

УДК: 338.14

## СОВРЕМЕННЫЕ НАПРАВЛЕНИЯ ПО СОВЕРШЕНСТВОВАНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

**Чан Кайцинь**

*магистрант, Уральский федеральный университет имени первого Президента  
России Б. Н. Ельцина, Институт экономики и управления, Екатеринбург,  
Россия, 786561394@qq.com*

**Научный руководитель: Р. Ю. Луговцов**

*кандидат экономических наук, доцент, Уральский федеральный университет  
имени первого Президента России Б. Н. Ельцина, Институт экономики  
и управления, Екатеринбург, Россия, lugovtsov@list.ru*

На сегодняшний день современный мир характеризуется участвующими киберугрозами и уязвимостью, и, следовательно, важность информационной безопасности в современных предприятиях трудно переоценить: информационная безопасность не просто технологическая проблема, а фундаментальный бизнес-императив. В статье рассматриваются основные современные методы совершенствования информационной безопасности предприятий, поскольку в условиях перехода к цифровой экономике, когда бизнес все больше полагается на цифровые технологии и операции, основанные на данных, постоянное совершенствование информационной безопасности предприятия имеет первостепенное значение.

**Ключевые слова:** информационная безопасность; экономическая безопасность; цифровая экономика

## MODERN DIRECTIONS FOR IMPROVING INFORMATION SECURITY OF THE ENTERPRISE

**Chang Kaiqin**

*master's student, Ural Federal University named after the first President of Russia  
B. N. Yeltsin, Institute of Economics and Management, Yekaterinburg, Russia,  
786561394@qq.com*

**Supervisor: R. Y. Lugovtsov**

*PhD in economics, associate professor, Ural Federal University named after the first  
President of Russia B. N. Yeltsin, Institute of Economics and Management, Yekaterinburg,  
Russia, lugovtsov@list.ru*

In the face of relentless cyber threats and vulnerabilities, the importance of information security cannot be overemphasized: information security is not just a technological issue, but a fundamental business imperative. This article examines key modern methods for improving enterprise information security, because in the transition to a digital economy, where businesses increasingly rely on digital technologies and data-driven operations, continuous improvement of enterprise information security is of paramount importance.

**Keywords:** information security; economic security; digital economy.

Сегодня повышение уровня информационной безопасности – это не просто выбор, а стратегический императив для снижения этих рисков. Во многих отраслях действуют жесткие требования к защите данных и кибербезопасности, которым организации должны следовать, следовательно, необходимо постоянно соблюдать такие требования, поскольку их несоблюдение приводит к серьезным штрафам для самой компании и юридическим обязательствам [1]. Постоянное совершенствование мер информационной безопасности позволяет предприятиям демонстрировать свою приверженность соблюдению нормативных требований, что особенно важно в условиях постоянного развития и ужесточения требований к защите данных и безопасности.

Следует отметить, что важность постоянного совершенствования информационной безопасности предприятия трудно переоценить, так как это не только защита конфиденциальных данных и снижение рисков, но и обеспечение соответствия нормативным требованиям, повышение устойчивости бизнеса и, в конечном счете, сохранение репутации и жизнеспособности организации в условиях все более цифрового и взаимосвязанного мира. Чтобы процветать в цифровую эпоху, предприятия должны рассматривать информационную безопасность как стратегический императив [2]. Далее авторами исследования представляются основные подходы к совершенствованию информационной безопасности предприятия (таблица).

Выделенные нами направления свидетельствуют о возрастающей необходимости комплексного подхода к такой безопасности современного предприятия, сочетающего технические и организационные меры. Авторами подчеркивается, что использование брандмауэров, антивирусного ПО и шифрования данных обеспечивает базовый уровень защиты от внешних и внутренних угроз. Однако технические средства сами по себе недостаточны без надлежащего управления доступом и регулярного мониторинга системы через аудиты и оценки безопасности. Ключевым элементом остается человеческий фактор: обучение и повышение осведомленности персонала значительно уменьшают риск человеческих ошибок, которые часто становятся причиной компрометации системы. Таким образом, эффективная стратегия информационной безопасности должна

быть многослойной и интегрированной, объединяя технологические решения с управлением практиками и человеческим участием для противодействия сложным и динамичным угрозам современного киберпространства.

### **Основные подходы к совершенствованию информационной безопасности предприятия**

Направления	Описание	Используемые программы
Использование брандмауэров для защиты информации	Защита сети предприятия от несанкционированного доступа путем фильтрации трафика	Cisco ASA, pfSense, Check Point Firewall
Установка антивирусного программного обеспечения	Обнаружение и удаление вредоносных программ для защиты систем и данных	Kaspersky, Avast, Norton Antivirus
Шифрование данных	Преобразование информации в защищенный формат для предотвращения несанкционированного доступа	BitLocker, VeraCrypt, OpenSSL
Обучение и повышение осведомленности персонала	Повышение знаний сотрудников в области информационной безопасности и лучших практик	Платформы для обучения, тренинги, семинары
Системы контроля доступа	Ограничение доступа к ресурсам компании только дляполномоченных пользователей	Active Directory, LDAP, RSA SecurID
Регулярные аудиты и оценки безопасности	Анализ текущих мер безопасности и выявление потенциальных уязвимостей	Nessus, Nmap, OpenVAS

Составлено по: [3–5].

### **Библиографические ссылки**

- 1 Босова Е. Д., Селищев В. А. Информационная безопасность: современные реалии // Известия Тульского государственного университета. Технические науки. 2019. № 2. С. 34–39.
- 2 Буквина Е. А. Экономические аспекты информационной безопасности предприятия // Глобальная экономика в XXI веке: роль биотехнологий и цифровых технологий. 2020. С. 192–194.
- 3 Бушуев А. Л., Деревцова И. В., Мальцева Ю. А., Терентьев В. Д. Роль информационной безопасности в условиях цифровой экономики // Baikal Research Journal. 2020. № 2. С. 31–34.
- 4 Вилкова А. В., Литвишиков В. М., Швырев Б. А. Проблемы непрерывного обучения персонала информационной безопасности // Мир науки, культуры и образования. 2019. № 9. С. 101–112.
- 5 Внуков А. А. Основы информационной безопасности: защита информации. М. : Юрайт, 2020. 1 с.