ информационной безопасности в педагогическом коллективе дал следующие результаты:

– более 50% правильных ответов дали 76% сотрудников, что на 67% больше, чем до внедрения комплекса по совершенствованию процесса противодействия угрозам информационной безопасности организации;

– менее 50% правильных ответов дали 24% сотрудников, что на 92% меньше, чем до внедрения комплекса по совершенствованию процесса противодействия угрозам информационной безопасности организации.

В рамках мероприятия 4 были разработаны рекомендации для персонала МОУ «Саргазинской СОШ» в сфере информационной безопасности. С разработанными рекомендациями сотрудники были ознакомлены на производственном совещании. Данные рекомендации размещены на сайте школы.

В рамках мероприятия 5 для управления процессом предоставления прав доступа к персональным компьютерам и информационным системам организации разработаны и используются формальные процедуры, которые затрагивают все стадии жизненного цикла управления доступом пользователей. Инструкции по правилам безопасного использования информационных систем были предоставлены для самостоятельного изучения под личную ответственность руководителей методических объединений.

В результате работы в рамках мероприятия 5 руководством организации было принято решение о назначении заместителя директора по хозяйственной части ответственным за инструктажи по информационной безопасности организации.

В рамках мероприятия 6 на всех автоматизированных рабочих местах школы:

1. Созданы учетные записи пользователей: администратор, пользователь 1, пользователь 2, …, гость. Для пользователей и гостей установлен запрет на установку программного обеспечения.

2. Постоянно используется межсетевой экран.

3. Используется и периодически обновляется антивирусное программное обеспечение.

4. Используется и периодически обновляется только лицензионное программное обеспечение.

5. Проводится регулярная проверка программ и данных.

Для доказательства эффективности разработанного комплекса до (на втором этапе исследования) и после (на третьем этапе исследования) внедрения мероприятий мы провели аудит информационной безопасности МОУ «Саргазинской СОШ». Процесс аудита информационной безопасности должен отвечать требованиям принятого в организации нормативного документа, описывающего процесс аудита информационной безопасности, либо требованиям признаваемого сообществом международного (национального) нормативного документа (стандарта, рекомендации). Таким нормативным документом для банковской системы Российской Федерации является стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации СТО БР ИББС–1.2–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» [40], принятый и введенный в действие Распоряжением Банка России № Р – 399 от 17 мая 2014 года. Настоящий стандарт устанавливает способы определения текущего уровня информационной безопасности Банка России при проведении аудита информационной безопасности и самооценки информационной безопасности.

В исследуемой организации нормативного документа описывающего процесс аудита информационной безопасности не принято. Стандарта для аудита информационной безопасности образовательной организации, признанного международным (национальным) сообществом так же не разработано. В связи с этим, мы провели аудит информационной безопасности МОУ «Саргазинской СОШ», взяв за основу

СТО БР ИББС–1.2–2014. Оценка текущего состояния информационной безопасности проводилась с учетом тематики диссертационного исследования, его целей и задач. В качестве экспертов выступили три человека: сотрудник школы (из руководящего состава), автор магистерской диссертации, сотрудник сетевого партнера школы (преподаватель кафедры информатики, информационных технологий и методики обучения информатике ФГБОУ ВО «ЮУрГГПУ»).

Для определения текущего уровня информационной безопасности исследуемой организации мы использовали групповые и частные показатели информационной безопасности [40]. Групповые показатели информационной безопасности M_i МОУ «Саргазинской СОШ» (управленческий – M_1, методический – M_2, инженерно-технический – M_3) образуют структуру направлений оценки EV_{M_i}, детализируя оценки текущего уровня информационной безопасности организации. Частные показатели информационной безопасности M_{ij} входят в состав групповых показателей и представлены в виде вопросов, ответы на которые дают возможность определить оценки $EV_{M_{ij}}$, которые затем формируют оценки EV_{M_i} групповых показателей.

В таблице 2 приведены форма, предназначенные для заполнения при проведении оценки текущего уровня информационной безопасности школы. Каждая из форм содержит групповой показатель информационной безопасности и входящие в него частные показатели информационной безопасности.

Для показателей устанавливается следующая шкала степени их выполнения:

– «нет» – оценке присваивается значение, равное нулю;

– «частично» – оценке присваивается значение 0,25, 0,5 или 0,75;

– «да» – оценке присваивается значение, равное единице.

Таблица 2 – Форма оценки уровня информационной безопасности МОУ «Саргазинской СОШ»

Обозначение показателя	Показатель информационной безопасности	Оценка показателя
1	2	3
M_1	**Управленческий**	
M_{11}	Предоставляется ли доступ к защищаемым данным только с целью выполнения служебных обязанностей?	
M_{12}	Определен ли, выполняется ли, регистрируется ли и контролируется ли порядок доступа персонала организации к конфиденциальной информации?	
M_{13}	Определены ли, выполняются ли и контролируются ли процедуры, необходимые для обеспечения сохранности носителей защищаемой информации?	
M_{14}	Проводятся ли руководством регулярные совещания для разработки изменений политики безопасности, перераспределения обязанностей по обеспечению защиты и координации действий по поддержанию режима безопасности?	
M_{15}	Определены ли, регистрируются ли и контролируются ли в организации зоны доступности (безопасности), которые учитывают степень важности различных частей объекта с точки зрения возможного ущерба от криминальных угроз?	
M_{16}	Проводится ли разработка и коррекция внутренних документов, регламентирующих деятельность в области обеспечения информационной безопасности в организации, с учетом законодательства Российской Федерации.	
M_{17}	Применяются ли защитные меры обеспечения непрерывности работы организации применительно к информационным активам?	
M_{18}	Осуществляется ли формирование и назначение ролей работников организации с учетом соблюдения принципа предоставления минимальных прав и полномочий, необходимых для выполнения служебных обязанностей?	
M_{19}	Определены ли в трудовых контрактах (соглашениях, договорах) и (или) должностных инструкциях обязанности персонала по выполнению требований информационной безопасности?	

1	2	3
M_2	**Методический**	
M_{21}	Определены ли, выполняются ли и регистрируются, выполняются и регистрируются ли в организации процедуры регулярной проверки в части профессиональных навыков и оценки профессиональной пригодности работников в сфере информационной безопасности?	
M_{22}	Организована ли санкционированная руководством организации работа с персоналом в направлении повышения осведомленности и обучения в области информационной безопасности?	
M_{23}	Организуется ли для работника, получившего новую роль, обучение или инструктаж в области информационной безопасности в соответствии с полученной ролью?	
M_{24}	Назначены ли в организации ответственные за выполнение ролей по разработке, реализации планов и программ обучения и повышения осведомленности в области информационной безопасности и по контролю их результатов?	
M_{25}	Разработаны ли и введены ли в действие инструкции и рекомендации для персонала организации по процедурам реагирования на инциденты информационной безопасности?	
M_{26}	Разработаны ли и введены ли в действие инструкции и рекомендации для персонала организации по поддержанию режима безопасности для оборудования, оставленного без присмотра.	
M_{27}	Разработаны ли и введены ли в действие инструкции для персонала организации и рекомендации по поддержанию режима безопасности при выборе и использовании паролей.	
M_{28}	Разработаны ли и введены ли в действие инструкции и рекомендации для персонала организации по использованию сети Интернет, учитывающие особенности образовательного процесса?	
M_{29}	Разработаны ли и введены ли в действие инструкции и рекомендации для персонала организации по антивирусной защите, учитывающие особенности образовательного процесса?	

1	2	3
M_3	**Инженерно-технический**	
M_{31}	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры идентификации, аутентификации, авторизации субъектов доступа?	
M_{32}	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры разграничения доступа к информационным активам на основе ролевого метода с определением для каждой роли полномочий по доступу к информационным активам?	
M_{33}	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры регистрации действий субъектов доступа с обеспечением контроля целостности и защиты данных регистрации?	
M_{34}	Осуществляется ли работа всех работников организации под уникальными и персонифицированными учетными записями?	
M_{35}	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры управления учетными записями субъектов доступа?	
M_{36}	Применяются ли на всех автоматизированных рабочих местах организации средства антивирусной защиты?	
M_{37}	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации процедуры установки и регулярного обновления средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах?	
M_{38}	Проведено ли в организации выделение ограниченного числа пакетов, содержащих перечень сервисов и ресурсов сети Интернет, доступных для пользователей?	
M_{39}	Определены ли, выполняются ли, регистрируются ли и контролируются ли процедуры установки на персональные компьютеры программного обеспечения?	

Оценка $EV_{M_{ij}}$ частного показателя формируется на основании выявленной проверяющей группой степени выполнения требований посредством экспертного оценивания.

Оценка группового показателя EV_{M_i} вычисляется из оценок входящих в него частных показателей $EV_{M_{ij}}$ по формуле (1):

$$EV_{M_i} = \frac{\sum_j EV_{M_{ij}}}{j}, \quad (1)$$

Итоговая экспертная оценка текущего состояния группового показателя EV_{M_i} вычисляется как среднее арифметическое оценок всех экспертов.

Опираясь на СТО БР ИББС–1.2–2014 введем шкалу оценивания текущего состояния информационной безопасности организации. Если итоговая оценка EV_{M_i} лежит в полуинтервале [0; 0,5), то данному направлению оценки присваивается низкий уровень информационной безопасности. Если оценка EV_{M_i} лежит в полуинтервале [0,5; 0,85), то данному направлению оценки присваивается средний уровень информационной безопасности. Если оценка EV_{M_i} лежит в отрезке [0,85; 1], то данному направлению оценки присваивается высокий уровень информационной безопасности.

Результаты экспертной оценки текущего состояния информационной безопасности МОУ «Саргазинской СОШ» до и после внедрения комплекса мероприятий по противодействию угрозам информационной безопасности организации со стороны собственного персонала показаны в Таблице 3 и Таблице 4 соответственно.

Таблица 3 – Результаты экспертной оценки текущего состояния информационной безопасности МОУ «Саргазинской СОШ» до внедрения комплекса мероприятий по противодействию угрозам информационной безопасности организации со стороны собственного персонала

Обозначение показателя		Оценка показателя			
		Эксперт 1	Эксперт 2	Эксперт 3	Итоговая оценка
Управленческий	M_1	0,33	0,31	0,19	0,28
	M_{11}	1,00	1,00	0,50	0,83
	M_{12}	0,75	0,50	0,50	0,58
	M_{13}	0,50	0,50	0,25	0,42
	M_{14}	0,25	0,25	0	0,17
	M_{15}	0	0	0	0
	M_{16}	0	0	0	0
	M_{17}	0	0	0	0
	M_{18}	0,50	0,50	0,50	0,50
	M_{19}	0,00	0,00	0,00	0,00
Методический	M_2	0,11	0,11	0,06	0,09
	M_{21}	0,00	0,00	0,00	0,00
	M_{22}	0,00	0,00	0,00	0,00
	M_{23}	1,00	1,00	0,50	0,83
	M_{24}	0,00	0,00	0,00	0,00
	M_{25}	0,00	0,00	0,00	0,00
	M_{26}	0,00	0,00	0,00	0,00
	M_{27}	0,00	0,00	0,00	0,00
	M_{28}	0,00	0,00	0,00	0,00
	M_{29}	0,00	0,00	0,00	0,00
Инженерно-технический	M_3	0,42	0,39	0,25	0,35
	M_{31}	0,50	0,25	0,25	0,33
	M_{32}	0,50	0,75	0,25	0,50
	M_{33}	0,00	0,00	0,00	0,00
	M_{34}	0,50	0,50	0,25	0,42
	M_{35}	0,50	0,50	0,50	0,50
	M_{36}	0,50	0,75	0,25	0,50
	M_{37}	0,25	0,00	0,00	0,08
	M_{38}	1,00	0,75	0,75	0,83
	M_{39}	0,00	0,00	0,00	0,00

Таблица 4 – Результаты экспертной оценки текущего состояния информационной безопасности МОУ «Саргазинской СОШ» после внедрения комплекса мероприятий по противодействию угрозам информационной безопасности организации со стороны собственного персонала

Обозначение показателя		Оценка показателя			
		Эксперт 1	Эксперт 2	Эксперт 3	Итоговая оценка
Управленческий	M_1	0,75	0,75	0,69	0,73
	M_{11}	1,00	1,00	0,75	0,92
	M_{12}	1,00	1,00	1,00	1,00
	M_{13}	1,00	1,00	0,75	0,92
	M_{14}	1,00	1,00	1	1,00
	M_{15}	1	1	1	1
	M_{16}	1	1	1	1
	M_{17}	0	0	0	0
	M_{18}	0,75	0,75	0,75	0,75
	M_{19}	0,00	0,00	0,00	0,00
Методический	M_2	0,94	0,94	0,94	0,94
	M_{21}	0,50	0,50	0,50	0,50
	M_{22}	1,00	1,00	1,00	1,00
	M_{23}	1,00	1,00	1,00	1,00
	M_{24}	1,00	1,00	1,00	1,00
	M_{25}	1,00	1,00	1,00	1,00
	M_{26}	1,00	1,00	1,00	1,00
	M_{27}	1,00	1,00	1,00	1,00
	M_{28}	1,00	1,00	1,00	1,00
	M_{29}	1,00	1,00	1,00	1,00
Инженерно-технический	M_3	0,83	0,81	0,72	0,79
	M_{31}	1,00	0,75	0,75	0,83
	M_{32}	1,00	1,00	0,75	0,92
	M_{33}	0,00	0,00	0,00	0,00
	M_{34}	1,00	1,00	1,00	1,00
	M_{35}	0,50	0,50	0,50	0,50
	M_{36}	1,00	1,00	1,00	1,00
	M_{37}	1,00	1,00	1,00	1,00
	M_{38}	1,00	1,00	0,75	0,92
	M_{39}	1,00	1,00	0,75	0,92

Для большей наглядности приведем сравнительную таблицу 5 оценки текущего уровня информационной безопасности организации до и после внедрения комплекса по противодействию угрозам информационной безопасности организации со стороны собственного персонала.

Таблица – 5 Оценка текущего уровня информационной безопасности МОУ «Саргазинской СОШ» до и после внедрения комплекса по противодействию угрозам информационной безопасности организации со стороны собственного персонала

Обозначение показателя	Итоговая оценка показателя			
	До внедрения		После внедрения	
	значение	уровень	значение	уровень
M_1	0,28	низкий	0,73	средний
M_2	0,09	низкий	0,94	высокий
M_3	0,35	низкий	0,79	средний

Оценка текущего уровня информационной безопасности МОУ «Саргазинской СОШ» после внедрения комплекса по противодействию угрозам информационной безопасности организации со стороны собственного персонала показала:

– значение управленческого показателя M_1 повысилось на 0,45 и составило 0,73;

– значение методического показателя M_2 повысилось на 0,85 и составило 0,94;

– значение инженерно-технического показателя M_3 повысилось на 0,44 и составило 0,79.

Представим данные Таблицы 5 в виде столбчатой диаграммы (рисунок 9). Итоговые оценки показателей информационной безопасности представим в процентном выражении (для этого значение показателя умножим на 100).

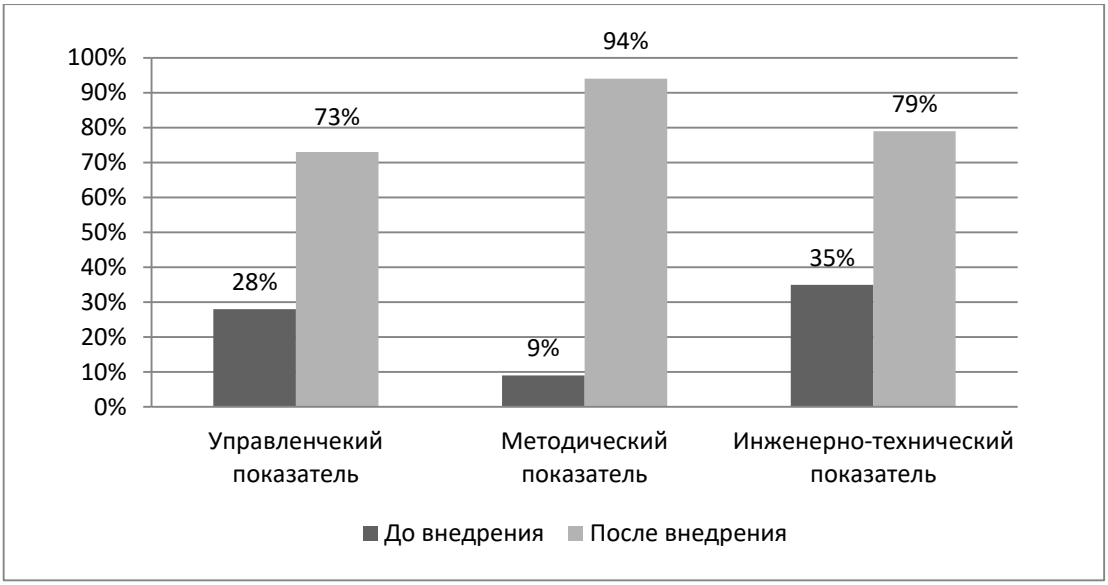

Рисунок 9 – Оценка текущего уровня информационной безопасности МОУ «Саргазинской СОШ» до и после внедрения комплекса по противодействию угрозам информационной безопасности организации со стороны собственного персонала

Как видно из сравнительной таблицы (Таблица 5) и диаграммы (рисунок 9), после внедрения комплекса мероприятий по противодействию угрозам информационной безопасности организации со стороны собственного персонала уровень информационной безопасности МОУ «Саргазинской СОШ» повысился: по управленческому и инженерно-техническому показателям с «низкого» до «среднего» уровня, по методическому показателю с «низкого» до «высокого» уровня.

Апробировав комплекс мероприятий на базе МОУ «Саргазинской СОШ», мы считаем, что данный комплекс мероприятий может быть внедрен и в другой образовательной организации с целью развития и совершенствования информационной безопасности и эффективному противодействию угрозам информационной безопасности со стороны собственного персонала.

Выводы по главе

В ходе выполнения второй главы, которая была посвящена практическим вопросам апробации комплекса мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности со стороны собственного персонала в МОУ «Саргазинской СОШ», автор пришел к следующим выводам:

1. Главным источником угрозы информационной безопасности в МОУ «Саргазинской СОШ» является собственный персонал организации. Исследования проблем информационной безопасности образовательной организации указывают на то, что большая часть нарушений в области безопасности приходится на неумышленные действия персонала организации, которые наносят наибольший вред информационной среде организации. Причиной неумышленных действий персонала, приводящих к нарушению информационной безопасности, чаще всего становится незнание основных правил информационной безопасности.

2. Значимость внедрения комплекса мероприятий по противодействию угрозам информационной безопасности со стороны собственного персонала для рассматриваемой организации является актуальной, так как организация осуществляет свою деятельность в информационной среде, и безопасность критической информации является основой работоспособности организации.

3. Цель данного комплекса: предложить мероприятия, способствующие развитию и совершенствованию информационной безопасности и эффективному противодействию угрозам информационной безопасности со стороны собственного персонала для МОУ «Саргазинской СОШ».

4. Оценка эффективности комплекса мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности организации со стороны собственного персонала показала,

что уровень информационной безопасности МОУ «Саргазинской СОШ» повысился.

5. Данный комплекс мероприятий может быть внедрен и в другой образовательной организации с целью развития и совершенствования информационной безопасности и эффективному противодействию угрозам информационной безопасности со стороны собственного персонала.

Заключение

В теоретической части магистерской диссертации рассмотрены основные аспекты проблематики информационной безопасности.

Автором предложено определение информационной безопасности в образовательной организации, как защищенности информации образовательной организации от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб самой образовательной организации или участникам образовательного процесса образовательной организации.

Рассмотрены уровни обеспечения информационной безопасности: мировой, государственный, уровень организации, гражданский.

Описаны основные угрозы информационной безопасности организации: угроза конфиденциальности, угроза целостности и угроза доступности.

Описаны способы оценки текущего состояния информационной безопасности: оценка по эталону, риск-ориентированная оценка и оценка по экономическим показателям.

Исследование теоретических основ информационной безопасности позволило определить меры, которые необходимо принять организации для нейтрализации и минимизации внутренних угроз конфиденциальной информации со стороны собственного персонала организации:

– управленческие мероприятия по защите информации (комплекс административных, ограничительных и контрольно-правовых мер);

– методические мероприятия (работа с кадрами: подбор персонала, инструктажи, обучение персонала по вопросам обеспечения защиты информации, воспитание бдительности сотрудников, повышение их квалификации);

– инженерно-технические мероприятия (кодирование информации, установка видеонаблюдения, ограничение прав доступа к

электронным носителям, внедрение защитных программно-технических средств и т.п.).

Практическая часть магистерской диссертации была посвящена экспериментальной работе по апробации комплекса мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности со стороны собственного персонала в МОУ «Саргазинской СОШ». В соответствии с целью, предметом, гипотезой и задачами данного исследования экспериментальная работа проводилась в три этапа.

На первом этапе был проанализирован процесс обеспечения информационной безопасности МОУ «Саргазинской СОШ» от угроз со стороны собственного персонала. На основе анализа сделаны следующие выводы:

– главным источником угрозы информационной безопасности в МОУ «Саргазинской СОШ» является собственный персонал организации;

– большая часть нарушений в области безопасности приходится на неумышленные действия персонала организации, которые наносят наибольший вред информационной среде организации;

– причиной неумышленных действий персонала, приводящих к нарушению информационной безопасности, чаще всего становится незнание основных правил информационной безопасности;

– значимость внедрения комплекса мероприятий по противодействию угрозам информационной безопасности со стороны собственного персонала для рассматриваемой организации является актуальной, так как организация осуществляет свою деятельность в информационной среде, и безопасность критической информации является основой работоспособности организации.

На втором этапе исследования разработан комплекс мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности действующей организации МОУ «Саргазинской СОШ» со

стороны собственного персонала, который включает в себя управленческий, методический и инженерно-технический блоки.

На третьем этапе экспериментальной работы разработанный комплекс мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности МОУ «Саргазинской СОШ» со стороны собственного персонала был внедрен в исследуемой организации.

С целью подтверждения гипотезы исследования в ходе второго и третьего этапов экспериментальной работы была проведена оценка текущего состояния информационной безопасности исследуемой организации, определяющая динамику уровня информационной безопасности образовательной организации, выявляющая эффективность разработанного нами комплекса мероприятий по совершенствованию процесса противодействия угрозам информационной безопасности со стороны собственного персонала.

Оценка текущего уровня информационной безопасности МОУ «Саргазинской СОШ» до и после внедрения комплекса по противодействию угрозам информационной безопасности организации со стороны собственного персонала показала:

– значение управленческого показателя M_1 изменилось с 0,28 на 0,73;

– значение методического показателя M_2 изменилось с 0,09 на 0,94;

– значение инженерно-технического показателя M_3 изменилось с 0,35 на 0,79.

После внедрения комплекса мероприятий по противодействию угрозам информационной безопасности организации со стороны собственного персонала значения управленческого, методического и инженерно-технического показателей стали выше, следовательно, уровень информационной безопасности МОУ «Саргазинской СОШ» повысился: по управленческому и инженерно-техническому показателям с «низкого» до

«среднего» уровня, по методическому показателю с «низкого» до «высокого» уровня.

Таким образом, на основании вышеизложенного мы можем сделать вывод о том, что гипотеза исследования полностью подтвердилась, поставленная цель исследования достигнута, необходимые задачи решены.

Подводя итоги нашего исследования, необходимо отметить, что рассматриваемая тема далеко не исчерпана. Дальнейшую работу можно продолжить в нескольких направлениях:

1. Разработать курс повышения квалификации по информационной безопасности для собственного персонала организации.

2. Расширить комплекс мероприятий управленческого и инженерно-технического блоков, с целью повышения уровня информационной безопасности со «среднего» уровня до «высокого».

3. Разработать мероприятия по противодействию угрозам информационной безопасности организации со стороны персонала сетевых партнеров и/или персонала организаций аутсортинга.

Библиографический список

1. Аверченков, В. И. Аудит информационной безопасности [Текст]: учеб. пособие для вузов / В. И. Аверченков. – Изд. 3-е, стер. – М.: ФЛИНТА, 2016. – 269 с.

2. Аверченков, В. И. Служба защиты информации: организация и управление [Текст]: учеб. пособие для вузов / В.И. Аверченков, М.Ю. Рытов.- Изд. 3-е, стер. – М.: ФЛИНТА, 2016. – 186 с.

3. Алавердов, А. Р. Кадровая безопасность как фактор конкурентноспособности современной организации [Текст]: статья / А. Р. Алавердов // Современная конкуренция: научно-практический журнал. – 2015. - №5(53). – С. 25-37.

4. Алавердов, А. Р. Управление кадровой безопасностью [Текст]: учебник / А. Р. Алавердов. – М.: Маркет ДС, 2008. – 176 с. – (Университетская серия).

5. Алавердов, А. Р. Управление персоналом [Текст]: учебное пособие / А. Р. Алавердов, Е. О. Куроедова, О. В. Нестерова . – М.: Московский финансово-промышленный университет «Синергия», 2013. – 536 с.

6. Алавердов, А. Р. Управление человеческими ресурсами организации [Текст]: учебник / А. Р. Алавердов. – М.: Московский финансово-промышленный университет «Синергия», 2017. – 830 с.

7. Аросимова, Е. М. Модели и процедуры оценки эффективности противодействия угрозам информационной безопасности укрупненных пунктов централизованной охраны [Текст]: дис. … канд. тех. наук / Аросимова Евгения Михайловна. – Воронеж, 2015. – 139 с.

8. Бачило, И. Л. Информационной право [Текст]: учебник для вузов / И. Л. Бачило, В. Н. Лопатин, М. А. Федотов. СПб.: Юридический центр Пресс, 2001. – 789 с.

9. Белов, Е. Б. Основы информационной безопасности [Текст]: учеб. пособие для вузов / Е. Б. Белов, В. П. Лось. Р. В. Мещеряков, А. А. Шелупанов. М.: Горячая линия - Телеком, 2006. — 544 с.

10. Биячуев, Т.А. Безопасность корпоративных сетей [Текст]: учеб. пособие / Т.А. Биячуев; под ред. Л. Г. Осовецкого. – СПб.: СПбГУ ИТМО, 2004. – 163 с.

11. Богатырева, Ю. И. Подготовка будущих педагогов к обеспечению информационной безопасности школьников [Текст]: дис. … д-ра. пед. наук / Богатырева Юлия Игоревна. – Тула, 2014. – 416 с.

12. Бычкова, А. В. Управление персоналом [Текст]: учеб. пособие / Бычкова А. В. – Пенза: Пензенский государственный университет, 2005. – 200 с.

13. Внуков, А. А. Основы информационной безопасности: защита информации [Текст]: учеб. пособие для СПО / А. А. Внуков. – Изд. 2-е. – М.: Юрайт, 2019. - 240 с.

14. Войскунский, А. Е. Информационная безопасность: психологические аспекты [Текст]: статья / А. Е. Войкунский // Вызовы XXI века: национальный психологический журнал. – 2010. - № 1(3). – 48-53 с.

15. Волоткин, А. В. Информационная безопасность [Текст]: монография / А. В. Волоткин, А. П. Маношкин. – М.: НТЦ «ФИОРД-ИНФО», 2002. – 354 с.

16. Галатенко, В.А. Основы информационной безопасности [Текст]: курс лекций: учебное пособие / А.В. Галатенко; под ред. Академика РАН В. Б. Бетелина. – М.: ИНТУИТ. РУ, 2006. – 208 с.

17. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения [Текст]. – [Введ. 2006-12-27]. – М.: Издательство стандартов, 2006. – 9с.

18. Груманова, Л. В. Охрана труда и техника безопасности в сфере компьютерных технологий [Текст]: учебник для спо / Л. В. Груманова, В. О. Писарева. – Изд. 4-е. – М.: Академия , 2018. - 160 с.

19. Девянин, П. Н. Теоретичесике основы компьютерной безопасности [Текст]: учеб. пособие для вузов / П. Н. Девянин. – М.: Радио и связь, 2000. – 192 с.

20. Доктрина информационной безопасности Российской Федерации [Электронный ресурс]: [Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. N 646]. – Режим доступа www.consultant.ru Дата обращения 16.12.2019.

21. Документационное обеспечение управления [Текст]: учебник / С. А. Глотова и др.; под ред. Т. А. Быкова. – М.: Кнорус, 2018. - 266 с.

22. Дронова, Г. А. Управление информационной безопасностью [Текст]: учеб.-метод. Пособие / Г. А. Дронова. – Новосибирск: Издательство НГТУ, 2016. – 28 с.

23. Дуракова, И. Б. Управление персоналом [Текст]: учебник / И. Б. Дуракова. – М.: ИНФРА-М, 2009. – 343 с.

24. Зегжда, Д. П. Основы безопасности информационных систем [Текст]: монография / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия - Телеком, 2005. – 452 с.

25. Казанцев, С.Я. Правовое обеспечение информационной безопасности [Текст]: учеб. пособие для студентов вузов / С. Я. Казанцев, О. Э. Згадзай, Р. М. Оболенский и др. - М.: Издательский центр «Академия», 2005. – 357 с.

26. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения [Текст]: учеб. пособие / О. В. Казарин, И. Б. Шубинский. – М.: Юрайт, 2019. - 342 с.

27. Кибанов, А. Я Управление персоналом организации: стратегия, маркетинг, интернационализация [Текст]: учебное пособие / А. Я. Кибанов, И. Б. Дуракова. – М.: Инфра-М, 2009. – 301 с.

28. Кибанов, А. Я. Управление персоналом организации: отбор и оценка при найме, аттестация [Текст]: учебное пособие / А.Я. Кибанов, И.Б. Дуракова. 2-е изд. – М.: Экзамен, 2005. – 289 с.

29. Конеев, И. Р. Информационная безопасность предприятия [Текст]: / И.Р. Конеев, А.В. Беляев. – Спб.: БХВ- Петербург, 2003.

30. Краковский, Ю.М. Информационная безопасность и защита информации [Текст]: учеб. пособие / Ю.М. Краковский. Ростов на Дону: Издательство «Март», 2008. – 224 с.

31. Курило, А. П. Аудит информационной безопасности [Текст]. Монография / А. П. Курило, С. Л. Зефиров, В. Б. Голованов. – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.

32. Мельников, В. П. Информационная безопасность и защита информации [Текст]: учеб. пособие для студентов вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под. ред. С. А.Клейменова. – Изд.4-е, стер. – М.: Издательский центр «Академия», 2009. – 336 с.

33. Нестеров, С. А. Информационная безопасность [Текст]: учебник и практикум для академического бакалавриата / С. А. Нестеров. – М.: Издательство Юрайт, 2016. – 321 с. – Серия: Университеты России.

34. Организационное и правовое обеспечение информационной безопасности [Текст]: учебник и практикум для бакалавриата и магистратуры / под ред. Т. А. Поляковой, А. А. Стрельцова. – М.: Издательство Юрайт, 2016. – 325 с. – Серия: Бакалавр и магистр. Академический курс.

35. Официальный сайт МОУ «Саргазинчкая СОШ» www.mousargazinskay.ucoz.ru

36. Петренко, В. И. Защита персональных данных в информационных системах [Текст] : учеб. пособие / В. И. Петренко, И. В. Мандрица. – СПб.: Лань, 2019. - 108 с.

37. Петренко, С. А. Анализ рисков в области защиты информации [Текст]: информационной-методическое пособие по курсу повышения квалификации «управление информационными рисками» / С. А. Петренко. – СПб.: Издательский дом «Афина», 2009. – 153 с.

38. Подготовка будущих учителей к обеспечению информационной безопасности [Текст]: монография / Г.Н. Чусавитина, Л. В. Курзаева, Л. З. Давлеткиреева, М.О. Чусавитин. – Изд. 2-е, стер. – М.: ФЛИНТА, 2014. – 188 с.

39. Полякова, Т. А. Правовое обеспечение информационной безопасности при построении информационного общества в России [Текст]: дис. … д-ра юр. наук / Полякова Татьяна Анатольевна. – Москва, 2008. – 438 с.

40. Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" [Электронный ресурс]. – Режим доступа: www.consultant.ru. Дата обращения 16.12.2019.

41. Расторгуев, С. П. Основы информационной безопасности [Текст]: учеб. пособие для студентов вузов / С. П. Расторгуев. – Изд. 2-е, стер. – М.: Издательский центр «Академия», 2009. – 192 с.

42. Скиба, В. Ю. Руководство по защите от внутренних угроз информационной безопасности [Текст]: монография / В. Ю. Скиба, В. А. Курбатов. – СПб.: Питер, 2008. – 320 с.

43. Стандарт Банка России СТО БР ИББС-1.0-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения / принят и введен в действие распоряжением Банка России от 17 мая 2014 г. № Р-399 [Электронный ресурс]. – Режим доступа: https://www.garant.ru. Дата обращения 16.12.2019.

44. Степанов, Е. А. Информационная безопасность и защита информации [Текст]: учеб. пособие / Е. А. Степанов, И. К. Корнеев. – М.: ИНФРА-М, 2001. – 304 с. – Серия: Высшее образование.

45. Тихонов, Д. В. Модели оценки эффективности систем информационной безопасности [Текст]: дис. … канд. эк. наук / Тихонов Денис Вахтангиевич. – Санкт-Петербург, 2009. – 126 с.

46. Трудовое право. Базовый уровень [Текст]: учебник / Ю. А. Кучина и др.; под ред. Ю. А. Кучина. - Москва: Юстиция, 2018. - 362 с. –

47. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 02.12.2019) [Электронный ресурс]. – Режим доступа: www.consultant.ru. Дата обращения 16.12.2019.

48. Тузова, А. А. Мотивация трудовой деятельности [Текст]: учебник / А. А. Тузова. – М.: МИЭМП, 2010. – 102 с.

49. Уголовный кодекс Российской Федерации [Текст]: путеводитель по судебной практике и сравнительная таблица последних изменений. – М..: Проспект, 2019. - 336 с.

50. Федеральный закон "О персональных данных" от 27.07.2006 №152-ФЗ [Электронный ресурс]. – Режим доступа: www.consultant.ru. Дата обращения 16.12.2019.

51. Хорев, П. Б. Программно-аппаратная защита информации [Текст]: учеб. пособие / П.Б. Хорев. - Москва : Форум, 2009. - 352 с.

52. Чекмарев О. П. Мотивация и стимулирование труда [Текст]: учебник / О. П. Чекмарев. – Спб.: СПбГАУ, 2013. – 343с.

53. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Текст]: учебник для вузов / В. Ф. Шаньгин. – М.: ДМК Пресс, 2010 - 544 с.

54. Шапиро С. А. Организационная культура [Текст]: учебник / С. А. Шапиро. – М.: КНОРУС, 2016. – 256 с.

55. Шапиро, С.А. Мотивация и стимулирование персонала [Текст]: монография / С. А. Шапиро. – М.: ГроссМедиа, 2005. – 224 с.

56. Шаталова Н. И. Организационная культура [Текст]: учебник для вузов / Н. И. Шаталова; под ред. В. И. Осипов. – М. Экзамен, 2006. – 656 с.

57. Шубинский, М. И. Информационная безопасность для работников бюджетной сферы. Защита персональных данных [Текст]: учеб. пособие / М. И. Шубинский. – СПб.: НИУ ИТМО, 2014. - 77 с.

58. Щеглов, А. Ю. Защита информации: основы теории [Текст]: учебник / А. Ю. Щеглов, К. А. Щеглов. – М.: Юрайт, 2019. - 309 с

59. Ясенев, В. Н. Информационная безопасность [Текст]: учеб. пособие / В. Н. Ясенев. – Нижний Новгород: Нижегородский госуниверситет им. Н. И. Лобачевского, 2017. – 198 с.

ПРИЛОЖЕНИЕ

ПРИЛОЖЕНИЕ 1

Анкета оценки уровня лояльности сотрудников

МОУ «Саргазинской СОШ»

Инструкция

Вам предложено несколько вопросов, выражающих разнообразные чувства, которые может испытывать сотрудник по отношению к своей организации. Определите свои собственные чувства. Для этого выберите приведенный вариант:

1 – абсолютно не согласен;

2 – умеренно не согласен;

3 – в чем-то не согласен;

4 – затрудняюсь ответить;

5 – согласен до некоторой степени;

6 – согласен в целом;

7 – полностью согласен.

№	Вопрос	Ответ
1	Я готов приложить усилия, даже превышающие общепринятые ожидания, чтобы школа преуспевала	
2	Я всегда говорю своим друзьям, что работаю в великолепной организации	
3	Я не испытываю никакой лояльности по отношению к школе	
4	Я соглашусь практически с любым назначением, лишь бы остаться работать в этой организации	
5	Я считаю, что мои личные ценности и ценности, принятые в школе, очень близки	
6	Я с гордостью заявляю другим, что являюсь частью этой организации	
7	С таким же успехом я работал бы в любой другой школе, если бы можно было выполнять аналогичную работу	
8	Моя организация действительно вдохновляет меня работать как можно лучше	
9	Требуются очень незначительные изменения в моих личных обстоятельствах, чтобы я оставил работу в этой школе	
10	Я очень рад, что выбрал именно эту школу, когда искал работу и рассматривал другие предложения	
11	Не имеет смысла надолго задерживаться в этой организации	

12	Во многих случаях я не согласен с основными направлениями политики организации по отношению к своим сотрудникам	
13	Мне действительно небезразлична судьба школы	
14	Для меня это самая лучшая из школ, где я мог бы работать	
15	Решение начать работать в этой организации было, безусловно, ошибкой с моей стороны	

Обработка результата

Для получения итоговой суммы необходимо сложить числа, записанные испытуемым в колонку с ответами.

Оценки на вопросы № 3, 7, 9, 11, 12, 15 необходимо преобразовать в обратные. Так, если сотрудник поставил 1, нужно изменить этот ответ на 7; 2 изменяется на 6; 3 – на 5; ответ 4 не изменяется.

После осуществления данного преобразования необходимо подсчитать итоговую сумму. В зависимости от количества баллов делается вывод.

№	Количество баллов	Интерпретация
1	0–30	Сотрудник абсолютно не лоялен к организации
2	31–45	Сотрудник регулярно выполняет предписываемые правила и требования, но лишь из опасения наказания или из-за ожидания вознаграждения
3	46–60	В целом лояльный сотрудник, внешнее поведение соответствует нормам корпоративной культуры
4	61–75	Лояльный к своей организации сотрудник, его устраивает практически все, он готов жертвовать некоторыми собственными интересами ради успеха организации
5	76–90	Лояльный и преданный сотрудник, разделяет убеждения организации и ее ценности
6	91–105	Завышенная оценка сотрудника – либо по причине желания понравиться руководству, либо чтобы избежать наказания за несоответствие. Такая оценка обозначает ложь или преувеличение, в связи с этим не используется в общем анализе

ПРИЛОЖЕНИЕ 2

Анкета для изучения мотивации сотрудников

МОУ «Саргазинской СОШ»

Просим Вас ответить на ряд вопросов, касающихся Вашей работы. Сопоставление Ваших ответов с мнениями других сотрудников позволит сделать правильные выводы об организации Вашего труда и его оплаты, а также мотивации вас как сотрудников нашей школы. Но это, конечно, зависит от искренности, точности и полноты Ваших ответов. Мы просим иметь в виду, что мнение каждого отдельного сотрудника не будет оглашено.

Ваши возможные ответы в большинстве случаев напечатаны в анкете. Нужно выделить те пункты, которые выражают Ваше мнение. Если ответ не напечатан или если ни один из напечатанных ответов Вас не устраивает, напишите ответ сами. Прежде чем отвечать на вопрос, внимательно прочтите все варианты возможных ответов.

1. Ваш пол (подчеркните).

М Ж

2. Ваш возраст (подчеркните):

до 30 лет 31 — 45 лет 45 и более

3. Каковы Ваши планы на ближайшие 1-2 года (ответ подчеркнуть)?

- продолжать работать на прежней должности;
- перейти на другую должность;
- перейти работать в другое структурное подразделение;
- перейти работать в другую организацию без смены специальности;
- перейти работать в другую организацию со сменой специальности;
- что еще (напишите)_____
  _____
  _____
  _____

4. В какой степени и как действуют на Вашу трудовую активность следующие факторы (зачеркните необходимый квадрат)?

	Снижает	Повышает	Не действует
1. Материальное стимулирование			
2. Моральное стимулирование			
3. Трудовой настрой коллектива			
4. Нововведения в организации			

5. Считаете ли Вы, что мотивация способствуют повышению эффективности работы вас лично (подчеркните)?

Да Нет Затрудняюсь ответить.

6. Выберите, пожалуйста, из перечисленных ниже характеристик работы 5 самых важных для Вас. Напротив самой важной для Вас характеристики поставьте цифру 1, менее важной 2, затем 3, 4, 5.

Характеристика работы	Балл
1. Обеспеченность оргтехникой	
2. Возможность профессионального роста	
3. Разнообразие работы	
4. Высокая заработная плата	
5. Самостоятельность в выполнении работ	
6. Престиж профессии	
7. Благоприятные условия труда	
8. Благоприятный психологический климат (коллектив)	
9. Радость от работы	
10. Участие в развитии организации	

7. Какой из видов мотивации вас заинтересует в первую очередь? Выберите, пожалуйста, из перечисленных ниже характеристик работы пять

самых важных для Вас. Напротив самой важной для Вас характеристики поставьте цифру 1, менее важной 2, затем 3, 4, 5.

Виды поощрений	Балл
1. Доплаты (премия, бонусы)	
2. Доплаты за стаж работы в школе	
3. Возмещение коммунальных платежей	
4. Оплачиваемый отпуск (56 рабочих дней)	
5. Бесплатное обучение (курсы, тренинги, семинары, вебинары и т.д.)	
6. Корпоративные праздники (концерты; выезды на природу; экскурсии)	
7. Грамоты, благодарности, похвала	
8. Уважение со стороны руководства	
9. Льготные профсоюзные путевки	
10. Другое (укажите, пожалуйста, что дополнительно вас могло бы заинтересовать)	

_____
_____
_____

Мы благодарим Вас за помощь в нашей работе!

ПРИЛОЖЕНИЕ 3

«Методика определения интегральной удовлетворенности трудом»

А. В. Батаршев

Тест «Определение удовлетворенности личности своим трудом»

Инструкция: внимательно прочтите каждое утверждение и оцените, насколько оно верно для Вас. Выберите один из предложенных вариантов ответа (а, б, в).

1. То, чем я занимаюсь на работе, меня интересует:

а) да б) отчасти в) нет

2. За последние годы я добился успехов в своей профессии:

а) да б) отчасти в) нет

3. У меня сложились хорошие отношения с членами нашего коллектива:

а) да б) не со всеми в) нет

4. Удовлетворение, получаемое от работы, важнее, чем высокий заработок:

а) да б) не всегда в) нет

5. Занимаемое мной служебное положение не соответствует моим способностям:

а) да б) отчасти в) нет

6. В работе меня прежде всего привлекает возможность узнавать что-то новое:

а) да б) отчасти в) нет

7. С каждым годом я ощущаю, как растут мои профессиональные знания:

а) да б) не уверен в) нет

8. Люди, с которыми я работаю, уважают меня:

а) да б) что-то среднее в) нет

9. В жизни часто бывают ситуации, когда не удается выполнить всю возложенную на Вас работу:

а) да б) среднее в) нет

10. В последнее время руководство не раз выражало удовлетворение по поводу моей работы:

а) да б) редко в) нет

11. Работу, которую я выполняю, не может выполнить человек с более низкой квалификацией:

а) да б) среднее в) нет

12. Процесс работы доставляет мне удовольствие:

а) да б) время от времени в) нет

13. Меня не устраивает организация труда в нашем коллективе:

а) да б) не совсем в) нет

14. У меня часто бывают разногласия с коллегами по работе:

а) да б) иногда в) нет

15. Меня редко поощряют за работу:

а) да б) иногда в) нет

16. Даже если бы мне предложили более высокий заработок, я не сменил бы место работы:

а) да б) может быть в) нет

17. Мой непосредственный руководитель часто не понимает или не хочет понять меня:

а) да б) иногда в) нет

18. В нашем коллективе созданы благоприятные условия для труда:

а) да б) не совсем в) нет

Обработка результатов

Для получения общей оценки удовлетворенности своим трудом и ее составляющих необходимо ответы перевести в баллы с помощью следующей таблицы:

Утверждения	Варианты ответов		
	а	б	в
1	2	1	0
2	2	1	0
3	2	1	0
4	2	1	0
5	2	1	0
6	2	1	0
7	2	1	0
8	2	1	0
9	0	1	2
10	2	1	0
11	2	1	0
12	0	1	2
13	0	1	2
14	0	1	2
15	0	1	2
16	2	1	0
17	0	1	2
18	2	1	0

Анализ

Данный опросник позволяет оценить общую удовлетворенность сотрудников трудом и рассмотреть ее составляющие.

Составляющие удовлетворенности	Утверждения	Максимальный балл
Интерес к работе	1, 6, 12	6
Удовлетворенность достижениями в работе	2, 7	4
Удовлетворенность взаимоотношениями с коллегами	3, 8, 14	6
Удовлетворенность взаимоотношениями с руководством	10, 15, 17	6
Уровень притязаний в профессиональной деятельности	5, 11	4
Предпочтение выполняемой работы заработку	4, 16	4
Удовлетворенность условиями труда	13, 18	4
Профессиональная ответственность	9	2
Общая удовлетворенность трудом	1–18	36

Интерпретация

Средний уровень удовлетворенности трудом – 45–55 % от общей суммы баллов.

Низкий уровень удовлетворенности трудом – 1–44 % от общей суммы баллов.

Высокий уровень удовлетворенности трудом – выше 56 % от общей сумма баллов.

ПРИЛОЖЕНИЕ 4

Тест на знание основ информационной безопасности

1. Информационная безопасность обеспечивает …

a) блокирование информации,

b) искажение информации,

c) сохранность информации,

d) утрату информации,

e) подделку информации.

2. Может ли сотрудник быть привлечен к уголовной ответственности за нарушение правил информационной безопасности организации:

a) нет, только к административной ответственности;

b) нет, если это государственное предприятие;

c) да;

d) да, но только в случае, если действия сотрудника нанесли непоправимый вред;

e) да, но только в случае осознанных неправомочных действий сотрудника.

3. Наиболее опасным источником угроз информационной безопасности организации являются:

a) другие предприятия (конкуренты);

b) сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам;

c) рядовые сотрудники предприятия;

d) возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных;

e) хакеры.

4. Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ - это

a) информация составляющая государственную тайну,

b) информация составляющая коммерческую тайну,

c) персональная,

d) конфиденциальная информация,

e) документированная информация.

5. Для того чтобы снизить вероятность утраты информации необходимо:

a) регулярно производить антивирусную проверку компьютера;

b) регулярно выполнять проверку жестких дисков компьютера на наличие ошибок;

c) регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты);

d) защитить вход на компьютер к данным паролем;

e) проводить периодическое обслуживание ПК.

6. «Персональные данные» - это

a) любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу;

b) фамилия, имя, отчество физического лица;

c) год, месяц, дата и место рождения, адрес физического лица;

d) адрес проживания физического лица;

e) сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна».

7. Пароль пользователя должен:

a) содержать цифры и буквы, знаки препинания и быть сложным для угадывания;

b) содержать только цифры;

c) содержать только буквы;

d) иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.);

e) быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.

8. Для защиты от злоумышленников необходимо использовать:

a) системное программное обеспечение,

b) прикладное программное обеспечение,

c) антивирусные программы,

d) компьютерные игры,

e) музыку, видеофильмы.

9. Что вы обычно делаете с ненужными напечатанными документами?

a) выбрасываю в мусорное ведро;

b) рву на мелкие кусочки и выбрасываю;

c) перечеркиваю ручкой «напечатанную» страницу и использую потом как черновик;

d) отдаю на черновики коллегам или родственникам;

e) ничего не делаю. Даже не знаю, куда они деваются.

10. Вам нужна отойти «на пару минут» из кабинета, что вы точно сделаете, прежде чем уйти?

a) закрою кабинет;

b) заблокирую компьютер;

c) закрою и сохраню все документы, с которыми работал(а);

d) возьму с собой свои личные вещи;

e) напишу в общем чате, что отлучусь ненадолго.

11. Вы получили письмо с неизвестного адреса с пометкой «ВАЖНО» и просьбой срочно посмотреть информацию по ссылке. Ваши действия?

a) письмо от незнакомца удалю, по ссылке не пойду;

b) раз письмо мне, открою его и перейду по ссылке;

c) перешлю письмо более опытному коллеге, чтобы разобраться вместе;

d) открою письмо, если что-то важное перейду по ссылке;

e) напишу ответ, чтобы уточнить информацию.

12. Вам нужно поработать из дома, но для этого нужно взять с собой некоторые конфиденциальные документы. Как вы поступите?

a) возьму с собой, всегда так делаю;

b) посоветуюсь с коллегами, если можно – возьму;

c) вообще-то это запрещено, но работу закончить надо, потому возьму;

d) задержусь и поработаю с этими документами на рабочем месте;

e) спрошу разрешения у директора.

13. Вы нашли флешку. Как поступите?

a) открою на рабочем компьютере и постараюсь выяснить, чья она;

b) отдам сотруднику по безопасности;

c) заберу домой и на личном компе посмотрю;

d) спрошу коллег, постараюсь найти хозяина;

e) выброшу.

14. Комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа - это

a) антивирус,

b) замок,

c) брандма́уэр,

d) криптография,

e) экспертная система.

15. В данном случае сотрудник организации может быть привлечен к ответственности за нарушение правил информационной безопасности:

a) выход в Интернет без разрешения администратора;

b) при установке компьютерных игр;

c) в случаях установки нелицензионного ПО;

d) в случае не выхода из информационной системы;

e) в любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности.

16. Доступ пользователя к информационным ресурсам компьютера и/или локальной вычислительной сети организации должен разрешаться только после:

a) включения компьютера,

b) идентификации по логину и паролю,

c) запроса паспортных данных,

d) запроса доменного имени,

e) запроса ФИО.

17. Какими будут Ваши действия, если Вам звонят из органов исполнительной власти и просят сообщить какую-либо информации об обучающихся или сотрудниках?

a) сообщу информацию;

b) положу трубку;

c) попрошу сделать запрос на официальном бланке и направить на адрес организации;

d) сообщу, что не владеете такой информацией;

e) попрошу подъехать лично.

18. Где вы обычно храните пароль для входа в систему?

a) под клавиатурой,

b) записываю в ежедневнике,

c) запоминаю,

d) дома в специальном блокноте,

e) в кошельке.

19. Защита информации - это

a) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

b) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

c) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

d) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

e) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на нее.

20. Искусственные угрозы безопасности информации вызваны:

a) деятельностью человека;

b) ошибками при проектировании автоматизированной системы, ее элементов или разработке программного обеспечения;

c) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

d) корыстными устремлениями злоумышленников;

e) ошибками при действиях персонала.

Спасибо за Ваши ответы!