

**Шумилина В.Е.**, доцент кафедры «Экономическая безопасность, учет и право»  
ФГБОУ ВО «Донской государственный технический университет»,  
Ростов-на-Дону, Россия; shumilina.vera@list.ru

**Коптева Ю.И.** студент 5 курса кафедры «Экономическая безопасность, учет и право» ФГБОУ ВО «Донской государственный технический университет»,  
Россия, г. Ростов-на-Дону; j-lia48@yandex.ru

**Тевосян С.А.** студент 5 курса кафедры «Экономическая безопасность, учет и право» ФГБОУ ВО «Донской государственный технический университет»,  
Россия, г. Ростов-на-Дону; sati\_tev@mail.ru

## **ОСНОВНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ПУТИ ИХ РЕШЕНИЯ**

**Аннотация.** Авторами раскрыты основные понятия данной темы, доказана актуальность, рассмотрены виды угроз конфиденциальной информации и способы защиты, как правовые, так и организационные, представлен алгоритм создания системы защиты конфиденциальной информации.

**Ключевые слова:** конфиденциальная информация, безопасность, защита информации, информационная безопасность

**Shumilina V. E.**, associate Professor of «Economic safety, accounting and law» of the «Donskoy state technical University», Rostov-on-don, Russia; shumilina.vera@list.ru

**Kopteva Yu.I.** 5th year student of department "Economic security, accounting and law" of the "Donskoy state technical University", Russia, Rostov-on-Don; j-lia48@yandex.ru

**Tevosyan S.A.** 5th year student of department "Economic security, accounting and law" of the "Donskoy state technical University", Russia, Rostov-on-Don; sati\_tev@mail.ru

## **MAJOR PROBLEMS OF CONFIDENTIAL INFORMATION PROTECTION AND THE WAYS OF THEIR SOLUTION**

**Abstract.** The authors disclose the basic concepts of this topic, prove the relevance, consider the types of threats to confidential information and methods of protection, both legal and organizational, presented an algorithm for creating a system for protecting confidential information.

**Keywords:** confidential security, information security, information security

Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Конфиденциальная информация (далее КИ) – это документированная информация, т.е. зафиксированная на материальном носителе и с реквизитами, позволяющими ее идентифицировать, доступ к которой ограничивается в соответствии с законодательством РФ.

На сегодняшний день сформулировано три базовых принципа информационной безопасности, которая должна обеспечивать:

- целостность данных;
- защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных;
- конфиденциальность информации;
- ее доступность для всех авторизованных пользователей.

Вся информация представляет различную ценность для хозяйствующего субъекта и, соответственно, ее разглашение может привести к угрозам экономической безопасности различной степени тяжести. Боязнь лишиться таких активов заставляет компании создавать различные системы защиты, в том числе и организационную, а главное - правовую. В связи с чем информация разделяется на три группы:

- информация для открытого пользования любым потребителем в любой форме;
- информация ограниченного доступа - только для органов, имеющих соответствующие законодательно установленные права (полиция, налоговая инспекция, прокуратура);
- информация только для работников (либо руководителей) организации.

Угрозы КИ - потенциально или реально возможные действия по отношению к информационным ресурсам, приводящих к неправомерному овладению охраняемыми сведениями.

Существуют различные виды угроз конфиденциальной информации: утечка, утрата, хищение, подделка, искажение, копирование, блокирование, заражение, уничтожение.

При создании комплексных систем защиты информации применяются 2 подхода – фрагментарный и комплексный. Комплексный подход – это принцип рассмотрения проекта, при котором анализируется система в целом, а не ее отдельные части. Его задачей является оптимизация всей системы в совокупности, а не улучшение эффективности отдельных частей. Фрагментарный подход – последовательное включение в комплексную систему пакетов защиты от отдельных классов угроз. В него входят антивирусные пакеты и системы шифрования файлов и регистрации действий пользователей[6].

В вопросах построения систем информационной безопасности необходим комплексный, взвешенный, многоуровневый подход, поскольку осечка в одном вопросе способна свести на нет усилия во всех остальных направлениях.

Правовые способы защиты КИ:

- уголовно – правовые;
- гражданско – правовые;
- административно правовые.

Организационные способы защиты КИ:

- создание службы конфиденциального делопроизводства;
- обучение сотрудников мерам в области защиты конфиденциальной информации;
- мониторинг лояльности персонала;
- организация охраны помещений и разграничения доступа в них;
- подбор и проверка персонала, создание отдельного акта либо включение пункта о неразглашении конфиденциальной информации в трудовых договорах сотрудников.

Электронный документооборот должен сопровождаться различными организационно-техническими мерами, позволяющими защитить передаваемые по компьютерным сетям электронные документы, как от несанкционированного прочтения, так и от случайной или преднамеренной модификации. На Рис. 1 представлены элементы защиты электронного документооборота.



Рис.1 - Элементы системы защиты электронного документооборота.

Так же необходима работа с персоналом. Одним из самых важных направлений деятельности является выстраивание правильной работы с трудовым коллективом. Здесь подразумевается организация работы по набору персонала, оптимизация существующих кадровых служб предприятия, дополнительное обучение персонала, его проверка, стимулирование и прочие мероприятия. Необходимо регулярное проведение инструктажей о важности соблюдения правил пользования конфиденциальными данными, а также вероятной ответственности за их разглашение.

На рисунке 2 представлен алгоритм создания защиты конфиденциальной информации. Данный алгоритм необходимо использовать

при создании организации. Если четко следовать данным пунктам, то в ближайшее время не придется сталкиваться с проблемами, связанными с конфиденциальной информацией.

Многосторонняя защита конфиденциальной информации - составляющая экономической безопасности.



Рис. 2 – Алгоритм создания системы защиты конфиденциальной информации

Выполнение перечисленных требований обеспечивает достаточный уровень защищенности КИ. Современная концепция информационной безопасности обуславливает необходимость создания специальных подразделений, которые должны обеспечивать информационную безопасность компании. 21 век – век информации и информационных технологий, следовательно, актуальность данной темы бесспорна.

### Список литературы:

- 1.Федеральный закон N 149-ФЗ от 27.07.2006 (ред. 19.07.2018) "Об информации, информационных технологиях и о защите информации"
- 2.Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»

3. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. - 586 с.

4. Малюк, А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015. - 230 с.

5. Кияев В.И, Граничин О.Н. Безопасность информационных систем: курс/ М.:НОУ "ИНТУИТ",2016.- 83с.

6. Шумилина В. Е., Абдуллаева К. Н., Топор Ю. А. Информационная безопасность как фактор обеспечения экономической информации // Актуальные вопросы обеспечения экономической безопасности в Российской Федерации в условиях цифровой экономики . AUS PUBLISHERS . 2018. С. 1-7. URL: [https://auspublishers.com.au/ru/nauka/conference\\_article/2116/view](https://auspublishers.com.au/ru/nauka/conference_article/2116/view) (дата обращения: 16.10.2018).

#### **References:**

1.Federal Law N 149-FZ of 07.27.2006 (ed. 07.19.2018) “On Information, Information Technologies and on Information Protection”

2. Presidential Decree of 06.03.1997 N 188 (as amended on 07.13.2015) “On Approval of the List of Confidential Information”

3. Buzov, G.A. Protection of restricted access information from leakage through technical channels / G.A. Buzov. - Moscow: GLT, 2016. - 586 p.

4. Malyuk A.A. Protection of information in the information society: Textbook for universities / A.A. Malyuk. - М .: GLT, 2015. - 230 p.

5. Kiyayev V.I., Granichin O.N. Security of information systems: course / М .: NOU "INTUIT", 2016.- 83s.

6. Shumilina V.E., Abdullaeva KN, Topor Yu. A. Information security as a factor in providing economic information // Actual issues of ensuring economic security in the Russian Federation in a digital economy. AUS PUBLISHERS. 2018. p. 1-7. URL: [https://auspublishers.com.au/ru/nauka/conference\\_article/2116/view](https://auspublishers.com.au/ru/nauka/conference_article/2116/view) (appeal date: 10.16.2018).