*УДК 331*

# БАЗОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

**Н. А. Герасимова[1)], А. М. Кулик[2)]**

[1)] *доцент, Белгородский государственный научно-исследовательский университет, г. Белгород, Российская Федерация, e-mail: ngerasimova@bsu.edu.ru*
[2)] *доцент, Белгородский государственный научно-исследовательский университет, г. Белгород, Российская Федерация, e-mail: kulik@bsu.edu.ru*

В данной статье приведены базовые аспекты информационной безопасности предприятия. В современных условиях хозяйствования информация является фактором, диаметрально влияющим на процесс эффективного управления, растет роль информационной безопасности предприятия. Охарактеризованы внешние угрозы информационной безопасности, приведены формы защиты, которые могут быть использованы с целью повышения уровня информационной безопасности предприятия.

***Ключевые слова:*** предприятие; экономическая безопасность предприятия; информационная экономическая безопасность предприятия; информация, угрозы информационной безопасности предприятия.

# BASIC ASPECTS OF INFORMATION ENTERPRISE SECURITY

**N. A. Gerasimova[1)], A. M. Kulik[2)]**

[1)] *Associate Professor, Belgorod State Research University, Belgorod, Russian Federation, e-mail: ngerasimova@bsu.edu.ru*
[2)] *Associate Professor, Belgorod State Research University, Belgorod, Russian Federation, e-mail: kulik@bsu.edu.ru*

This article presents the basic aspects of enterprise information security. In modern economic conditions, information is a factor diametrically influencing the process of effective management, the role of information security of the enterprise is growing. External threats to information security are characterized, the forms of protection that can be used to increase the level of information security of the enterprise are given.

***Keywords:*** enterprise; economic security of the enterprise; information economic security of the enterprise; information, threats to information security of the enterprise.

Информационная безопасность компании, общественной организации или промышленного предприятия – это комплекс мер, направленных на предотвращение несанкционированного доступа [1]. В настоящее время информация играет все более важную роль в управлении совре-

менного предприятия. Она стала четвертым производственным фактором, формирующим стоимость доходов и расходов наряду с трудом, капиталом и землей. Отметим, что в условиях жесткой конкуренции компания должна функционировать и гибко реагировать на постоянные изменения окружающей среды. Это свидетельствует о том, что информация является фактором, диаметрально влияющим на процесс эффективного управления. В современных условиях хозяйствования возрастает задача повышения уровня безопасности, в том числе и информационной. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода [3].

Главная задача информации в управлении предприятием есть снижение неопределенности в процессе принятия решения. Организация должна собирать и обрабатывать данные, чтобы, в свою очередь, на их основе она могла делать анализ и принимать правильные решения. Развитие технологий способствует изменениям в скорости и простоте обработки, а также возникновению современных формы передачи информации. Одновременно с началом процесса внедрения информационных технологий возникают новые риски, связанные с техническими средствами передачи и обработки массивов производственной информации. Хранение информации в цифровом виде, на компьютерных носителях, передача их на расстоянии благодаря сети передачи данных способствуют появлению новых, до сих пор не используемых форм незаконного сбора информации, таких как подслушивание, удаленное вмешательство и т. д.

Среди актуальных внешних угроз информационной безопасности можно выделить следующие: кража информации (конфиденциальная, коммерческая тайна и т. д.), вирусные атаки, фишинг, дефейс сайта и т. д. [2].

Но не менее опасны и внутренние угрозы информационной безопасности. Такие угрозы могут исходить от внутреннего окружения предприятия – то есть от самих сотрудников. Это может быть связано так же с кражей информации, передачи ее конкурентам и т. д.

Формы защиты, которые могут быть применены к информационным источникам информации, могут быть следующих видов. Защита физического характера состоит из: контроля прав доступа к помещениям и компьютерным системам, особенно к местам, где хранится самая ценная информация, копии безопасности и т. д.; внедрения систем мониторинга, безопасности; сокращение злоупотреблений путем эффективного надзора; роста реакции на новые угрозы, возникающие в результате преобразований, в том числе и технологических. Необходимо, чтобы физическая защита была эффективной и своевременно выявляла любые опасности, например, связанными с взломом или противодействием всем последст-

виям, связанными с непредвиденным перебоям в подаче электроэнергии и т. д. Диапазон физической защиты он также охватывает вопросы вещания и передачи данных. Большую роль в процессе информационной безопасности играют организационные методы. Организационные методы включают в себя такие мероприятия, как: разработка конкретных процедур, связанных с реализацией программы информационной безопасности, для пользователей компьютерной системы; внедрение политики информационной безопасности на предприятии; политика приобретения необходимых современных компьютерных систем для обеспечения информационной безопасности; мониторинг работников, ответственных за доступ в информационные системы компании; обучение персонала необходимым нормам и правилам, с учетом элементы защиты информации.

Отметим, что ведение политики информационной безопасности предусматривает составление документа, представляющего концепцию информационной безопасности, стратегию, методы и методики, для достижения установленного уровня безопасности. Так же поддержание уровня информационной безопасности в организации связано с постоянным контролем, надзором и наблюдением за методами, которые были использованы, с целью повышения уровня информационной безопасности, и их совершенствованием. Эффективная защита информационной безопасности – одна из составляющих успешно функционирующего предприятия.

**Библиографические ссылки**

1. *Герасимова Н. А., Нежурина Д. О., Герасимов С. В.* Аспекты информационной безопасности бизнеса // Экономическая безопасность социально-экономических систем: вызовы и возможности: сборник трудов III Международной научно-практической конференции, Белгород, 22 апреля 2021 года. Белгород: ООО «Эпицентр», 2021. С. 176–178. EDN QTZYEE.

2. Информационная безопасность предприятий [Электронный ресурс]. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionnaya-bezopasnost-predpriyatij/ (дата обращения 10.03.2023).

3. *Храмогин П. А.* Принципы информационной безопасности // Молодежь и наука: сборник материалов X Юбилейной Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых с международным участием, посвященной 80-летию образования Красноярского края [Электронный ресурс]. Красноярск: Сибирский федеральный ун-т, 2014. URL: http://conf.sfu-kras.ru/sites/mn2014/directions.html (дата обращения 01.04.2023).