

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ОРГАНИЗАЦИИ

Большакова Полина Дмитриевна

студент, Казанский (Приволжский) федеральный университет, РФ, г. Казань

Шевко Наиля Рашидовна

научный руководитель, канд. экон. наук, доцент, Казанский (Приволжский) федеральный университет, РФ, г. Казань

Существует множество представлений о том, как должно выглядеть современное предприятие. В основе этих представлений лежит система эффективного обмена информацией, направленная на обеспечение условий оптимального функционирования элементов организации, а также их взаимодействия. Именно поэтому основные функции процесса управления ресурсами компании, выполняемые на различных иерархических уровнях, сводятся к выработке и обоснованию тех или иных управленческих решений, контролю их исполнения на основе имеющейся информации, а также безопасности коммерческих данных.

Документационное обеспечение как вид управления организацией, включает фиксацию, передачу и хранение массивов информации о состоянии организации и управляющих воздействий по изменению ее состояния. Это объясняет применение информационных технологий как одного из способов осуществления функций документационного обеспечения.

Обеспечение безопасности финансово-хозяйственной деятельности предприятия представляет собой сложный многоэтапный информационный процесс, охватывающий получение, анализ, обработку, хранение, использование и наращивание информации. В результате чего не только информационное обеспечение, но и информационная безопасность становятся ответственными за функционирование всех жизненно важных процессов внутри предприятия [4].

Информационная безопасность электронного документооборота организации является одной из **проблем**, с которой столкнулось общество в эпоху развития капитализма и остается актуальной по сей день. Использование множества автоматизированных средств частично упростили процесс безопасности документооборота, но в то же время создали новую угрозу, такую как электронные махинации, утрата и хищение информации в процессе массового использования автоматизированных средств, некачественная оцифровка бумажных носителей.

Информационная безопасность организации воплощает собой состояние информационной среды организации, ответственной за ее формирование, функционирование и развитие.

Таким образом, информационная безопасность представляет собой состояние защищенности информационной среды и сопутствующей поддерживающей инфраструктуры от вредных воздействий.

Как и в современном обществе, в сфера информационной безопасности представлена двумя составляющими:

1. Информационно – технологическая - воплощает в себе искусственно-созданный мир

технологий.

2. Информационно – психологическая - отражает естественный природный мир в том числе и человека

Независимо от сфер, информационная безопасность имеет 3 базовых критерия: конфиденциальность (доступность обозначенному кругу лиц), целостность (точность и полнота изложения) и доступность информации (возможность получения по требованию).

В период информационной эпохи, когда мир каждый день сталкивается с огромными массивами данных, все большее внимание уделяется вопросам хранения, систематизации и конечно же защите информации.

Представляя собой составной элемент системы коммуникаций и взаимодействий, информационная безопасность имеет следующие составляющие:

1. Нормативно - правовая база.
2. Структура и задачи подразделений, ответственных за обеспечение информационной безопасности в организации.
3. Политика информационной безопасности компании или организационно технические методы обеспечения информационной безопасности.
4. Программные технические компоненты и средства, обеспечивающие безопасность информации об организации.

Информационный базис службы документационного обеспечения представляет собой симбиоз следующих видов информации: оперативная информация, нормативно-справочная информация, технико-экономическая информация, классификаторы, унифицированные и специальные системы документации [3]. Из чего следует разделение информационной безопасности документационного информационного обеспечения на две группы

1 группа. Внемашинное информационное обеспечение. Представляет собой совокупность информационных сообщений воспринимаемых человеком непосредственно и включает систему классификации и кодирования информации; системы управленческой документации; систему организации, хранения, внесения изменений в документацию.

2 группа Внутримашинное информационное обеспечение. Представляет собой массивы данных, формирующие информационную базу системы управления человеческими ресурсами на машинных носителях; совокупность программ накопления, ведения и доступа к информации организации.

Стоит отметить, что в настоящее время технологии информационной безопасности активно применяются во всех группах информационного обеспечения и наступательно автоматизируются.

По мере модернизации технологических и управленческих аспектов нашей жизни и производства в частности, все большие массивы информации пригождаются ежедневно. От оперативности изъятия и применения знаний зависит множество факторов. Применение методик по упрощению способов работы с информацией было необходимым следствием, способным качественно повлиять на все отрасли.

Автоматизированная система документационного обеспечения управления (АСДОУ) за счет автоматизации комплекса операций с документами нацелена повысить не только уровень эффективности управленческой деятельности, но и обезопасить информационный обмен внутри компании. К числу задач АСДОУ относят: документирование информации; обеспечение документооборота; контроль исполнения и автоматизация процедур архивного хранения, ограничение распространения и определение уровня доступа.

В рамках информационной безопасности внедрение АСДОУ на предприятии происходит тремя путями: разработка оригинальной АСДОУ, адаптированной под нужды заказчика; установка типовой системы; настройка инструментальных средств автоматизированной защиты.

Однако независимо от способов внедрения, концепция АСДОУ остается неизменной – функциональная полнота и информационная безопасность документооборота.

Придерживаясь принципа информационной совместимости системы документационного обеспечения должна обеспечить максимально широкие функциональные возможности на базе единой системной архитектуры.

Учитывая множественность подходов к организации АСДОУ, на основе международного стандарта ISO, была разработана эталонная модель взаимосвязи и безопасности данных открытых систем (Open System Interconnection – OSI [2]).

В качестве национального нормирующего документа, обозначающего комплекс допустимых мер информационной безопасности документооборота компании, на территории России используется "Стандарт взаимодействия систем автоматизации документационного обеспечения управления".

Современные АСДОУ имеют трехзвенную архитектуру и соответствующий ей протокол информационной безопасности, и включают в себя: сервер базы данных, сервер приложений для работы с базой данных и сервер для работы с пользователями (подключение через сети Internet или LAN).

С позиции практического применения готовых инфо-безопасных систем, по данным исследовательских компаний International Data Corporation и TAdviser по состоянию на 2019 год на российском рынке наибольшим спросом пользуется система OPTIMA-WorkFlow [1] – система предназначена для управления информационным обменом в организациях разного масштаба, как в коммерческих, так и в государственных. К числу крупнейших пользователей программной платформы на территории Российской Федерации причислены компании: ООО «Лукойл-Информ», ПАО «Газпром», АО «Дхл Интернешнл» (DHL International), ПАО «Сбербанк» и др.

Среди менее крупных компаний спросом пользуются системы 1С:Документооборот и DIRECTUM, оснащенная интеграцией в 1С, а также Microsoft SharePoint, IBM Notes (ранее известная как Lotus Notes) и «Дело». Активными пользователями данных платформ, помимо многочисленных индивидуальных предприятий являются такие крупные региональные компании как: ООО «Мяснофф-Дон», ООО «Новая деревня», ООО «Алиби», ООО «Леген-Авто», ООО «Юг-Связь-Информ», ООО «Интенсагро», ООО «Еврокомфорт» и др.

Заняли свою нишу и специализированные АСДОУ. По мере накопления массивов информации все большим спросом стало пользоваться программное обеспечение в области информационной безопасности архивного дела. Одним из первых программных комплексов, представляющих собой АСДОУ, являются «Архивный фонд» и «Фондовый каталог», а также интегрированные программы «Автофонд» и «АвтоАФ». Целевой аудиторией данных систем являются архивы (государственные, ведомственные и др.).

Таким образом, информационная безопасность как часть глобального процесса не могла обойти автоматизационно-документальную сторону деятельности предприятий и организаций. Но как показал перечень существующих проблем, предложенные инструменты не способны в полной мере восполнить урон, нанесенный организационными и техническими системами. В первую очередь необходимо рассмотреть человеческий фактор – как основную угрозу информационной безопасности электронного документооборота компании.

Проанализировав все выше сказанное, были предложены следующие **пути усовершенствования** системы информационной безопасности электронного документооборота:

1. Исключение доступа посторонних лиц к системе электронного документооборота и

печатной технике, путем актуализации должностной инструкции и обозначения маршрута делегирования полномочий.

2. Система «Личного кабинета» в рамках электронного документооборота для каждого допущенного сотрудника, с обозначением уровня доступа и разрешением вывода документа на внешний носитель только после авторизации.
3. Отчетность по пользователям и запрашиваемой документации.
4. Ограничение не санкционированного проникновения в ПК, путем установления сертифицированных средств криптографической защиты информации и физического ограничения доступа к ПК.
5. Надежное хранение сертификатов ключей доступа на отчужденных носителях.

В условиях постоянного развития информационного-коммуникативных технологий, вопрос информационной безопасности не теряет своей актуальности. По мере развития интернет-систем происходит рост числа вероятных угроз.

Соблюдение базовых требований информационной безопасности позволяет любой-компании участнику экономического рынка исключить внештатные экономические ситуации по утрате информации, носящей коммерческую тайну. Конечно, список предложенных рекомендаций не является исчерпывающим и может оказаться не актуален для «промышленных гигантов». Но стоит отметить, что обозначенные пути усовершенствования подходят для организаций всех масштабов: от микро-компаний и до крупнейших холдингов. Единственным отличием будет масштабность реализации и конечно же стоимость затрат на информационную безопасность электронного документооборота.

Список литературы:

1. IDC. Международная организация предоставлению консалтинговых услуг. Официальный сайт. [электронный ресурс]. Режим доступа: <https://www.idc.com/>
2. ISO. Международная организация по стандартизации. Официальный сайт. [электронный ресурс]. Режим доступа: <https://www.iso.org/ru/home.html>.
3. Губарев, А. В. Информационное обеспечение системы менеджмента качества / А.В. Губарев. - М.: Горячая линия - Телеком, 2013. - 132 с.
4. Емельянова, Н. З. Информационные системы в экономике / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, Инфра-М, 2015. - 464 с.