УДК 336.018 JEL E42 DOI 10.26425/2309-3633-2020-1-134-140
Получено: 13.02.2020 Одобрено: 16.03.2020 Опубликовано: 25.03.2020

# Цифровизация бизнеса увеличивает затраты на информационную безопасность

**Махалина Оксана Михайловна**
д-р экон. наук, ФГБОУ ВО «Государственный университет управления»,
г. Москва, Российская Федерация, ORCID: 0000-0002-1234-8499, e-mail: moxanam@mail.ru

**Махалин Виктор Николаевич**
канд. экон. наук, ФГБОУ ВО «Государственный университет управления»,
г. Москва, Российская Федерация, ORCID: 0000-0001-5294-5856, e-mail: mahalinviktor@mail.ru

**Аннотация**

Раскрыты причины роста затрат на обеспечение информационной безопасности в связи с повышением уровня развития цифровой экономики. Одной из главных причин является постоянно возрастающий объем информации, которую необходимо хранить и анализировать. По прогнозам IDC, по сравнению с 2017 г. к 2025 г. объем данных во всем мире возрастет в 10 раз. Приведены средние расходы на восстановление деятельности компаний, связанные с киберпреступлениями. Расходы на информационную безопасность формируются под воздействием многих факторов, важнейшие из которых – киберугрозы. Их содержание рассмотрено на примере промышленных предприятий.

В мире постоянно растет количество киберугроз, увеличивается их сложность и разнообразие в зависимости от объекта нападения, целей и задач. В статье рассмотрены наиболее распространенные в мире типы кибератак, описан механизм их осуществления, их источник и масштаб ущерба, который они причиняют.

В связи с переходом к цифровой экономике постоянно растет число киберугроз. В 2018 г. в России было выявлено 4,3 млрд компьютерных воздействий на критическую инфраструктуру (в 2017 г. – 2,4 млрд). Из них свыше 17 тыс. – наиболее опасные компьютерные атаки. Для этих целей использовались бот-сети из 30 тыс. компьютеров в 86 странах мира. Средние затраты компаний среднего бизнеса на ликвидацию последствий лишь одного киберинцидента по России, составляют около 1,6 млн руб., а для крупного бизнеса – 16,1 млн руб.

В статье обоснованы рекомендации компаниям считать затраты на информационную безопасность стратегическими инвестициями, обеспечивающими непрерывность их бизнес-процессов, которые создают преимущества в эпоху стремительно развивающихся киберугроз. Для целей выбора и анализа источников затрат компаний на обеспечение информационной безопасности, предложено их классифицировать на 9 категорий. Результаты анализа позволят компаниям определять основные направления первоочередного финансирования мероприятий по снижению уровня потерь от инцидентов и обоснованно формировать бюджеты информационной безопасности.

**Ключевые слова:** информационная безопасность, кибербезопасность, киберинциденты, ущерб компаний, утечка данных, затраты, выбор и анализ.

**Цитирование:** Махалина О.М., Махалин В.Н. Цифровизация бизнеса увеличивает затраты на информационную безопасность//Управление. 2020. № 1. С. 134–140.



JEL E42 DOI 10.26425/2309-3633-2020-1-134-140
Received: 13.02.2020 Approved: 16.03.2020 Published: 25.03.2020

# Digitalization of business increases the costs of information security

**Makhalina Oksana**
Doctor of Economic Sciences, State University of Management, Moscow, Russia,
ORCID: 0000-0002-1234-8499, e-mail: moxanam@mail.ru

**Makhalin Victor**
Candidate of Economic Sciences,State University of Management, Moscow, Russia,
ORCID: 0000-0001-5294-5856, e-mail: mahalinviktor@mail.ru

## Abstract

The reasons for the increase in the cost of ensuring information security, in connection with the increase in the level of development of the digital economy have been revealed. One of the main reasons is the ever-increasing amount of information that needs to be stored and analysed. According to IDC forecasts, by 2025 the volume of data worldwide will increase by 10 times compared to 2017. The average costs of restoring companies ' activities related to cybercrimes have been given. The costs of information security are formed under the influence of many factors, the most important of which are cyber threats. The content of cyber threats on the example of industrial enterprises has been considered.

The number of cyber threats is constantly growing in the world, their complexity and diversity increase depending on the object of the attack, goals and objectives. The most common types of cyber attacks in the world has been considered in the article, the mechanism of their implementation, their source and the scale of damage they cause, have been described.

In connection with the transition to a digital economy, the number of cyber threats is constantly growing. In 2018, 4.3 billion computer impacts on critical infrastructure were identified in Russia (2.4 billion in 2017). Of these, more than 17 thousand are the most dangerous computer attacks. Bot networks of 30 thousand computers in 86 countries were used for these purposes. The average costs of medium-sized companies to eliminate the consequences of only one cyber incident in Russia are about 1.6 million rubles, and for large businesses – 16.1 million rubles.

The recommendations to companies to consider the cost of information security as a strategic investment, ensuring the continuity of their business processes, which create advantages in an era of rapidly developing cyber threats, have been substantiated in the article. For the purposes of selecting and analysing the sources of costs of companies to provide information security, it has been proposed to classify them into 9 categories. The results of the analysis will allow companies to determine the main directions of priority financing of measures to reduce the level of losses from information security incidents and to form reasonably information security budgets.

**Keywords:** information security, cybersecurity, cyber incidents, company damage, data leakage, costs, selection and analysis.

**For citation:** Makhalina O.M., Makhalin V.N. Digitalization of business increases the costs of information security (2020) *Upravlenie*, 8 (1), pp. 134–140. doi: 10.26425/2309-3633-2020-1-134-140



Современная конкурентная экономика, основанная на использовании новых информационных систем и технологий, разработке систем управления на базе цифровых платформ, использования технологий блокчейна и интернета вещей (англ. internet of things), анализа больших данных (англ. big data), порождает разнообразие и число угроз информационной безопасности (далее – ИБ) [5; 9]. Появляется все большая необходимость защиты персональных данных человека, обеспечения безопасности информационной инфраструктуры Российской Федерации, защиты рабочей среды, технологий и инструментов. Эти задачи формируются из понятия информационной безопасности – «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое развитие Российской Федерации, оборона и безопасность и государства» [1].

Угрозы ИБ представляют «совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере» [1]. Одним из таких факторов является возрастающий объем информации, большую часть которой будут производить компании. По прогнозам International Data Corporation (далее – IDC), к 2025 г. объем данных во всем мире вырастет в 10 раз по сравнению с 2017 г. Это приведет к увеличению расходов компаний на хранение и анализ больших данных. Если в 2017 г. эти расходы составляли 150 млрд долл. США, то к 2020 г., по прогнозу экспертов, они достигнут около 210 млрд долл. США.

Аналитики IDC прогнозируют, что в мире с каждым годом все больше будут расти расходы на обеспечение ИБ. Это зачастую связано с тем, что:

- коммерческие компании и другие организации осознают то, что информационная безопасность является таким же ресурсом, как технологии и средства производства, поэтому расходы на построение системы ИБ, теперь будут рассматриваться как инвестиции;
- финансовая стабильность предприятия обеспечивается информационной безопасностью, поэтому от компаний постоянно требуется осуществление все более активных инвестиций в обеспечение безопасности как информации, так и инфраструктуры;
- необходимы расходы на разработку комплексной стратегии ИБ, инвентаризацию и улучшение своих активов в информационных технологиях, стратегии реагирования на угрозы, борьбу с эпидемиями вирусов-вымогателей и др.;
- темпы роста расходов на информационную безопасность, связаны с внутренней политикой государства, провозгласившего курс на развитие цифровой экономики, включающей все сферы: от здравоохранения и образования до транспорта и финансов;
- сохраняющаяся нехватка квалифицированных специалистов и регуляторные изменения, такие как Общий регламент по защите данных (GDPR), способствуют дальнейшему росту расходов на ИБ;
- одним из ключевых факторов, способствующих повышению расходов на ИБ, является внедрение новых методов обнаружения угроз и реагирования на них;
- главной движущей силой, стоящей за ростом расходов на кибербезопасность, являются ИБ-риски (кибератаки и утечки информации), которые могут нанести ущерб компаниям,связанный с расходами на восстановление их нормального функционирования.

Эксперты прогнозируют более активный ежегодный рост расходов компаний на ИБ. При этом возникают резонные вопросы: каков предел этого роста;какой уровень средних расходов на ИБ будет оптимальным для крупных компаний; каков размер среднего ущерба компаний от различных инцидентов с кибербезопасностью; сколько должны тратить компании на свою информационную безопасность. Вероятность правильного ответа на эти и другие вопросы, когда речь идет о цифровой защите данных и серверов, просчитать возникающие финансовые риски и необходимые издержки, представляет собой сложную задачу [4; 8]. Поэтому эксперты дают различные оценки, связанные с расходами компаний на обеспечение ИБ. Это могут быть как абсолютные, так и относительные показатели, характеризующие расходы на мировом уровне крупных коммерческих компаний, банков, финансовых организаций и другие мировые расходы на обеспечение информационной безопасности которые эксперты могут представлять по различным сегментам (направлениям). Рассмотрим такое распределение, по прогнозам экспертов компании Gartner на 2018 г., которое предусматривает увеличение расходов по всем направлениям. Так, на сервисы киберзащиты будет потрачено около 57,7 млрд долл. США (+4,65 млрд долл. США), на обеспечение безопасности инфраструктуры – порядка 17,5 млрд долл. США (+1,25 млрд долл. США), на оборудование для защиты сетей – 11,67 млрд долл. США (+735 млн долл. США), на потребительское программное обеспечение – 4,74 млрд (+109 млн долл. США) и на IAM-системы – 4,69 млрд долл. США (+416 млн долл. США) [10].

Отсутствует единство мнений экспертов, по относительной оценке, вероятного объема расходов на информационную безопасность. Некоторые эксперты полагают, что крупные коммерческие компании должны тратить на обеспечение ИБ своего бизнеса примерно 1 % совокупной годовой выручки, а, например, эксперты IDC считают, что для этого необходимо 9,8–13,7 % от общего бюджета ИТ компании.

В абсолютных показателях, оценки расходов на ИБ тоже нет единства среди экспертов. Например, глобальные мировые расходы на информационную безопасность в 2017 г. достигли 101,5 млрд долл. США, то есть оцениваются конкретной величиной, а расходы на кибербезопасность, например, отечественных банков и финансовых организаций – 300 млрд руб. в год, промышленных предприятий – до 50 млн руб. в год, сетевых компаний – от 10 до 50 млн руб. в год, оцениваются лишь по средним величинам.

В общие расходы на ИБ включаются средние расходы на восстановление деятельности компании, связанные с киберпреступлениями и которые могут нанести ущерб компании от утечки информации и кибератак. Эти расходы являются довольно значительными, как следует из ниже приведенных цифр:

- в 2017 г. расходы из-за киберпреступности увеличились на 23 % в сравнении с 2016 г. В среднем эта сумма составляет 11,7 млн долл. США;
- средняя сумма убытков компании, вызванных атакой вредоносной программы, составляет 2,4 млн долл. США;
- если говорить о времени, одна атака в среднем равняется 50 дням простоя для компании;
- с 2016 г. по 2017 г. расходы на кибербезопасность выросли на 22,7 %, средняя сумма ущерба от киберпреступности по всему миру выросла более чем на 27 %. Самый дорогой аспект кибератаки для предприятий – потеря информации. Она составляет 43 % всех затрат, вызванных вторжениями злоумышленников;
- в 2017 г. убытки от атак вымогателей превысили 5 млрд долл. США. Это в 15 раз больше, чем аналогичная сумма, зафиксированная в 2015 г. утечка Equifax в общей сумме стоила кредитному бюро более 4 млрд долл. США;
- средняя стоимость утерянных или украденных данных на одного человека составляет 141 долл. США, но стоит учитывать, что эта сумма серьезно варьируется в зависимости от страны. Самые дорогие утечки в США – 225 долл. США и Канаде – 190 долл. США;
- для компаний, у которых число скомпрометированных данных превышает 50 тыс. записей (паролей и т. д.), средняя стоимость убытков составляет 6,3 млн долл. США;
- проблемы с клиентами и репутацией из-за утечек ударили больше всех по американским компаниям – 4,13 млн долл. США убытков в среднем на одну компанию США;
- по прогнозам, к 2021 г. ущерб от киберпреступности достигнет 6 трлн долл. США [11].

Расходы на информационную безопасность формируются под воздействием многих факторов, важнейшие из которых – киберугрозы. Киберпреступники в зависимости от объекта нападения устанавливают цели и задачи, определяют тип, способы и методы. Рассмотрим этот процесс на примере промышленных предприятий [6]. Обеспечение кибербезопасности промышленных предприятий в настоящее время является острейшей проблемой. Это связано с ростом количества и сложности киберугроз и отсутствием четких способов борьбы с ними. Перечислим наиболее значимые варианты киберугроз в зависимости от их целей и специфики деятельности предприятий:

- взломщики компьютерной сети предприятия пытаются похитить техническую и экономическую информацию о разрабатываемой продукции у предприятия-конкурента;
- преступники, используя вирус-шифровальщик, могут попытаться остановить работу предприятия, отключить противоаварийную защиту;
- киберпреступники могут манипулировать стоимостью котировок ценных бумаг необходимой компании на биржах;
- промышленный фрод, представляющий собой мошенничество в области информационных технологий, в частности, несанкционированные действия и неправомочное пользование ресурсами и услугами в сетях;
- другие киберугрозы, такие как: скрытый майнингкриптовалюты в технологическом сегменте, наличие вредоносного программного обеспечения, ожидающего боевую команду от командного центра из другой страны и т. д.

Рассмотрим, какие типы кибератак наиболее распространены в мире, как они осуществляются, откуда приходят и какой ущерб они наносят компаниям и организациям, рассмотрим на примере приведенной ниже информации:

- больший процент детекта программ-вымогателей был зафиксирован в странах с наиболее доступным для населения интернетом. США держит среди них первое место с 18,2 % ото всех атак вредоносных программ такого типа;

• знаменитый троян Ramnit в значительной степени затронул финансовый сектор. В 2017 г. 53 % атак Ramnit пришлись именно на эту отрасль;
• большинство вредоносных доменов (около 60 %) связаны со спам-кампаниями;
• у 74 % компаний есть более 1 000 устаревших чувствительных файлов;
• вредоносные программы и сетевые атаки – два наиболее убыточных для компаний типа атак. Организации потратили в среднем 2,4 млн долл. США на защиту от них;
• индустрия финансовых услуг по максимуму оценивает все, что связано с киберпреступностью; В среднем с компании берут 18,3 млн долл. США.
• файлы Microsoft Office (например, Word, PowerPoint и Excel) представляют самую распространенную группу вредоносных расширений – 38 % от общей суммы;
• около 20 % вредоносных доменов совершенно новые, они используются примерно спустя неделю после их регистрации;
• более 20 % кибератак в 2017 г. были совершены из Китая, 11 % из США и 6 % из России;
• наибольший процент приложений с проблемами кибербезопасности – это так называемые lifestyle приложения. Из них 27 % являются вредоносными. Среди приложений для музыки и аудио злонамеренных 20 %;
• чаще всего вредоносные приложения сливают злоумышленникам номера телефонов (63 %), на втором месте местоположение устройства (37 %);
• в прошлом году целевой фишинг стал основным вектором распространения вредоносных программ. Этот метод использовал 71 % киберпреступных групп.
• в период с 2015 г. по 2017 г. от таргетированных кибератак больше всего пострадали США – были зарегистрированы 303 крупномасштабные атаки;
• в 2017 г. общий объем вредоносных программ вырос на 88 %;
• в числе самых детектируемых вредоносных программ находятся Heur.AdvML.C, Heur.AdvML.B и JS. Downloader [11].

В России, в связи с переходом к цифровой экономике, резко растет число киберугроз. По данным «Лаборатории Касперского» каждая российская компания в 2017 г. столкнулась с тем или иным видом киберугроз. Одной из массовых в 2017 г. стала кибератака во время «прямой линии» президента России, а также еще одна атака во время выборов президента страны. Для атаки использовалась новая модификация вредоносного программного обеспечения семейства Russkill. «Мы пришли к выводу, что имеем дело со спецслужбой иностранного государства, в совершенстве знающей алгоритмы работы корневых DNS-серверов», – заявил заместитель директора Национального координационного центра по компьютерным инцидентам Николай Мурашов [10]. Для атаки использовалась бот-сеть из 30 тыс. компьютеров в 86 странах мира. Ежедневно каждый бот генерировал 15 млрд запросов к DNS-серверам, что создавало запредельные нагрузки на серверы и могло физически вывести их из строя.

Всего в 2018 г. в России было выявлено более 4,3 млрд компьютерных воздействий на критическую информационную инфраструктуру, из них свыше 17 тыс. – наиболее опасные компьютерные атаки. Об этом рассказал замдиректора Национального координационного центра по компьютерным инцидентам Н. Мурашов. Например, только на информационную инфраструктуру чемпионата мира по футболу в России было совершено более 25 млн вредоносных воздействий. По словам Н. Мурашова, в 2017 г. было зафиксировано почти в два раза меньше кибератак – 2,4 млрд [2].

По всему миру, постоянно растет ущерб от инцидентов, связанных с кибербезопасностью. Компаниям приходится принимать различные превентивные меры, чтобы быть подготовленными для борьбы с возникающими новыми угрозами, а это связано с значительным увеличением расходов на обеспечение защиты от киберугроз [7]. Средние затраты компаний на ликвидацию последствий лишь одного киберинцидента, составляет по России, для среднего бизнеса, порядка 1,6 млн руб., а для сегмента крупного бизнеса – 16,1 млн руб. В этих условиях компаниям необходимо понять, что их затраты на информационную безопасность не являются отрицательным фактором, который понижает степень экономической эффективности, а необходимо считать их стратегическими инвестициями, обеспечивающих непрерывность их бизнес-процессов и, которые, создают преимущества в эпоху стремительно развивающихся киберугроз. Однако источники этих затрат необходимо тщательно выбирать и анализировать. С этой целью предлагается все источники затрат компании, связанные с финансированием предупреждения либо преодоления проблем в информационной безопасности, разделить на 9 категорий [3].

В таблице 1 приведены средние затраты компаний, столкнувшихся с ИБ-инцидентами, а сумма всех предлагаемых категорий определяет общий ущерб компании, нанесенный ИБ-инцидентом. Эти затраты определены на основании опроса 57 крупных компаний, хотя бы раз сталкивавшихся с ИБ-инцидентом. Крупный бизнес (свыше 250 сотрудников), в среднем и в силу своего размера, несет больше потерь вследствие ИБ-инцидентов, однако

*Таблица 1*

**Категории затрат компаний, вызванных ИБ-инцидентами**

Table 1. Categories of costs incurred by companies due to IB-incidents

| Категории затрат компаний вызванных ИБ-инцидентами | Годы | | | Годы | | |
|---|---|---|---|---|---|---|
| | затраты, тыс. руб. | | в %, 2017 г. к 2016 г. | Структура затрат, % | | |
| | 2016 | 2017 | | 2016 | 2017 | 2017 г. к 2016 г. |
| Обучение сотрудников | 1008 | 1411 | 139,98 | 6,72 | 8,76 | 130,36 |
| Упущенная выгода | 2419 | 1008 | 41,67 | 16,13 | 6,26 | 38,81 |
| Обращение к сторонним экспертам | 1747 | 941 | 53,86 | 11,65 | 5,84 | 50,13 |
| Ухудшение кредитного рейтинга/рост страховых выплат | 1814 | 2285 | 125,86 | 12,09 | 14,19 | 117,37 |
| Дополнительная работа с общественностью | 1411 | 3158 | 223,81 | 9,41 | 19,61 | 208,4 |
| Компенсации | 1478 | 605 | 40,93 | 9,85 | 3,76 | 38,17 |
| Улучшение ПО/структуры | 2150 | 2755 | 128,14 | 14,33 | 17,11 | 119,4 |
| Дополнительные выплаты сотрудникам | 2083 | 1814 | 87,09 | 13,89 | 11,27 | 81,14 |
| Наем новых сотрудников | 806 | 2150 | 266,75 | 5,37 | 13,35 | 248,6 |
| Итого | 15000 | 16100 | 107,33 | 100 | 100 | |

Составленоавторамипоматериалам[3] / *Compiled by the authors on the materials of the source [3]*

представляет интерес анализ распределения затрат по категориям. Такой анализ позволяет выявит динамику изменения средних затрат, определить их структуру и ее изменение по годам. В 2017 г. наибольший рост средних затрат выявлен по следующим категориям: наем новых сотрудников – 266,75 %; дополнительная работа с общественностью – 223,81 %; обучение сотрудников – 139,98 % и при этом по категориям: упущенная выгода, компенсации, дополнительные выплаты сотрудникам, средний уровень затрат значительно снизился по сравнению с 2016 г. Результаты такого анализа позволяют компаниям осознать важность повышения собственного уровня кибербезопасности и определять основные направления работы, направленной на снижение уровня ущерба от ИБ-инцидентов, формировать бюджеты информационной безопасности и определять процент IT-бюджета, выделяемого на ИБ.

**Библиографический список**


1. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс» [Электронный ресурс]. – Режим доступа:http://www.consultant.ru/document/cons_doc_LAW_208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/ (дата обращения: 12.02.2020).
2. Егоров, И. Атаки в сети и наяву // Российская газета. 2018. 11 дек. № 279 (7742) [Электронный ресурс]. – Режим доступа: https://rg.ru/2018/12/11/direktor-fsb-aleksandr-bortnikov-rasskazal-o-predotvrashchennyh-teraktah.html (дата обращения: 12.02.2020).
3. «Лаборатория Касперского» выяснила: утечка данных стоила российскому крупному бизнесу 246 тысяч долларов // Лаборатория Касперского [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/about/press-releases/2018_data-leaks (дата обращения: 12.02.2020).
4. Мамаева, Л. Н. Характерные проблемы информационной безопасности в современной экономике // Информационная безопасность регионов. 2016. № 1. С. 21–24.


**References**


1. Ukaz Prezidenta RF ot 05.12.2016 № 646 "Ob utverzhdenii Doktriny informatsionnoi bezopasnosti Rossiiskoi Federatsii" [*Decree of the President of the Russian Federation "On Approval of the Information Security Doctrine of the Russian Federation" No. 646 dated on December 5, 2016*], legal reference system "Consultant plus". Available at: http://www.consultant.EN/document/cons_doc_LAW_208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/ (accessed 12.02.2020).
2. Egorov I. Ataki v seti i na yavu [*Attacks in the network and in reality*], Rossiiskaya Gazeta, 2018, 11 dek, no. 279 (7742). Available at: https://rg.ru/2018/12/11/direktor-fsb-aleksandr-bortnikov-rasskazal-o-predotvrashchennyh-teraktah.html (accessed 12.02.2020).
3. "Laboratoriya Kasperskogo" vyyasnila: utechka dannykh stoila rossiiskomu krupnomu biznesu 246 tysyach dollarov [*Kaspersky Lab found out: the data leak cost Russian big business 246 thousand dollars*], Laboratoriya Kasperskogo [*Kaspersky Lab*]. Available at: https://www.kaspersky.ru/about/press-releases/2018_data-leaks (accessed 12.02.2020).
4. Mamaeva L. N. Kharakternye problemy informatsionnoi bezopasnosti v sovremennoi ekonomike [*Typical problems*

5. Махалин, В. Н. Угрозы экономической безопасности России // Актуальные вопросы права, экономики и управления: сборник статей научно-практической конференции. Пенза: Наука и просвещение. 2017. 302 с.
6. Махалин, В. Н., Махалина, О. М. Управление вызовами и угрозами в цифровой экономике России // Управление. 2018. № 2. С. 57–60.
7. Остроглазов, А., Липов, Д. Как повысить эффективность затрат финансовых организаций на кибербезопасность // Bankir.ru [Электронный ресурс]. – Режим доступа: https://bankir.ru/publikacii/20181105/kak-povysit-effektivnost-zatrat-finansovykh-organizatsii-na-kiberbezopasnost-10009623/ (дата обращения: 12.02.2020).
8. Удалов, Д. В. и др. Государственная политика в сфере обеспечения национальной безопасности: экономико-правовой аспект:монография / Под общ. ред. С. Ю. Наумова, Б. В. Чернышева. Саратов: Саратовский социально-экономический институт (филиал РЭУ им. Г. В. Плеханова), 2016. 284 с.
9. Удалов, Д. В. Угрозы и вызовы цифровой экономики // Экономическая безопасность и качество. 2018. № 1. С. 12–18.
10. Информационная безопасность (мировой рынок) // TAdviser [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/a/275984 (дата обращения: 12.02.2020).
11. Иванов, О. Информационная безопасность в цифрах // Anti-Malware.ru [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/2018-cybersecurity-statistics (дата обращения: 12.02.2020).

*of information security in modern economy*], Informatsionnaya bezopasnost` regionov, 2016, no. 1, pp. 21–24.
5. Makhalin V. N. Ugrozy national`noi bezopasnosti Rossii [*Threats to economic security of Russia*], Aktual'nye voprosy prava, ekonomiki i upravleniya: sbornik statei nauchno-prakticheskoi konferentsii [*Topical issues of law, economics and management: collection of articles of the scientific and practical conference*], Penza, Nauka i prosveshchenie, 2017, 302 p.
6. Makhalin V. N., Makhalina O. M. Upravlenie vyzovami i ugrozami v tsifrovoi ekonomike Rossii [*Managing challenges and threats in the digital economy of Russia*], Upravlenie, 2018, no. 2, pp. 57–60.
7. Ostroglazov A., Lipov D. Kak povysit` effektivnost` zatrat finansovykh organizatsii na kiberbezopasnost› [*How to improve the cost-effectiveness of financial institutions for cybersecurity*], Bankir.ru. Available at: https://bankir.ru/publikacii/20181105/kak-povysit-effektivnost-zatrat-finansovykh-organizatsii-na-kiberbezopasnost-10009623/ (accessed 12.02.2020).
8. Udalov D. V. [et al.]. Gosudarstvennaya politika v sfere obespecheniya national`noi bezopasnosti: ekonomiko-pravovoi aspekt [*State policy in the sphere of national security: economic and legal aspect*], pod obshch. red. S. Yu. Naumova, B. V. Chernyshcheva, Saratov, Saratovskii sotsial`no-ekonomicheskii institute (filial REU im. G. V. Plekhanova), 2016, 284 p.
9. Udalov D. V. Ugrozy i vyzovy tsifrovoi ekonomiki [*Threats and challenges of digital economy*], Ekonomicheskaya bezopasnost` i kachestvo, 2018, no. 1, pp. 12–18.
10. Informatsionnaya bezopasnost› (mirovoi rynok) [*Information security (world market)*], TAdviser. Available at:http://www.tadviser.ru/a/275984 (accessed 12.02.2020).
11. Ivanov O. Informatsionnaya bezopasnost› v tsifrakh [*Information security in numbers*], Anti-Malware.ru. Available at: https://www.anti-malware.ru/analytics/Threats_Analysis/2018-cybersecurity-statistics (accessed 12.02.2020).