Шумилина В.Е., к.э.н., доцент кафедры «Экономическая безопасность, учет и право» ДГТУ, Ростов-на-Дону, Россия;
Shumilina.vera@list.ru
Тетунашвили Е.В., студент 5 курса кафедры «Экономическая безопасность, учет и право» ДГТУ, Ростов-на-Дону, Россия;
lena.tetunaschvili498@mail.ru

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК СОСТАВЛЯЮЩАЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

**Аннотация.** Статья посвящена изучению информационной безопасности как неотъемлемой части экономической безопасности любого современного предприятия. Описываются угрозы, которые могут привести к разглашению конфиденциальной информации, утечки конфиденциальной информации, несанкционированному доступу к защищаемой информации и т.п. Также приведены средства и способы противодействия представленным угрозам.

**Ключевые слова:**Информация, информационная безопасность, обеспечение информационной безопасности, экономическая безопасность, угрозы, программы, средства, конфиденциальность, разглашение, защита информации.

Shumilina V. E., PhD, associate Professor of the Department of Economic security, accounting and law, DSTU, Rostov-on-don, Russia;
Shumilina.vera@list.ru

Tetunashvili E.V., 5th year student of the Department of Economic security, accounting and law, DSTU, Rostov-on-don, Russia;
lena.tetunaschvili498@mail.ru

# INFORMATION SECURITY AS A COMPONENT OF THE ECONOMIC SECURITY OF THE ENTERPRISE

**Annotation.** The article is devoted to the study of information security as an integral part of the economic security of any modern enterprise. Threats are described that can lead to disclosure of confidential information, leakage of confidential information, unauthorized access to protected information, etc. Means and ways of countering the presented threats are also given.

**Keywords:**Information, information security, information security, economic security, threats, programs, tools, confidentiality, disclosure, protection of information.

В настоящее время информация является неотъемлемой частью жизни общества. Возрастает роль информационной сферы, которая включает в себя совокупность всех видов информации, субъекты, которые осуществляют сбор, формирование, использование и распределение, информационную инфраструктуру и т.д. Нужно отметить, что информация для любого современного предприятия является одним из важнейших ресурсов, сохранение и правильное распоряжение которым имеет ключевое значение для развития бизнеса и снижения уровня разнообразных рисков.

Отдельно стоит заметить, что в настоящий момент число преступлений, совершенных в России с помощью информационных технологий выросло. Например, увеличилось число информационных преступлений в январе на 75,2% по сравнению с аналогичным периодом 2019 года, как сообщается на портале правовой статистики Генпрокуратуры РФ.

За январь 2020 года правоохранительными органами РФ зарегистрировано 28,14 тысячи (+75,2%) преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Из общего числа предварительно расследовано 6,15 тысячи преступлений, что на 51,7% выше уровня 2019 года.

Также в феврале МВД России сообщило, что в структуре ведомства появились подразделения по борьбе с киберпреступлениями. В общем количестве, по информации МВД, в 2019 году было зарегистрировано 294,4 тысячи преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Поэтому для любого предприятия актуальной проблемой становится обеспечение информационной безопасности.

Информационная безопасность предприятия — это совокупность мер технического и организационного характера, которые направлены на защиту и сохранение информации, а также обеспечение ее конфиденциальности, целостности, а также доступности. Структура понятия информационная безопасность приведена на рисунке 1.


Рисунок 1. Структура понятия «Информационная безопасность»

Если же говорить об информационной безопасности с точки зрения экономической безопасности, то это состояние защищенности деятельности

предприятия, ее информационных ресурсов и среды от негативного влияния дестабилизирующих факторов, которое обеспечивает сохранность основных свойств информации и достижение социально-экономических целей создания организации. Если предприятие поддерживает информационную безопасность на должном уровне, то это также гарантирует соответствующий уровень экономической безопасности.[6]

Обеспечение информационной безопасности, помогает защитить информационные ресурсы предприятия от различных угроз. Такие угрозы могут быть как случайными, так и преднамеренными, внутренними и внешними и т.д.

К задачам обеспечения ИБ относят:

1. Прогнозирование, выявление и оценку источников угроз информационной безопасности;
2. Развитие и совершенствование системы обеспечения ИБ;
3. Разработка методов и средств предотвращения, нейтрализации и парирования угроз информационной безопасности, а также дальнейшая ликвидация последствий ее нарушения;
4. Обеспечение надлежащей защищенности разных носителей информации;
5. Разграничение доступа к определенным видам документов.

Для того чтобы предприятие могло правильно определить методы и способы защиты информации, необходимо определить, что именно угрожает безопасности данных. Угрозы информационной безопасности — это возможные события и действия, которые способны привести к утечке или потере данных, несанкционированному доступу к ним и т.п. Это, в свою очередь, приведет к моральному или материальному ущербу. На рисунке 2 представлены типы угроз в значимости от источников происхождения. [1]


Рисунок 2. Угрозы информационной безопасности в зависимости от источников происхождения

Если говорить о каждом из источников более подробно, то к техногенным источникам относятся угрозы, вызванные проблемами с техническим обеспечением, нужно заметить, что их прогнозирование затруднительно. Антропогенные источники вызваны человеческими ошибками, то есть могут быть как случайными, так и преднамеренными. Стихийные источники связаны с возникновением каких-либо непреодолимых обстоятельств. Это, например, различные стихийные бедствия, пожары, землетрясения, прекращение подачи электричества из-за ураганов и т.д. Данные виды угроз имеют низкую вероятность прогнозирования, и их предотвращение по большей части невозможно.

Еще одна группа угроз информационной безопасности — это внешние и внутренние угрозы. Внешние угрозы – это атаки со стороны хакеров, компаний-конкурентов, а внутренние угрозы обычно обусловлены следующим:

- низким уровнем программно-технического обеспечения;
- низкой компьютерной грамотностью пользователей;
- на государственном уровне – плохим развитием технологии передачи данных и ИТ-сектора в целом.

Также нужно заметить, что одними из важнейших угроз ИБ является разглашения конфиденциальной информации, утечка конфиденциальной информации и несанкционированный доступ к защищаемой информации. На

рисунке 3 представлено описание данных видов угроз, способы их реализации.


Рисунок 3. Действия и события, нарушающие информационную безопасность

Для борьбы с выше перечисленными уразами и необходимо правильно обеспечивать информационную безопасность предприятия. В настоящее время доступно множество средств и методов для защиты информации. Выбор определенных, зависит от различных факторов, в том числе от:

1. Размера бизнеса;
2. Сферы деятельности предприятия;
3. Технической оснащенности предприятия;
4. Уровня и опыта персонала в вопросе обслуживания информационной инфраструктуры и т.д.

Существуют следующие средства защиты информации предприятия (рисунок 4)

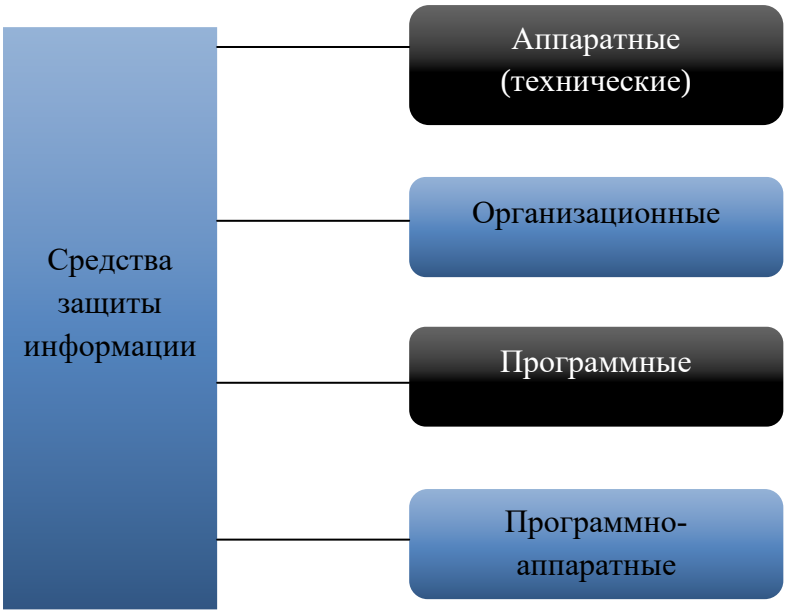


Рисунок 4. Средства защиты информационной безопасности

Если подробнее остановится на каждом, то основными из средств защиты являются организационные. Они сочетают в себе организационно-технических средства, а также организационно-правовые. То есть в данный вид средств будет входить подготовка помещений с компьютерами, прокладка кабельной системы, правила работы, устанавливаемые руководством конкретного предприятия и т.д. [2]

Аппаратные средства. Это различного типа устройства, например, электромеханические, механические, электронные, которые препятствуют свободному доступу к информации. К таким устройствам можно отнести: сетевые фильтры, генераторы шума и т.д.

Программные средства защиты включают следующие программы:

1. Для идентификации пользователей;
2. Для контроля доступа;
3. Для шифрования информации;
4. Для удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты.

Программно-аппаратные, то есть смешанные средства выполняют по сути те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.

На сегодняшний день существует множество программного обеспечения способного защитить информацию предприятия. К основным типам программ относятся:

1. Облачные антивирусы;
2. Антивирусное ПО;
3. Системы криптографии;
4. Межсетевые экраны;
5. Виртуальные частные сети VPN;
6. Решения SIEM;
7. Прокси-сервер и т.д.

Но нужно учесть тот факт, что чаще всего самостоятельно предприятия не в силах реализовать все средства и методы нужные для обеспечения информационной безопасности. Поэтому в большинстве случаев целесообразно прибегать к помощи специализированных компаний и профессионалов в данной области. [7]

Таким образом можно сделать вывод, что в настоящее время существенно возрастает роль информационной безопасности, так как от нее напрямую зависит и экономическая безопасность предприятия в целом. Основными угрозами является разглашения конфиденциальной информации, утечки конфиденциальной информации и несанкционированный доступ к защищаемой информации и т.п. Данные угрозы могут привести к ряду последствий, в том числе к:

1. Потери прибыли предприятия;
2. Потери репутации;
3. Потери интеллектуальной собственности;
4. Появлению скрытых расходов;
5. Интернет-вандализму на сайте предприятия.

Поэтому важно поддерживать информационную безопасность на должном уровне, так как это гарантирует соответствующий уровень экономической безопасности предприятия.

## Список использованных источников


1. Балановская А.В. Анализ угроз информационной безопасности деятельности промышленных предприятий // Вестник Самарск. муниц. инст. упр. №2. 2017 г.
2. Балановская А.В. Управление рисками в реализации политики информационной безопасности промышленного предприятия. Управление экономическими системами: сборник статей IV Международной научно-методической конференции. Пенза: Приволжский Дом знаний, 2016.
3. Волкодавева А.В., Балановская А.В. Организационно-экономические механизмы обеспечения эффективности управления информационной безопасностью промышленных предприятий. Самара, САГМУ, 2016.
4. Шумилина В. Е., Абдуллаева К. Н., Топор Ю. А. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ФАКТОР ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ // Актуальные вопросы обеспечения экономической безопасности в Российской Федерации в условиях цифровой экономики . AUS PUBLISHERS . 2020. С. 1-7. URL: https://auspublishers.com.au/ru/nauka/conference_article/2116/view (дата обращения: 02.12.2020).
5. Мамаева Л.Н., Кондратьева О.А. Основные направления обеспечения информационной безопасности предприятия // Информационная безопасность регионов, 2016.

6. Кожунова Е.А. Обеспечение информационной безопасности на современном предприятии // Школа науки, 2018
7. Шумилина В. Е., Юнкина И. В., Суслов А. А. СОЗДАНИЕ И ФУНКЦИОНИРОВАНИЕ СЛУЖБЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА // Экономическая безопасность, учет и право в Российской Федерации: реалии и перспективы. Том I . AUS PUBLISHERS . 2020. С. 51-55. URL: https://auspublishers.com.au/ru/nauka/conference_article/3409/view (дата обращения: 02.12.2020).
8. Сенаторова А.С., Захарова Е.А. Обеспечение информационной безопасности на предприятии // Современная техника и технологии, 2017

**References**

1. Balanovskaya A.V. Analysis of threats to information security of industrial enterprises // VestnikSamarsk. munitz. inst. ex. № 2. 2017
2. Balanovskaya A.V. Risk management in the implementation of the information security policy of an industrial enterprise. Management of economic systems: collection of articles of the IV International scientific and methodological conference. Penza: Privolzhsky House of Knowledge, 2016.
3. Volkodaveva A.V., Balanovskaya A.V. Organizational and economic mechanisms to ensure the efficiency of information security management of industrial enterprises. Samara, SAGMU, 2016.
4. Shumilina V.E., Abdullaeva KN, Topor Yu. A. INFORMATION SECURITY AS A FACTOR OF ENSURING ECONOMIC SECURITY // Actual issues of ensuring economic security in the Russian Federation in the digital economy. AUS PUBLISHERS. 2020.S. 1-7. URL:

https://auspublishers.com.au/ru/nauka/conference_article/2116/view (date accessed: 02.12.2020).

5. Mamaeva L.N., Kondratieva O.A. The main directions of ensuring the information security of the enterprise // Information security of regions, 2016.

6. Kozhunova E.A. Ensuring information security in a modern enterprise // School of Science, 2018

7. Shumilina V. E., Yunkina I. V., Suslov A. A. CREATION AND FUNCTIONING OF THE SERVICE OF ECONOMIC SECURITY OF THE BUSINESS ENTITY // Economic security, accounting and law in the Russian Federation: realities and prospects. Volume I. AUS PUBLISHERS. 2020.S. 51-55. URL: https://auspublishers.com.au/ru/nauka/conference_article/3409/view (date accessed: 02.12.2020).

8. Senatorova A.S., Zakharova E.A. Ensuring information security at the enterprise // Modern equipment and technologies, 2017