УДК 65.016.2
JEL: O12, L25
DOI 10.17238/issn1998-5320.2020.39.226

*А. В. Волкодаева,*
Самарский филиал Московского городского педагогического университета
*А. В. Балановская,*
Самарский государственный экономический университет

# АНАЛИЗ И ТЕНДЕНЦИИ РЫНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ

**Проблема и цель.** Исследование анализа и тенденций рынка информационной безопасности. Цель исследования – выявление факторов, влияющих на развитие российского рынка информационной безопасности.
**Методология.** Исследование проводится на основе эмпирических методов, основанных на изучении разнообразных источников информации. Из теоретических методов применялись анализ, синтез, дедукция и индукция. Исследование было проведено с применением статистических методов.
**Результаты.** В статье исследуется рынок информационной безопасности, который за последнее время демонстрирует положительную динамику своего развития.
**Выводы.** Авторы пришли к выводу, что в условиях открывающихся возможностей по освоению новых рынков сбыта российские компании успешно разрабатывают конкурентные решения в сфере информационной безопасности. Предлагаемые подходы позволяют решить разнообразные проблемы соответствия требованиям изменяющегося нормативного обеспечения информационной безопасности, достижения требуемого уровня защиты информации, коммуникаций, соответствующей инфраструктуры. Именно открывающиеся возможности внешней среды позволяют российским компаниям улучшить экономические результаты своей деятельности.
*Ключевые слова:* информация, информационная безопасность, информационные технологии, рынок, внешняя среда, угрозы, возможности, факторы развития.

**Проблема и цель.** Рынок информационных технологий в России постепенно набирает темпы развития. Рост рынка во многом связан с появлением всё большего количества информационных угроз, положительная динамика которых в том числе определяется вектором цифровизации современного общества. Происходит быстрое устаревание программного оборудования и обеспечения, требующее его своевременной смены. Однако дело не только в этом. Предъявляются новые требования со стороны регуляторов к решению вопросов защиты персональных данных, к системам защиты банковских организаций, защиты критической информационной инфраструктуры и т. д. Системы информационной безопасности стремятся соответствовать современным требованиям нормативных документов.

Также важной тенденцией является импортозамещение [1]. Этот тренд стал объективным отражением сложившейся ситуации. Перед российскими компаниями открываются новые возможности, которые на протяжении последних лет успешно реализуют. Это подтверждается экономическими показателями деятельности российских компаний, динамикой финансовых результатов. Открывающие возможности подталкивают компании к созданию и разработке собственных решений по информационной безопасности. Внедрение собственных подходов к обеспечению информационной безопасности российских компаний связан с такими технологиями-новинками, как облака, big-data, роботизация, мобильные технологии.

Стремление компаний IT-сферы к достижению технологической независимости и снижению расходов выводит их на повышение эффективности финансово-хозяйственной деятельности и рост уровня конкурентоспособности не только на российском, но и на мировом рынке. Рассмотрим темпы роста выручки российских компаний на рынке IT-технологий за последние три года.

Таблица 1

Выручка российских компаний на рынке IT-технологий в 2016 – 2018 гг., млн руб. [2–4]

| Компания | 2016 г. | 2017 г. | 2018 г. | 2017 г. к 2016 г. | 2018 г. к 2017 г. |
|---|---|---|---|---|---|
| АО «Лаборатория Касперского» | 43 083,60 | 40 714,34 | 45 404,04 | 94,50 | 111,52 |
| ООО «Софтлайн» | 57 291,37 | 71 680,89 | 94 820,00 | 125,12 | 132,28 |
| ООО «Информзащита» | 6 867,68 | 8 313,83 | 8 044,59 | 121,06 | 96,76 |
| ОАО «Инфотекст» | 3 704,90 | 3 757,77 | 4 059,04 | 101,43 | 108,02 |

Продолжение таблицы 1

| Компания | 2016 г. | 2017 г. | 2018 г. | 2017 г. к 2016 г. | 2018 г. к 2017 г. |
|---|---|---|---|---|---|
| АО «Инфосистемы Джет» | 19 182,22 | 20 432,33 | 24 895,69 | 106,52 | 121,84 |
| АО «АйСиЭл – КПО ВС» | 9 252,40 | 9 527,10 | 10 847,68 | 102,97 | 113,86 |
| ЗАО «Крок Инкорпорейтед» | 28 504,86 | 22 539,87 | 30 320,32 | 79,07 | 134,52 |
| ООО ПК «Аквариус» | 9 491,35 | 9 880,02 | 8 982,88 | 104,09 | 90,92 |
| ЗАО «Ланит» | 114 514,00 | 137 073,00 | 164 241,33 | 119,70 | 119,82 |
| АО «ДиалогНаука» | 1 366,93 | 1 571,13 | 1 998,41 | 114,94 | 127,20 |
| ЗАО «МВП «Свемел» | 1 343,23 | 1 061,98 | 1 402,60 | 79,06 | 132,07 |
| АО «Актив-софт» | 778,45 | 1 104,40 | 1 371,45 | 141,87 | 124,18 |
| ООО «Ангара Технолоджис Групп» | 539,64 | 988,19 | 1 305,04 | 183,12 | 132,06 |
| ООО «Системный софт» | 2 450,00 | 5 748,03 | 3 626,00 | 234,61 | 63,08 |
| ООО «Талмер» | 534,31 | 2308,07 | 17 906,36 | 431,97 | 775,82 |
| АО «АМТ-Групп» | 6 034,18 | 7 415,67 | 7 518,63 | 122,89 | 101,39 |
| ООО «С-Терра СиЭсПи» | 277,33 | 341,01 | 777,94 | 122,96 | 228,13 |
| ООО «Икс-Ком Интеграция» | 7 055,00 | 8 390,00 | 9 581,40 | 118,92 | 114,20 |
| АО «Калуга Астрал» | 998,66 | 1 355,56 | 1 926,95 | 135,74 | 142,15 |
| ООО «ПКБ «Эшелон» | 890,00 | 1417,00 | 1513,00 | 159,21 | 106,77 |
| Совокупная выручка по представленным компаниям | 313 160,11 | 355620,19 | 44054,35 | 113,19 | 123,88 |

Совокупная выручка по представленным компаниям в сфере IT-технологий в 2018 г. составила 440 054,35 млн руб., что на 23,88 п.п. выше по сравнению с 2017 г. Годовой темп роста к 2017 г. ниже, чем к 2016 г. и составляет 13,19 п. п. В 2018 г. только три компании имеют отрицательную тенденцию роста выручки от основной деятельности. Тенденции анализируемого периода свидетельствуют о преодолении стагнации прошлых периодов и возобновлении роста рынка IT-технологий.

Представленные компании специализируются в сфере информационной безопасности. В таблице 2 представлена выручка российских компаний на рынке информационной безопасности в 2016–2018 гг.

Таблица 2

Выручка российских компаний на рынке информационной безопасности в 2016–2018 гг., млн руб. [5]

| Компания | 2016 г. | 2017 г. | 2018 г. | 2017 г. к 2016 г. | 2018 г. к 2017 г. |
|---|---|---|---|---|---|
| АО «Лаборатория Касперского» | 43 083,60 | 40 714,34 | 45 404,04 | 94,50 | 111,52 |
| ООО «Софтлайн» | – | 14 700 | 15800 | – | 107,48 |
| ООО «Информзащита» | 6 867,68 | 8 313,83 | 8 044,59 | 121,06 | 96,76 |
| ОАО «Инфотекст» | 3 704,90 | 3 757,77 | 4 059,04 | 101,43 | 108,02 |
| АО «Инфосистемы Джет» | 3100 | 3 900 | 4 400 | 125,81 | 112,82 |
| АО «АйСиЭл – КПО ВС» | 2765,5 | 3 008 | 4 193 | 108,77 | 139,39 |
| ЗАО «Крок Инкорпорейтед» | 2239,4 | 2 464 | 3 553 | 110,03 | 144,20 |
| ООО ПК «Аквариус» | 2235,6 | 2 236 | 2 504 | 100,02 | 111,99 |
| ЗАО «Ланит» | 1863,3 | 2 235 | 2 481 | 119,95 | 111,01 |
| АО «ДиалогНаука» | 1 366,93 | 1 571,13 | 1 998,41 | 114,94 | 127,20 |
| ЗАО «МВП «Свемел» | 1 343,23 | 1 061,98 | 1 402,60 | 79,06 | 132,07 |
| АО «Актив-софт» | 778,45 | 1 104,40 | 1 371,45 | 141,87 | 124,18 |
| ООО «Ангара Технолоджис Групп» | 539,64 | 988,19 | 1 305,04 | 183,12 | 132,06 |
| ООО «Системный софт» | 453 | 563 | 1 104 | 124,28 | 196,09 |
| ООО «Талмер» | – | 198 | 853 | – | 430,81 |
| ООО «АМТ-Групп» | – | 899 | 838 | – | 93,21 |
| ООО «С-Терра СиЭсПи» | 277,33 | 341,01 | 777,94 | 122,96 | 228,13 |
| ООО «Икс-Ком Интеграция» | 647 | 721 | 788 | 111,44 | 109,29 |
| АО «Калуга Астрал» | – | 605 | 718 | – | 118,68 |

| | | | | | |
|---|---|---|---|---|---|
| ООО «ПКБ «Эшелон» | 779,3 | 665 | 639 | 85,33 | 96,09 |

По результатам анализа выручки российских компаний на рынке систем информационной безопасности в 2016–2018 годах преимущественно наблюдается рост. Минимальный темп роста выручки составил 7 п. п., максимальный темп показал рост более чем в 4 раза. Только у одной компании наблюдается снижение показателя.

Для анализа интерес представляет структура выручки (рис. 1).

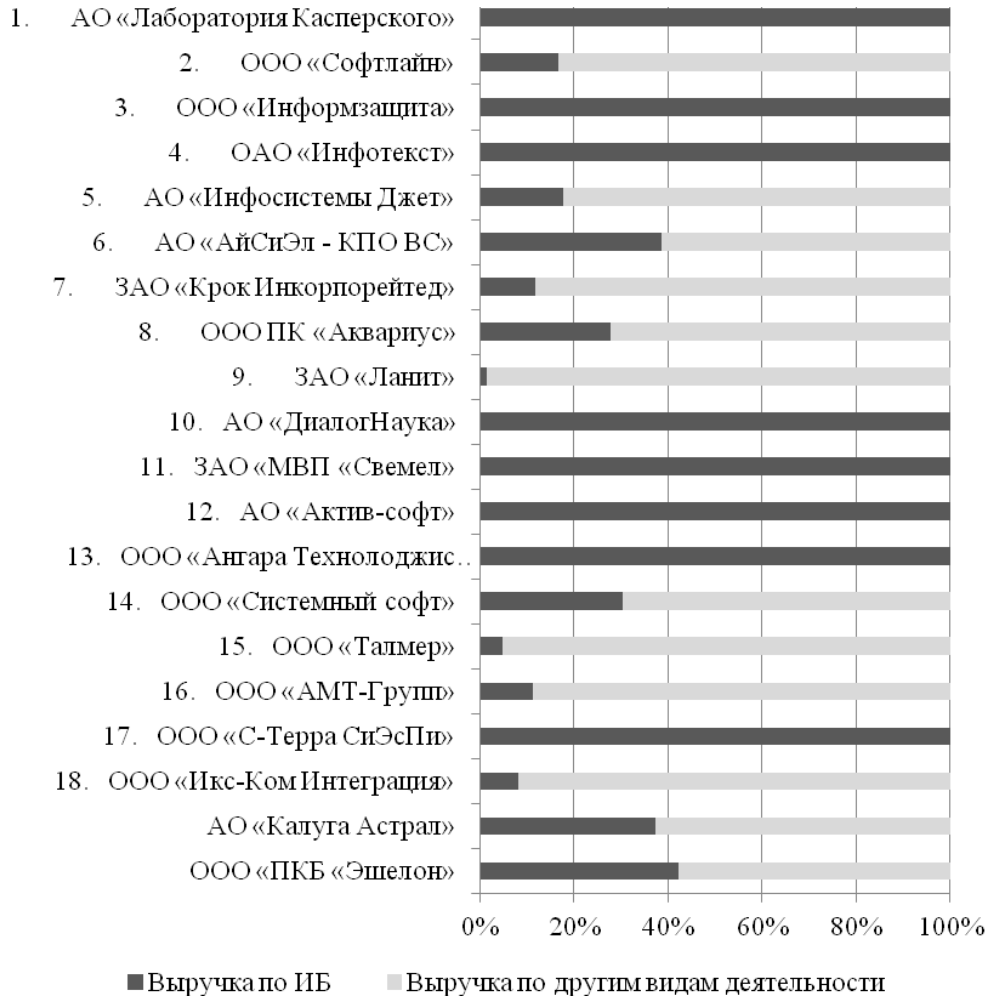


Рис. 1. Объём выручки российских компаний по обеспечению информационной безопасности в структуре выручки по IT-технологиям в 2018 г.

**Результаты.** Рассматривая структуру выручки анализируемых российских компаний в 2018 г., следует отметить, что часть компаний специализируется исключительно на информационной безопасности (40 %), демонстрируя прирост финансовых показателей. Другая часть компании предпочитает кроме продуктов для обеспечения информационной безопасности включать в свой портфель другие разработки (60 %).

Однако необходимо провести анализ темпов роста рынка информационной безопасности. По данным экспертных оценок рынок информационной безопасности в России будет расти в связи с ужесточением требований к безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий [6], а также ввиду реализации политики импортозамещения и вытеснения с российского рынка зарубежных производителей программных и аппаратных средств защиты.

Рынок информационной безопасности в России вырастет по итогам 2019 г. минимум на 10 %, прогнозируют в TAdviser, рис. 2. Рост рынка аналитики связывают прежде всего с новыми требованиями регуляторов, в том числе в части защиты критической информационной инфраструктуры и данных банков, а также с ужесточением требований к средствам защиты информации [7].

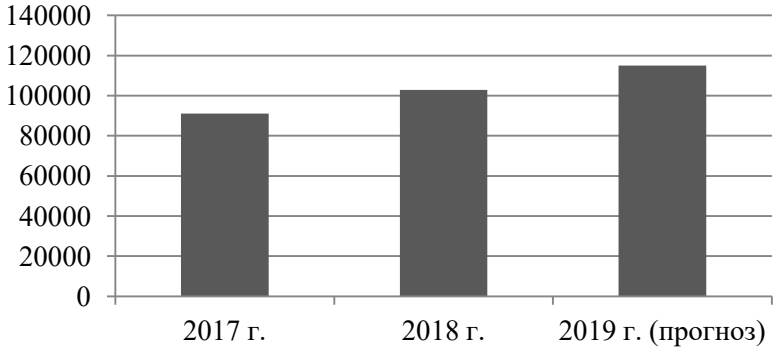


Рис. 2. Прогноз роста рынка информационной безопасности в России, млрд руб.

Согласно Федеральному закону «О безопасности критической информационной инфраструктуры Российской Федерации» субъекты критической информационной инфраструктуры должны обеспечить безопасность значимого объекта критической информационной инфраструктуры на основе создания систем безопасности таких объектов и обеспечения их функционирования. В частности:

1) обеспечить предотвращение неправомерного доступа к информации, её уничтожения, модифицирования, блокирования, копирования, предоставления и распространения;

2) не допустить воздействие на технические средства обработки информации;

3) при необходимости восстановить функционирование объекта;

4) взаимодействовать с органами государственной власти по вопросам обнаружения, предупреждения и ликвидации последствий воздействия на информационную систему и ресурсы значимых объектов критической информационной инфраструктуры [8].

К августу 2018 г. внесены изменения в требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, согласно которым определение угроз безопасности информации осуществляется на каждом из уровней автоматизированной системы управления и должно включать:

1) выявление источников угроз безопасности информации;

2) оценку вероятности воздействия внешних и внутренних нарушителей;

3) анализ потенциальных уязвимостей автоматизированной системы, а также её программных продуктов и программно-аппаратных средств;

4) определение возможных сценариев реализации угроз безопасности информации;

5) оценку последствий от реализации угроз безопасности информации, в частности нарушения отдельных её свойств и автоматизированной системы управления в целом [9].

Согласно сообщению ФСТЭК России от 29 марта 2019 г. N 240/24/1525, требования к уровням доверия устанавливают требования к разработке и производству средств защиты информации, к проведению испытаний средств защиты информации, а также к поддержке безопасности средств защиты информации в ходе их применения (таблица 3).

Таблица 3

Соотношение требований уровней доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий в соответствии с категорией значимых объектов критической информационной инфраструктуры и классом защищённости

| Уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий | Категории значимых объектов критической информационной инфраструктуры | Класс защищённости | | |
|---|---|---|---|---|
| | | в государственных информационных системах | в автоматизированных системах управления производственными и технологическими процессами | в информационных системах персональных данных при необходимости обеспечения |
| Первый | Применяются в информационных (автоматизированных) системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну | | | |
| Второй | | | | |
| Третий | | | | |
| Четвертый | 1 | 1 | 1 | 1 |
| Пятый | 2 | 2 | 2 | 2 |
| Шестой | 3 | 3 | 3 | 3, 4 |

Требования к уровню доверия подлежат применению при сертификации средств защиты информации, кроме:

1. Средств защиты информации на соответствие требованиям руководящего документа «Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».
2. Требований к системам обнаружения вторжений.
3. Требований к средствам антивирусной защиты.
4. Требований к средствам доверенной загрузки.
5. Требований к средствам контроля съёмных машинных носителей информации.
6. Требований к межсетевым экранам.
7. Требований безопасности информации к операционным системам [6].

**Выводы.** Таким образом, в связи с внесением изменений в требования безопасности информации, они будут способствовать вытеснению с российского рынка зарубежных производителей, монополизации рынка российских программных и аппаратных средств защиты, и тем самым это обеспечит рост рынка информационной безопасности в России. Тем более эксперты отмечают зрелость готовых решений по продуктам российского производства, позволяющую принять обоснованное управленческое решение на основе требуемого функционального назначения [10].

Пользователи всё чаще прибегают к отечественным аналогам, особенно это касается принятий решений в сфере реализации новых проектов с учётом возможных санкционных и политических рисков.

Меняется государственная политика в области системных инвестиций в производство качественных решений по средствам обеспечения информационной безопасности. Сегодня имеются все шансы разработки конкурентоспособных продуктов, ориентированных не только под соответствие формальным требованиям законодательства, но и отвечающих современным требованиям данного рынка. Новые технологии, продукты и сервисы активно претендуют на финансирование, которое ранее выделялось на более традиционные решения по безопасности, создавая дополнительное давление на устоявшихся игроков [11]. Если ранее чемпионом в вопросах финансирования инвестиционной безопасности был однозначно финансовый сектор, то в последние годы наблюдается неуклонный рост интереса и, что самое важное, финансирования проектов по информационной безопасности в других отраслях. Дополнительный фактор роста рынка информационной безопасности в России – федеральные целевые программы с инициативами в области безопасности информации, направленные на развитие цифровой экономики.

Анализируемый рынок находится в активном развитии, что подтверждается конкурентной борьбой даже в устоявшихся сегментах как за новых клиентов, так и за клиентов, которые принимают решение о смене поставщика продукта и услуг. Развивается и конкуренция между сегментами внутри рынка. Все вышеобозначенные тенденции приводят к существенному росту эффективности деятельности основных игроков рынка.

## Библиографический список

1. Ashmarina S. I., Mantulenko V. V., Troshina, E. P. Readiness to changes as one entrepreneurial value of the innovation-oriented economy. In: Ashmarina S., Vochozka M. (eds) Sustainable Growth and Development of Economic Systems. Contributions to Economics, pp. 157–166. Springer, Cham. DOI: 10.1007/978-3-030-11754-2_12 (дата обращения 18.11.2019).

2. Рынок ИТ: итоги 2018 [Электронный ресурс] // Интернет-издание о высоких технологиях – CNews. URL: https://www.cnews.ru/reviews/rynok_it_itogi_2018 (дата обращения 21.11.2019).

3. Рынок ИТ: итоги 2017 [Электронный ресурс] // Интернет-издание о высоких технологиях – CNews. URL: https://www.cnews.ru/reviews/rynok_it_itogi_2017 (дата обращения 11.11.2019).

4. Рынок ИТ: итоги 2016 [Электронный ресурс] // Интернет-издание о высоких технологиях – CNews. URL: https://www.cnews.ru/reviews/rynok_it_itogi_2016 (дата обращения 18.11.2019).

5. Информационная безопасность (рынок России) [Электронный ресурс] // TAdviser – портал выбора технологий и поставщиков. URL: http://www.tadviser.ru/index.php (дата обращения 18.11.2019).

6. Информационное сообщение о требованиях по безопасности информации, устанавливающих уровень доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий от 29 марта 2019 г. N 240/24/1525 [Электронный ресурс] // Федеральная служба по техническому и экспортному контролю. URL: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1812-informatsionnoe-soobshchenie-fstek-rossii-ot-29-marta-2019-g-n-240-24-1525 (дата обращения 21.11.2019).

7. Кибербезопасности отрегулировали выручку. Доходы ИБ-компаний продолжат расти по закону [Электронный ресурс] // Коммерсантъ. 2019. № 126 от 19.07.2019. URL: https://www.kommersant.ru/doc/4034402 (дата обращения 21.11.2019).

8. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. N 187-ФЗ [Электронный ресурс] // URL: http://www.consultant.ru (дата обращения 21.11.2019).

9. Приказ ФСТЭК России от 09.08.2018 N 138 О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утверждённые приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. N 31, и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённые приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. N 239 (Зарегистрировано в Минюсте России 05.09.2018 N 52071) [Электронный ресурс] // URL: http://www.consultant.ru (дата обращения 21.11.2019).

10. Ашмарина С. И., Пудовкина О. Е. Перспективы информационного развития маркетинговой деятельности на отраслевом рынке. // Вестник университета. 2018. № 3. С. 47–52. [Электронный ресурс] // URL: https: //elibrary.ru/item.asp?id=32867480 (дата обращения 21.11.2019).

11. Обзор TAdviser: Безопасность информационных систем 2019 [Электронный ресурс] // TAdviser – портал выбора технологий и поставщиков. URL: http://www.tadviser.ru/index.php (дата обращения 21.11.2019).

*A. V. Volkodayeva,*
Candidate of Science in Economics, Associate Professor,
Samara branch State Autonomous Educational Institution
of Higher Education of Moscow “Moscow City University”,
76 Stara Zagora st., Samara, 443081, Russian Federation
ORCID ID: https://orcid.org/0000-0002-8044-3789
e-mail: arina-21@mail.ru
*A. V. Balanovskaya,*
Candidate of Science in Economics, Associate Professor,
Samara State University of Economics,
141 Sovetskoi Armii st., Samara, 443090, Russian Federation
ORCID ID: https://orcid.org/0000-0002-8399-9598
e-mail: balanovskay@mail.ru

## ANALYSIS AND TRENDS OF THE MARKET OF INFORMATION SECURITY IN RUSSIA

**Introduction.** The article researches the analysis and trends of the market of information security. The research objective is to identify the factors influencing the development of the Russian market of information security.

**Materials and Methods.** The research is based on the empirical methods of studying various sources of information. Such theoretical methods as analysis, synthesis, deduction and induction were applied. The research was conducted with the application of statistical methods.

**Results.** The article investigates the market of information security, which shows positive dynamics of the development.

**Conclusions.** The authors conclude that in the conditions of the opening opportunities for development of new sales markets, the Russian companies successfully develop competitive decisions in the sphere of information security. The offered approaches enable to solve various problems of compliance to requirements of the changing standard ensuring information security, the achievement of the required level of information security, communications, the corresponding infrastructure. Opening possibilities of the external environment allow the Russian companies to improve economic results of the activity.

*Keywords:* Information, information security, information technologies, market, external environment, threats, opportunities, development factors.

**References**

1. Ashmarina, S. I., Mantulenko, V. V., Troshina, E. P. Readiness to changes as one entrepreneurial value of the innovation-oriented economy. In: Ashmarina S., Vochozka M. (eds) Sustainable Growth and Development of Economic Systems. Contributions to Economics, pp.157-166. Springer, Cham. DOI: 10.1007/978-3-030-11754-2_12 (accessed 18.11.2019).

2. IT market: results of 2018. Online edition about high technologies CNews. Available at: https://www.cnews.ru/reviews/rynok_it_itogi_2018 (accessed 21.11/2019). (In Russian).

3. IT market: results of 2017. Online edition about high technologies – CNews. Available at: https://www.cnews.ru/reviews/rynok_it_itogi_2017 (accessed 11.11.2019). (In Russian).

4. IT market: results of 2016. Online edition about high technologies – CNews. Available at: https://www.cnews.ru/reviews/rynok_it_itogi_2016(accessed 18.11.2019). (In Russian).

5. Information security (the market of Russia). TAdviser as the portal of the choice of technologies and suppliers. Available at: http://www.tadviser.ru/index.php (accessed 18.11.2019). (In Russian).

6. The information message about the requirements for safety of information establishing the level of credibility to the means of technical information security and the means of ensuring of safety of information technologies of 29.03.2019, no 240/24/1525. The Federal Service for Technical and Export Control. Available at: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1812-informatsionnoe-soobshchenie-fstek-rossii-ot-29-marta-2019-g-n-240-24-1525 (accessed 21.11.2019). (In Russian).

7. Cyber security adjusted revenue. Revenues of the IB-companies will continue to grow under the law. Kommersant Publ.. 2019. No. 126 of 19.07.2019. Available at: https://www.kommersant. ru/doc/4034402 (accessed 21.11/2019). (In Russian).

8. Federal Law On Safety of Critical Information Infrastructures of the Russian Federation of 26.07.2017. No. 187-FZ. Available at: http://www.consultant.ru (accessed 21.11/2019). (In Russian).

9. The Order of FSTEC of Russia of 09.08.2018, no 138 "On modification of the Requirements to ensuring information security in automated control systems for production and technological processes on crucial objects, potentially dangerous objects and also the objects posing the increased hazard to life and human health and for the surrounding environment approved by the order of the Federal Service for Technical and Export Control of 14.03.2014, no. 31 and of the Requirements for safety of significant objects of critical information infrastructure of the Russian Federation approved by the order of the Federal Service for Technical and Export Control of 25.12.2017, no. 239" (It is registered in the Ministry of Justice of the Russian Federation 05.09.2018, No. 52071). Available at: http://www.consultant.ru (accessed 21.11.2019). (In Russian).

10. Ashmarina S. I., Pudovkina O. E. The prospects of information development of marketing activity in the branch market. Bulletin of the University. 2018. No. 3. 47-52 pp. Available at: https://elibrary.ru/item.asp?id=32867480 (accessed 21.11/2019). (In Russian).

11. Review of TAdviser: Safety of information systems 2019. TAdviser as the portal of the choice of technologies and suppliers. Available at: http://www.tadviser.ru/index.php (access-ed 21.11/2019). (In Russian).

Поступила в редакцию 20.11.2019 © А. В. Волкодаева, А. В. Балановская, 2019

*Авторы статьи:*

**Арина Валерьевна Волкодаева,** кандидат экономических наук, доцент, зав. кафедрой экономики, управления и социологии, Самарский филиал Московского городского педагогического университета, 443081, Самара, ул. Стара Загора, 76, e-mail: arina-21@mail.ru

**Анна Вячеславовна Балановская,** кандидат экономических наук, доцент кафедры менеджмента, Самарский государственный экономический университет, 443090, Самара, ул. Советской Армии, 141, e-mail: balanovskay@mail.ru

*Рецензенты:*

И. А. Григорьянц, кандидат экономических наук, руководитель отдела НИР, Поволжский казачий институт управления и пищевых технологий (филиал) Московского государственного университета технологий и управления им. К. Г. Разумовского (Первый казачий университет).

Т. Л. Сыщикова, кандидат экономических наук, доцент, Самарский университет государственного управления, Международный институт рынка.