



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004

## СОВРЕМЕННЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

<sup>1</sup>Иванова Е.Д., <sup>2</sup>Шарыпова Т.Н.

*Ростовский государственный экономический университет, Россия (344002, г. Ростов-на-Дону, Ростовская обл., ул. Большая Садовая, 69); e-mail: <sup>1</sup> ivlenaa01@mail.ru, <sup>2</sup> newstyd1222@yandex.ru*

Развитие общества сегодня характеризует возрастающую роль информационной сферы, которую можно определить как совокупность информации, информационной инфраструктуры, единиц, осуществляющих сбор, формирование, распространение и использование информации, а также систему регулирования получаемых PR. Информационная сфера, выступая системообразующим фактором в жизни общества, оказывает существенное влияние на состояние политической, экономической, оборонной и других составляющих безопасности общества или организации. В статье рассмотрены современные аспекты защиты информации.

Ключевые слова: информационная безопасность, защита информации, аспекты защиты.

## MODERN ASPECTS OF INFORMATION PROTECTION

<sup>1</sup>Ivanova E.D., <sup>2</sup>Sharypova T.N.

*Rostov State University of Economics, Russia (344002, Rostov-on-Don, Bolshaya Sadovaya street, 69), e-mail: <sup>1</sup> ivlenaa01@mail.ru, <sup>2</sup> newstyd1222@yandex.ru*

The development of society today characterizes the growing role of the information sphere, which can be defined as a set of information, information infrastructure, units that collect, form, disseminate and use information, as well as a system for regulating received PR. The information sphere, acting as a backbone factor in the life of society, has a significant impact on the state of the political, economic, defense and other components of the security of a society or organization. The article deals with modern aspects of information security.

Keywords: information security, information protection, protection aspects.

Термин «информационная безопасность» является базовым понятием теории информационной безопасности. Эти понятия взаимосвязаны и взаимозависимы. На сегодняшний день не существует единого научного подхода к толкованию этих терминов. Различия касаются как содержания концепции, так и способов ее реализации. Защита информации определяется следующими функциями [1,2]:

- предотвращение несанкционированного доступа к информации;
- создание условий, ограничивающих распространение информации;
- защита права владельца на владение и распоряжение информацией;
- предотвращение утечки, хищения, утраты, несанкционированного уничтожения, копирования, модификации, искажения, блокирования, разглашения информации, несанкционированных и случайных действий над ней;

- сохранять полноту, достоверность, целостность, достоверность и конфиденциальность информации;
- организационные, программно-технические средства и методы, направленные на выполнение ограничений, установленных для типов, данных или экземпляров в системе обработки данных;
- деятельность обладателя информации или уполномоченных им лиц по:
  - а) обеспечивать свои права на владение, распоряжение и управление защищенной информацией,
  - б) предотвращение утечки и потери информации,
  - в) сохранять конфиденциальность или тайну охраняемой информации в соответствии с правилами, установленными законодательством и иными нормативными правовыми актами [3].

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными обладателем информации.

Целью защиты информации (потенциальным результатом) является предотвращение причинения вреда собственнику, владельцу или пользователю информации. Под эффективностью защиты информации понимается степень соответствия результатов защиты информации поставленной цели. Объектом защиты может быть информация, ее носитель или информационный процесс, для которого необходимо обеспечить защиту в соответствии с целью. Однако в настоящее время нет четкого определения термина «информационная безопасность» [3].

Защита информации осуществляется в соответствии с требованиями Конституции Российской Федерации, законодательства и иных нормативных документов в области защиты информации. Согласно статье 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" под защитой информации понимается принятие правовых, организационных и технических мер, направленных на:

1. обеспечивать защиту информации от неправомерного доступа, уничтожения, изменения, блокирования, копирования, доставки, распространения, а также от иных неправомерных действий в отношении такой информации;
2. сохранение конфиденциальности информации ограниченного доступа;
3. реализация права на доступ к информации [4].

Информация стала одним из важнейших активов бизнеса. Об этом свидетельствуют данные о компаниях, которые используют для ее защиты: по прогнозам Gartner, в 2022 году на информационную безопасность в мире будет потрачено более 124 миллиардов долларов. Большие бюджеты на безопасность оправданы, достаточно вспомнить последствия недавнего заражения вирусом. Тогда была нарушена работа сотен компаний из разных отраслей по всему миру. Вирусы распространяются через фишинговые письма, полученные сотрудниками организаций [6].

Есть семь основных направлений работы по защите корпоративных данных от утечек:

1. Правовые меры (создание режимов, например, коммерческой тайны, патентов, авторских прав и т.д.).

2. Меры, связанные с кадровой работой (подбор, обучение, увольнение, контроль, действие в нестандартных ситуациях, подбор ИТ специалиста и т.д.).
3. Создание конфиденциального делопроизводства (создание, хранение, уничтожение, передача документов и т.д.).
4. Режимные мероприятия (пропускной режим, внос-вынос документов, использование гаджетов на территории, удаленный доступ, охрана, доступ к информации и т.д.).
5. Организационные мероприятия (деление информации на части, дублирование на ключевых точках, использование облачных систем хранения, банковских ячеек, резервное копирование, аудит и т.д.).
6. Мероприятия по инженерно-технической защите (защита помещений, мест хранения информации, сигнализации, видеонаблюдение и т.д.).
7. Мероприятия по применению технических средств защиты информации (DLP – системы, шифрование, правильная настройка оборудования, защищенное программное обеспечение и т.д.) [5].

Современное положение дел в России требует постоянного решения проблем информационной безопасности во всех сферах деятельности. В настоящее время с учетом политических, правовых и социально-экономических реалий проблема защиты информации перерастает в более общую проблему целенаправленного управления информационными ресурсами. При этом необходим системный подход, так как сумма даже высокоэффективных самостоятельных решений важнейших проблем безопасности вовсе не гарантирует эффективной защиты информации в целом, что и обеспечивает комплексность защиты информации.

### Список литературы

1. О Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 – 2020 годы и на перспективу до 2025 года: Распоряжение Правительства РФ от 1 ноября 2013 г. № 2036-р // Собр. законодательства Рос. Федерации. – 2013. – № 46. – Ст. 5954.
2. Селиванов С.А., Шарыпова Т.Н. Анализ угроз информационной безопасности и способы ее защиты. Наукосфера. 2021. №1.
3. Пахомова А.Е., Шарыпова Т.Н. Типы преступлений в информационном пространстве и способы их противодействия. Заметки ученого. 2021. №2.
4. Шарыпова Т.Н., Д.К. Зархатаев. Система защиты персональных данных с точки зрения противодействия угрозам информационной безопасности в Российской Федерации. В сборнике: Юридическая наука в XXI веке: актуальные проблемы и перспективы их решений: круглый стол №2 со всероссийским и международным участием. Сборник научных статей по итогам работы круглого стола №2 со всероссийским и международным участием. УМК «Актуальные знания»; Ассоциация «Союз образовательных учреждений». Шахты, 2022. С. 45-46.
5. Жигулин Г. П. Организационное и правовое обеспечение информационной безопасности / Г. П. Жигулин. – СПб. : СПбНИУИТМО, 2014. – 173 с.

6. Информационная безопасность: учебное пособие в 2 ч. / В. В. Гафнер ; ГОУ ВПО «Урал. гос. пед. ун-т». – Екатеринбург, 2009. – Ч.1.- 26 с.
7. Камышев Э.Н. Информационная безопасность и защита информации: Учебное пособие. - Томск: ТПУ, 2022. - 24 с.

## References

1. On the Strategy for the Development of the Information Technology Industry in the Russian Federation for 2014 - 2020 and for the Perspective until 2025: Decree of the Government of the Russian Federation dated November 1, 2013 No. 2036-r // Collected. legislation Ros. Federation. - 2013. - No. 46. - Art. 5954.
  2. Selivanov S.A., Sharypova T.N. Analysis of threats to information security and are capable of protecting it. Science sphere. 2021. №1.
  3. Pakhomova A.E., Sharypova T.N. Types of crimes in the information space and ways to counter them. Scientist's Notes. 2021.№2.
  4. Sharypova T.N., D.K. Zarkhataev. Personal data protection system in terms of countering information security threats in the Russian Federation. In the collection: Legal Science in the 21st Century: Actual Problems and Prospects for Their Solutions: Round Table No. 2 with All-Russian and International Participation. Collection of scientific articles on the results of the round table No. 2 with all-Russian and international participation. UKK "Actual knowledge"; Association "Union of Educational Institutions". Mines, 2022, pp. 45-46.
  5. Zhigulin G. P. Organizational and legal support of information security / G. P. Zhigulin. - St. Petersburg. : SPbNIUITMO, 2014. - 173 p.
  6. Information security: a textbook in 2 hours / VV Gafner; GOU VPO "Ural. state ped. un-t. - Ekaterinburg, 2009. - Part 1. - 26 p.
  7. Kamyshev E.N. Information Security and Information Protection: Textbook. - Tomsk: TPU, 2022. - 24 p.
-