

**Шумилина В.Е., к.э.н., доцент,** кафедры «Экономическая безопасность, учет и право», Донской государственной технической университет,  
Ростов-на-Дону, Россия,  
[shumilina.vera@list.ru](mailto:shumilina.vera@list.ru)

**Абдуллаева К.Н.** студентка 3 курса кафедры «Экономическая безопасность, учет и право» Донской государственной технической университет, Ростов-на-Дону, Россия;  
[kamila2804@yandex.ru](mailto:kamila2804@yandex.ru)

**Топор Ю.А.** студентка 5 курса кафедры «Экономическая безопасность, учет и право» Донской государственной технической университет, Ростов-на-Дону, Россия; [uliy-topor@yandex.ru](mailto:uliy-topor@yandex.ru)

## **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ФАКТОР ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ**

**Аннотация.** В современном обществе во время развития передовых технологий информация принимает стоимостной характер. Информационная безопасность выступает составляющим элементом экономической безопасности предприятия, его гарантом получения прибыли и сохранения места на рынке. Статья посвящена основным актуальным проблемам в области обеспечения информационной безопасности, ее рискам, а также ключевым направлениям путей совершенствования данной сферы.

**Ключевые слова:** информационная безопасность, экономическая безопасность, защита информации, информация.

**Shumilina V. E., Ph. D., associate Professor,** Department of economic security, accounting and law, don state technical University, Rostov-on-don, Russia;  
[shumilina.vera@list.ru](mailto:shumilina.vera@list.ru)

**Abdullayeva K. N.** 3rd year student of the chair "Economic security, accounting and law" don state technical University, Rostov-on-don, Russia; kamila2804@yandex.ru

**Topor U.A.** 5th year student of the Department "Economic security, accounting and law" don state technical University, Rostov-on - don, Russia; uliy-topor@ yandex.ru

## **INFORMATION SECURITY AS A FACTOR OF ECONOMIC SECURITY**

**Annotation.** In modern society, during the development of advanced technologies, information takes on value. Information security is a constituent element of the economic security of the enterprise, its guarantor of profit and preservation of market place. The article is devoted to the main current problems in the field of information security, its risks, as well as key areas of improvement of this sphere.

**Keywords:** Information security, economic security, information protection, information.

В условиях рыночной экономики одной из главных задач предприятий является обеспечение информационной безопасности. Защита информации способствует более устойчивому положению организации, снижает ее риски и удерживает конкурентоспособное состояние предприятия. В настоящее время информация приобрела стоимостной вес, который четко определяется реальной прибылью, получаемой при ее использовании или размерами ущерба, наносимого владельцу информации. Создание технологий сбора, обработки, передачи информации, а также ее сохранения не только сократили время работы, но и «принесли» за собой ряд проблем.

Проблема поиска путей устойчивого развития в последнее время приобретает все более актуальный характер, как в глобальном общемировом порядке, так и на национальных, региональных и муниципальных уровнях. Все более очевидной становится зависимость общего уровня экономической безопасности предприятия от защиты, в первую очередь, информационных ресурсов. Практика показывает, что любая целенаправленная недружественная

акция, направленная против хозяйствующего субъекта, начинается, прежде всего, со сбора информации. Именно поэтому данная тема является особо актуальной, что послужило причиной ее выбора для исследования в настоящей статье.

Одной из глобальных проблем, касающаяся информационного оборота в мире, является угроза сохранности информации и потеря ее ключевых признаков. К признакам информации относятся [ 1, с.15] :

- 1) Актуальность;
- 2) Полнота;
- 3) Достоверность;
- 4) Непротиворечивость;
- 5) Конфиденциальность.

В современных условиях развитие информационных технологий, в частности технологий развития всемирной паутины, приводит к необходимости защиты информационных ресурсов, передаваемых в рамках распределительной корпоративной сети, использующей сети открытого доступа.

Безопасность информационных технологий является одной из проблем обеспечения экономической безопасности хозяйствующего субъекта. В условиях развития правовой базы, ее использования в области экономики появляется ряд проблем в сфере обеспечения национальной, социальной и корпоративной безопасности в информационной структуре. Для определения направлений путей совершенствования следует более конкретно описать данную проблему, поскольку ее появление обусловлено определенными узконаправленными ситуациями, такими как:

- 1) «Взламывание» внешними злоумышленниками информационных систем организаций для получения конфиденциальных данных об организации и ее сотрудниках;
- 2) Совершение атак через сети «Internet»; Данная ситуация является одной из наиболее часто встречающихся способов нанесения угрозы

информационной безопасности организации, особенно если для хранения данных она использует сети открытого доступа. Через сеть «Internet» проводятся различные мошеннические действия, которые могут нести в себе различные цели. Например, использование специальных сайтов, которые загружают процессор ЭВМ, что способствует замедлению работы компьютера. Еще одним примером является попытка получения информации платежных средств для обеспечения финансовых потерь организации.

3) Манипулирование доступом внутреннего информационного процесса, то есть, внедрение вирусов через «Internet». Например, вирус «Conficker» особо опасен для информационных систем Windows. Он инфицировал 12 млн. компьютеров по всему миру, в том числе государственных и корпоративных, проникал в компьютер через открытую электронную почту и повреждал электронные файлы. Ущерб, нанесенный вредоносной программой, оценивается примерно в 9,18 млрд. долларов.

Таким образом, направление путей совершенствования вышеперечисленных проблем можно подразделить на 4 сектора:

1) Обеспечение конфиденциальности данных и программ. Одним из путей решения проблем в этой области является использование организациями закрытого физического канала доступа. В сеть подобного рода доступ посторонним воспрещен. Это решение способствует сохранению конфиденциальных данных организации, следовательно, избегая подобным образом нанесения ущерба экономической безопасности фирмы.

2) Обеспечение целостности используемых программ. Часто подвергающимися хакерским атакам, является платформа Windows, на которой работает большинство российских организаций. В таких условиях специалисты по информационной безопасности должны уметь противостоять внешним и внутренним угрозам, выявить проблемы в системах защиты программного обеспечения и на основе соответствующей политики вырабатывать эффективные меры по компенсации угроз и уменьшению рисков организации. Стоит учесть, что целесообразно рассматривать данный сектор не только с

точки зрения использования программ, но и их создания. К сожалению, современная технология программирования не позволяет создавать полностью безопасные программы. Для достижения данной цели следует четко соблюдать принципы архитектурного построения программных комплексов и осуществлять контроль над состоянием защищенности программно-аппаратного обеспечения, сетей на всем протяжении жизненного цикла информационных систем.

3) Обеспечение защиты данных. Безопасность информационной системы достигается путем обеспечения конфиденциальности данных, а также целостности системы. Одним из самых эффективных методов защиты данных является маскировка путем криптографического закрытия информации. Криптография - это наука об обеспечении секретности и аутентичности передаваемых сообщений. Преобразование криптографической системы достигается путем специального алгоритма. Его действие достигается специальным информационным ключом.

4) Обеспечение безопасных выполнений транзакций. Данную цель можно достичь при создании единой системы юридических лиц для принятия, отслеживания и учета платежных документов. Целесообразно развивать механизмы арбитража, которые обеспечивают подтверждение характеристик данных, передаваемых между объектами АИТ, третьей стороной (арбитром).

В завершении следует отметить, что принятие управленческих решений организации зависит от информации. Она на сегодняшний день является важнейшим ресурсом. Конфиденциальность информации может быть обеспечена исключительно комплексным подходом. Таким образом, целесообразно выявить основные пути совершенствования информационной безопасности в области экономики:

- 1) Использование организациями закрытого канала информационного доступа;
- 2) Совершенствование работы специалистов информационной безопасности;

- 3) Четкое соблюдение архитектурного построения программ при их создании;
- 4) Использование специальных криптографических ключей;
- 5) Создание единой транзакционной системы для юридических лиц.

### **Список литературы**

1. Борисов М. А., Романов О. А. Основы организационно-правовой защиты информации. (Гриф УМО по дополнительному профессиональному образованию). № 2. Изд.3, перераб. и доп. М.: Книжный дом «ЛЕНАНД», 2014. — 248 с.
2. Понятия экономической и информационной безопасности [Электронный ресурс]//Интуит. Официальный сайт – Режим доступа <https://www.intuit.ru/studies/courses/13845/1242/lecture/27496>.; свободный, дата обращения (15.02.2017)
3. Экономическая и информационная безопасность [Электронный ресурс]//Межвузовский информационный образовательный портал. Официальный сайт – Режим доступа: <http://edu-on.ru/predmet/ekonomicheskaya-i-informacionnaya-bezopasnost-4-2fkbupi/>, свободный, дата обращения (17.02.2017)
4. Информационная безопасность [Электронный ресурс]//Информатика Официальный сайт – Режим доступа <http://allrefs.net/c21/4e0iq/p27/>: свободный, дата обращения (17.02.2018)
5. Информационная безопасность экономических систем [Электронный ресурс]//Студопедия/ Официальный сайт – Режим доступа : <https://studopedia.su>; свободный, дата обращения (17.02.2018)
6. Информационная составляющая экономической безопасности [Электронный ресурс]/Киберленинка/ Официальный сайт – Режим доступа : <https://cyberleninka.ru>; свободный, дата обращения (17.02.2018)

7. Информационная безопасность. [Электронный ресурс]/Википедия/Официальный сайт – Режим доступа: <https://ru.wikipedia.org/wiki/>; свободный, дата обращения (16.02.2018)

#### **References:**

1. Borisov M. A., Romanov O. A. Fundamentals of organizational and legal protection of information. (UMO vulture on additional professional education). No..Ed.3, revised. and add., Moscow: knizhnyi Dom "LENAND", 2014. - 248 p.
2. Concepts of economic and information security [Electronic resource] / / Intuit. Official site-access Mode [https://www.intuit.ru/studies/courses/13845/1242/lecture/27496:](https://www.intuit.ru/studies/courses/13845/1242/lecture/27496/), free, circulation date (15.02.2018).
3. Economic and information security [Electronic resource]//the interuniversity educational information portal. Official website – access Mode: <http://education.ru/predmet/ekonomicheskaya-i-informacionnaya-bezopasnost-4-2fkbupi/>, casual, date of treatment (17.02.2018).
4. Information security [Electronic resource]//Informatika Official website – access Mode <http://allrefs.net/c21/4e0iq/p27/>: casual, date of treatment (17.02.2018).
5. Information security of economic systems [Electronic resource] / / Studopedia / Official site-access Mode : <https://studopedia.su/>; free, circulation date (17.02.2018).
6. Information component of economic security [Electronic resource] / Cyberleninka / Official site - mode of access : <https://cyberleninka.ru/>; free, circulation date (17.02.2018).
7. Information security. [Electronic resource]/Wikipedia/Official website – Mode of access: <https://ru.wikipedia.org/wiki/>; free, date accessed (16.02.2018).