Междисциплинарные науки

УДК 004

Р.Х. Багдасарян

А.С. Матвеева

Е.С. Лосева

Багдасарян Рафаэль Хачикович, кандидат технических наук, доцент кафедры библиотечно-библиографической деятельности и информационных технологий Краснодарского государственного института культуры (Краснодар, ул. им. 40-летия Победы, 33), e-mail: rafael_555@mail.ru

Матвеева Анастасия Сергеевна, кандидат педагогических наук, доцент кафедры документоведения и проектной деятельности Краснодарского государственного института культуры (Краснодар, ул. им. 40-летия Победы, 33), e-mail: kas_dok_04@mail.ru

Лосева Екатерина Сергеевна, студентка 4 курса группы Док/бак-18 информационно-библиотечного факультета Краснодарского государственного института культуры (Краснодар, ул. им. 40-летия Победы, 33), e-mail: katyhka-losewa@mail.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ В ДОКУМЕНТОВЕДЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Рассматривается информационная безопасность и конфиденциальность информации в документоведческой деятельности. Даны понятия – «информационная безопасность», «конфиденциальное делопроизводство в документоведческой деятельности», а также «средства защиты информации».

Ключевые слова: информационная безопасность, конфиденциальность данных, документоведческая деятельность, конфиденциальное делопроизводство, информация, документы.

R.Kh. Bagdasaryan

A.S. Matveeva

E.S. Loseva

Bagdasaryan Rafael Khachikovich, candidate of technical sciences, associate professor of department of library and bibliographic activity and information technologies of the Krasnodar state institute of culture (33, im. 40-letiya Pobedy st., Krasnodar), e-mail: rafael_555@mail.ru

Matveeva Anastasia Sergeevna, candidate of pedagogical sciences, associate professor of the department of document management and project activities of the Krasnodar state institute of culture (33, im. 40-letiya Pobedy st., Krasnodar), e-mail: kas_dok_04@mail.ru

Loseva Ekaterina Sergeevna, 4th course student of Doc/bak-18 information and library faculty group of the Krasnodar state institute of culture (33, im. 40-letiya Pobedy st., Krasnodar), e- mail: katyhka-losewa@mail.ru

INFORMATION SECURITY AND CONFIDENTIALITY OF DATA IN DOCUMENTATION ACTIVITIES

Information security and confidentiality of information in document management are considered. The concepts of "information security", "confidential clerical work in documentation activities", as well as "means of information protection" are given.

Key words: information security, data confidentiality, document management, confidential office work, information, documents.

Информацию как одну из важнейших составляющих каждой компании необходимо защищать.

Информационные технологии не стоят на месте, что, в свою очередь, делает вопрос по обеспечению информационной безопасности наиболее важным в документоведческой деятельности компании.

Информационная безопасность – это защита информации от действий, которые могу нанести ущерб пользователям и владельцам данной информации [1, с. 18].

Главной целью информационной безопасности является защита информации от случайного или умышленного вмешательства, которое может повлечь за собой потерю данных.

Для внедрения систем информационной безопасности организация должна следовать трем принципам (см. Таблица 1).

Таблица 1

1. Конфиденциальность
2. Целостность
3. Доступность

Рассмотрим более подробно каждый принцип.

Конфиденциальность.

Если рассматривать конфиденциальность со стороны документоведческой деятельности, то термин "конфиденциальное делопроизводство" достаточно понятен.

Конфиденциальное делопроизводство в документоведческой деятельности – это обеспечение защиты данных компании (коммерческая тайна и другие немаловажные данные, разглашение которых может негативно отразиться на деятельности компании) [2, с. 72].

Особенности конфиденциального делопроизводства:

1. Установка правил по работе с конфиденциальными данными.

2. Предоставление доступа только уполномоченным пользователям.

3. Установка ответственности за учет и хранение данных и использование документов по установленным правилам.

4. Регламентация создания, изменения, печати и удаления документов.

5. Учет всех документов.

6. Фиксация всех данных в журнале.

7 Проверка сроков исполнения, изучения и обработки.

8. Регистрация местоположения и перемещения документов.

9. Периодический контроль наличия конфиденциальных данных у исполнителей.

10. Строгие требования к условиям хранения информации в соответствии с нормативными документами.

Все эти пункты являются наиболее важными в конфиденциальном делопроизводстве.

Конфиденциальная информация – это информация, ограниченная законодательством страны и уровнем доступа к информационному ресурсу [3,с. 25].

К видам конфиденциальной информации относятся:

1. Персональные данные.

2. Коммерческая тайна.

3. Профессиональная тайна.

4. Служебная тайна.

5. Государственная тайна.

Для защиты конфиденциальной информации требуется:

1. Определить информацию, к которой следует ограничить доступ.

2. Установить порядок документирования информации.

3. Определить порядок доступа к информации.

4. Установить права доступа к документам в информационных системах [4, с. 566].

Целостность.

Целостность информации подразумевает обеспечение внутренней и внешней последовательности информации, а также предотвращает искажение информации, то есть обеспечение неизменности данных при их хранении и передаче.

Доступность.

Доступность предоставляет безопасное и эффективное получение к информации для санкционированных пользователей. При возникновении сбоев в работе системы должна быть возможность ее восстановления без негативных последствий на работу системы.

Безопасность информации обеспечивается главным образом системным и всесторонним подходом к защите, что требует постоянного учета возможных угроз и уязвимостей [5, с. 71].

Введение контроля безопасности способно значительно снизить возможные риски.

Контроль безопасности бывает нескольких видов:

1. Административный.

2. Логический.

3. Физический.

Теперь остановимся на этих видах и рассмотрим каждый более детально.

Административный.

Данный вид контроля базируется на установленных правилах и стандартах. К данному виду относятся нормативные документы и законы, установленные государственными органами.

Логический.

Данный вид основывается на защите и контроле доступа к информационным системам и программным средствам.

Физический.

Физический вид подразумевает контроль рабочих мест и средств вычислительной техники.

Далее остановимся на угрозах информационной безопасности.

Их можно разделить на несколько групп:

1. Угрозы природного характера (чрезвычайные ситуации, независимые от человека: землетрясения, пожары, наводнения и т.д.).

2. Искусственные, подразделяющиеся на:

– неумышленные угрозы, совершенные человеком по неосторожности и неопытности;

– преднамеренные угрозы, связанные со злым умыслом (создание и внедрение вирусов, хакерские атаки и т.д.).

3. Внутренние угрозы в самой системе.

4. Внешние угрозы вне системы.

Угрозы по своему воздействию на системы делятся также на пассивные и активные. Пассивные угрозы не меняют структуру и состав информации в отличие от активных.

Для защиты своего финансового положения и данных компании необходимо применять средства защиты информации, которые способны обезопасить данные от перечисленных угроз.

Средства защиты информации – это набор различных технических и программных средств, направленных на обеспечение защиты информации от возможных атак и уязвимостей.

Средства защиты информации подразделяются на: организационные, технические, программные и аппаратно-программные.

С большим ростом количества хакерских атак, вирусных программ и иных угроз все более популярными и актуальными становятся программные средства защиты информации.

К средствам защиты относятся:

1. Антивирусы.

2. Технологии межсетевого экранирования.

3. Криптографическая защита информации.

4. Прокси-серверы.

В заключение следует отметить, что информация должна быть определенным образом защищена, ведь она очень важна в любой компании и напрямую влияет на ее успешное развитие. Из-за стремительно развивающихся информационных технологий угрозы различного вида усложняются, а количество атак увеличивается. Из этого следует, что компаниям необходимо в обязательном порядке вводить средства защиты, для того чтобы обезопасить свои данные от возможных угроз и уязвимостей.

Список используемой литературы:

1. *Исхаков, Р. И.* О возможности использования теории скрытности для определения источника (канала) утечки конфиденциальной информации / Р. И. Исхаков. – Текст : непосредственный // Вестник Удмуртского университета. Серия «Экономика и право». – 2018. – № 2. – С. 16-21.

2. *Сидельникова, Н. В.* Информационная безопасность / Н. В. Сидельникова. – Текст : непосредственный // Образование. Карьера. Общество. –2020. – № 1. – С. 71-77.

3. *Сомов, Ю. И.* Использование механизма отнесения информации к конфиденциальным сведениям / Ю. И. Сомов. – Текст : непосредственный // Пробелы в российском законодательстве. Юридический журнал. – 2017. – № 1. – С. 24-29.

4. *Сорокина, М. Ю.* Информационная безопасность vs информационные технологии / М. Ю. Сорокина. – Текст : непосредственный // Научные труды Вольного экономического общества России. – 2019. – № 1. – С. 566-569.

5. *Ушаков, Н. О.* Информационная безопасность в системах электронного документооборота / Н. О. Ушаков. – Текст : непосредственный // Техническая эксплуатация водного транспорта: проблемы и пути развития. – 2021. – № 4. – С. 70-76.