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

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

Анализ эффективности защиты конфиденциальной информации в образовательной организации и разработка рекомендаций по ее совершенствованию

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

Проверка на объем заимствований:
79,63% авторского текста

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

Выполнил:
Студент группы ЗФ-309-210-2-1
Занков Кирилл Игоревич

Научный руководитель:
к.т.н., доцент
Руднев Валерий Валентинович

Челябинск
2022

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Южно-Уральский Государственный Гуманитарно-Педагогический Университет»
(ФГБОУ ВО «ЮУрГГПУ»)
Профессионально-педагогический институт
Кафедра автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

Направление подготовки 44.04.04 – Профессиональное обучение (управление информационной безопасностью в профессиональном образовании)

З А Д А Н И Е

на выпускную квалификационную работу

Студенту группы ЗФ-309/210-3-1 заочного отделения Занкову Кириллу Игоревичу, обучающемуся по программе магистратуры Управление информационной безопасностью в профессиональном образовании.

Научный руководитель квалификационной работы: к.т.н., доцент Руднев Валерий Валентинович.

1. Тема квалификационной работы: «АНАЛИЗ ЭФФЕКТИВНОСТИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ И РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ЕЕ СОВЕРШЕНСТВОВАНИЮ» утверждена приказом ректора Южно-Уральского государственного гуманитарно-педагогического университета №_____ от «___» ___ 20__ г.

Срок сдачи студентом законченной работы на кафедру 19.01.2022 г .

2. Материалы для выполнения квалификационной работы:

2.1. Учебная, научно-техническая, теоретико-методическая литература по теме квалификационной работы, основные положения об обработке и защите персональных данных; научные, практические, методические рекомендации по организации защиты конфиденциальной информации ведущих специалистов в этой области.

2.2. Материалы преддипломной практики по теме квалификационной работы.

3. Основные части ВКР (перечень подлежащих разработке вопросов) и сроки их выполнения представлены в таблице 1.

Таблица 1 - Основные части магистерской диссертации

№ п/п	Перечень вопросов, подлежащих разработке в диссертации	Сроки выполнения ВКР
1.	Разработка плана работы и примерного перечня, необходимых для анализа нормативно-правовых, научных, статистических, и практических материалов	
2.	Составление предварительной библиографии по теме ВКР	
3.	Сбор информации и ее обработка	
4.	Написание первой и второй (теоретической) части работы	
5.	Написание третьей части работы	
6.	Написание введения и заключения	
7.	Представление первой редакции работы руководителю ВКР	
8.	Подготовка окончательной редакции работы, ее оформление и сдача на отзыв руководителю ВКР	
9.	Получение акта внедрения авторской разработки	
10.	Оформление пояснительной записки и презентации ВКР	
11.	Защита ВКР на заседании Государственной экзаменационной комиссии	

Дата выдачи задания: «25» ноября 2020 г.

Заведующий кафедрой АТ, ИТ и МОТД:

Руднев Валерий Валентинович, к.т.н, доцент

Фамилия, Имя, Отчество, ученое звание — Подпись заведующего кафедрой

Задание выдал:

Руднев В.В., к.т.н., доцент

Фамилия, Имя, Отчество, ученое звание и степень — Подпись научного руководителя

Задание принял:

Занков К.И.

Фамилия, Имя, Отчество студента — Подпись магистранта

АННОТАЦИЯ

Магистрант Занков Кирилл Игоревич

Тема магистерской диссертации «АНАЛИЗ ЭФФЕКТИВНОСТИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ И РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ЕЕ СОВЕРШЕНСТВОВАНИЮ»

Магистерская диссертация содержит 100 страниц, 5 таблиц, 17 рисунков, 38 источника литературы.

Проанализированы состав и структура информационной системы современной образовательной организации, инструментарий оценки её информационной безопасности, организационно-технические и инженерно-технические мероприятия сохранения конфиденциальной информации, а также способы оценки информационной безопасности современной образовательной организации: методика комплексной оценки состояния её информационной безопасности организации, парадоксы и реальность оценки эффективности информационных систем. Обоснована необходимость трансформации информационной защиты в образовательной организации за счет контроля профессиональных компетенций педагогических работников образовательной организации посредством тест-анализа ИКТ-компетенции педагогических работников образовательной организации.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Проникновение информационных технологий во все сферы жизни общества, их вхождение, по сути, в каждый дом среди многочисленных положительных моментов имеет своим следствием и целый ряд негативных.

Существует широкий класс сведений, именуемый конфиденциальной информацией, которые подлежат защите. В ряде случаев ценность такой информации приближается к ценности сведений, составляющих государственную тайну.

Имеют место несколько возможных каналов утечки ценной информации. Прямые каналы утечки информации – это непосредственное копирование важных документов или нарушение сохранности информации, сведений конфиденциального характера. К косвенным каналам нарушение сохранности информации относят:

– потерю или кражу устройств – носителей информации;

– неправильную утилизацию данных, подлежащих уничтожению;

– дистанционное прослушивание или фотографирование документов с секретной информацией;

– радиоперехват сообщений.

Категории «конфиденциальная информация», «сведения конфиденциального характера» в настоящее время не имеют под собой четкого законодательного основания, хотя продолжают на достаточно высоком уровне правового регулирования (Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» и ряд других) использоваться для обозначения относительно обособленного класса информации.

Изучение проблем, связанных с отнесением сведений к категории конфиденциальной информации и упорядочением их оборота, на примере организаций образования имеет весьма актуальное значение.

В век высокого уровня развития информационных технологий организации образования перешли на электронный документооборот. Использование-

электронных документов, подразумевает хранение, обработку и передачу информации, в том числе и конфиденциальной с помощью электронных средств. Система защиты информации конфиденциального характера в организации образования, имеющая правовую, организационную и техническую составляющие, должна гарантировать исключение возможности неконтролируемого доступа или утечки защищаемых сведений, а также искажения их содержания.

Анализ научных источников, касающихся рассматриваемых вопросов, позволяет утверждать, что проблема правового регулирования защиты конфиденциальной информации в организациях образования освещена недостаточно. Следует констатировать, что комплексного правового исследования, посвященного проблемам правового регулирования оборота и защиты конфиденциальной информации в организациях образования и выработке предложений по совершенствованию нормативной правовой базы в сфере интересов организаций образования, до настоящего времени не проводилось.

Как показывает практика, в последние годы возросло количества случаев, а также масштабы ущерба от практических действий «инсайдеров», иными словами, от действий сотрудников организации или иных лиц, которые получили доступ и намеренно или непреднамеренно совершили действие, которое привело к нанесению ущерба конфиденциальности организации образования. Проблеме существования инсайдерской деятельности в КС было посвящено большое количество работ как отечественных ученых (П.Д. Зегжды, И.В. Котенко, А.В. Лукацкого, А.А. Молдовяна, В.Ю. Осипова, И.Б. Саенко и др.), так и зарубежных (S. Bellovin, C. Cheh, M. Collins, F. Kammüller, Y. Shuang-Hua, X. Wang и др.). Значительное место вопросы правового обеспечения конфиденциальности заняли в работах И.Л. Бачило, С.Н. Братановского, В.Н. Верютина, Е.К. Волчинской, М.А. Вуса, А.А. Дозорцева, А.К. Жаровой, А.В. Коломийца, В.Н. Лопатина, О.С. Макарова, А.В. Минбалеева, А.А. Опалевой, И.Л. Петрухина, Ю.С. Пилипенко, Т.А. Поляковой,

Р.В. Северина, Р.Б. Ситдикова, И.В. Смольковой, Л.К. Терещенко, А.А. Фатьянова, М.А. Федотова, Е.Н. Яковца и многих других.

Многие проблемы разработки и применения научно-методического обеспечения защиты конфиденциальной информации в организациях образования не решены как в теоретическом, так и в практическом аспектах.

Практика использования ИКТ в профессиональном образовании свидетельствует о наличии множества противоречий, по меньшей мере одно из которых представляется наиболее значимой:

– между потребностью в информационно компетентных педагогических кадрах и отсутствием эффективной системы системной оценки владения ими ресурсными возможностями (потенциями) ИКТ.

Данное противоречие привело к формированию комплекса проблем профессионального образования. Две из них наиболее актуальные:

– адекватности двух систем – научных теорий и информационных технологий, используемых для их освоения;

– системного анализа профессионального обучения с учетом современных требований философии образования, педагогики и информатизации защиты конфиденциальной информации в организациях образования к современным информационно-обучающим комплексам;

– трансформации традиционных технологий защиты конфиденциальной информации в организациях образования в компьютерные и информационные формы.

Объект исследования – политика информационной безопасности о организации профессионального образования с применением современных информационных технологий, компьютерных и физических средств.

Гипотеза диссертационного исследования состоит в том, что можноповысить уровень защиты информации в организации профессионального образования, если при разработке её политики информационной безопасности сделать уклон на защиту от внутренних угроз («инсайда»).

Предмет исследования – разработка методологических аспектов системы инсайд-защиты конфиденциальной информации в организации профессионального образования.

Цель исследования – обобщение исследований ведущих учѐных в области защиты конфиденциальной информации образовательной организации в части реализации комплекса показателей её совершенствования с методикой оценки обеспечиваемого уровня в рамках современной образовательной парадигмы.

1. Провести анализ современных методологических аспектов состояния и построения системы обеспечения защиты конфиденциальности, целостности и доступности информации;
2. Исследовать инструментарий (методики, модели, алгоритмы) методов защитного предупреждения (нивелирования, минимизации) деструктивных воздействий на целостность и сохранность конфиденциальной информации, без снижения регламентации её доступности.

Задачи исследования:

1. Проанализировать структуру научно-методического обеспечения защиты информации организаций профессионального образования при использовании современных ресурсов процесса информатизации организаций профессионального образования.

2. Разработать методологические аспекты системы инсайд-защиты конфиденциальной информации в организации профессионального образования.

Теоретико-методологическая основа исследования – основные положения об обработке и защите персональных данных; научные, учебные, практические, методические рекомендации по организации защиты конфиденциальной информации ведущих специалистов в этой области, таких как А.И. Алексенцев [22, 23] и Е.А. Степанов [67; 68] и др.

Нормативно-правовая основа - Конституция как основном законе Российской Федерации; статья 23 Конституции РФ гарантирует право на личную, семейную тайну, тайну переписки, телефонных переговоров, почтовых,

телеграфных и иных сообщении; ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 №149; основными в области безопасности конфиденциальной информации также являются законы РФ: ФЗ «О государственной тайне» от 22 июля 2004 г.; ФЗ №98 «О коммерческой тайне» от 29 июля 2004 г.; Указ Президента РФ №188 «Об утверждении Перечня сведений конфиденциального характера»; ФЗ №152 «О персональных данных» от 27 июля 2006 г. ; Постановление Правительства № 731 «Об утверждении Перечня сведений, которые не могут составлять коммерческую тайну»; стандарт, закрепляющий основные термины и определения в области защиты информации - ГОСТ Р 50922-96.

База исследования: Профессионально-педагогический институт ФГБОУ ВО «ЮУрГГПУ, г. Челябинск.

ГЛАВА 1 СОСТАВ, СТРУКТУРА ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1. Современная информационная система образовательной организации и её особенности

Современная информационная система (ИС) образовательной организации – это комплекс технического, программного и организационного обеспечения в виде различных программ автоматизации основных её процессов (делопроизводства, ведения личных кабинетов преподавателей, сотрудников и обучаемых, составления расписания и т.д.), а также персонала, предназначенная для того, чтобы своевременно обеспечивать персонал образовательной организации и обучающихся надлежащей информацией.

Основная цель и задача таких ИС заключается в обеспечение необходимой интегративности при создании единого образовательного информационного пространства. Решение этой задачи начинается с обеспечения однозначности, полной эквивалентности и интерпретации описания предметной области образовательной организации в информационном пространстве для разных операционных систем и приложений.

Как правило, ИС образовательной организации – многоагентные системы (Multi-Agent Systems) с реализацией многопользовательского режима использования данных, причём с разграничением прав доступа к ним.

Основными информационными подсистемами ИС образовательной организации являются подсистемы поддержки:

– принятия решений управления образовательной организации;

– учебно-образовательного процесса;

– научно-методических исследований и научно-образовательной информации;

– обеспечения повседневной деятельности образовательной организации;

– защиты информационной безопасности (ЗИБ) ИС образовательной организации.

Подсистема ЗИБ ИС, помимо функций регламентации разграничения прав доступа к информации ИС образовательной организации, в свою очередь, включает такие функции эффективного использования средств вычислительной техники как:

– организация технического обслуживания;

– учет и контроль состояния технических средств;

– профилактика технического парка вычислительной и оргтехники, в том числе телекоммуникационного и дистанционного инструментария обеспечения коммуникаций, взаимодействия основных информационных потоков, иными словами, в самом общем виде, формирование информационного пространства образовательной организации;

– диагностирование и ремонт технических средств;

– модернизация устройств,

а также:

– организация сопровождения программного обеспечения;

– установка операционных систем;

– установка прикладного программного обеспечения;

– установка программного обеспечения по заявкам педагогов.

В последние годы усилился интерес к теории оптимизации управления образовательным процессом на основе информационных ресурсов. В свете таких обстоятельств ИС образовательной организации должны учитывать постоянное совершенствование компьютерных и сетевых технологий с целью максимального повышения уровня оптимальности принимаемых управленческих решений учебно-образовательным процессом. Основной проблемой оптимального управления учебно-образовательным процессом является выбор аналитических методов и численных алгоритмов нахождения оптимального решения [1–3].

Подсистема ЗИБ ИС, выполняющая функции регламентации разграничения прав доступа к информации ИС образовательной организации, обусловлена необходимостью надёжной защиты конфиденциальной информации образовательной организации. Нормативной основой для понятия «конфиденциальности» информации являются (рис. 1.1):

– Статья 23, 24 Конституции РФ;

– Статья 727 Гражданского кодекса РФ;

– Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон № 152-ФЗ «О персональных данных»;

– Федеральный закон № 98-ФЗ «О коммерческой тайне»;

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

Рис. 1.1 – Нормативно-правовые акты в области информационной безопасности в РФ

К нормативно-методическим документам можно отнести - Методические документы государственных органов России:

– Доктрина информационной безопасности РФ (Утверждена указом Президента Российской Федерации от 5 декабря 2016 г. №646);

– Руководящие документы ФСТЭК (Гостехкомиссии России);

– Приказы ФСБ.

– Документы и стандарты, регламентирующие защиту объектов информатизации от несанкционированного доступа к информации.

– Документы и стандарты, регламентирующие требования к подсистеме криптографической защиты.

– Документы, регламентирующие защиту объектов информатизации от воздействий вредоносных программ.

– Документы и стандарты, регламентирующие особенности защиты сетей передачи данных.

– Документы и стандарты, регламентирующие защиту объектов информатизации от утечки информации по техническим каналам.

– Документы и стандарты, регламентирующие защиту зданий, помещений и контролируемых зон объекта информатизации.

– Документы и стандарты, регламентирующие защиту объекта информатизации от внешних воздействующих факторов.

– Стандарты, регламентирующие требования к оформлению документации и документов на объект информатизации.

– Документы и стандарты, регламентирующие оценку качества объекта информатизации, виды испытаний этих объектов.

– Стандарты в области терминов и определений.

– Правовой режим информации, средств информатики, индустрии информатизации и систем информационных услуг в условиях риска, средства и формы защиты информации.

– Правовой статус участников правоотношений в процессах информатизации.

– Порядок отношений субъектов с учетом их правового статуса на различных стадиях и уровнях процесса функционирования информационных структур и систем.

Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации” Итак, правовое обеспечение компьютерной безопасности включает нормы, осуществляющие общественные отношения, возникающие в процессе деятельности физических лиц, организаций и государственных органов.

К подзаконным нормативным актам в области информатизации относятся соответствующие Указы Президента РФ, Постановления Правительства РФ, Приказы и другие документы, издаваемые федеральными министерствами и ведомствами. Например, Указ Президента РФ об утверждении перечня сведений конфиденциального характера от 6 марта 1997 г. № 188 (прил. №2).

Информации образовательной организации разделяется на три группы:
Первая – несекретная (или открытая), которая предназначена для использования как внутри образовательной организации, так и вне нее.
Вторая – для служебного пользования (ДСП), которая предназначена только для использования внутри образовательной организации. Она подразделяется, в свою очередь, на две подкатегории:

– Доступная для всех сотрудников образовательной организации;

– Доступная для определенных категорий сотрудников образовательной организации, но данная информация может быть передана в полном объеме другому сотруднику для исполнения трудовых обязанностей.

Третья – информация ограниченного доступа, которая предназначена для использования только специально уполномоченными сотрудниками образовательной организации и не предназначена для передачи иным сотрудникам в полном объеме или по частям.

Информация второй и третьей категории является конфиденциальной.

Примерный перечень конфиденциальной информации образовательной организации [1–3]:

– Информация, составляющая коммерческую тайну – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам;

– Банковская тайна – сведения об операциях, о счетах и вкладах организаций, клиентов банков и корреспондентов;

– Информация, имеющая интеллектуальную ценность – техническая, технологическая: программное обеспечение, производственные показатели, химические формулы, результаты испытаний опытных образцов, данные контроля качества и т.п. и деловая: стоимостные показатели, результаты педагогического исследования и т.п.

В подсистеме ЗИБ ИС образовательной организации должны быть реализованы надежные средства разграничения полномочий и контроля за доступом к документам, особенно к документам, содержащим конфиденциальную информацию. Защищенность конфиденциальной информации – свойство, характеризующее невозможность несанкционированного её использования или изменения. В большинстве случаев с помощью функционального инструментария ЗИБ ИС образовательной организации определяются следующие виды доступа:

– полный контроль над документом;

– право читать документ, но не редактировать его;

– право доступа к карточке, но не к содержимому документа;

– полное отсутствие прав доступа к документу.

Наиболее важной проблемой внедрения подсистемы ЗИБ ИС образовательной организации – фактор персонала. Консерватизм персонала, низкая образованность, нежелание обучаться и переобучаться. Боязнь прозрачности

собственной деятельности для руководства. Серьезным препятствием для внедрения подсистемы ЗИБ ИС образовательной организации является технический фактор – отсутствие устойчивых каналов передачи данных с архитектурой типа «клиент-сервер» [5–8].

В соответствии с ГОСТами, эффективность функционирования ИС образовательной организации и её подсистемы ЗИБ определяется соотношением результата и затраченными ресурсами. Выбор платформы ИС образовательной организации – чрезвычайно важный шаг, поскольку он предопределяет всю структуру стоимости системы, достижимый результат и ее эффективность. За последние сформировалось новое направление в программировании ИС образовательной организации CASE (Computer-Aided Software/ System Engineering). Это инструментарий для системных аналитиков, разработчиков и программистов, который позволяет автоматизировать процесс проектированияи разработки программного обеспечения. CASE-технологии успешно применяются для построения практически всех типов программного обеспечения, как системного и управляющего, так и прикладного. Ключевым признаком CASE-средства является поддержка методологий структурного системного анализа и проектирования [4].

1.2. Инструментарий оценки информационной безопасности образовательной организации

В настоящее время существует достаточное число публикаций, отражающих различные аспекты экономической и, в частности, информационной безопасности (физические аспекты защиты, контроль доступа, защита конфиденциальной информации и персональных данных, риски недостоверности информации и их влияние на экономическую безопасность и т. д.), каждый отражает разные подходы к проблеме. Однако, несмотря на это, можно отметить, что комплексный подход к анализу и оценке информационной составляющей экономической безопасности в большинстве случаев не применя-

ется. При этом часто исследованию подлежит какой-то один аспект информационной безопасности.

Можно выделить несколько причин данной проблемы:

1. Методы оценки информационных рисков и угроз являются недостаточно проработанными в связи с постоянно меняющейся ситуацией в сфере информационной безопасности и появлением новых технологий.

2. События нарушения информационной безопасности и их последствия часто не являются идентичными и стандартизированными, что зависит от субъектов и объектов информационной безопасности.

3. Достигаемый итоговый результат зависит от комплекса решений, поэтому выделить конкретные решения, в большей степени повышающие уровень информационной безопасности, достаточно трудно.

Таким образом, в условиях повышения значения информационной составляющей экономической безопасности для всех организаций существует потребность в оптимизации системы информационной безопасности и организации ее мониторинга и оценки.

Организация работы по обеспечению информационной безопасности в образовательной организации является непрерывным процессом (рис. 1.2.).

Рис. 1.2 – Процесс обеспечения информационной безопасности

Исходя из рис. 1 видно, что аналитические работы в области информационной безопасности проводятся по следующим направлениям [11]:

1) комплексный анализ информационной системы на правовом, методологическом, организационно-управленческом, технологическом и техническом уровнях. В данном случае проводится анализ соответствия существующей информационной системы нормам действующего законодательства, анализ

используемой в процессе деятельности информации, средств и способов ее защиты и т. д.;

2) анализ существующих рисков и угроз информационной безопасности;

3) определение уровня информационной безопасности с определением количественных или качественных показателей для мониторинга;

4) разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому и техническому, а также программно-аппаратному обеспечению информационной безопасности, включая анализ предлагаемых решений и проектов по повышению общего уровня информационной безопасности, работы по поддержанию практической реализациданных рекомендаций.

При проведении комплексного анализа информационной системы важным является выделение из всего объема информации, представляющей ценность. Всю используемую информацию необходимо разделять на:

– общедоступную, доступ к которой не ограничен;

– информацию с доступом, ограниченным федеральными законами и регламентами или правилами организации [12].

Для выявления и оценки существующих рисков и угроз информационной безопасности могут использоваться методы:

– экспертных опросов;

– анкетирование;

– интервьюирование;

– brainshtorm;

– Delfy [10].

Анкетирование в оценке рисков предполагает заполнение анкет респондентами и проведение анализа полученных результатов. Интервьюирование обеспечивает устное непосредственное общение отдельно с каждым сотрудником по поводу определенной проблемы.

Метод brainshtorm предполагает коллективное обсуждение информационных рисков, когда участники поочередно высказываются о поднятой

проблеме и создается единый письменный «реестр» с перечислением озвученных мнений, а затем происходит их коллективное обсуждение и принятие решений.

Особенностями метода Delfy являются анонимность, многоуровневость и заочность, когда проводится многократное анкетирование с оглашением предыдущих результатов.

После применения вышеперечисленных выше методов заполняется сводная таблица, которая отражает основные выявленные риски и пути возможного их снижения (табл. 1).

Таблица 1.1 – Сводная таблица по идентификации и анализу рисков

	Риск № 1	Риск № 2
Наименование риска	x	x
Краткое описание риска	x	x
Сотрудник, идентифицирующий риск	x	x
Процесс, в котором участвует сотрудник	x	x
Источник риска	x	x
Вероятность наступления риска	x	x
Оценка значимости риска	x	x
Мероприятия по разрешению рисковой ситуации	x	x

Анализ и управление рисками является процессом идентификации уязвимых мест и угроз в отношении ресурсов информационной системы и определения мер, способствующих снижению риска до приемлемого уровня.

Процесс управления информационными рисками можно представить в виде схемы (рис.1.3) [13].

Согласно данным рис. 1.3 можно отметить, что процесс управления рисками включает в себя ряд этапов.

1. Идентификация и классификация активов (ресурсов) организации, (когда определяется перечень всех ресурсов в информационной системе и их

качественные или количественные характеристики), уязвимых мест в информационной системе и построение модели существующих угроз (в том числе составляется и описывается перечень возможных угроз, источников их возникновения и механизмов возникновения).

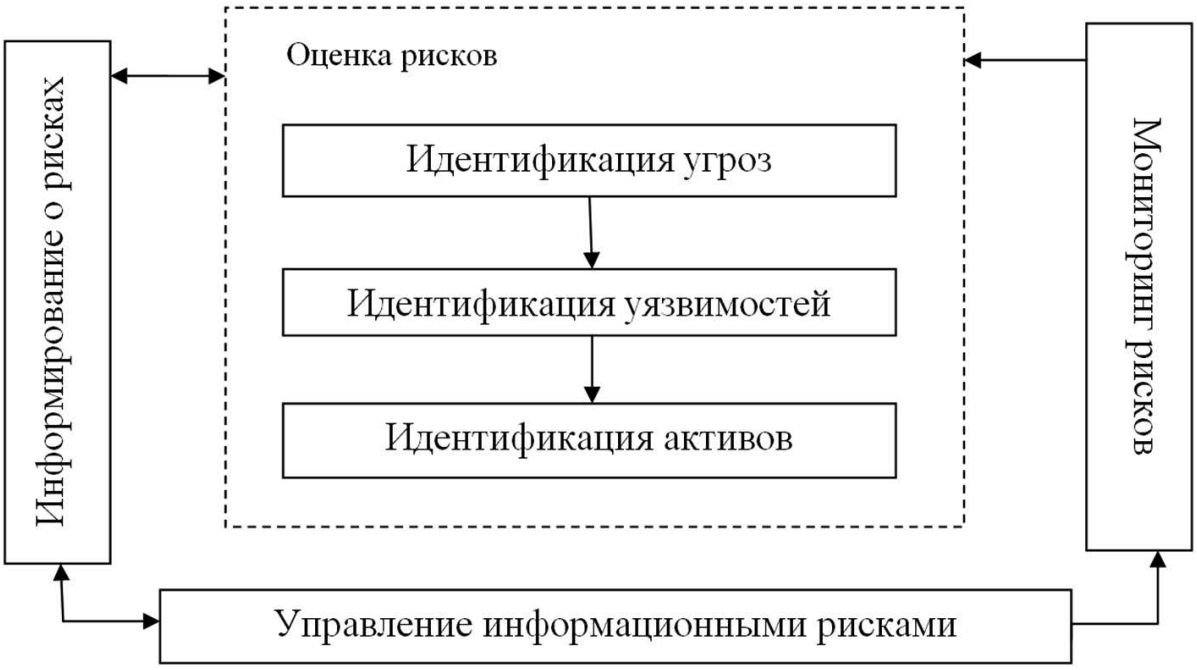

Рис. 1.3 – Схема управления рисками информационной безопасности

2. Оценка существующих рисков на основе проведенного анализа и определение зависимости деятельности организации от функционирования информационной системы.

3. Формирование требований по обеспечению информационной безопасности, в том числе формирование требований к системе обеспечения информационной безопасности, т. е. на данном этапе и происходит формирование основных направлений повышения уровня информационной защищенности организации.

Переходя к этапу оценки уровня информационной безопасности организации, можно отметить, что на сегодняшний день не существует единой методики расчета количественного и качественного значения уровня информационной безопасности организации.

Методы и средства обеспечения информационной безопасности экономического объекта представлены на рис. 1.4.

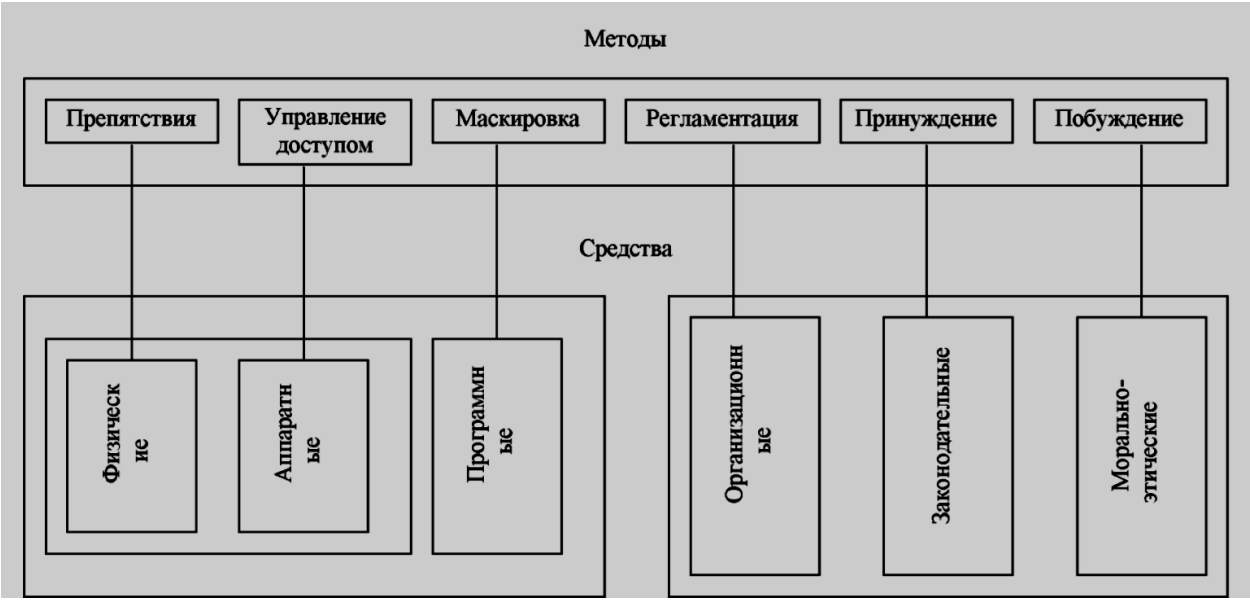

Рис. 1.4 – Методы и средства информационной безопасности экономического объекта

Методами обеспечения защиты информации на предприятии являются следующие: Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.). Управление доступом – метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы предприятия.

Управление доступом включает следующие функции защиты:

– идентификацию пользователей, персонала и ресурсов информационной системы (присвоение каждому объекту персонального идентификатора);

– аутентификацию (установления подлинности) объекта или субъекта по предъявленному им идентификатору;

– проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

– регистрацию обращений к защищаемым ресурсам;

– реагирование (сигнализация, отключение, задержка работ, отказ в запросе при попытках несанкционированных действий).

Маскировка – метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия.

Регламентация – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму.

Принуждение – метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности.

Побуждение – метод защиты информации, который побуждает пользователей и персонал системы не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм.

Указанные выше методы обеспечения информационной безопасности реализуются с помощью следующих основных средств: физических, аппаратных, программных, аппаратно-программных, криптографических, организационных, законодательных и морально-этических. Физические средства защиты предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.

Аппаратные средства защиты – это электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками. Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т.д.

Программные средства защиты предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в состав программного обеспечения автоматизированной информационной системы, либо

в состав средств, комплексов и систем аппаратуры контроля. Программные средства защиты информации являются наиболее распространенным видом защиты, обладая следующими положительными свойствами: универсальностью, гибкостью, простотой реализации, возможностью изменения и развития. Данное обстоятельство делает их одновременно и самыми уязвимыми элементами защиты информационной системы предприятия.

Аппаратно-программные средства защиты – средства, в которых программные (микропрограммные) и аппаратные части полностью взаимосвязаны и неразделимы.

Криптографические средства – средства защиты с помощью преобразования информации (шифрование). Организационные средства - организационно-технические и организационно-правовые мероприятия по регламентации поведения персонала.

Законодательные средства – правовые акты страны, которые регламентируют правила использования, обработки и передачи информации ограниченного доступа и которые устанавливают меры ответственности за нарушение этих правил.

Морально-этические средства – нормы, традиции в обществе, например: Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ в США. Все рассмотренные средства защиты разделены на формальные (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и «неформальные» (определяемые целенаправленной деятельностью человека либо регламентирующие эту деятельность). Для реализации мер безопасности используются различные механизмы шифрования (криптографии). Криптография – это наука об обеспечении секретности или аутентичности (подлинности) передаваемых сообщений.

Одним из методов определения уровня экономической, и информационной в частности, безопасности является разработка системы индикаторов, т. е. системы мониторинговых показателей, нарушение которых

приводит к развитию негативных кризисных тенденций в сфере экономической безопасности [14, с. 18]. Индикаторы в данном случае рассматриваются как граничные значения показателей, характеризующих различные области деятельности организации, ее специфические отраслевые особенности.

При этом проблемой в данном случае является определение индикаторов применительно к отраслевым особенностям деятельности предприятия и, соответственно, степени точности данных индикатора в связи с отсутствием разработанной методической базы для установления индикаторов.

Применительно к оценке информационной составляющей экономической безопасности можно отметить, что индикаторы информационной безопасности организации подразделяются на две группы — количественные и стоимостные индикаторы [15, с. 57].

Количественные индикаторы определяют работы по информационно-аналитическому обеспечению деятельности организации. Примером данных индикаторов могут быть:

– доля сотрудников информационно-аналитического подразделения в общей численности персонала;

– количество источников информации, необходимых для осуществления непосредственной деятельности;

– наличие и состав структуры подотделов информационно-аналитического подразделения.

Анализ количественных индикаторов необходимо производить в динамике за определенный период.

Стоимостным индикатором информационной составляющей экономической безопасности может быть удельный вес затрат на обеспечение информационной безопасности в общей сумме затрат предприятия.

Другим методом определения уровня информационной составляющей экономической безопасности является определение долей неполной (ограниченной), неточной, противоречивой информации, которая используется субъектами в процессе принятия управленческих решений.

Ильяшенко С.Н. предлагает при определении уровня информационной безопасности использовать ряд коэффициентов [16].

1. Коэффициент полноты информации (Кпл) – определяется как отношение объема информации, которая необходима для принятия обоснованного решения, ко всему объему информации, имеющемуся у лица, принимающего решения.

2. Коэффициент точности информации (Кт) – определяется как отношение релевантной информации к общему объему информации, имеющемуся в распоряжении субъекта.

3. Коэффициент противоречивости информации (Кпр) – определяется как отношение количества независимых свидетельств в пользу принятия управленческого решения к общему количеству независимых свидетельств в суммарном объеме релевантной информации.

Объем оцениваемой информации может быть определен в станицах текста (формата А4), в количестве символов в текстовом файле, в весе данного файла (Кбайт, Мбайт) и т. п.

Общий уровень информационной безопасности рассчитывается как произведение данных коэффициентов:

$$Ки = Кпл \times Кт \times Кпр.$$

Коэффициент уровня информационной безопасности в данном случае принимает числовое значение от 0 до 1 (табл. 1.2).

Данная методика является ограниченной в применении в связи с трудностями в точном выделении из всей имеющейся информации данных, необходимых для принятия управленческих решений.

При оценке используемых организационных и программно-технических мер по обеспечению уровня информационной безопасности Дмитриева М.А. предлагает использовать модель зрелости процессов, которая позволяет выявить зоны развития организации [17]. Определение зрелости процесса информационной безопасности показывает, насколько данный процесс управляем и прогнозируем.

Таблица 1.2 – Определение уровня информационной безопасности

Значение коэффициента	Уровень информационной безопасности
Ки ≥ 0,7	Высокий
0,3 ≤ Ки < 0,7	Средний
Ки < 0,3	Низкий

Можно выделить 5 уровней зрелости процессов организации информационной безопасности организации (табл. 1.3).

В качестве процессов, используемых при анализе информационной безопасности, могут выступать следующие процессы [18]:

1) построение системы менеджмента информационной безопасности:

– стратегическое планирование информационной безопасности;

– осознание руководством важности информационной безопасности;

– управление рисками информационной безопасности;

– аудит информационной безопасности;

– политика информационной безопасности;

2) построение технической системы информационной безопасности:

– управление доступом;

– управление уязвимостями,

– управление информационными активами;

Таблица 1.3 – Уровни зрелости управления процессами информационной безопасности

Уровень	Описание
0 (нулевой)	Процессы отсутствуют
1 (начальный)	Процессы не определены либо неконтролируемые и выполняются на нерегулярной основе
2 (повторяемый)	2 (повторяемый) Процессы выполняются на регулярной основе и поддерживаются на уровне планирования
3 (определенный)	Процессы выполняются и исполняются в соответствии с существующими регламентами и стандартами
4 (измеримый)	4 (измеримый) Процессы четко структурированы и описаны. существует постоянный кон-

	троль и измерение процессов
5 (оптимизируемый	Процессы полностью описаны и структурированы, исключено дублирование процессов, регулярно проводятся мероприятия по совершенствованию ключевых процессов

3) функционирование процессов информационной безопасности при воздействии дестабилизирующих факторов:

– управление инцидентами информационной безопасности;

– определение угроз информационной безопасности,

– обеспечение непрерывности деятельности;

4) обеспечение информационной безопасности при работе с персоналом:

– повышение осведомленности персонала;

– безопасность персонала.

Так как одной из главных задач процесса обеспечения информационной безопасности является снижение потенциальных угроз и минимизация и купирование рисков, то, оценивая зрелость процессов информационной безопасности, необходимо учитывать достижение вышеуказанной цели.

Процессы обеспечения информационной безопасности наиболее высокой зрелости характеризуются:

– четкой и документально закрепленной системой категорирования информации;

– регулярными мероприятиями по прогнозированию и выявлению угроз и рисков информационной безопасности;

– разработанной и функционирующей системой информационной поддержки пользователей.

На основе проведенного анализа и определения уровня информационной безопасности необходимо разрабатывать комплексные рекомендации по обеспечению и повышению уровня информационной безопасности.

Основными направлениями повышения уровня информационной защищенности организации могут являться:

– построение системы защиты информации;
– внедрение современных информационных технологий;
– создание специальных подразделений отдела экономической безопасности; определение ответственных за обеспечение информационной безопасности, повышение уровня квалификации персонала в области информационной безопасности.

Защита информации и обеспечение информационной безопасности осуществляются с помощью построения системы защиты информации, обеспечивающей:
– предотвращение хищения, несанкционированного доступа, искажения, уничтожения информации;
– создание информационной, физической защиты информации, предотвращая ее разглашение и искажение;
– сохранение эффективности используемой информации путем предотвращения несанкционированного доступа и использования информации;
– обеспечение защиты информации как объекта собственности
с точки зрения соблюдения законности и правовых гарантий.

Меры защиты включают в себя [19]:
– проверку подлинности информации;
– контроль за доступом к информации, включающий обеспечение контроля за доступом к помещениям, шифрование информации, применение цифровой подписи, применение электронных карт;
– контроль целостности информации, включающий использование средств антивирусной защиты;
– создание службы или отдела, обеспечивающего информационную безопасность;
– регламентирование правил и способов доступа к информации, защиты документов, использования полученных данных.

Для организации защиты информации и повышения информационной безопасности можно предъявить ряд требований [19]:

1) экономичность, которая подразумевает разумное расходование средств на создание и функционирование системы, когда ущерб от утечки информации превышает затраты на ее создание;

2) комплексность, т. е. система защиты должна объединять законодательные, технические и организационные меры;

3) одновременное взаимодействие системы защиты с другими системами, действующими на предприятии, в первую очередь с системой управления предприятием;

4) иерархичность, означающую структурное построение системы защиты по вертикальным уровням и горизонтальным звеньям.

Для успешного функционирования организации на рынке и повышения ее конкурентоспособности необходимо внедрять современные информационные технологии, интегрированные в информационную, процессную и технологическую среду управления [20]. Именно своевременное и уместное применение информационных технологий помогает обеспечивать экономическую, в частности информационную, безопасность хозяйствующего субъекта.

В крупных организациях для осуществления информационной безопасности могут создаваться специальные подразделения, входящие в структуру отдела экономической безопасности, призванные решать ряд вопросов, связанных с определением рисков и угроз информационной безопасности, а также защитой информации от несанкционированного доступа.

Подводя итоги анализа и оценки процесса обеспечения информационной безопасности в организации, необходимо отметить, что важным показателем является экономическая эффективность принятия решений.

Оценка эффективности организации информационной безопасности предполагает оценку общего уровня затрат (материальных, трудовых, финансовых) на построение системы информационной безопасности и оценку достигаемого эффекта [17]. Грамотное распределение ресурсов в целях обеспечения информационной безопасности приводит к повышению уровня информационной безопасности.

Таким образом, информационная безопасность является одной из функциональных составляющих экономической безопасности, которая обеспечивает конфиденциальность, целостность и доступность информации. Обеспечение информационной безопасности организации должно происходить ежегодно и обеспечиваться стандартизированными системами защиты информации.

При оценке и управлении рисками и угрозами информационной безопасности особенностью является интегрирование данного непрерывного процесса в общую систему обеспечения экономической безопасности предприятия.

Можно отметить, что на сегодняшний день нет единой разработанной методики комплексной оценки информационной безопасности организации с определением ее количественных или качественных показателей. Существующие методы и методики необходимо применять в комплексе, учитывая отраслевые, экономические особенности конкретной организации.

1.3. Организационно-технические и инженерно-технические мероприятия сохранения конфиденциальной информации

Комплекс организационно-технических мероприятий сохранения конфиденциальной информации, состоит:

– в ограничении доступа посторонних лиц внутрь корпуса оборудования за счет установки различных запорных устройств и средств контроля;

– в отключении от ЛВС, Internettex СКТ, которые не связаны с работой с конфиденциальной информацией, либо в организации межсетевых экранов;

– в организации передачи такой информации по каналам связи только с использованием специальных инженерно-технических средств;

– в организации нейтрализации утечки информации по электромагнитным и акустическим каналам;

– в организации защиты от наводок на электрические цепи узлов и блоков автоматизированных систем обработки информации;
– в проведении иных организационно-технических мероприятий, направленных на обеспечение компьютерной безопасности.

Организационно-технические мероприятия по обеспечению компьютерной безопасности предполагают активное использование инженерно-технических средств защиты. Например, в открытых сетях для защиты информации применяют межсетевые экраны (МЭ). Межсетевые экраны – это локальное или функционально-распределенное программно-аппаратное средство (комплекс средств), реализующее контроль за информацией, поступающей в автоматизированные системы или выходящей из них.

Проведение организационно-экономических мероприятий по обеспечению компьютерной безопасности предполагает:
– стандартизацию методов и средств защиты информации;
– сертификацию средств компьютерной техники и их сетей по требованиям информационной безопасности;
– страхование информационных рисков, связанных с функционированием компьютерных систем и сетей;
– лицензирование деятельности в сфере защиты информации.

Инженерно-техническое обеспечение компьютерной безопасности – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах обеспечения безопасности предприятия. По области применения технические средства противодействия подразделяются на две категории:

1. Устройства пассивного противодействия:
– детекторы радиоизлучений;
– средства защиты помещений;
– средства защиты телефонных аппаратов и линий связи;
– средства защиты информации от утечки по оптическому каналу;
– генераторы акустического шума;

– средства защиты компьютерной техники и периферийных устройств и др.

2. Устройства активного противодействия:

– системы поиска и уничтожения технических средств разведки;

– устройства постановки помех.

Противодействие угрозам несанкционированного доступа к информации (утечке) с помощью специальных технических средств основывается на двух ключевых идеях: ликвидация (ослабление) канала утечки информации; исключение возможности злоумышленника принимать и воспринимать информацию.

Методы обеспечения информационной безопасности организации в части угроз несанкционированного доступа (НСД) к информации реализуют вышеизложенные принципы. Противодействие утечке информации осуществляется методом скрытия информации. На рис. 1.5 приведена классификация методов обеспечения информационной безопасности, основанных на использовании инженерно-технических средств (ИТС).

Рис. 1.5 – Классификация методов обеспечения информационной безопасности, основанных на использовании ИТС

Для эффективного применения технических средств обеспечения информационной безопасности необходимо комплексное проведение организационных (в части технических средств), организационно-технических и технических мероприятий.

В настоящее время существует развитый арсенал мер и средств обеспечения информационной безопасности от воздействия угроз НСД. Многие из них являются альтернативными, поэтому необходимо выбрать их оптимальный состав. Для выявления утечки информации необходим систематический контроль возможности образования каналов утечки и оценки их энергетической опасности на границах контролируемой зоны (территории, помещения).

Одним из основных направлений противодействия утечке информации по техническим каналам и обеспечения безопасности информационных ресурсов является проведение специальных проверок (СП) по выявлению электронных устройств перехвата информации и специальных исследований (СИ) на побочные электромагнитные излучения и наводки технических средств обработки информации, аппаратуры и оборудования, в том числе и бытовых приборов. Защита информации от утечки по техническим каналам в общем плане сводится к следующим действиям:

– Своевременному определению возможных каналов утечки информации.

– Определению энергетических характеристик канала утечки на границе контролируемой зоны (территории, кабинета).

– Оценке возможности средств злоумышленников обеспечить контроль этих каналов.

– Обеспечению исключения или ослабления энергетики каналов утечки соответствующими организационными, организационно-техническими или техническими мерами и средствами.

Защита информации от утечки по визуально-оптическому каналу – это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за

счет распространения световой энергии. С целью защиты информации от утечки по визуально-оптическому каналу рекомендуется:

– располагать объекты защиты так, чтобы исключить отражение света в стороны возможного расположения злоумышленника (пространственные ограждения);

– уменьшить отражательные свойства объекта защиты;

– уменьшить освещенность объекта защиты (энергетические ограничения);

– использовать средства преграждения или значительного ослабления отраженного света: ширмы, экраны, шторы, ставни, темные стекла и другие преграждающие среды, преграды;

– применять средства маскирования, имитации и другие с целью защиты и введение в заблуждение злоумышленника;

– использовать средства пассивной и активной защиты источника от неконтролируемого распространения отражательного или излученного света и других излучений;

– осуществлять маскировку объектов защиты, варьируя отражательными свойствами и контрастом фона;

– применять маскирующие средства сокрытия объектов можно в виде аэрозольных завес и маскирующих сеток, красок, укрытий.

В качестве оперативных средств сокрытия находят широкое применение аэрозольные завесы. Это взвешенные в газообразной среде мельчайшие частицы различных веществ, которые в зависимости от размеров и агрегатного сочетания образуют дым, копоть, туман. Они преграждают распространение отраженного от объекта защиты света. Хорошими светопоглощающими свойствами обладают дымообразующие вещества. Аэрозольные образования в виде маскирующих завес обеспечивают индивидуальную или групповую защиту объектов и техники, в том числе и выпускаемую продукцию.

Защита информации по акустическому каналу – это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических

полей. Основными мероприятиями в этом виде защиты выступают организационные и организационно-технические меры. Организационные меры предполагают проведение архитектурно-планировочных, пространственных и режимных мероприятий, а организационно-технические – пассивных (звукоизоляция, звукопоглощение) и активных (звукоподавление) мероприятий. Не исключается проведение и технических мероприятий за счет применения специальных защищенных средств ведения конфиденциальных переговоров.

Архитектурно-планировочные меры предусматривают предъявление определенных требований на этапе проектирования зданий и помещений или их реконструкцию и приспособление с целью исключения или ослабления неконтролируемого распространения звуковых полей непосредственно в воздушном пространстве или в строительных конструкциях в виде структурного звука. Эти требования могут предусматривать как выбор расположения помещений в пространственном плане, так и их оборудование необходимыми для акустической безопасности элементами, исключающими прямое или отраженное в сторону возможного расположения злоумышленника распространение звука. В этих целях двери оборудуются тамбурами, окна ориентируются в сторону охраняемой (контролируемо) от присутствия посторонних лиц территории и пр. Режимные меры предусматривают строгий контроль пребывания в контролируемой зоне сотрудников и посетителей.

Организационно-технические меры предусматривают использование звукопоглощающих средств. Пористые и мягкие материалы типа ваты, ворсистые ковры, пенобетон, пористая сухая штукатурка являются хорошими звукоизолирующими и звукопоглощающими материалами – в них очень много поверхностей раздела между воздухом и твердым телом, что приводит к многократному отражению и поглощению звуковых колебаний. В тех случаях, когда пассивные меры не обеспечивают необходимого уровня безопасности, используются активные средства.

К активным средствам относятся генераторы шума – технические устройства, вырабатывающие шумоподобные электронные сигналы. Эти

сигналы подаются на соответствующие датчики акустического или вибрационного преобразования. Акустические датчики предназначены для создания акустического шума в помещениях или вне их, а вибрационные – для маскирующего шума в ограждающих конструкциях. Вибрационные датчики приклеиваются к защищаемым конструкциям, создавая в них звуковые колебания.

Защита информации от утечки по электромагнитным каналам – это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок.

Конструкторско-технологические мероприятия по локализации возможности образования условий возникновения каналов утечки информации за счет побочных электромагнитных излучений и наводок в технических средствах обработки и передачи информации сводятся к рациональным конструкторско-технологическим решениям, к числу которых относятся:

– экранирование элементов и узлов аппаратуры; ослабление электромагнитной, емкостной, индуктивной связи между элементами и токонесущими проводами;

– фильтрация сигналов в цепях питания и заземления и другие меры, связанные с использованием ограничителей, развязывающих цепей, систем взаимной компенсации.

Экранирование позволяет защитить их от нежелательных воздействий акустических и электромагнитных сигналов и излучений собственных электромагнитных полей, а также ослабить (или исключить) паразитное влияние внешних излучений. Эксплуатационные меры ориентированы на выбор мест установки технических средств с учетом особенностей их электромагнитных полей с таким расчетом, чтобы исключить их выход за пределы контролируемой зоны. В этих целях возможно осуществлять экранирование помещений,

в которых находятся средства с большим уровнем побочных электромагнитных излучений (ПЭМИ).

Защита от прослушивания средствами ИТО обеспечивается:

– применением звукопоглощающих облицовок, специальных дополнительных тамбуров дверных проемов, двойных оконных переплетов (при использовании направленного микрофона и стетоскопа);

– оклеиванием стекол светопрозрачным материалом, рассеивающим лазерный луч (при использовании лазерных средств);

– использованием специальных аттестованных помещений, исключающих появление каналов утечки акустической конфиденциальной информации.

Средства обнаружения закладных микрофонов включают:

– средства радиоконтроля помещений;

– средства поиска неизлучающих закладных устройств;

– средства подавления закладных устройств.

Защита информации от утечки по материально-вещественному каналу – это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода информации за пределы контролируемой зоны.

Следует отметить, что при защите информации от утечки по любому из рассмотренных каналов следует придерживаться следующего порядка действий:

– Выявление возможных каналов утечки.

– Обнаружение реальных каналов.

– Оценка опасности реальных каналов.

– Локализация опасных каналов утечки информации.

– Систематический контроль за наличием каналов и качеством их защиты.

Защита информации от утечки по техническим каналам – это комплекс мероприятий, исключающих или ослабляющих бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны. Постулаты такой защиты:

– Безопасных технических средств нет.

– Любой электронный элемент при определенных условиях может стать источником образования канала утечки информации.

– Любой канал утечки информации может быть обнаружен и локализован. «На каждый яд есть противоядие».

– Канал утечки информации легче локализовать, чем обнаружить.

При построении системы защиты компьютерной информации необходимо учитывать тезис, что «рано или поздно любой компьютер подвергнется разрушительным последствиям угроз, будь то вирусная атака, кража или выход жесткого диска из строя». Надежная работа с компьютерной информацией достигается только тогда, когда любое неожиданное событие не приведет к катастрофическим последствиям. Для этого применяют:

1. Резервное копирование наиболее ценных данных. В случае реализации любой угрозы жесткий диск компьютера переформатируют, устанавливают операционную систему и другое программное обеспечение с дистрибутивных носителей, восстанавливают данные, которые берут с резервных носителей. Резервное копирование проводят регулярно по плану. Копии хранят отдельно от компьютера (минимум две копии, которые хранят в разных местах).

2. Антивирусные программы, которые необходимо регулярно применять и регулярно обновлять.

3. Средства аппаратной защиты, например, отключение перемычки на материнской плате защитит от стирания ПЗУ (флеш-BIOS), независимо от того, кто будет пытаться это сделать: вирус, злоумышленник или неаккуратный пользователь.

4. Ограничение доступа посторонних лиц к компьютерам (физическое ограничение доступа, парольная защита и т.д).

Каждую систему защиты информации следует разрабатывать индивидуально, учитывая следующие особенности:

– организационную структуру организации;

– объем и характер информационных потоков (внутри объекта в целом, внутри отделов, между отделами, внешних);
– количество и характер выполняемых операций: аналитических и повседневных;
– количество и функциональные обязанности персонала;
– количество и характер клиентов;
– график суточной нагрузки.

Защита должна разрабатываться для каждой системы индивидуально, но в соответствии с общими правилами. Построение защиты предполагает следующие этапы:
– анализ риска, заканчивающийся разработкой проекта системы защиты и планов защиты, непрерывной работы и восстановления;
– реализация системы защиты на основе результатов анализа риска;
– постоянный контроль за работой системы защиты и автоматической информационной системой (АИС) в целом (программный, системный и административный).

На каждом этапе реализуются определенные требования к защите; их точное соблюдение приводит к созданию безопасной системы.

На сегодняшний день защита АИС – это самостоятельное направление исследований. Поэтому легче и дешевле использовать для выполнения работ по защите специалистов, чем дважды учить своих людей (сначала их будут учить преподаватели, а потом они будут учиться на своих ошибках). Главное при защите АИС специалистами (естественно после уверенности в их компетенции в данном вопросе) – наличие здравого смысла у администрации системы. Обычно, профессионалы склонны преувеличивать реальность угроз безопасности АИС и не обращать внимания на такие «несущественные детали» как удобство ее эксплуатации, гибкость управления системой защиты и т.д., без чего применение системы защиты становится трудным делом. Построение системы защиты – это процесс поиска компромисса между уровнем

защищенности АИС и сохранением возможности работы в ней. Здравый смысл помогает преодолеть большинство препятствий на этом пути.

Для обеспечения непрерывной защиты информации в АИС целесообразно создать из специалистов группу информационной безопасности. На эту группу возлагаются обязанности по сопровождению системы защиты, ведения реквизитов защиты, обнаружения и расследования нарушений политики безопасности и т.д.

Для нейтрализации существующих угроз и обеспечения информационной безопасности предприятия организуют систему менеджмента в сфере информационной безопасности, в рамках которой (системы) проводят работу по нескольким направлениям (рис. 1.6):

– формирование и практическая реализация комплексной многоуровневой политики информационной безопасности предприятия и системы внутренних требований, норм и правил;

– организация департамента (службы, отдела) информационной безопасности;

– разработка системы мер и действий на случай возникновения непредвиденных ситуаций ("Управление инцидентами");

– проведение аудитов (контроля, комплексных проверок) состояния информационной безопасности в образовательной организации [21].

Рис. 1.6 – Структура организационной деятельности в сфере информационной безопасности

В основе средств контроля доступа лежат механизмы опознавания личности и сравнения с установленными параметрами. Политика предприятия может устанавливать как упрощенные подходы к опознаванию, так и использование автоматизированных средств.

Физическая защита объектов, как правило, предполагает усиление конструкций ограждений, элементов зданий, сооружений и отдельных помещений. С физической защитой непосредственно связано использование средств сигнализации и видеонаблюдения.

В зависимости от характера охраняемого объекта в средствах сигнализации могут применяться датчики, работающие на различных физических принципах, имеющие различные настройки и использующие различные каналы связи. В отличие от средств сигнализации средства видеонаблюдения позволяют не только установить факт нарушения, но и в деталях отслеживать его, контролировать ситуацию, а также вести видеозапись, которую можно будет использовать для принятия дальнейших мер (поиск нарушителей, уголовное преследование и т.п.) [22].

Выводы по главе 1

Современная информационная система (ИС) образовательной организации – это комплекс технического, программного и организационного обеспечения в виде различных программ автоматизации основных её процессов (делопроизводства, ведения личных кабинетов преподавателей, сотрудников и обучаемых, составления расписания и т.д.), а также персона-ла, предназначенная для того, чтобы своевременно обеспечивать персонал образовательной организации и обучающихся надлежащей информацией.

Как правило, ИС образовательной организации – многоагентные системы (Multi-Agent Systems) с реализацией многопользовательского режима использования данных, причём с разграничением прав доступа к ним.

Основными информационными подсистемами ИС образовательной организации являются подсистемы поддержки:

– принятия решений управления образовательной организации;

– учебно-образовательного процесса;

– научно-методических исследований и научно-образовательной информации;

– обеспечения повседневной деятельности образовательной организации;

– защиты информационной безопасности (ЗИБ) ИС образовательной организации.

Основной проблемой оптимального управления учебно-образовательным процессом является выбор аналитических методов и численных алгоритмов нахождения оптимального решения.

Подсистема ЗИБ ИС, выполняющая функции регламентации разграничения прав доступа к информации ИС образовательной организации, обусловлена необходимостью надёжной защиты конфиденциальной ин-формации образовательной организации.

Информации образовательной организации разделяется на три группы:

Первая – несекретная (или открытая), которая предназначена для использования как внутри образовательной организации, так и вне нее.

Вторая – для служебного пользования (ДСП), которая предназначена только для использования внутри образовательной организации. Она подразделяется, в свою очередь, на две подкатегории:

– Доступная для всех сотрудников образовательной организации;

– Доступная для определенных категорий сотрудников образователь-ной организации, но данная информация может быть передана в полном объеме другому сотруднику для исполнения трудовых обязанностей.

Третья – информация ограниченного доступа, которая предназначена для использования только специально уполномоченными сотрудниками образовательной организации и не предназначена для передачи иным сотрудникам в полном объеме или по частям.

Информация второй и третьей категории является конфиденциальной.

В подсистеме ЗИБ ИС образовательной организации должны быть реализованы надежные средства разграничения полномочий и контроля за доступом к документам, особенно к документам, содержащим конфиденциальную информацию. Защищенность конфиденциальной информации – свойство, характеризующее невозможность несанкционированного её использования или изменения.

Для выявления и оценки существующих рисков и угроз информационной безопасности могут использоваться методы экспертных опросов, анкетирование, интервьюирование, brainshtorm, Delfy.

На сегодняшний день не существует единой методики расчета количественного и качественного значения уровня информационной безопасности организации.

Методы обеспечения информационной безопасности реализуются с помощью следующих основных средств: физических, аппаратных, программных, аппаратно-программных, криптографических, организационных, законодательных и морально-этических. Физические средства защиты предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.

Своевременное и уместное применение информационных технологий помогает обеспечивать экономическую, в частности информационную, безопасность.

Для успешного функционирования организации на рынке и повышения ее конкурентоспособности необходимо внедрять современные информационные технологии, интегрированные в информационную, процессную и технологическую среду управления

Глава 2. Комплексная оценка состояния обеспечения защищенности информационной безопасности образовательной организации

2.1. Способы оценки информационной безопасности

Образовательные организации, успехи функционирования которых во многом зависят от информационной обеспеченности, для достижения высоких результатов должны все время поддерживать на необходимо-достаточном уровне подсистему ЗИБ своей ИС, включающей комплексную совокупность аппаратно-программных, технических и организационных защитных мер (ЗМ), функционально инициирующей и непрерывно поддерживающей в работоспособном состоянии обеспечение ее защищенности.

Желание образовательной организации иметь подсистему ЗИБ своей ИС, полностью адекватную ее целям по обеспечению доступности, целостности и конфиденциальности информационных активов, приводит к стремлению совершенствовать подсистему ЗИБ ИС. Совершенствование, улучшение ЗИБ своей ИС возможно при условии знания состояний характеристик и параметров используемых ЗМ, осознания угроз информационной безопасности образовательной организации и понимания степени их соответствия требуемым результатам. Понять эти аспекты подсистемы ЗИБ ИС можно только по результатам оценки угроз информационной безопасности образовательной организации, полученной с помощью модели оценки подсистемы ЗИБ ИС на основании свидетельств оценки, критериев оценки и с учётом контекста оценки [30].

Критерии оценки – это всё то, что позволяет установить значения оценки для объекта оценки – конфиденциальности информационных активов, в частности, образовательной организации. В качестве критериев оценки подсистемы ЗИБ ИС образовательной организации могут использоваться требования, процедуры и сочетание требований и процедур подсистемы ЗИБ ИС образовательной организации, уровень инвестиций, затрат на подсистему

ЗИБ ИС в целом – на ее трансформацию, обслуживание и переподготовку пользователей ИС образовательной организации.

К свидетельствам оценки подсистемы ЗИБ ИС образовательной организации относятся записи, контент фактов или любая информация, которая имеет отношение к критериям оценки функционирования подсистемы ЗИБ и может быть проверена. Такими свидетельствами оценки подсистемы ЗИБ ИС образовательной организации могут быть доказательства выполняемой и выполненной деятельности по обеспечению информационной безопасности ИС в виде отчётных, нормативных, распорядительных документов, результатов опросов, наблюдений.

Контекст оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации 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 подсистемы ЗИБ ИС образовательной организации определяет сферу оценки, отражающую контекст оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации в рамках критерия оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации, отображение и преобразование оценки в параметры объекта оценки – конфиденциальности информационных активов, в частности, образовательной организации, а также устанавливает показатели, обеспечивающие оценку оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации в сфере количественной и качественной оценки.

В общем виде процесс проведения оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации (рис. 2.1) представлен основными компонентами процесса: контекст, свидетельства, критерии и модель оценки, необходимыми для реализации процесса оценки. Оценка информационной безопасности подсистемы ЗИБ ИС образовательной органи-

зации заключается в выработке оценочного суждения относительно пригодности (зрелости) процессов обеспечения информационной безопасности подсистемы ЗИБ ИС образовательной организации, адекватности используемых защитных мер или целесообразности (достаточности) инвестиций (затрат) для обеспечения необходимого уровня информационной безопасности подсистемы ЗИБ ИС образовательной организации на основе измерения и оценивания критических элементов (факторов) объекта оценки.

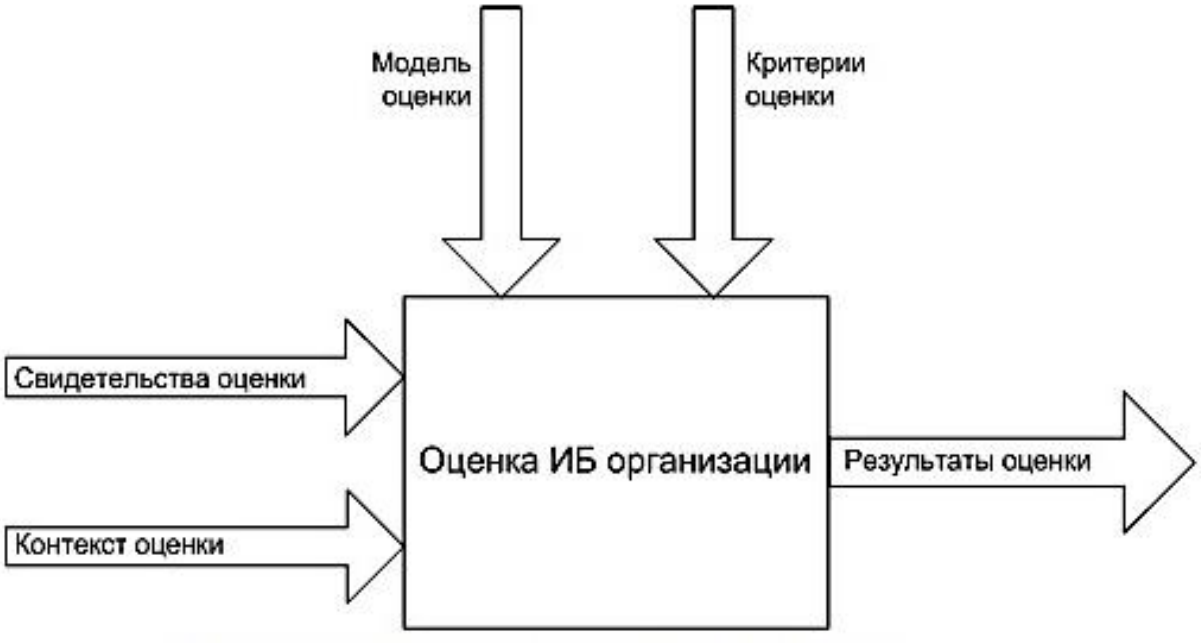

Рис. 2.1 – Схема общего вида процесса оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации

Наряду с важнейшим назначением оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации – созданием информационной потребности для трансформации информационной безопасности подсистемы ЗИБ ИС образовательной организации, возможны и другие цели проведения оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации такие, как:

– определение степени соответствия установленным критериям отдельных областей обеспечения информационной безопасности подсистемы ЗИБ ИС

образовательной организации, процессов обеспечения информационной безопасности подсистемы ЗИБ ИС образовательной организации, ЗМ;

– выявление влияния критических элементов (факторов) и их сочетания на информационной безопасности подсистемы ЗИБ ИС образовательной организации;

– сравнение зрелости различных процессов обеспечения информационной безопасности подсистемы ЗИБ ИС образовательной организации и сравнение степени соответствия различных защитных мер установленным требованиям.

Результаты оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации могут также использоваться заинтересованной стороной для сравнения уровня информационной безопасности подсистемы ЗИБ ИС образовательной организаций с одинаковым уровнем подсистемы ЗИБ своей ИС и сопоставимым масштабом. В зависимости от выбранного для оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации критерия можно разделить способы оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации (рис. 2.2) на оценку по эталону, риск-ориентированную оценку и оценку по экономическим показателям.

Рис. 2.2 – Способы оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации

2.2. Методика комплексной оценки состояния информационной безопасности организации

Назначение системы информационной безопасности организации заключается в разработке безопасных и надѐжных мер по доступу или ограничения допуска к информации, способов передачи и хранения информации, методов обработки информации, правил управления доступом к информации, способов восстановления информации, методов резервирования информации и т.п. [31].

Задачи системы информационной безопасности оговариваются еѐ назначением и заключаются в:

- обеспечении безопасного, надѐжного хранения и передачи информации в электронном виде, расположенной на различных носителях;
- организации надѐжного доступа или ограничения допуска к электронной информации;
- ограничении и контроле доступа к информации, с которой работают сотрудники;
- создании правил безопасной работы с информацией; проведении мероприятий по резервированию информации; обеспечении восстановления информации в аварийных ситуациях; поддержке информационной безопасности на заданном уровне.

Обеспечение информационной безопасности в эпоху постиндустриальной экономики становится жизненно важным для успешного существования предприятия. С другой стороны, встаѐт вопрос надлежащего определения состояния информационной безопасности организации, показателей, его характеризующих, а также значений этих показателей, которые обеспечивают надлежащий уровень информационной безопасности организации [32]. Также важным является вопрос оценки значений этих показателей в условиях неопределѐнности, которая присуща сфере безопасности.

Постановка проблемы в общем виде и еѐ связь с важными научными или практическими задачами. В настоящее время для обеспечения надлежащего

состояния информационной безопасности нужна не просто разработка отдельных ЗМ, а реализация системного подхода, включающего комплекс взаимосвязанных мероприятий (использование специальных технических и программных средств, организационных мероприятий, нормативно-правовых актов и т.д.). Главной целью любой системы обеспечения информационной безопасности является создание условий функционирования организации, предотвращения угроз его безопасности, защита законных интересов организации от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечения в рамках производственной деятельности всех подразделений организации.

Анализ последних исследований и публикаций свидетельствует о том, что вопросам построения и анализа системы информационной безопасности посвящены работы ведущих мировых и отечественных учѐных. В работах одних авторов приведено большое количество показателей, характеризующих состояние информационной безопасности [33], в работах других – указаны меры по повышению уровня защищѐнности информации организации [34], в работах третьих – предлагаются комплексные методики, которые, к сожалению, во-первых, очень трудно внедрять из-за большого количества сложно оцениваемых показателей, а, с другой стороны, – нелегко согласовать с существующим законодательством и международными и национальными стандартами, регламентирующими деятельность, связанную с информационной безопасностью [35].

Таким образом, возникла необходимость разработки комплексного показателя состояния информационной безопасности организации, методики его расчѐта и определения экстремальных значений отдельных показателей, обеспечивающих надежно-достаточный уровень информационной безопасности.

Обобщение исследований ведущих учѐных в области информационной безопасности организации показывает, что иформационная безопасность ор-

ганизации в целом отображает еѐ защищѐнность и эффективность в обеспечении процесса управления.

Процесс обеспечения информационной безопасности организации можно представить как взаимодействие трѐх подсистем:

- подсистемы информационного обеспечения процесса управления на организации;
- подсистемы ЗИБ ИС организации;
- подсистемы диагностики уровня информационной безопасности организации.

Ключевыми задачами подсистемы информационного обеспечения процесса управления на предприятии являются:

- сбор необходимой информации;
- обработка и систематизация информации, оценка и анализ информации;
- прогнозирование всех аспектов деятельности организации, предоставление необходимой информации лицам, принимающим решения.

Непрерывное выполнение всех этих задач необходимо для эффективного функционирования указанной подсистемы.

Защита информационной среды организации включает защиту от вредоносных действий, как конкурентов, так и собственных сотрудников, а также защиту от неумышленных внутренних негативных воздействий.

Для обеспечения защиты информационной среды организации необходимо систематическое выполнение следующих этапов (рис. 2.3):

- анализ внутренних и внешних угроз информационной безопасности организации;
- планирование и разработка мероприятий по обеспечению информационной безопасности;
- оперативная реализация запланированных действий.

Диагностику уровня информационной безопасности предприятия предлагается проводить по трѐм ключевым направлениям (рис. 2.4): оценка про-

граммно-технической защищѐнности информации; оценка информационной надѐжности персонала; оценка ин- формации, предоставляемой лицам, принимающим решения, информационной службой организации.

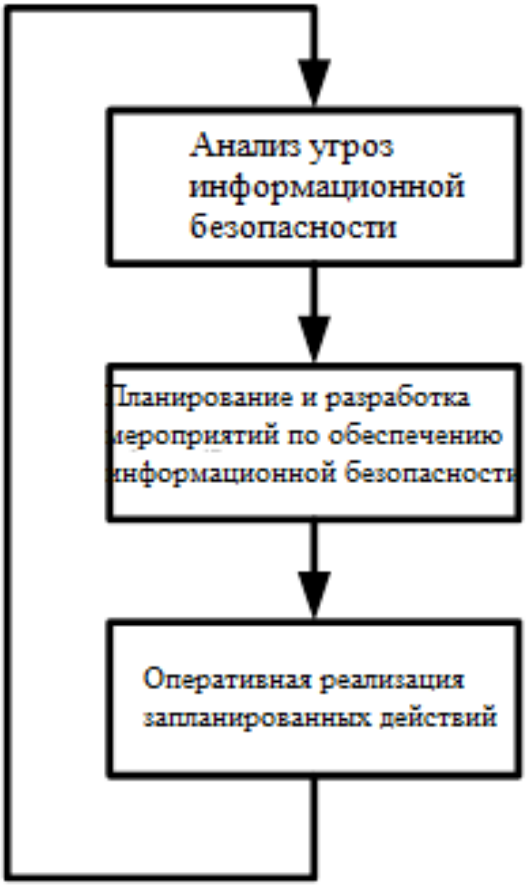

Рис. 2.3 – Схема функционирования информационной безопасности организации

Рис. 2.4 – Определение состояния информационной безопасности организации

Для оценки информационной надѐжности персонала организации предлагается рассчитывать коэффициент правовой защищѐнности информации, коэффициент опыта работы персонала, который обеспечивает информационную безопасность организации, коэффициент надѐжности организации, обеспечивающего информационную безопасность организации и коэффициент подготовленности персонала к распознаванию внутренних и внешних угроз организации.

Оценку информации, предоставляемой лицам, принимающим решения, информационной службой организации предлагается проводить с помощью трѐх показателей: коэффициент полноты информации, коэффициент точности информации и коэффициент противоречивости информации, которые следует дополнить коэффициентом своевременности предоставления информации и коэффициентом надѐжности информации.

При получении информации, необходимой для расчѐта приведѐнных показателей, обязательным условием является наличие системы мониторинга деятельности информационной службы организации [32].

Количественный анализ и моделирование являются теми инструментальными средствами, которые позволяют оценить, выделить, пусть и приближѐнно, существенные риски и угрозы из несущественных (надуманных). Однако в большинстве случаев одного лишь анализа недостаточно для идентификации и выделения существенных факторов риска и пренебрежения несущественными (надуманными). С этой целью необходимо осуществять количественный анализ опасности, что требует получения соответствующей информации.

Методы экспертных оценок включают комплекс логических и математико-статистических методов и процедур, связанных с деятельностью эксперта по переработке необходимой для анализа и принятия решений информации. Центральной "фигурой" экспертной процедуры является сам эксперт – это специалист, который использует свои способности (знания, умения, опыт, интуицию и т.п.) для нахождения наиболее эффективного решения.

Эксперты, привлекаемые для оценки опасности (угроз и рисков), в том числе и информационной, должны:

- иметь доступ ко всей имеющейся в распоряжении разработчика информации;
- обладать достаточным уровнем креативности мышления и необходимыми знаниями в соответствующей предметной области;
- быть свободным от личных предпочтений по проекту.

Методом экспертных оценок с предварительным подбором (отсевом) экспертов посредством их кармы (опыта, квалификации и др.), ранжирование (расположение объектов в порядке возрастания или убывания какого-либо присущего им свойства (значимости) с выбором из сформированной совокупности наиболее существенного фактора, назначение факторам весовых коэффициентов в долях единицы по отношению к наиболее существенному фактору с присвоением ему признака значение, равного единице (A1=1) можно расположить выявленные признаки в виде матрицы (рис. 2.5) для их парного сравнения, например.

	1	2	…	j	…	n
1	a_{11}	a_{12}	…	a_{1j}	…	a_{1n}
2	a_{21}	a_{22}	…	a_{2j}	…	a_{2n}
…	…	…	…	…	…	…
i	a_{i1}	a_{i2}	…	a_{ij}	…	a_{in}
…	…	…	…	…	…	…
n	1_{ni}	a_{n2}	…	a_{nj}	…	a_{nn}

Рис. 2.5 – Матрица сравниваемых объектов

Основные применяющиеся для анализа опасностей (угроз и рисков) методы, кроме метода экспертных оценок, следующие: вопросники; SWOT-анализ; роза (звезда) и спираль рисков; оценка риска стадии проекта; метод Дельфи, метод критических значений (рис. 2.6 и 2.7) [36–39].

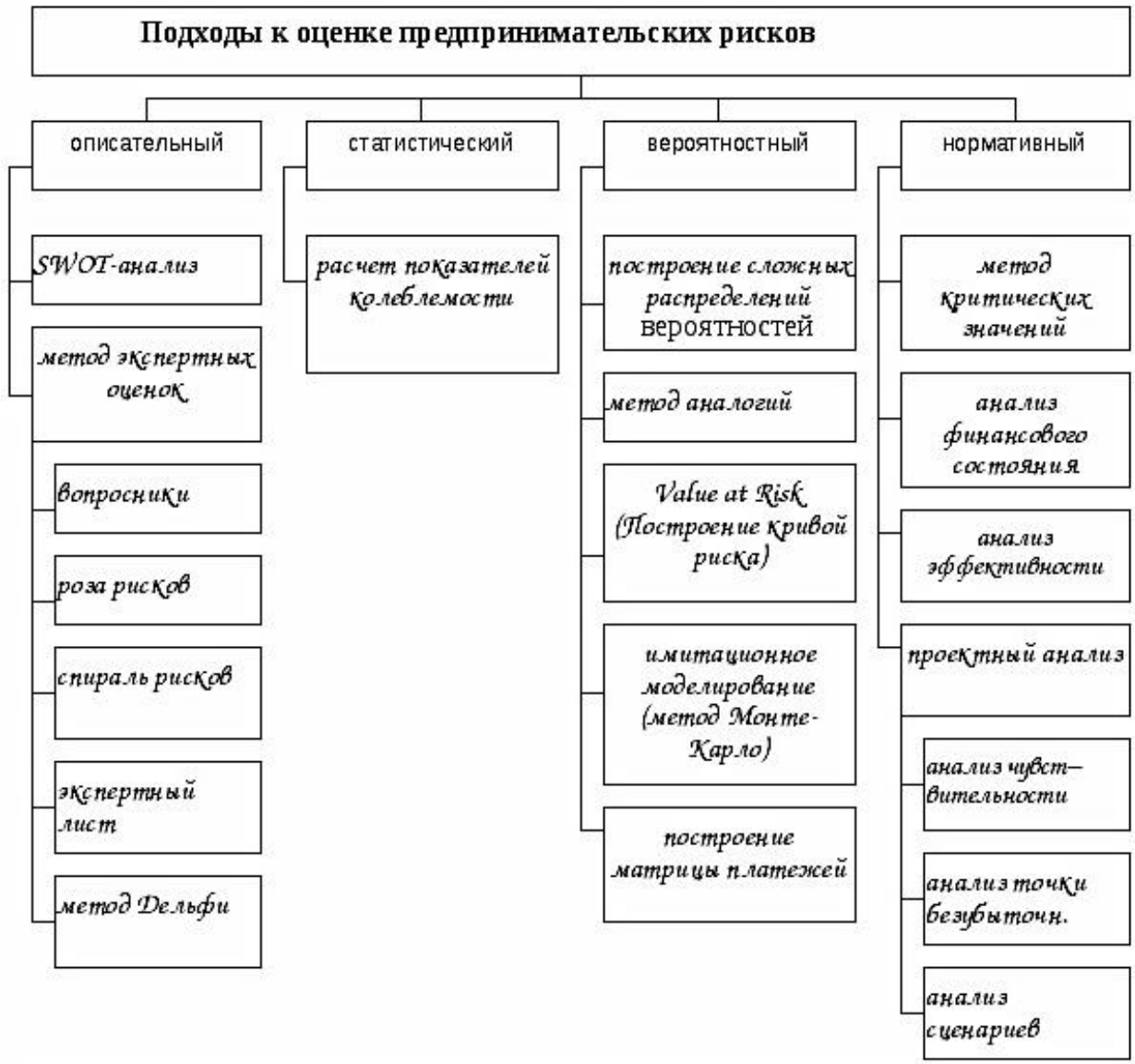

Рис. 2.6 – Структура методов оценки рисков и угроз

Рис. 2.7 – Структура вопросов SWOT-анализа

Информация может существовать в самых разных формах. Еѐ можно печатать или писать на бумаге, хранить на электронных носителях, пересылать по традиционной или электронной почте, показывать в фильмах или передавать в устной беседе. Какую бы форму ни принимала информация, и какие бы средства ни использовались для еѐ передачи и хранения, необходимо всегда обеспечивать соответствующий уровень еѐ защиты.

Информационная безопасность достигается путѐм внедрения совокупности всех необходимых средств защиты, в число которых могут входить рекомендации, инструкции, организационные структуры и программные функции. Эти средства ЗМ необходимо реализовывать для того, чтобы гарантировать выполнение требований к безопасности в конкретной организации.

Система показателей оценки уровня информационной безопасности организации по каждому из предложенных направлений с расчѐтными формулами и пороговыми значениями приведена ниже.

Оценка программно-технической защищѐнности информации

Коэффициент технической защиты информации $К_{Т.З.}$:

$$К_{Т.З.}= ИА_{Н.О.},$$

где:

$А_{Н.О.}$ – количество не отвращенных информационных атак.

Коэффициент программной защищѐнности информации $К_{П.З}$:

$$К_{П.З} = В_{Б.Ф}/ В_{Н.Ф},$$

где:

$В_{Б.Ф}$ – время бесперебойного функционирования корпоративной информационной системы, ч;

$В_{Н.Ф}$ – нормативное время функционирования корпоративной информационной системы, ч.

Коэффициент финансовой защиты информации $К_{Ф.З}$:

$$К_{Ф.З} = Р_{З.ИН}/ Р_{ПР.ИН}) 0,15 – рост$$

где: $Р_{З.ИН.}$ – расходы на защиту информационных ресурсов, руб.;

$Р_{ПР.ИН}$ – расходы на приобретение информационных ресурсов, руб.

Коэффициент финансирования информационных служб организации $К_{Ф.З.}$: $К_{Ф.З} = Р_{ФИН}/ Р_{ОБЩ})$ 0,5 – 0,15 – рост

где:

$Р_{ФИН}$ – расходы на финансирование информационных служб организации, руб.;

$Р_{ОБЩ}$– общие расходы организации.

Оценка информационной надѐжности персонала

Коэффициент правовой защищѐнности информации $К_{Пр.З.}$:

$$К_{Пр.З.}= И / И_{Юр.Л.}, 1 – уменьшение$$

где:

И – объѐм информации, разглашение которой может повлечь негативные последствия для организации, %;

$И_{Юр.Л}$ – общий объѐм юридически защищѐнной информации, %.

Коэффициент опыта работы персонала, обеспечивающего информационную безопасность организации $К_{О.Р.}$:

$$К_{О.Р.}= ЧП_1 / ЧП_З, 1 – рост$$

где:

$ЧП_1$ – численность работников, имеющих доступ к коммерческой тайне, работающих в организации более одного года, чел.;

$ЧП_З$ – общая численность работников, имеющих доступ к коммерческой тайне, чел.

Коэффициент надѐжности персонала, обеспечивающего информационную безопасность организации $К_{Н.О.}$:

$$К_{Н.О.}= (ЧП_{Об.Ув.} – ЧП_{УТ}) / ЧП_{Об.Ув}, 1 – рост$$

где:

$ЧП_{УТ}$ – численность работников, непреднамеренные действия которых привели к утечке информации из-за низкого уровня подготовки персонала к распознаванию угроз безопасности, чел.;

$ЧП_{Об.Ув}$ – общая численность уволенных работников, чел.

Коэффициент подготовленности персонала к распознаванию угроз $К_{П.П.}$:

$$К_{П.П.}= (ЧП_{Общ.} – ЧП_{П}) \ / ЧП_{Общ}, 1 – рост$$

где:

$ЧП_{П}$ – численность работников, непреднамеренные действия которых привели к утечке информации из-за низкого уровня подготовки персонала к распознаванию угроз безопасности, чел.;

$ЧП_{Общ}$, – общая численность работников, имеющих доступ к закрытой информации, чел.

SEP Оценка информации, предоставляемой лицам, принимающим решения (ЛПР), информационной службой организации

Коэффициент полноты информации $К_{П.Ин.}$:

$$К_{П.Ин.}= И_{Н} \ / И_{Необх}, 1 – уменьшение$$

где:

$И_{Н}$ – объѐм информации, которым располагает ЛПР, %;

$И_{Необх}$ – объѐм информации, необходимой для принятия обоснованного решения.

Коэффициент точности информации $К_{Т.Ин.}$:

$$К_{Т.Ин.}= И_{Р} \ / И_{ИМ}, 1 – рост$$

где:

$И_{Р}$ – объѐм релевантной информации, %;

$И_{ИМ}$ – общий объѐм имеющейся в распоряжении ЛПР информации, %.

Коэффициент противоречивости информации $И_{Пр.Ин.}$

$$К_{П.Пр.}= И_{Од} / И_{Общ}, 1 – рост$$

где:

$И_{Од}$ – количество независимых свидетельств в пользу принятия решения, %;

$И_{Общ}$– общее количество независимых свидетельств в суммарном объѐме релевантной информации, %.

Коэффициент своевременности предоставления информации $К_{С.Пр.}$.:

$$К_{С.Пр.} = И_{С.Пр} / И_{Необх}, 1 – рост$$

где:

$И_{С.Пр.д}$ – объѐм своевременно оказанной ЛПР информации, %;

$И_{Необх}$ – объѐм информации, необходимой для принятия обоснованного решения, %.

Коэффициент надѐжности информации $К_{Н.Инф.}$:

$$К_{Н.Иинф.} = И_{Н.Ист} / И_{Общ.Пред}, 1 – рост$$

где:

$И_{Н.Ист}$ – объѐм информации, предоставляемой ЛПР из надѐжных источников, %;

$И_{Общ.Пред}$ – общий объѐм предоставленной ЛПР информации, %.

Любая организация должна определить свои требования к безопасности. При оценке требований используются три основных показателя:

- первый показатель служит для оценки опасностей, с которыми сталкивается организация. Путѐм оценки опасностей определяются угрозы для информации, еѐ уязвимость и вероятность возникновения угроз, а также возможный ущерб;
- второй показатель – это законодательные, нормативные и договорные требования, которые должна соблюдать организация, еѐ партнѐры по образовательной деятельности, подрядчики и поставщики услуг;
- третий показатель – это определѐнный набор принципов, целей и требований к обработке информации, разработанных организацией для поддержки своей деятельности.

Определение требований к безопасности проводится путѐм методической оценки рисков [33]. Расходы на поддержание безопасности необходимо сбалансировать с ущербом для организации, который может возникнуть при нарушении безопасности. Методы оценки опасностей могут применяться ко всей организации или только еѐ частям, а также к отдельным информационным системам, системным компонентам и сервисам, в зависимости от того, что окажется наиболее практичным, реалистичным и полезным.

Важными методами анализа состояния обеспечения информационной безопасности являются методы описания и классификации. Для осуществления эффективной защиты системы управления информационной безопасностью следует, во-первых, описать, а только потом, во-вторых, классифицировать различные виды угроз и опасностей, рисков и вызовов и соответственно сформулировать систему мер по осуществлению управления ими.

В качестве распространѐнных методов анализа уровня обеспечения информационной безопасности используются методы исследования причинных связей — простейшие логические методы установления причинных логических связей между явлениями и вытекающими из причин следствиями. С помощью данных методов (сходства; различия; остатков; сопутствующих изменений) [40–42]:

- устанавливаются причинные связи между угрозами и опасностями;
- осуществляется поиск причин, которые стали источником и вызвали актуализацию тех или иных факторов опасности;
- разрабатываются меры по их нейтрализации или нивелирования, по максимально возможной степени, угроз и опасностей.

В числе данных методов причинных связей можно назвать следующие: метод сходства, метод различия, метод сообщения сходства и различия, метод сопровождаемых изменений, метод остатков.

При обеспечении режима информационной безопасности (ИБ) ИС организации достаточно важное место отводится задаче анализа информационных угроз организации и управления ими.

Независимо от размеров организации и специфики еѐ ИС, работы по обеспечению режима ИБ обычно состоят из следующих этапов:

- выработка политики безопасности;
- определение сферы (границ) системы управления ИБ ИС и конкретизация целей еѐ создания;
- оценка опасностей, выбор контрмер, которые обеспечивают режим ИБ ИС организации, управление рисками;

– аудит системы управления ИБ ИС организации.

Для управления информационной безопасностью ИС организации разрабатывается стратегия управления опасностями. Например, здесь возможны следующие подходы к управлению информационными рисками организации:

– уменьшение риска;
– уклонение от риска;
– изменение характера риска;
– принятие риска.

Выделяют несколько типов методов управления ИБ ИС организации:

– одноуровневые методы строятся на основании одного принципа управления ИБ;
– многоуровневые методы строятся на основе нескольких принципов управления ИБ, каждый из которых служит для решения собственного задания. При этом частные методы не связаны между собой и направлены только на конкретные факторы информационных угроз;
– комплексные методы – многоуровневые методы, которые объединены в единую систему координирующих функций на организационном уровне с целью обеспечения ИБ ИС организации, исходя из анализа совокупности факторов опасности, которые имеют семантическую связь или генерируются из единого информационного центра информационного воздействия;
– интегрированные высокоинтеллектуальные методы – многоуровневые, многокомпонентные технологии, построенные на основании мощных автоматизированных интеллектуальных средств с организационным управлением.

Общие методы обеспечения ИБ ИС организации активно используются на любой стадии управления угрозами. К таким стадиям относятся:

– принятие решения по определению области и контекста информационной угрозы и состава участников процесса противодействия;

- принятие общей стратегии и схемы действий в политической, экономической, социальной и других сферах жизнедеятельности;
- обеспечение адекватного восприятия угрозы и опасности в низших организационных звеньях системы управления ИБ ИС организации;
- выделение необходимых политических, экономических, социальных, административных и организационных ресурсов, достаточных для реализации программы отражения информационной угрозы и сохранения устойчивого развития информационных ресурсов системы управления;
- трансформации результатов оценки рисков в соответствующую политику безопасности, включая национальную.

Специфика используемых методов значительно зависит от субъекта деятельности, объекта воздействия, а также преследуемых целей. Так, методы деятельности индивидуума в связи с его ограниченной возможностью по обеспечению ИБ ИС организации, в основном, сводятся к источнику угрозы, апеллирование к общественному мнению, а также к государству, которое должно принимать решительные меры по нейтрализации информационных угроз. Само общество использует в своей деятельности методы социального регулирования, оказания помощи отдельным индивидам и общественным организациям, которым нанесѐн ущерб в результате обнаружения угрозы. Другой задачей защиты конфиденциальность информации является обеспечение неизменности информации во время еѐ хранения или передачи, т.е. обеспечение еѐ целостности.

Таким образом, конфиденциальность информации, которая обеспечивается с помощью криптографических методов, не является главным требованием при управлении ИБ ИС организации. Выполнение процедур криптокодирования и декодирования может замедлить передачу данных и уменьшить доступ к ним из-за того, что пользователь будет лишѐн возможности своевременного и быстрого доступа к этим данным и информации. Именно поэтому обеспечение конфиденциальности информации должно соответствовать возможности доступа к ней.

Важно, чтобы управление в сфере ИБ ИС организации должно осуществляться на основе принципа доступности и безопасности. Система обеспечения информационной безопасности, в первую очередь, должна гарантировать доступность и целостность информации, и еѐ конфиденциальность в случае необходимости.

Для эффективного обеспечения ИБ ИС организации важно многообразие моделей и методов оценки угроз и опасностей. Их вариативность слишком лабильная и зависит как от уровня развития той или иной цивилизации, так и от контекста проводимой оценки, наличия всесторонних данных по факторам угрозы, алгоритма расчѐта коэффициента вероятности наступления и размера негативных последствий. Наличие конкретных данных по этому вопросу позволяет достаточно точно определить степень влияния информационного оружия, уровень угроз и опасностей.

Важным методом обеспечения ИБ ИС организации является метод критических сценариев. В указанных сценариях анализируются ситуации, когда воображаемый противник парализует систему государственного управления и соответственно снижает способность поддерживать государственное управление в пределах оптимальных параметров.

Существуют методы, которые можно считать основополагающими, позволяющие создать надѐжную основу для реализации информационной безопасности. Эти методы или базируются на важных законодательных требованиях, или относятся к общеизвестным методам работы в области управления информационной безопасностью.

С законодательной точки зрения важнейшими для организации считаются следующие мероприятия: защита данных и неразглашение личной информации, защита организационных записей, защита прав на интеллектуальную собственность.

К общепризнанным методам обеспечения информационной безопасности относятся следующие: создание документа, определяющего политику информационной безопасности, распределение ответственности за информа-

ционную безопасность, обучение и подготовка в области информационной безопасности, создание отчѐтов об инцидентах, поддержка непрерывности бизнеса. Эти методы могут применяться в большинстве организаций и в большинстве сред. Следует заметить, что несмотря на то что все описанные методы являются важными, значимость каждого метода следует определять в свете конкретных рисков, с которыми сталкивается организация.

Основным фактором, от которого зависит отношение организации к вопросам информационной безопасности, является степень еѐ зрелости. Так, например, известная аналитическая компания GartnerGroup и университет CarnegieMellon предложили свои модели определения зрелости компании и состояния информационной безопасности. Разным уровням зрелости соответствуют разные потребности в области информационной безопасности. GartnerGroup выделяет четыре уровня зрелости компании – начиная с нулевого и заканчивая третьим. Значительно расширенную модель определения уровня зрелости компании с точки зрения информационной безопасности предложил университет CarnegieMellon. Согласно этой модели, выделяется пять уровней зрелости компании, которым можно поставить в соответствие разное понимание проблем информационной безопасности организации.

Проблема обеспечения режима информационной безопасности будет формулироваться (хотя бы в неявном виде) и решаться по-разному для организаций, находящихся на разных уровнях развития.

На первом уровне эта проблема, как правило, руководством формально выдвигается. Но это не значит, что она не решается сотрудниками по собственной инициативе – и, возможно, эффективно. Тем не менее, с точки зрения руководства организации, кото- рая находится на первом уровне зрелости, задачи обеспечения режима информационной безопасности, как правило, неактуальны. И всѐ же такие организации могут быть вполне жизнеспособными.

На втором уровне проблема обеспечения информационной безопасности решается неформально, на основе постепенно сложившейся практики. Ком-

плекс мероприятий (организационных и программно-технических) позволяет защититься от наиболее вероятных угроз, как возможных, так и тех, что имели место ранее. Вопрос об эффективности защиты не поднимается. Таким образом, постепенно складывается неформальный список актуальных для организации классов рисков, который постепенно пополняется. Если серьѐзных инцидентов не происходило, руководство организации, как правило, не считает вопрос информационной безопасности приоритетным. В случае серьѐзного инцидента сформированная система обеспечения безопасности корректируется, а необходимость поиска других возможных слабых мест в защите иногда осознаѐтся руководством. Для данного уровня зрелости организации типична локальная (не связанная с другими этапами жизненного цикла технологии) постановка задачи анализа рисков: считается достаточным перечислить актуальные для конкретной информационной системы классы рисков и, возможно, описать модель нарушителя, а задачи анализа вариантов контрмер, их эффективности, управления рисками, как правило, не рассматриваются в качестве актуальных.

На третьем уровне в организации принято следовать в той или иной степени (возможно, частично) стандартам и рекомендациям, обеспечивающим базовый уровень информационной безопасности (например, ISO 17799). Вопросам документирования уделяется должное внимание. Задача анализа рисков не является, по мнению руководства, своевременной. Анализ рисков рассматривается как один из элементов технологии управления режимом информационной безопасности на всех стадиях жизненного цикла. Понятие риска включает несколько аспектов: вероятность, угрозу, уязвимость, иногда стоимость. Один из вариантов оценки риска (определѐнного класса) в этом случае: вероятность возникновения инцидента в результате того, что имеется уязвимость, будет способствовать реализации угрозы. Технология управления режимом информационной безопасности в полном варианте содержит следующие элементы: документирование информационной системы организации с позиции информационной безопасности; категорирование инфор-

мационных ресурсов с позиции руководства организации, определение возможного влияния разного рода событий в области безопасности на информационную технологию; анализ рисков, технология управления рисками на всех этапах жизненного цикла; аудит в области информационной безопасности. На данном уровне зрелости организации анализ рисков связан с другими компонентами технологии управления режимом информационной безопасности.

На четвѐртом уровне для руководства организации актуальны вопросы изменения параметров, характеризующих режим информационной безопасности. На этом уровне руководство отвечает за выбор определѐнных величин остаточных рисков (которые остаются всегда). Риски, как правило, оцениваются по нескольким критериям (не только стоимостным). Технология управления режимом информационной безопасности остаѐтся бывшей, но на этапе анализа рисков применяются количественные методы, которые позволяют оценить параметры остаточных рисков и эффективность различных вариантов контрмер при управлении рисками.

На пятом уровне ставятся и решаются различные варианты оптимизационных заданий в области обеспечения режима информационной безопасности. Примеры постановки задач: выбрать вариант подсистемы информационной безопасности, оптимизированной по критерию "стоимость–эффективность" при заданном уровне остаточных рис- ков; выбрать вариант подсистемы информационной безопасности, при котором минимизируются остаточные риски при фиксированной стоимости подсистемы безопасности; выбрать архитектуру подсистемы информационной безопасности с минимальной стоимостью владения в течение жизненного цикла при установленном уровне остаточных рисков.

Выводы. Использование предлагаемых подходаов к оценке состояния и управления информационной безопасностью предприятия позволяет существенно повысить качество управленческих решений, обеспечить эффектив-

ное использование информационных ресурсов предприятия, сократить расходы на обеспечение информационной безопасности.

Следующим шагом должна стать разработка автоматизированной системы мониторинга состояния информационной безопасности, которая накапливала бы сведения о состоянии информационной безопасности, вычисляла значения показателей и предоставляла рекомендации по управлению состоянием информационной безопасности организации.

2.2. Парадоксы и реальность оценки эффективности информационных систем

Подходы к оценке эффективности информационной безопасности образовательной организации в целом и ее конфиденциальной информации, в частности, все более и более усложняются, поскольку показатели, которые ранее казались наиболее важными, могут с течением времени отходить на второй план, а на ведущие роли выходят показатели, которые ранее недооценивались [24]. Сегодня результат внедрения и эффективности информационных систем понимается значительно глубже, чем в конце 90-х годов XX века. В современных условиях роль информационных технологий и систем в функционировании предприятий и организаций существенно изменилась: они перестали быть просто мощными вычислителями, а стали средой информационной поддержки реальных процессов подготовки и принятия решений. Информационные системы вторглись в «святая святых» предприятий – процессы планирования и управления всех уровней. Современная оценка эффективности ИС – уже не число, а скорее дорожная карта, которая описывает текущее состояние предприятия и предлагает возможный путь наиболее рациональной организации использования ИС. В ней содержатся рекомендации по необходимым изменениям в организационных практиках, архитектуре, интеллектуальном обеспечении для создания условий максимального использования информационных и вычислительных ресурсов. В этих условиях оценки скалярных характеристик финансовых результатов внедрения теряют свою привлекательность. Выгоды от внедрения возникают отнюдь не авто-

матически, они требуют новой организации и обновления знаний и измеряются не только в финансовых единицах [25].

Природа ИТ-среды такова, что ИТ-технологии меняются гораздо быстрее, чем на это способно реагировать сообщество пользователей, а тем более организаций, их применяющих. Таким образом, ИС не может быть «хорошей» или «плохой» сама по себе. Она «хороша» в той мере, в какой она согласуется с организационными практиками организации, возможностями его сотрудников и их мотивацией. Это не значит непременного приспособления технологии к организационной и кадровой ситуации в организации. Напротив, наиболее успешные внедрения ИТ выступают катализатором развития самой организации, развития ее сотрудников и совершенствования реализуемых ей процессов. Важной метрикой успеха в этом случае становится согласованность ИТ-технологии, организации и кадров в динамике, при переходе от одной «ступеньки» развития предприятия к другой. В противном случае разрыв в возможностях ИТ-технологии и возможностях ее продуктивного использования может существенно снизить отдачу либо полностью ее исключить. В предельном случае результаты организации могут стать существенно хуже, чем были до внедрения [25].

Таким образом, современная оценка эффективности ИС – это уже не число, а, прежде всего, дорожная карта, которая описывает текущее состояние предприятия и предлагает возможный путь наиболее рациональной организации использования ИС. В ней содержатся рекомендации по необходимым изменениям в организационных практиках, архитектуре, интеллектуальном обеспечении для создания условий максимального использования информационных и вычислительных ресурсов.

2.3. Эффективность информационных систем: проблемы определения и измерения

Для оценки результата ИТ значительно более подходит понимание «эффективности» как результативности, нежели как экономичности. Переход от

количественного показателя к стоимостной оценке – отдельная нетривиальная задача, которая далеко не всегда имеет решение. Корень проблемы может быть в различии между результативностью (способностью достигать результатов, в том числе и принципиально новых) и экономичностью (соотношением результатов и затрат в денежной форме). Стоимостные методики обычно измеряют экономичность, тогда как внедрение ИТ и ИС влияет прежде всего на результативность. Крупные вложения в ИТ и ИС, проводимые в 70–80-е гг., не обнаруживают сколько-нибудь значимой связи с производительностью фирм, которые эти вложения осуществляют. В 1990-е гг. XX века было предложено несколько направлений разрешения данного парадокса (рис. 2.8) [25].

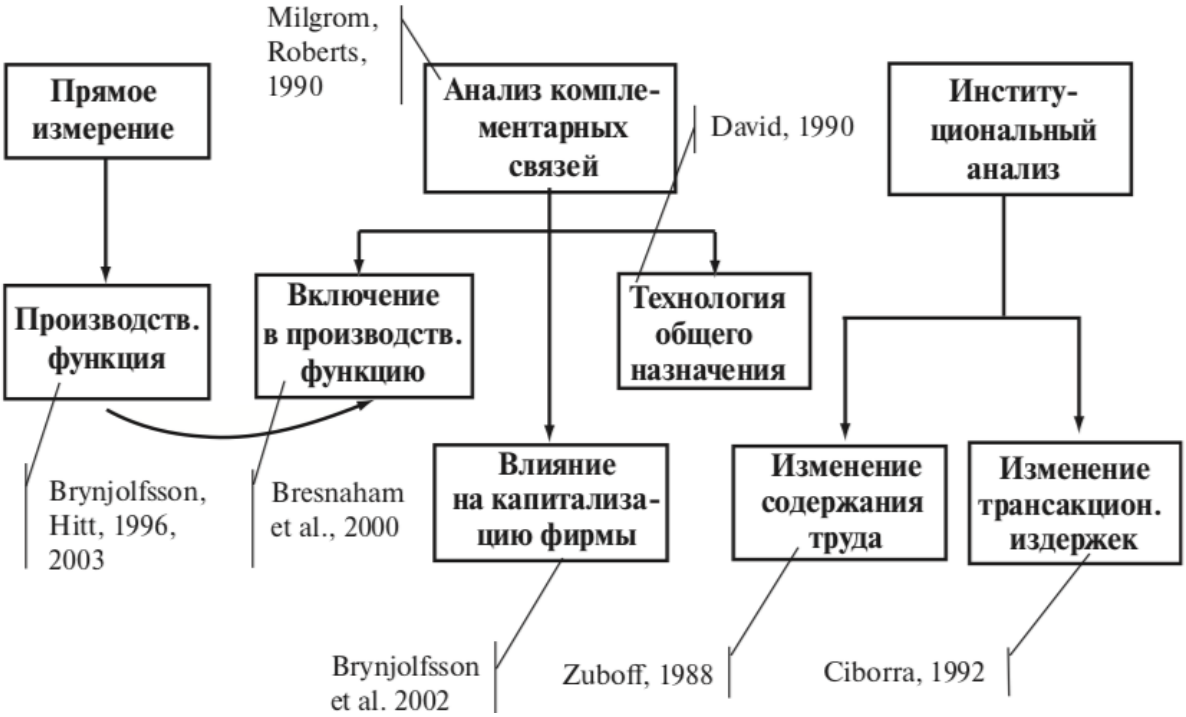

Рис. 2.8 – Основные направления разрешения парадокса производительности

Если наряду с внедрением или трансформацией ИТ создаются новые организационные практики, новые требования возникают и к человеческому капиталу и новые способы его мотивации. Анализ на уровне организации породил в этом случае теоретическую модель комплементарных взаимосвязей [26], а также ряд методов ее эмпирической проверки.

В работе [27] был проведен ряд тестов комплементарных взаимосвязей с использованием косвенных оценок вложений в организационный и челове-

ческий капитал. Была построена функция спроса на компьютерный капитал в зависимости от уровня организационного и человеческого капитала, которая оказалась статистически значимой. Коэффициенты при организационном (ORG) и человеческом капитале (Computer assets) оказались значимыми, а коэффициент детерминации рыночной стоимости ИТ-системы (Market value) при включении этих переменных существенно возрастал (рис. 2.9).

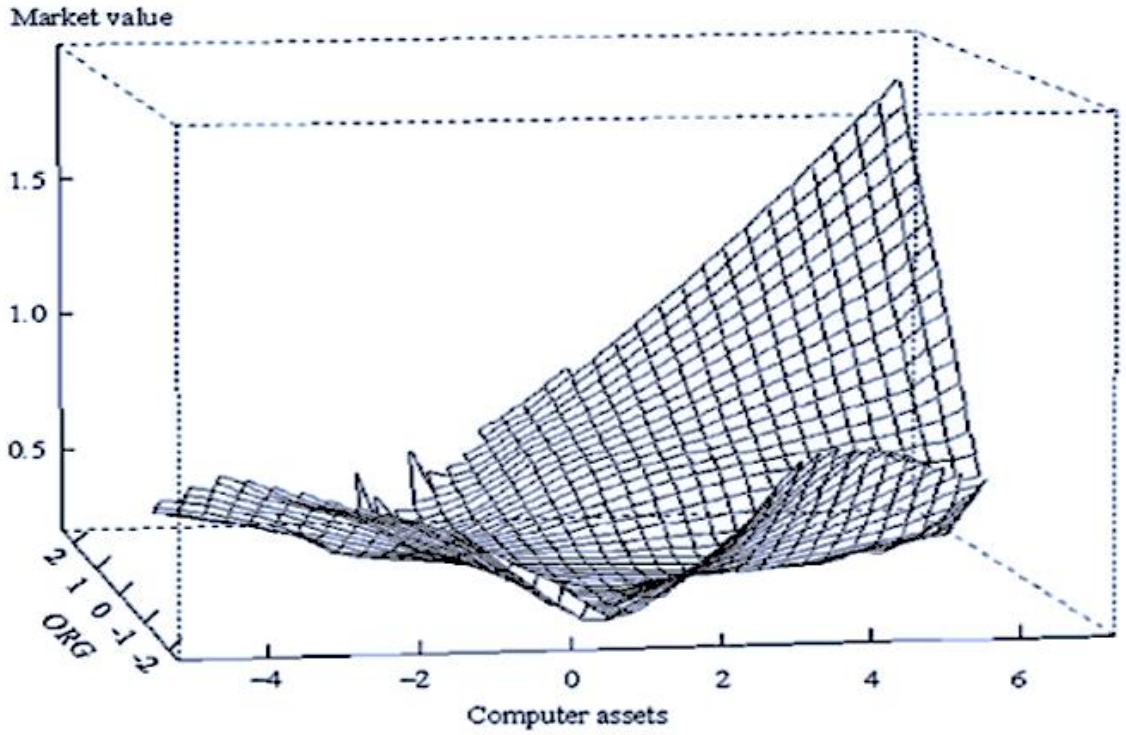

Рис. 2.9 – Зависимость коэффициента детерминации рыночной стоимости ИТ-системы (Market value) от значений величины коэффициентов при организационном (ORG) и человеческом капитале (Computer assets)

В англоязычной экономической и управленческой литературе давно уже различаются два ракурса эффективности: экономичность (англ. efficiency) и результативность (англ. effectiveness). Под результативностью понимается способность решить поставленную задачу, а под экономичностью – соотношение затрат и результатов в ходе такого решения [28, с. 89].

Бесспорное преимущество экономичности – простота измерения. Напротив, измерение результативности – сложная проблема, не имеющая однознач-

ного решения. Это связано с несколькими факторами. Во-первых, результативность фирмы измеряется несколькими различными показателями, т.е. эта величина векторная, а не скалярная. Во-вторых, для разных проектов результативность определяется разными показателями. Сравнить результативность разных проектов становится крайне сложно. Важным косвенным измерителем результативности может стать согласованность между ИТ-сервисами, органиационными практиками и требованиями к человеческому капиталу. Прежде всего именно такая согласованность – необходимое условие получения отдачи от внедрения ИС. Кроме того, изменения в организационном и человеческом капитале требуют значительного времени и ресурсов. Если организация идет на эти изменения, это значит, что она весьма высоко ценит те ИТ-сервисы, которые получает от новой ИС. В работе [29] для этой задачи предложен полезный инструмент – матрица изменений (рис. 2.10).

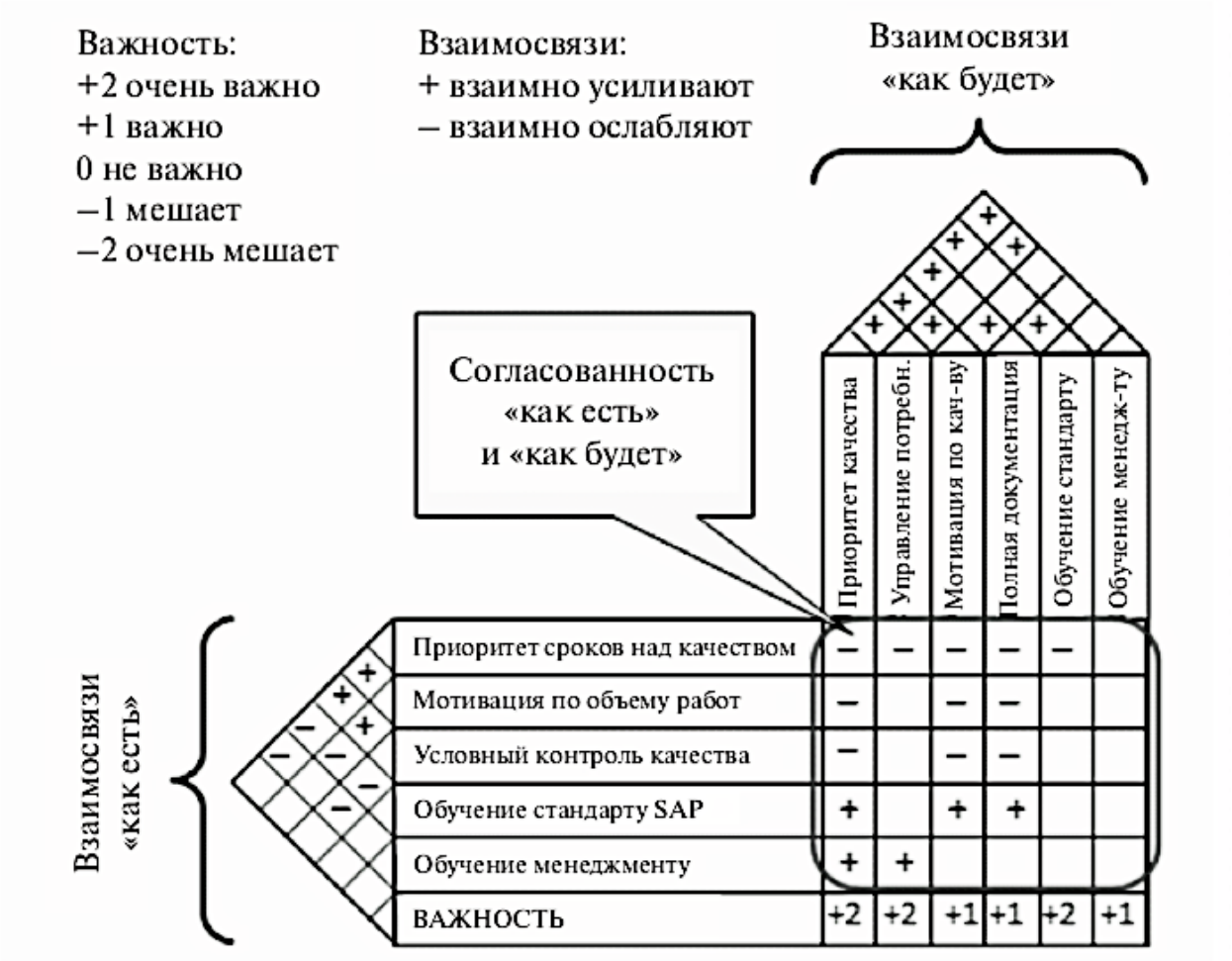

Рис. 2.10 – Пример матрицы изменений

Матрица изменений представляет собой по существу единственный на сегоднишний день инструмент анализа комплементарных взаимосвязей между организационными практиками предприятия или организации. В то же время этот инструмент не лишен недостатков: взаимосвязи не квантифицированы, хотя степень их влияния на результат процесса может сильно отличаться; размерность матрицы ограничена примерно десятком строк и столбцов, превышение этого предела приводит к запретительно высоким трудозатратам на создание матрицы и ее анализ.

Для устранения этих недостатков было предложено расширить матрицу изменений. Ее отличия от матрицы изменений, приведенной на рис. 2.5, состоят в следующем: 1) Расширенная матрица – база данных, поддерживающая иерархическое описание организационных практик: каждая практика может быть раскрыта в несколько практик нижнего уровня (системный подход). В то же время для каждого отдельно взятого уровня можно собрать матрицу текущего состояния (сходную с горизонтальной частью матрицы на рис. 2.5), а для оценки планируемого проекта собрать обе части матрицы изменений. Матрица во всех случаях содержит дополнительную информацию, перечисленную ниже. 2) В расширенной матрице изменений указывается не просто наличие или отсутствие комплементарной взаимосвязи, а ее степень по шкале Ликерта. Вариант такой шкалы приведен в табл. 2.2.

Таблица 2.2 Количественные оценки комплементарных взаимосвязей

Балл	Содержание
−2	При совместном использовании неработоспособны
−1	Совместное использование снижает эффективность
0	Связи нет
+1	Совместное использование повышает эффективность
+2	По отдельности неработоспособны

Основной результат использования ИС – повышение результативности, так что модели оценки экономичности заведомо оценивают второстепенные (хотя в ряде случаев важные) результаты.

Эта проблема имеет и объективную основу – результативность намного сложнее измерить, нежели экономичность, а если и удается, результаты измерений обычно не столь однозначны. Для того чтобы использовать на практике новейшие теоретические результаты, необходимо построить систему измерения результативности.

Выводы по главе 2

Образовательные организации, успехи функционирования которых во многом зависят от информационной обеспеченности, для достижения высоких результатов должны все время поддерживать на необходимо-достаточном уровне подсистему ЗИБ своей ИС, включающей комплексную совокупность аппаратно-программных, технических и организационных защитных мер (ЗМ), функционально инициирующей и непрерывно поддерживающей в работоспособном состоянии обеспечение ее защищенности.

В качестве критериев оценки подсистемы ЗИБ ИС образовательной организации могут использоваться требования, процедуры и сочетание требований и процедур подсистемы ЗИБ ИС образовательной организации, уровень инвестиций, затрат на подсистему ЗИБ ИС в целом – на ее трансформацию, обслуживание и переподготовку пользователей ИС образовательной организации.

Оценка информационной безопасности подсистемы ЗИБ ИС образовательной организации заключается в выработке оценочного суждения относительно пригодности (зрелости) процессов обеспечения информационной безопасности подсистемы ЗИБ ИС образовательной организации, адекватности используемых защитных мер или целесообразности (достаточности) инвестиций (затрат) для обеспечения необходимого уровня информационной безопасности подсистемы ЗИБ ИС образовательной организации на основе измерения и оценивания критических элементов (факторов) объекта оценки.

В зависимости от выбранного для оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации критерия можно раз-

делить способы оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации на оценку по эталону, риск-ориентированную оценку и оценку по экономическим показателям.

Основные применяющиеся для анализа опасностей (угроз и рисков) методы, кроме метода экспертных оценок, следующие: вопросники; SWOT-анализ; роза (звезда) и спираль рисков; оценка риска стадии проекта; метод Дельфи, метод критических значений.

Определение требований к безопасности проводится путѐм методической оценки рисков.

Подходы к оценке эффективности информационной безопасности образовательной организации в целом и ее конфиденциальной информации, в частности, все более и более усложняются, поскольку показатели, которые ранее казались наиболее важными, могут с течением времени отходить на второй план, а на ведущие роли выходят показатели, которые ранее недооценивались. Современная оценка эффективности ИС – уже не число, а скорее дорожная карта, которая описывает текущее состояние предприятия и предлагает возможный путь наиболее рациональной организации использования ИС. В ней содержатся рекомендации по необходимым изменениям в организационных практиках, архитектуре, интеллектуальном обеспечении для создания условий максимального использования информационных и вычислительных ресурсов. Для оценки результата ИТ значительно более подходит понимание «эффективности» как результативности, нежели как экономичности. Переход от количественного показателя к стоимостной оценке – отдельная нетривиальная задача, которая далеко не всегда имеет решение. Стоимостные методики обычно измеряют экономичность, тогда как внедрение ИТ и ИС влияет прежде всего на результативность.

Основной результат использования ИС – повышение результативности, так что модели оценки экономичности заведомо оценивают второстепенные (хотя в ряде случаев важные) результаты.

Глава 3 Разработка проекта рекомендаций по совершенствованию защиты конфиденциальной информации в образовательной организации

3.1. Необходимость трансформации информационной защиты в образовательной организации

Информационные системы разнообразной архитектуры достаточно давно и эффективно используются в только в качестве обучающих сред организациях, активизируя познавательную активность обучающихся (студентов), оказывая положительное влияние на их творческие способности, вовлеченность в образовательный процесс. Однако использование информационных систем образовательных организаций только в качестве комплекса учебно-образовательных программно-аппаратных сред, обучающего контента и контрольно-измерительного инструментария лишь одна из их граней, поскольку насущным является еще и в поддержке организации данного процесса, и в управлении образовательной организацией.

С середины 2000-х годов в образовательных организациях активно внедряются информационные системы, осуществляющие обработку персональных данных, конфиденциальной информации, программы электронного документооборота, бухгалтерские программы и др. Назначение этих систем заключается в ведении баз данных, содержащих в себе личные дела обучающихся (студентов), работников образовательной организации, в расширении административных возможностей при управлении образовательной организацией. Работа с контентом массивов такой информации требует от образовательной организации, с одной стороны, соответствующей современным требованиям скорости доступа и обработки этих массивов, с другой стороны, – соблюдения норм, правил и требований законодательной базы в области организации обработки данных. Кроме персональных данных, в образовательных организациях циркулирует информация научно-методологического, экономического и управленческого характера, нередко содержащая конфиденциальные сведения. Таким образом, любое современное образовательная ор-

ганизации испытывает потребность в защите информации, циркулирующей в данной организации. Вопрос организации надежной защиты информации в образовательной организации является в достаточной степени актуальным.

Информация различного рода поступает в ИС образовательной организациииз совершенно различных источников. Это внешние и внутренние источники информации. Прежде всего, это руководящие документы, поступающие из центральных и местных органов государственного управления, из вышестоящих органов, а также из других образовательных организаций, и информация, не относящаяся напрямую или косвенно к образовательному процессу. Внутренняя информация в общеобразовательной организации содержит в себе руководящие документы, акты и отчеты, бухгалтерскую информацию, статистическую информацию, описывающую образовательный процесс и персональные данные.

Наибольший интерес с точки зрения обязательной защищенности и ответственности руководства образовательной организации представляют собой персональные данные (работников организации, обучающихся), а также конфиденциальная информация, протекающих в общеобразовательной организации процессов. Информационные потоки, циркулирующие в типовом образовательной организации на объекте защиты, обозначены на рисунке 3.1.

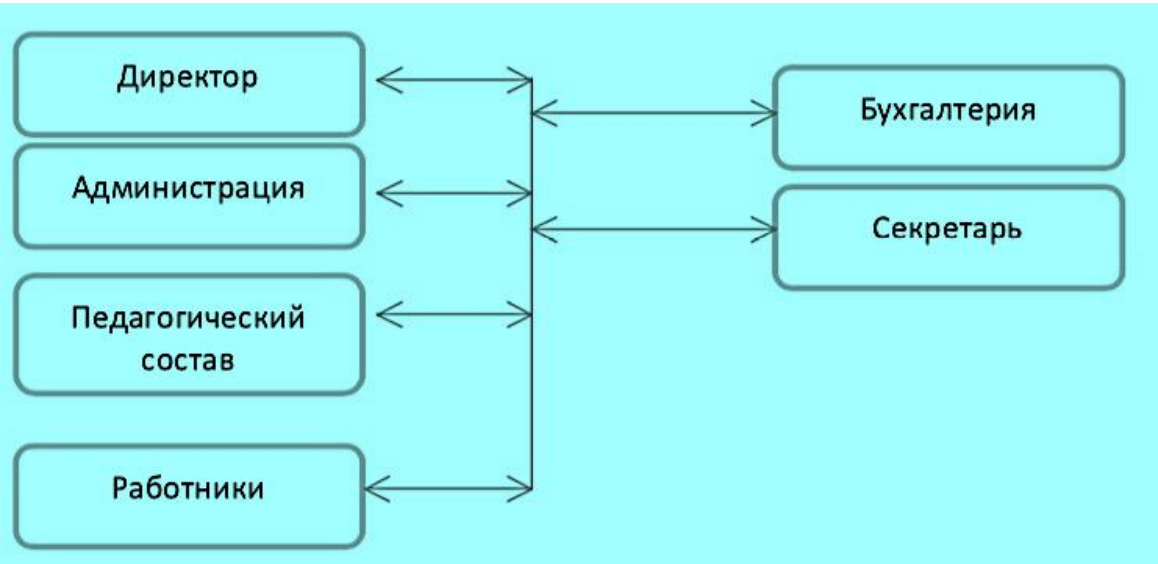

Рис. 3. 1 – Примерная схема информационных потоков организации

Рассматривая процесс обмена информацией и организации доступа к конфиденциальной информации, необходимо отметить, что доступ к такой информации могут получать как директор образовательной организации, так и секретарь, работники администрации, бухгалтерии и педагогический состав образовательной организации.

Основополагающим моментом появления прецедентов утечки информации на объектах являлось прежде всего нарушение правил обращения с техническими средствами, программно-аппаратными средствами защиты данных, некорректная организация хранения и доступа к информации, несовершенство нормативной базы образовательной организации в рамках инициации защиты информации.

Причины утечки информации в образовательной организации, на наш взгляд, кроются в следующих факторах:

- высокая текучесть кадров, в том числе имевших доступ к сведения конфиденциального характера (сюда относится и высокий отток кадров из-за сравнительно невысокой заработной платы);
- отсутствие соответствующих компетенций работников образовательных организаций в области обеспечения правил и норм защиты информации и требований выполнения этих норм и правил;
- отсутствие аттестованных средств защиты информации в организациях образования или их недостаточное количество;
- недостаточный контроль за соблюдением правил и норм защиты информации в образовательной организации, неэффективная организация правовых, организационных и инженерно-техническими мер защиты.

Большинство причин, влияющих на появление предпосылок и возможностей утечки информации в образовательной организации, возникает из-за отсутствия нормативной базы, недостаточной квалификации сотрудников в области защиты информации и в отсутствие средств защиты на объекте.

Основная причина утечек данных – собственные сотрудники организаций. Но дело не в злом умысле, а в недостатке знаний о безопасности. Семь

утечек из десяти случаются по вине сотрудников. Проанализировав в начале 2021 года данные по утечкам в 130 странах, эксперты IBM и вовсе пришли к выводу, что человеческая ошибка стала их причиной в 95% случаев. Ответом на новый вызов стали обучающие платформы, главная цель которых – повысить осведомленность сотрудников орий в области информационной безопасности [44].

В качестве возможного нарушителя системы защиты информации в рамках образовательной организации могут выступать: бывшие сотрудники (педагоги, работники администрации, обслуживающий персонал); обучающиеся образовательной организации.

В свете отмеченного определены основные направления для трансформации системы защиты информации на объектах системы образования:

– ввод дополнительных мер в политике информационной безопасности образовательной организации;

– проведение ряда мероприятий, направленных на соблюдение политик безопасности и инструкций, направленных на защиту информации в образовательной организации (рис. 3.2).

Предложенная модель может позволить повысить надежность и эффективность системы защиты информации в общеобразовательной организации при соблюдении норм эксплуатации системы, организационных требований и рекомендаций.

3.2 Необходимость анализа профессиональных компетенций педагогических работников образовательной организации

Одним из направлений развития российского общества в 2000-е г.г. явилось активное внедрение информационно-коммуникационных технологий в образовательный процесс профессиональных образовательных организаций (ПОО). Из этого вытекает понимания того, что профессиональная компетентность педагога, работающего в образовательной организации, немыслима

сегодня без овладения им информационно-коммуникационными технологиями (ИКТ).

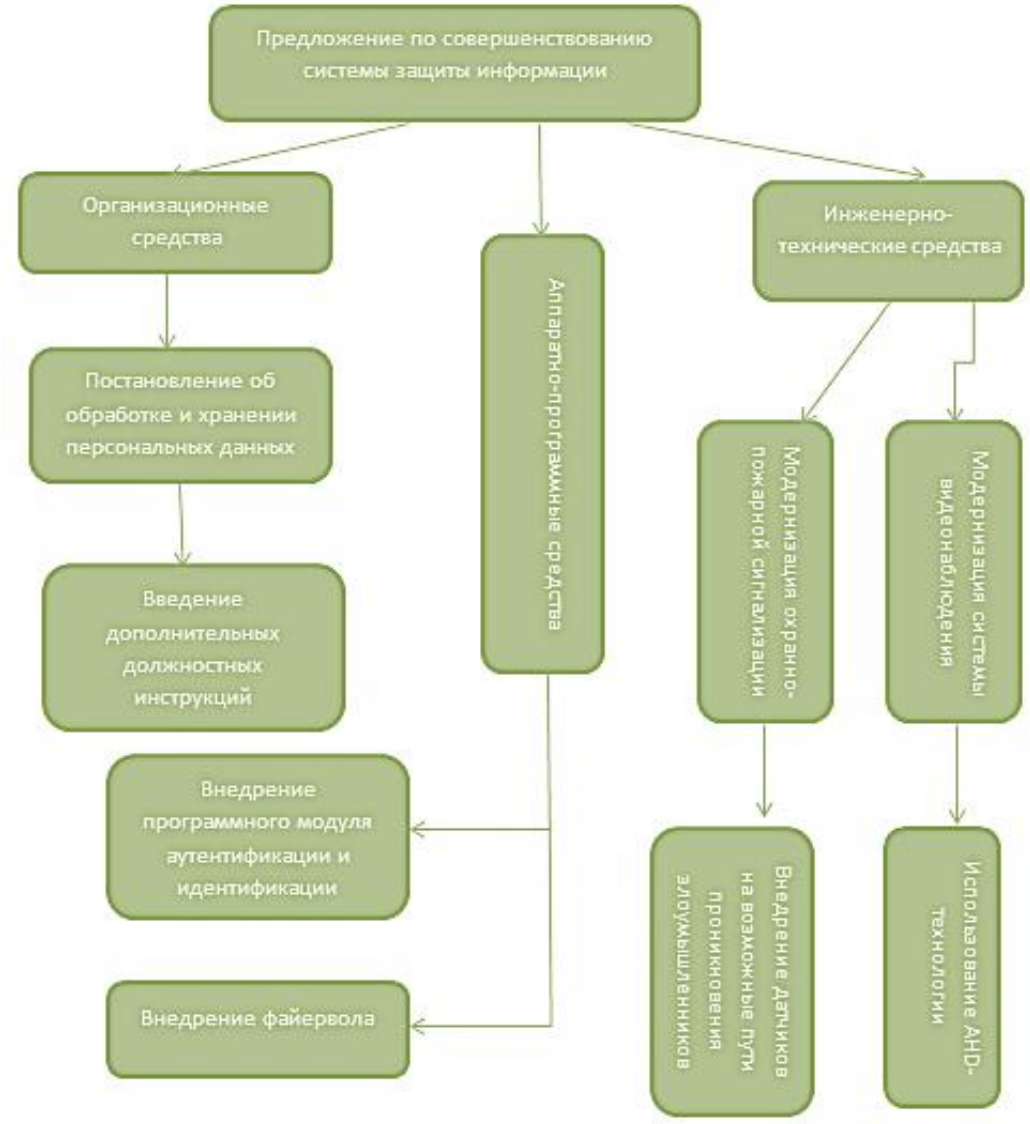

Рис. 3.2 – Модель предложения по совершенствованию системы защиты образовательной организации

В соответствии с принятым в 2015 г. Министерством труда и социальной защиты РФ профессиональным стандартом «Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования» вводится понятие «трудовая функция» педагога профессионального образования, которое связано с понятием «профессиональная компетенция» в федеральных государственных образовательных стандартах профессионального образования, так как действия, составляющие тру-

довую функцию в профессиональном стандарте, подразумевают «наличие у работника определенных умений и знаний, а также готовность их применять»

Возникает проблема: как сформировать профессиональные компетенции педагогов для успешной организации не только с целью трансформации образовательного процесса с помощью ИКТ, но и защиты конфиденциальной информации в образовательной организации, поскольку, как было показано выше, до 70 процентов угроз и нарушений принадлежит сотрудникам образовательной организации, в числе которых педагоги составляют свыше 60 процентов.

Для этого необходимо решить следующие задачи:

1) проанализировать профессиональные компетенции педагогических работников образовательной организации в соответствии с новым профессиональным стандартом;

2) определить предусмотренные профессиональным стандартом обязательные знания и умения педагогического работника, которые можно формировать с использованием ИКТ;

3) обосновать необходимые педагогические условия, способствующие эффективному использованию ИКТ для формирования и развития профессиональных компетенций педагогических работников, в том числе для надлежащей защиты конфиденциальной информации в образовательной организации.

3.3 Тест-анализ ИКТ-компетенции педагогических работников образовательной организации

В первую очередь в настоящее время следует выявить нынешний уровень ИКТ-компетенции педагогических работников, с помощью тест-анализа.

Затем по итогам тест-анализа необходимо решение администрации образовательной организации о повышении ИКТ-компетентности педагогов, нынешний уровень ИКТ-компетенции которых недостаточен для, по мень-

шей мере, надлежащей защиты конфиденциальной информации в образовательной организации.

В итоге представляется необходимым также решение администрации образовательной организации о постоянном контроле уровня ИКТ-компетенции педагогических работников с помощью тест-анализа в обеспечение, по меньшей мере, надлежащей защиты конфиденциальной информации в образовательной организации, что несомненно даст положительный результат в части предотвращения ее убытков.

Тест №1 проверки ИКТ-компетентности современного педагога:

1) Вопрос №1. Выберите программу для работы с текстовой информацией

1. MS Word
2. MS PowerPoint
3. Paint
4. Adobe Flash Player

Вопрос №2. Программа, которая позволяет пользователю обеспечить любое взаимодействие с интернет сайтами и является одной из самых часто используемых программ на компьютере.

1. Браузер
2. Командная строка
3. Adobe Flash Player
4. Microsoft Outlook

Вопрос №3. Выберите те форматы, которые присущи графическим файлам.

1. .Bmp
2. .Gif
3. .doc
4. .png
5. .avi
6. .ppt

7. .exe

Вопрос №4. Рабочая область мультимедийной презентации называется...

1. Поле
2. Слайд
3. Страница
4. Лист

Вопрос №5. Выберите средства вывода информации.

Выберите средства вывода информации

1.
2.
3.
4.
5.
6.

Вопрос №6. Microsoft Excel – это...

1. Программа для работы с электронными таблицами
2. Программа для работы с изображениями
3. Программа для работы с текстом
4. Программа для работы с мультимедиа

Вопрос №7. Выберите названия тех систем, которые не являются операционными.

1. Yandex
2. iOS
3. Android
4. Windows
5. Google
6. Linux
7. CMS

Вопрос №8. Программа, которая осуществляет сжатие одного или множества файлов с последующей упаковкой в архив.

1. Архиватор
2. Архивация
3. WinRAR
4. WinZIP

Вопрос №9. Часть гипертекстового документа, ссылающаяся на другой элемент в самом документе, на другой объект, либо на элементы этого объекта называется ...

1. Мультимедиа
2. Интерактив
3. Гипертекст

4. Гиперссылка

Вопрос №10. Телекоммуникация означает ...

1. проверку работоспособности компьютера

2. обмен информации на расстоянии

3. свойство модема

4. синоним термина мультимедиа

Тест №2 проверки ИКТ-компетентности современного педагога:

Вопрос №1 ФГОС профессионального образования определяет:

1. минимальный уровень освоения содержания образования в образовательной организации;

2. избыточный уровень освоения содержания образования в образовательной организации;

3. определяет возможное содержание, изучаемое обучающимися образовательной организации;

4. возможные программы, технологии, методы и способы организации обучения в образовательной организации.

Вопрос №2 Какое место отводится предметным знаниям в новом ФГОС:

1. Является основным компонентом содержания образования, который определяет тип учебно-познавательной деятельности на занятиях.

2. Являются одним из основных компонентов содержания образования и на ряду с другими определяют типы учебно-познавательной деятельности.

3. Не являются основным компонентом содержания образования, уступая лидирующее место универсальным учебным действиям.

4. Не является компонентом содержания образования и может быть заменен другим компонентом.

Вопрос №3 Какое определение универсальные учебные действия является наиболее полным и точным:

1. умение учится;
2. способность субъекта к саморазвитию и самосовершенствованию путем сознательного и активного присвоения нового социального опыта;
3. учебные умения, обуславливающие успешное осуществление учебно-познавательной деятельности.

Вопрос №4 Функциями универсальных учебных действий являются:

1. обеспечивают субъекта развитием универсальных качеств, необходимых при реализации любых видов деятельности;
2. обеспечивают успешное усвоение знаний, формирование умений, навыков и компетентностей в любой предметной области;
3. обеспечивают возможности учащихся самостоятельно осуществлять деятельность учения, ставить учебные цели, искать и использовать способы их достижения, контролировать и оценивать процесс и результаты деятельности;
4. обеспечивают субъекта совокупностью умений, которые могут заменять недостаток предметных знаний.

Вопрос №5 К метапредметным результатам не относятся:

1. личностные;
2. познавательные;
3. коммуникативные;
4. регулятивные.

Вопрос №6 Федеральный государственный образовательный стандарт – это совокупность систем требований:

1. к образовательным результатам, образовательным программам, условиям реализации образовательного процесса;

2. к содержанию общеобразовательных дисциплин;

3. к уровню освоения предметных знаний учащихся и универсальных учебных действий.

Вопрос №7 Принципиальными особенностями деятельностного образования являются:

1. основным компонентом содержания образования является деятельность, что должно находить отражение в целевом, процессуальном и контрольно-оценочных компонентах учебного процесса.

2. формирование универсальных учебных действий осуществляется по средствам изучения предметного содержания.

3. ориентация на развитие индивидуальных, личностных качеств обучающихся.

Вопрос №8 Организация рефлексии учащихся обеспечивает формирование:

1. регулятивных учебных действий;

2. универсальных учебных действий;

3. универсальных учебных действий и предметных знаний, умений и навыков.

Вопрос №9 Схема «компонент содержания образования» позволяет определить:

1. единицы содержания образования;

2. условия реализации предметных знаний умений и навыков;

3. условия реализации как предметных ЗУН, так и универсальных учебных действий.

Вопрос №10 В каком аспекте рассматриваются коммуникативные учебные действия в ФГОС:

1. философском;

2. системно-мыследеятельностном;
3. психологическом;
4. филологическом.

Вопрос №11 Какое умение не относится к группе коммуникативных учебных действий:
1. умения строить продуктивное взаимодействие и сотрудничество со сверстниками и взрослыми – в парах, группах, командах;
2. умения выражать свои мысли в устной и письменной форме, слушать и читать с пониманием;
3. умения перерабатывать информацию и представлять ее в разных формах.

Вопрос №12 Общие умения коммуникации это:
1. умения, обеспечивающие адекватное восприятие письменной и устной информации, а также адекватное ее изложение;
2. умения, обеспечивающие продуктивное сотрудничество и взаимодействие между различными участниками учебного процесса;
3. умения, позволяющие работать с текстами (устными и письменными) из разнообразных предметных областей.

Вопрос №13. Регулятивные учебные действия это:
1. группа умений, позволяющая планировать, осуществлять и оценивать учебную деятельность;
2. группа умений, отвечающая за контроль и оценку результатов собственной учебной деятельности;
3. группа умений, отвечающих за планирование и организацию самостоятельной учебной деятельности;

Вопрос №14 Схема целеполагания включает следующие блоки:

1. познавательные и учебные мотивы, учебные действия и операции (ориентировка, преобразование материала), контроль и оценка, рефлексия;
2. собственные потребности, внешние вызовы и заказы, ограничивающие условия, способствующие условия;
3. мотивация, прогнозирование, планирование.

Вопрос №15 Каким компонентом задаются искусственные процессы в социальной действительности?
1. намерениями и желаниями субъекта;
2. деятельностью субъекта;
3. рефлексивным охватом субъекта ситуации

Вопрос №16. Рефлексия – это:
1. способность субъекта видеть со стороны свои действия, определяя их достоинства и недостатки;
2. способность субъекта к анализу собственной деятельности и деятельности других;
3. метод мышления, способ получения субъектом знаний об основаниях собственной деятельности при смене «позиции», осуществляется рефлексивный выход и происходит формирование собственной нормы.

Вопрос №17 Проектно-исследовательская деятельность обеспечивает формирование регулятивных учебных действий, так как:
1. предполагает решение обучающимися исследовательских задач;
2. позволяет осваивать научный тип мышления обучающимися;
3. предполагает высокую степень самостоятельности обучающихся при выполнении исследовательских задач.

Вопрос №18 Индивидуальная образовательная программа учащегося складывается из:

1. образовательных потребностей обучающегося, стандарта образования, индивидуальных способов и средств освоения содержания;
2. способностей обучающегося и его целевых установок и мотивов;
3. намерений и возможностей обучающегося.

Вопрос №19 К познавательным универсальным действиям не относится:
1. умения определять понятия, создавать обобщения, устанавливать аналогии, классифицировать, самостоятельно выбирать основания и критерии для классификации, устанавливать причинно- следственные связи, строить логическое рассуждение, умозаключение (индуктивное, дедуктивное и по аналогии) и делать выводы;
2. умения создавать, применять и преобразовывать знаки и символы, модели и схемы для решения учебных и познавательных задач;
3. умения определять способ работы и действовать согласно этого способа.

Вопрос №20. Анализ – это :
1. (от греч. – разложение) – мысленное или фактическое разделение (расчленение, дробление) целого предмета на составные части.
2. (от греч. – соединение) – мысленное или фактическое объединение полученных в результате анализа отдельных объектов или их частей в единое целое.
3. сходство в каком-нибудь отношении между явлениями, предметами, понятиями. Аналогия в биологии — сходство каких-либо структур или функций, не имеющих общего происхождения, например, аналогичные и гомологичные органы.

Выводы по Главе 3

Кроме персональных данных, в образовательных организациях циркулирует информация научно-методологического, экономического и управленческого характера, нередко содержащая конфиденциальные сведения. Та-

ким образом, любое современное образовательная организации испытывает потребность в защите информации, циркулирующей в данной организации. Вопрос организации надежной защиты информации в образовательной организации является в достаточной степени актуальным.

Основополагающим моментом появления прецедентов утечки информации на объектах являлось прежде всего нарушение правил обращения с техническими средствами, программно-аппаратными средствами защиты данных, некорректная организация хранения и доступа к информации, несовершенство нормативной базы образовательной организации в рамках инициации защиты информации.

Большинство причин, влияющих на появление предпосылок и возможностей утечки информации в образовательной организации, возникает из-за отсутствия нормативной базы, недостаточной квалификации сотрудников в области защиты информации и в отсутствие средств защиты на объекте. Возникла проблема: как сформировать профессиональные компетенции педагогов для успешной организации не только с целью трансформации образовательного процесса с помощью ИКТ, но и защиты конфиденциальной информации в образовательной организации, поскольку, как было показано выше, до 70 процентов угроз и нарушений принадлежит сотрудникам образовательной организации, в числе которых педагоги составляют свыше 60 процентов. Представляется необходимым также решение администрации образовательной организации о постоянном контроле уровня ИКТ-компетенции педагогических работников с помощью тест-анализа в обеспечение, по меньшей мере, надлежащей защиты конфиденциальной информации в образовательной организации, что несомненно даст положительный результат в части предотвращения ее убытков.

ЗАКЛЮЧЕНИЕ

Образовательные организации, успехи функционирования которых во многом зависят от информационной обеспеченности, для достижения высоких результатов должны все время поддерживать на необходимо-достаточном уровне подсистему ЗИБ своей ИС, включающей комплексную совокупность аппаратно-программных, технических и организационных защитных мер (ЗМ), функционально инициирующей и непрерывно поддерживающей в работоспособном состоянии обеспечение ее защищенности.

В качестве критериев оценки подсистемы ЗИБ ИС образовательной организации могут использоваться требования, процедуры и сочетание требований и процедур подсистемы ЗИБ ИС образовательной организации, уровень инвестиций, затрат на подсистему ЗИБ ИС в целом – на ее трансформацию, обслуживание и переподготовку пользователей ИС образовательной организации.

Оценка информационной безопасности подсистемы ЗИБ ИС образовательной организации заключается в выработке оценочного суждения относительно пригодности (зрелости) процессов обеспечения информационной безопасности подсистемы ЗИБ ИС образовательной организации, адекватности используемых защитных мер или целесообразности (достаточности) инвестиций (затрат) для обеспечения необходимого уровня информационной безопасности подсистемы ЗИБ ИС образовательной организации на основе измерения и оценивания критических элементов (факторов) объекта оценки.

В зависимости от выбранного для оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации критерия можно разделить способы оценки информационной безопасности подсистемы ЗИБ ИС образовательной организации на оценку по эталону, риск-ориентированную оценку и оценку по экономическим показателям.

Основные применяющиеся для анализа опасностей (угроз и рисков) методы, кроме метода экспертных оценок, следующие: вопросники; SWOT-

анализ; роза (звезда) и спираль рисков; оценка риска стадии проекта; метод Дельфи, метод критических значений.

Определение требований к безопасности проводится путѐм методической оценки рисков.

Подходы к оценке эффективности информационной безопасности образовательной организации в целом и ее конфиденциальной информации, в частности, все более и более усложняются, поскольку показатели, кото-рые ранее казались наиболее важными, могут с течением времени отходить на второй план, а на ведущие роли выходят показатели, которые ранее недооценивались. Современная оценка эффективности ИС – уже не число, а скорее дорожная карта, которая описывает текущее состояние предприятия и предлагает возможный путь наиболее рациональной организации использования ИС. В ней содержатся рекомендации по необходимым изменениям в организационных практиках, архитектуре, интеллектуальном обеспечении для создания условий максимального использования информационных и вычислительных ресурсов. Для оценки результата ИТ значительно более подходит понимание «эффективности» как результативности, нежели как экономичности. Переход от количественного показателя к стоимостной оценке – отдельная нетривиальная задача, которая далеко не всегда имеет решение. Стоимостные методики обычно измеряют экономичность, тогда как внедрение ИТ и ИС влияет прежде всего на результативность.

Основной результат использования ИС – повышение результативности, так что модели оценки экономичности заведомо оценивают второстепенные (хотя в ряде случаев важные) результаты.

Современная информационная система (ИС) образовательной организации – это комплекс технического, программного и организационного обеспечения в виде различных программ автоматизации основных её процессов (делопроизводства, ведения личных кабинетов преподавателей, сотрудников и обучаемых, составления расписания и т.д.), а также персона-ла, предназначенная для того, чтобы своевременно обеспечивать персонал образователь-

ной организации и обучающихся надлежащей информацией.

Как правило, ИС образовательной организации – многоагентные системы (Multi-Agent Systems) с реализацией многопользовательского режима ис-пользования данных, причём с разграничением прав доступа к ним.

Основными информационными подсистемами ИС образовательной организации являются подсистемы поддержки:

– принятия решений управления образовательной организации;

– учебно-образовательного процесса;

– научно-методических исследований и научно-образовательной информации;

– обеспечения повседневной деятельности образовательной организации;

– защиты информационной безопасности (ЗИБ) ИС образовательной организации.

Основной проблемой оптимального управления учебно-образовательным процессом является выбор аналитических методов и численных алгоритмов нахождения оптимального решения.

Подсистема ЗИБ ИС, выполняющая функции регламентации разграничения прав доступа к информации ИС образовательной организации, обусловлена необходимостью надёжной защиты конфиденциальной ин-формации образовательной организации.

Информации образовательной организации разделяется на три группы:

Первая – несекретная (или открытая), которая предназначена для использования как внутри образовательной организации, так и вне нее.

Вторая – для служебного пользования (ДСП), которая предназначена только для использования внутри образовательной организации. Она подразделяется, в свою очередь, на две подкатегории:

– Доступная для всех сотрудников образовательной организации;

– Доступная для определенных категорий сотрудников образовательной организации, но данная информация может быть передана в полном объеме другому сотруднику для исполнения трудовых обязанностей.

Третья – информация ограниченного доступа, которая предназначена для использования только специально уполномоченными сотрудниками образовательной организации и не предназначена для передачи иным сотрудникам в полном объеме или по частям.

Информация второй и третьей категории является конфиденциальной.

В подсистеме ЗИБ ИС образовательной организации должны быть реализованы надежные средства разграничения полномочий и контроля за доступом к документам, особенно к документам, содержащим конфиденциальную информацию. Защищенность конфиденциальной информации – свойство, характеризующее невозможность несанкционированного её использования или изменения.

Для выявления и оценки существующих рисков и угроз информационной безопасности могут использоваться методы экспертных опросов, анкетирование, интервьюирование, brainshtorm, Delfy.

На сегодняшний день не существует единой методики расчета количественного и качественного значения уровня информационной безопасности организации.

Методы обеспечения информационной безопасности реализуются с помощью следующих основных средств: физических, аппаратных, программных, аппаратно-программных, криптографических, организационных, законодательных и морально-этических. Физические средства защиты предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.

Своевременное и уместное применение информационных технологий помогает обеспечивать экономическую, в частности информационную, безопасность.

Для успешного функционирования организации на рынке и повышения ее конкурентоспособности необходимо внедрять современные информационные технологии, интегрированные в информационную, процессную и

технологическую среду управления

Кроме персональных данных, в образовательных организациях циркулирует информация научно-методологического, экономического и управленческого характера, нередко содержащая конфиденциальные сведения. Таким образом, любое современное образовательная организации испытывает потребность в защите информации, циркулирующей в данной организации. Вопрос организации надежной защиты информации в образовательной организации является в достаточной степени актуальным.

Основополагающим моментом появления прецедентов утечки информации на объектах являлось прежде всего нарушение правил обращения с техническими средствами, программно-аппаратными средствами защиты данных, некорректная организация хранения и доступа к информации, несовершенство нормативной базы образовательной организации в рамках инициации защиты информации.

Большинство причин, влияющих на появление предпосылок и возможностей утечки информации в образовательной организации, возникает из-за отсутствия нормативной базы, недостаточной квалификации сотрудников в области защиты информации и в отсутствие средств защиты на объекте. Возникла проблема: как сформировать профессиональные компетенции педагогов для успешной организации не только с целью трансформации образовательного процесса с помощью ИКТ, но и защиты конфиденциальной информации в образовательной организации, поскольку, как было показано выше, до 70 процентов угроз и нарушений принадлежит сотрудникам образовательной организации, в числе которых педагоги составляют свыше 60 процентов. Представляется необходимым также решение администрации образовательной организации о постоянном контроле уровня ИКТ-компетенции педагогических работников с помощью тест-анализа в обеспечение, по меньшей мере, надлежащей защиты конфиденциальной информации в образовательной организации, что несомненно даст положительный результат в части предотвращения её убытков.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Гершунский, Б. С. Компьютеризация в сфере образования: Проблемы и перспективы / Б. С. Гершунский. – М.: Педагогика, 2004. – 135 с.
2. Новые педагогические и информационные технологии в системе образования: учеб. пособие для сотрудников пед. вузов и системы повышения квалификации пед. кадров / Е.С. Полат, М.Ю. Бухаркина, М.В. Моисеева, А.Е. Петров. – М.: Издат. центр «Академия», 2003. – 224 с.
3. Меньшикова, Н.В. Информационные системы организации и управления учебным процессом: курс лекций. // Пол ред. И.А. Сусловой. Екатеринбург: 2008. 74 с. – URL. https://elar.rsvpu.ru/bitstream/ 123456789/ 18345/1/Menshikova_2008.pdf.
4. Гнатуш А. CASE-технологии: что, когда, как? [Электронное издание] // <http://itm.finestreet. ru/> (18.04.208)
5. Каракозов С.Д. Принципы построения информационных систем вобласти управления образованием [Электронный ресурс]// Заседания научно-методического семинара при кафедре НТО ВОИПКРО: [web-сайт] 17.12.2001<http://www.informika.ru/text/magaz/pedagog/pedagog_3/at21 .html>(15.01.2006)
6. Корнещук Н.Г. Теоретико-методологические основы комплексной-оценки качества деятельности образовательной системы // Автореферет дисии на соискание ученой степени доктора педагогических наук. - Магнитогорск: 2007. 55 с.
7. Костенко К.И., Некрасов С.Д. Моделирование информационной системы оценки качества образования. [Электронный ресурс]//<http://www.ecsocman.edu.ru/db/msg/152402.html > (25.02.2006)
8. Суббето А.И. Квалиметрия человека и образования: итоги, проблемы, направления// Материалы X симпозиума «Квалиметрия в образовании:

методология и практика». - М.: Исследовательский центр проблем качества подготовки специалистов, 2002.

9. Защита конфиденциальной информации (сведений конфиденциального характера). – URL. https://rtmtech.ru/articles/zashhita-konfidentsialnoj-informatsii/.
10. Инструментарий оценки информбезопасности образовательной организации. – URL.: http://case.asu.ru/files/form_312-36760. pdf.
11. Ковалев, Д. В. Информационная безопасность: учеб. пос. / Д. В Ковалев, Е. А. Богданова; Южный федеральный университет. — Ростов-н/Д: Изд-во Южного фед. ун-та, 2016. – 74 с.
12. Кикоть, И. Р. Анализ угроз информационной безопасности предприятия, занимающегося научно-исследовательской и производственной деятельностью / И. Р. Кикоть // Молодой исследователь Дона. — 2017. — № 1 (4). — С. 39–45.
13. Кривякин, К. С. Методический подход к оценке рисков информационной безопасности предприятия / К. С. Кривякин, А. Р. Изотова, В. М. Федоров // ЭКОНОМИНФО. — 2018. — № 2. — С. 82–90.
14. Кротенко, Т. Ю. Методические подходы к разработке индикаторов экономической безопасности организации / Т. Ю. Кротенко // Вестник университета. — 2018. — № 11. — С. 18–22.
15. Морозюк, Ю. В. Индикативные составляющие экономической безопасности организации / Ю. В. Морозюк // Вестник Финансовой академии. — 2006. — № 4. — С. 50–60.
16. Ильяшенко С. Н. Составляющие экономической безопасности предприятия, их оценки. – URL. https://docplayer.ru/47237310-Sostavlyayushchie-ekonomicheskoy-bezopasnosti-predpriyatiya-i-podhody-k-ih-ocenke-ilyashenko-s-n.html (дата обращения: 07.06.2019).
17. Дмитриева, М. А. Применение анализа зрелости информационной безопасности в системе оценки зрелости бизнес-процессов предприя-

тия в целом / М. А. Дмитриева // Информационная безопасность регионов. — 2015. — № 3(20). — С. 20–24.

18. Оценка зрелости процессов обеспечения информационной безопасности в российских банках. – URL.: https://www.pwc.ru/en/blogs/ cybersecurity/posts/27ndpost.pdf (дата обращения: 26.12.2021).
19. Юкаева, В. С. Принятие управленческих решений: учебник / В. С. Юкаева, Е. В. Зубарева, В. В. Чувикова. — М.: Издательско-торговая корпорация «Дашков и Ко», 2016. — 324 с.
20. Корчак, В. Ю. Развитие средств информационной безопасности для роста конкурентоустойчивости предприятия / В. Ю. Корчак, Н. С, Ефимова, В. В. Калачанов, Д. А. Давыдов // Компетентность. — 2017. — № 8 (149). — С. 6–12.
21. Зегжда Д.П., Ивашко А.М.. Основы безопасности информационных систем. М., Горячая линия-Телеком, 2005.
22. Государственная тайна и её защита. Серия «Закон и право» М.: Ось-89, 2004 г.
23. Дойникова Е. В. Оценивание защищенности информационных систем и реагирование на инциденты информационной безопасности с учетом текущей ситуации по безопасности // Материалы конф-ии «Информационные технологии в управлении». – 2014. – С. 601-604.
24. Крутин, Ю.В. Эффективность информационных систем и технологий / Ю.В. Крутин.– Екатеринбург, 2020. – 62 с.
25. Лугачев, М.И., Парадоксы и реальность оценки экономической эффективности информационных систем. Исследования по экономике информационных систем: мат-лы науч. практ. конф. «Экономическая эффективность информационных бизнес-систем» / Под науч. ред. М. И. Лугачева, К. Г. Скрипкина. – М.: Экон-й фак-т МГУ имени М.В. Ломоносова, 2015 – 248 с. – URL.: https://www.econ.msu.ru/sys/raw.php?o=26739&p=attachment.

26. Milgrom P., Roberts J. The Economics of Modern Manufacturing: Technology, Strategy and Organization // American Economic Review, June 1990, Vol. 80, No. 3, pp. 511–528.
27. Bresnahan T., Brynjolfsson E., Hitt L. Information Technology, Workplace Organization and the Demand for Skilled Labor // Quarterly Journal of Economics, Vol. 117, No. 1 (Feb., 2002), pp. 339–376.
28. Фостер Р. Обновление производства: атакующие выигрывают. – М.: Про- гресс, 1987. – 292 с.
29. Brynjolfsson E., Renshaw A., van Alstyne M. The Matrix of Change // Sloan Management Review, Vol. 38, No. 2 (Winter 1997), pp. 37–54.
30. Способы оценки информационной безопасности. – URL.: https://www.tadviser.ru/index.php/Статья:Способы_оценки_информационной_безопасности.
31. ГОСТ Р 50922. Защита информации. Основные термины и определения. – М.: ИПК Издательство стандартов, 2004. – 6 с.
32. ГОСТ Р ИСО/МЭК 17799 2005. Информационная технология. Практические правила управления информационной безопасностью. – М: Стандартинформ, 2006. – 55 с.
33. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.
34. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. – М.: Горячая линия-Телеком, 2004. – 280 с.
35. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: учебное пособие. – М.: Гелиос АРВ, 2006. – 528 с.
36. Характеристика методов анализа рисков. – URL.: https://helpiks.org/8-63154.html.
37. Методы экспертных оценок. – URL.: https://habr.com/ru/post/189626/.

38. SWOT-анализ. – URL.: https://cyberpedia.su/5x9faf.html.
39. Метод Делфи (Delfi). – URL.: https://bstudy.net/687860/bzhd/metody_ekspertnyh_otsenok_metod_delfi
40. Методы исследования причинной связи явлений. – URL.: https://info.wikireading.ru/hs9gjWDRXc.
41. Методы выявления причинной связи явлений. – URL.: https://mydocx.ru/4-88757.html.
42. Методы установления причинных связей между явлениями. – URL.: https://ozlib.com/943039/sotsium/metody_ustanovleniya_prichinnyh_svyazey_yavleniyami.
43. Метод сценариев. – URL.: https://zaochnik.com/spravochnik/menedzhment/strategicheskij-menedzhment/metod-stsenariev/.
44. Информационная безопасность и антифишинг по подписке: как это работает. – URL.:https://trends.rbc.ru/trends/industry/cmrm/61b314859a7947a3f6173cde?utm_source=rbc&utm_medium=cpc&utm_campaign=TR-DEC-29-MEGAFON-848724-2S-61b314859a7947a3f6173cde.3.