

УДК: 338.2:004

*Хусаинова Э.Э.*

*студентка*

*4 курс, Факультет Экономики*

*ФГБОУ ВО «Ульяновский Государственный Университет»*

*Россия, г. Ульяновск*

*Кузнецова А.С.*

*студентка*

*4 курс, Факультет Экономики*

*ФГБОУ ВО «Ульяновский Государственный Университет»*

*Россия, г. Ульяновск*

## **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ: ТЕНДЕНЦИИ И СТРАТЕГИИ**

***Аннотация:** В работе рассматривается развивающаяся ситуация на российском рынке информационной безопасности. В статье анализируются текущие тенденции, возникающие угрозы и изменения в итоговых экономических показателях организаций-лидеров, поставляющих решения в области информационной безопасности.*

***Ключевые слова:** информационное общество, цифровая экономика, информационная безопасность, ИТ-рынок.*

***Annotation:** The present article examines the developing situation in the Russian Federation information security market. It analyzes current trends, emerging threats and changes in the final economic indicators of leading organizations providing solutions in the field of information security.*

***Keywords:** information society, digital economy, information security, IT-market.*

Цифровые системы присутствуют во всех отраслях общества, а сохранность внутренней информации необходима при обеспечении безопасности субъекта. Следовательно, факт развития ИКТ имеет влияние на информационную безопасность (ИБ), в т. ч. отрицательное, в виде появления новых источников угроз. В экономической сфере ИБ значима в производстве, логистике, перевозке продукции, финансах и многих других направлениях. Изучая экономические аспекты информационной безопасности, предприятия могут оценить потенциальные издержки, связанные с нарушениями кибербезопасности, и инвестировать в соответствующие превентивные меры. Мы живём в информационном обществе, которое, в соответствии с Указом Президента РФ "О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы" является обществом, в котором информация и уровень её применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан[4]. Поэтому вопрос ИБ остро стоит в каждом периоде времени и в каждой сфере.

Так, ИБ в автоматизированных системах имеет решающее значение для защиты данных и информации, обеспечения непрерывности работы, защиты интеллектуальной собственности, снижения финансовых потерь, укрепления доверия клиентов, соблюдения нормативных требований и защиты от киберугроз. Определение приоритетов и мер ИБ необходимо для снижения рисков и обеспечения надежной работы автоматизированных систем [1]. Обеспечение информационной безопасности подразумевает осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления [3].

В настоящее время наблюдается восстановление рынка информационной безопасности после периода пандемии и его рост 2023 году

из-за угроз, которые становятся всё более сложными. По словам руководителя исследовательской группы отдела аналитики ИБ Positive Technologies, на 19 декабря 2023 года наиболее атакуемыми отраслями кибербезопасности были: государственные учреждения (столкнулись с утечкой персональных данных и конфиденциальной государственной информации ввиду сложной политической ситуации), медицинские организации (атаковались с помощью ВПО, столкнулись с утечкой персональных данных и медицинской информации), организации науки и образования (столкнулись с утечкой персональных данных на «Госуслугах», хакерскими атаками), финансовые учреждения (столкнулись с утечкой данных с целью кражи денег и данных клиентов, коммерческой информации; временно останавливались работы систем, обеспечивающих бизнес-процессы, атаковались цепочки поставок), ИТ-компании (атаковались методом социальной инженерии и компрометации учётных записей), организации торговли (столкнулись с утечкой ПД клиентов и учётных данных, например, сайтов компаний «АШАН-Россия», «Буквоед», «Леруа Мерлен», «ТВОЁ», «Твой Дом», «Читай-город», book24.ru и др.).

Лидеров-поставщиков решений в сфере ИБ в России за 2023 год можно посмотреть в таблице 1 [2]. Представленные компании по ОКВЭД занимаются: разработкой компьютерного программного обеспечения; деятельностью, связанной с использованием вычислительной техники и информационных технологий, прочей деятельностью; деятельностью консультативной и работой в области компьютерных технологий.

*Таблица 1.*

**Изменения финансовых показателей поставщиков решений в сфере информационной безопасности в России за 2023 год**

Компания	Выручка за 2023	Чистая прибыль за 2023	Выручка за 2022	Чистая прибыль за 2022	Измене ние	Измене ние чистой

	год в тыс. руб.	год в тыс. руб.	год в тыс. руб.	год в тыс. руб.	выручка и	прибыль и
АО «Лаборатория Касперского»	47 735 577	10 629 248	36 439 120	71 070	31,0%	14856,0%
ПАО "Софтлайн"	33 687 512	98 766	35 663 836	187 482	-5,5%	-47,3%
ООО "ГАЗИНФОРМ СЕРВИС"	35 985 496	12 637 752	15 552 163	4 800 443	131,4%	163,3%
ООО "СОЛАР СЕКЬЮРИТИ"	3 852 066	894 005	2 785 558	- 1 343 570	38,3%	166,5%
АО "ИНФОСИСТЕМЫ ДЖЕТ"	28 188 208	2 068 257	25 638 262	2 301 322	9,9%	-10,1%
АО НИП "ИНФОРМЗАЩИТА"	4 626 546	245 595	4 601 896	243 497	0,5%	0,9%
ООО "ЦИТАДЕЛЬ"	8 736 972	12 954 710	5 208 494	8 097 382	67,7%	60,0%
ООО "УЦСБ"	8 673 974	784 094	5 349 876	484 793	62,1%	61,7%
АО "АЙ-ТЕКО"	18 154 144	842 601	14 056 293	3 277 663	29,2%	-74,3%

Таким образом, среди компаний-лидеров в сфере информационной безопасности в основном наблюдаются изменения в сторону увеличения по выручке и чистой прибыли. Однако у некоторых компаний, например, ПАО «Софтлайн» оба показателя сократились. Чистая прибыль снизилась по

причине высокой базы 2022 года, обусловленной значительными единоразовыми доходами от переоценки справедливой стоимости финансовых инструментов, увеличились процентные расходы. В 2023 году были понесены нетипичные и разовые расходы, связанные с многочисленными сделками M&A, получением компанией публичного статуса, а также с размещением 5 облигационного выпуска ПАО «Софтлайн». Чистая прибыль сократилась и у компаний «Инфосистемы Джет» и «Айтеко».

Стратегия и рекомендация для разработки устойчивых систем ИБ может быть предложена для крупных организаций, у которых в области ИБ действуют: руководители организации, работники службы информационных технологий и специалисты службы информационной безопасности.

Так, обязанностями руководителей в данном вопросе являются: утверждение и поддержка политики ИБ организации; определение и назначение ответственных за ИБ и ИТ; выделение необходимых финансовых, технических и трудовых ресурсов для обеспечения ИБ; проведение регулярного мониторинга и требование отчётности по выполнению мер ИБ; анализ и управление рисками, связанными с ИБ. В зависимости от условий внутренней и внешней среды компании, руководители должны обращать внимание и учитывать такие факторы, как: связь стратегии в сфере ИБ с общей бизнес-стратегией, их интеграция; обеспечение достаточного финансирования для выполнения мер ИБ; оценка и управление рисками (учёт потенциальных потерь); соблюдение всех законов, регламентов и стандартов в области ИБ; формирование корпоративной культуры, поддерживающей и стимулирующей соблюдение правил ИБ.

Работники службы информационных технологий обязаны: администрировать и поддерживать ИТ-инфраструктуру; обеспечивать своевременное обновление операционных систем и прикладного ПО для устранения уязвимостей; управлять правами доступа пользователей к информационным ресурсам; организовывать и контролировать резервное

копирование данных для их восстановления в случае инцидента; проводить обучение сотрудников по вопросам использования IT-ресурсов и соблюдения мер безопасности.

В круг обязанностей специалистов службы ИБ входит: создание и внедрение мер защиты информации (антивирусные программы, межсетевые экраны и системы обнаружения вторжений); проведение мониторинга состояния информационной безопасности, выявление и устранение уязвимостей; разработка планов реагирования на инциденты и обеспечение их выполнения в случае угрозы; обучение сотрудников организации правилам ИБ и повышение их осведомлённости о возможных угрозах; обеспечение соответствия политики и практики организации требованиям законодательства и стандартов в области ИБ.

Для того, чтобы обеспечить информационную безопасность в крупной организации, создаются внутренние документы, такие как: политика ИБ, положения, распоряжения, должностные инструкции, утвержденный список лиц с доступом к информации, имеющей стратегическое значение и др. Помимо данных документов, может возникать потребность в составлении стратегии ИБ для компаний, входящих в наиболее кибератакуемые отрасли. В отличие от политики, стратегия более мобильная - должна меняться в зависимости от текущих обстоятельств и угроз, а также разрабатывается для достижения конкретных целей организации. Стратегию целесообразно разрабатывать крупным организациям, которые по итогам года вошли в перечень атакуемых отраслей, а также тем, кто регулярно входит в него.

#### **Список использованных источников:**

1. Козырь, Н. С. Экономические аспекты информационной безопасности : учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. — Москва : Издательство Юрайт, 2024. — 131 с. — (Высшее

образование). — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 15 — URL: <https://urait.ru/bcode/545066/p.15>.

2. Официальный сайт Государственного информационного ресурса бухгалтерской (финансовой) отчетности Федеральной налоговой службы [Электронный ресурс]. — URL: <https://bo.nalog.ru/>

3. "Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. N 646)" от 05.12.2016 № 646 // Российская газета. – 2016.

4. Указ Президента Российской Федерации "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" от 09.05.2017 № 203 // Официальный интернет-портал правовой информации. - 2016 г. - Ст. 2