Оригинальные статьи / Original articles

https://doi.org/10.21869/2223-1560-2019-23-4-93-104

Анализ организации защиты информации в России и других странах мира

А.Л. Ханис [1] ✉, Е.И. Щедрина [1], С.В. Спевакова [1]

[1] ФГБОУ ВО «Юго-Западный государственный университет», ул. 50 лет Октября, 94, г. Курск, 305040, Российская Федерация

✉ e-mail: hanis.a_@mail.ru

Резюме

Цель исследования. *В данной статье рассматриваются различные способы защиты информации, применяющиеся в разных странах, а также проводится анализ и сравнение степени развития данной сферы в Российской Федерации. Приводится краткая история возникновения и последующая динамика развития этой области в разных государствах. Целью данной статьи является анализ законодательств различных стран (законов, подзаконных актов, указов), связанных со сферой информации и защитой персональных данных, и разработка метода, позволяющего повысить долю предотвращенных атак на информационные системы.*

Методы. *Была изучена специфика форм защиты информации в следующих странах: Российская Федерация, Соединенные Штаты Америки, Германия, Франция. В статье описываются существующие на сегодняшний момент глобальные международные стандарты по стандартизации мер и систем безопасности, относящиеся к системе под названием ISO/IEC 27000, и уровень их внедрения в России. В качестве метода исследования был выбран метод иерархий Саати.*

Результаты. *Проведенное исследование позволило выявить возможные недостатки защиты информационного поля России с помощью проведения аналогии с другими, более развитыми в данном аспекте странами. Законодательная база России содержит множество законов и постановлений, которые затрагивают тему защиты и обработки персональных данных пользователей, но их количество и четкость организации не является достаточной и требует улучшения.*

Заключение. *В ходе анализа был сделан вывод, что в России охране информационных данных уделяется значительное внимание, действует ряд федеральных законов, однако нормативно-правовая база Российской Федерации, целью которой является защита информации и персональных данных, имеет относительно небольшую историю развития и нуждается в доработке.*

Ключевые слова: *информационная безопасность; кибератака; законы об информационной безопасности; персональные данные.*

Конфликт интересов: *Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Ханис А.Л., Щедрина Е.И., Спевакова С.В. Анализ организации защиты информации в России и других странах мира // Известия Юго-Западного государственного университета. 2019; 23(4): 93-104. https://doi.org/10.21869/2223-1560-2019-23-4-93-104.

Статья поступила в редакцию 14.06.2019

Статья подписана в печать 05.08.2019

https://doi.org/10.21869/2223-1560-2019-23-4-93-104

Analysis of the Information Security Arrangement in Russia and Other Countries

Andrey L. Hanis [1] ✉, Yekaterina I. Shhedrina [1], Svetlana V. Spevakova [1]

[1] Southwest State University, 94, 50 Let Oktyabrya str., Kursk, 305040, Russian Federation

✉ e-mail: hanis.a_@mail.ru

Abstract

Purpose of research. *This article discusses various techniques for information security implementation used in certain countries; presents analysis and comparison of the degree of information security development in the Russian Federation. A brief history of the origin and subsequent dynamics of the development of this area in different countries is given. The objectives of this article are to analyze the legislation basis of different countries, namely the laws, regulations, decrees related to the sphere of information and personal data security and to develop a technique to increase the share of prevented attacks against information systems.*

Methods. *The peculiarities of forms of information security implementations in the Russian Federation, the United States of America, Germany,and France was studied. The article analizes the current global international standards for standardization of security measures and systems related to the ISO / IEC 27000 system, and the level of their implementation in Russia. The method of Saati hierarchies was chosen as the research method.*

Results. *The conducted research allowed us to reveal possible shortcomings of information security implementation in Russia by means of drawing an analogy with other countries with a more developed information security systems. Russian legislative framework contains many laws and regulations that affect personal data protection and processing, but their number and arrangement clarity is not sufficient and needs to be enhanced.*

Conclusion. *As a result of the analysis it can be concluded that Russia pays considerable attention to information security implementation; different measures have been taken to its ensurance; a number of Federal laws have been enacted. However, the regulatory framework of the Russian Federation, the purpose of which is to protect information and personal data, has a relatively short history of development and needs enhancement.*

Keywords: *information security; cyberattack; information security laws; personal data.*

Conflict of interest. *The Author declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Hanis A. L., Shhedrina Y. I., Spevakova S. V. Analysis of the Information Security Arrangement in Russia and Other Countries. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2019, 23(4): 93-104 (In Russ.). https://doi.org/ 10.21869/2223-1560-2019-23-4-93-104.

Received 14.06.2019

Accepted 05.08.2019

***

Введение

Защита информации – одна из наиболее необходимых задач в функционировании целого государства и, соответственно, деятельности отдельно взятых крупных, либо небольших предприятий. В XXI веке этот факт считается вполне очевидным. Прежде чем приступать к анализу, необходимо уточнить суть основного в этой теме понятия. Что же обычно подразумевается под определением информационной безопасности? Это такая совокупность мер, в том числе организационных и технических, которые принимаются с целью обеспечения ряда необходимых требований: защиты, целостности, доступности и управляемости массивов информации. Правильная и надежная защита данных укрепляет суверенитет, обороноспособность, положение государства в мире, обеспечивает надежную поддержку сохранения государственной тайны [1].

Одна из самых острых проблем современного общества – ведение информационных войн. Главным оружием и одновременно преимуществом в таких войнах, конечно же, является владение информацией. Каждый из нас слышал выражение «кто владеет информацией, тот владеет миром». Оно особенно актуально в наши дни, когда каждое государство стремится завоевать главенствующую позицию на данном поприще.

По этим причинам защита данных в современном мире становится необходимостью. Требуется создание особого аппарата и разработка в этой сфере собственной инфраструктуры. Различные государства в этом плане развиты неравномерно, они используют значительно отличающиеся друг от друга подходы и методы решения задач. Некоторые страны начали формирование такого аппарата намного раньше относительно других, поэтому логично предположить, что они имеют более развитую систему.

Но даже та защита информации, которую может обеспечить государство, не является абсолютно надежной, она требует постоянного совершенствования. На протяжении 2018 года в России на муниципальные и частные компьютерные ресурсы только за период проведения Чемпионата мира по футболу было совершено примерно 25 млн кибернападений. Это число не является пределом, во всем мире оно возрастает с каждым годом. По данным Лаборатории Касперского, Россия занимает первое место в мире по количеству кибератак [2].

В рамках статьи рассматриваются страны, которые смогли зарекомендовать себя как информационные державы. Сравнивается степень развития РФ с другими странами.

Материалы и методы

Основным документом, обеспечивающим регулировку защиты информации в масштабах всего государства, выступает Доктрина информационной безопасности. В 2016 году она была существенно переработана из-за значительно устаревшего содержания документа, вступившего в силу шестнадцать лет назад.

В общих положениях доктрины говорится об являющихся наиболее значимыми угрозах для информационной безопасности РФ, взглядах на обеспечение национальной безопасности. Особый упор делается на важность продолжения развития информационных технологий [3].

Также имеет место ряд соответствующих законов: Конституция РФ; Федеральный закон о персональных данных (ред. от 31.12.2017); Конвенция о защите физических лиц; Закон о государственной тайне (ред. от 29.07.2018); Федеральный закон о коммерческой тайне (ред. от 18.04.2018) [4].

Как можно видеть по вышеприведенному списку, регулированию обеспечения информационной защиты и охране персональных данных отводится немалая роль.

Помимо этого, можно назвать ряд государственных организаций, которые реализуют надзор за деятельностью в сфере защиты информации: ФСТЭК России, ФСБ РФ, МВД РФ, Россвязьохранкультура, Межведомственная комиссия по защите государственной тайны [5].

Россия потребность в защите данных на уровне государства осознала лишь в 1990-2000 годах, в то время как в Соединенных Штатах Америки еще в 1906 году был принят самый первый в своем роде закон об охране информации. В наши дни, спустя более чем через столетие длительного формирования в данной сфере, в США насчитывается уже приблизительно пятьсот различных законодательных актов, имеющих непосредственное отношение к данной области. РФ же, в свою очередь, очевидно, не обладает подобным разнообразием законов об информационной безопасности [6].

Проблемы, вызывающие повышенное внимание служб охраны информации, в США решаются под руководством Агентства национальной безопасности (АНБ) и Совета национальной безопасности.

Уже упоминалось ранее, что формирование законодательства США в области информационной безопасности исторически началось намного раньше. Так, например, некоторые законы были зафиксированы законодательством еще до начала двухтысячного года:

- "О свободе информации" (1967 год);
- "О секретности" (1974 год);
- "О праве на финансовую секретность" (1978 год) [7].

Сравнивая нормативную основу Российской Федерации и США, не лишним будет отметить, что в России она носит скорее оборонительный характер, имеет

курс на сохранение суверенитета, государственной тайны, ук-репление обороны страны [8].

Государством с одной из наиболее развитых в мире информационной инфраструктурой является также Великобритания. Ее власти осознали всю важность разработки законодательства в области обеспечения защиты данных значительно раньше других стран Европы. В стране на данный момент действует самая строгая концепция организации защиты информации.

Основополагающим законодательным актом Великобритании, призванным обеспечить государственную безопасность, считается Стратегия национальной безопасности (2010г.). Согласно ей, безопасность информации и антитеррористические мероприятия становятся приоритетными направлениями.

Закон «The Official Secret Act» 1911 года составляет фундамент защиты государственной тайны Британии. Он претерпел поправки и дополнения 1920, 1939, 1989 гг. Также ее регулируют законы:

- «О государственных архивах» (1958 г.);
- «О нарушении конфиденциальности» (1981 г.);
- «О следственных органах» (1985 г.);
- «О службе безопасности» (1989 г.).

Любая организация Великобритании должна самостоятельно заботиться об охране собственных коммерческих тайн, в связи с чем для крупных компаний формируются собственные службы безопасности.

Государственная организация по обеспечению безопасности страны строится, отталкиваясь от определения информационной войны, как операций, которые способны нанести значительный ущерб информационной системе противника, защищая вместе с тем собственные системы, что вполне можно назвать оптимальной тактикой.

Германию без сомнения можно назвать бесспорным лидером среди Европейских стран в области регулирования защиты личной информации, ее представления на законодательном уровне. Первый законодательный акт этого государства «О защите персональных данных» был принят в 1970 году. Федеральный закон был пересмотрен в 1990 году во взаимосвязи с быстрыми темпами развития СМИ и телекоммуникационных технологий. Были внесены соответствующие дополнения и правки в статью 41 и статью 42.

Федеральная служба безопасности информационной техники, основанная в 1991 году, несет ответственность за обеспечение безопасности каналов информации Германии. С этой целью и создавалась специальная Федеральная комиссия в сфере охраны личных данных. В лице Федеральных уполномоченных она осуществляет контроль исполнения закона на высшем федеральном уровне.

Немецкое понимание информационной войны следующее: наступающая и защитная составляющие объединяются в единое целое, причем иностранные государства отделяются от негосудар-

ственных организаций, рассматриваясь отдельно.

Вопросами информационной безопасности Франции занимаются не только государственные структуры. В данном процессе участвуют также негосударственные организации. Любое французское полицейское управление имеет собственный особый отдел по борьбе с информационными правонарушениями в каждом регионе.

Термин «государственная тайна» во Франции заменен определением «тайна национальной обороны». Характером тайны национальной обороны обладают документы, сведения, технологии и т.п., имеющие непосредственное отношение к национальной обороне (в соответствии со ст. 413-9).

За все кибератаки и несанкционированные посягательства на данные, соответственно, несется уголовная либо административная ответственность в зависимости от тяжести правонарушения. В качестве санкций для физических лиц предусмотрено заключение в тюрьму длительностью от 1 года до 3 лет и штраф в размере от 100 000 франков (6 631 990 рублей) до 300 000 франков (19 895 970 рублей) [9].

Также в наиболее важные системы активно внедряется криптографическое программное обеспечение. Это связано с мнением французских экспертов о том, что с помощью методов шифрации достигается наилучшее обеспечение защищенности информации в сетях.

Под руководством Министерства обороны Франции функционируют три службы по информационной защите: Генеральная дирекция внешней безопасности (1982г.), Управление военной разведки (1992г.) и Управление военной контрразведки (1981г.). Общий состав разведсообщества Франции является приблизительно равным 12779 сотрудников.

Следовательно, задачу информационной безопасности на сегодняшний день невозможно охарактеризовать как узконаправленную, она постепенно, но все больше перетекает в область международных проблем. Хотя в обеспечении международной информационной безопасности по-прежнему присутствует одна из основных трудностей: она не является объектом регулирования международного права [10].

Однако в сфере стандартизации мер и систем безопасности подобные нормы существуют и активно используются. Это эталоны производственного и торгового оборота, которые относятся к системе под названием ISO/IEC 27000. В данном случае двойная аббревиатура ISO/IEC показывает, что стандарты разработаны Международной комиссией по стандартизации (ISO), которая своими нормативными актами определяет качество процессов производства, и Международной Энергетической комиссией (IEC).

ISO/IEC 27000 включают в себя ряд рекомендаций и практических советов с целью внедрения концепции менедж-

мента информационной безопасности (СМИБ) [11].

Предложенный метод предполагает проведение анализа уязвимостей в области информационной безопасности и повышения доли предотвращенных атак на информационные ресурсы в процентном выражении, а также сравнение законодательств развитых стран-лидеров в этой сфере, разработку на их базе адаптированных нормативно-правовых актов и внедрение в отечественное законодательство. Алгоритм представлен на рис. 1.

В ходе выполнения данного алгоритма был сделан вывод, что для усовершенствования функционирования данной системы и улучшения результатов ее работы следует предпринять следующие действия:

– расширение границ сотрудничества РФ в сфере развития и формирования защиты информации на международной арене, а также сопротивление противоборству и его возможному развязыванию в данной сфере;

– осуществление борьбы с правонарушениями в сфере информационной безопасности с помощью фиксирования в соответствующих статьях Уголовного кодекса РФ, доработка уже существующих статей 280 и 282 УК РФ;

– более четкое определение таких видов информации, как персональные данные, семейная тайна и тайна личной жизни, государственная тайна, коммерческая тайна, а также улучшение гарантии их безопасности.

Необходимым также можно назвать организацию по расширению производства в нашей стране таких ключевых элементов, как системы и средства информатизации, а также стремление России зафиксироваться в международной кооперации их производителей. Это довольно важный факт, ведь без современных компьютерных и телекоммуникационных систем и их постоянного усовершенствования невозможно полное и надежное обеспечение защиты информационных данных [12].

Результаты и их обсуждение

Для проверки предложенных в качестве улучшения методов были произведены расчеты с помощью метода анализа иерархий (МАИ). В ходе сравнения для определения важности критериев используется девятибалльная шкала. Определенным критериям ставятся в соответствие веса в зависимость от значимости, затем расставляются баллы, отражающие влияние предложенных методов на критерии.

С помощью метода Саати рассчитываются коэффициенты важности для критериев, представленных в столбцах, а затем вычисляется интегральный показатель Q, который отражает улучшение показателей в процентах.

На основе полученных в ходе вычислений результатов строится наиболее наглядно представляющая информацию диаграмма, отражающая значение интегрального показателя для всех указанных критериев [13].

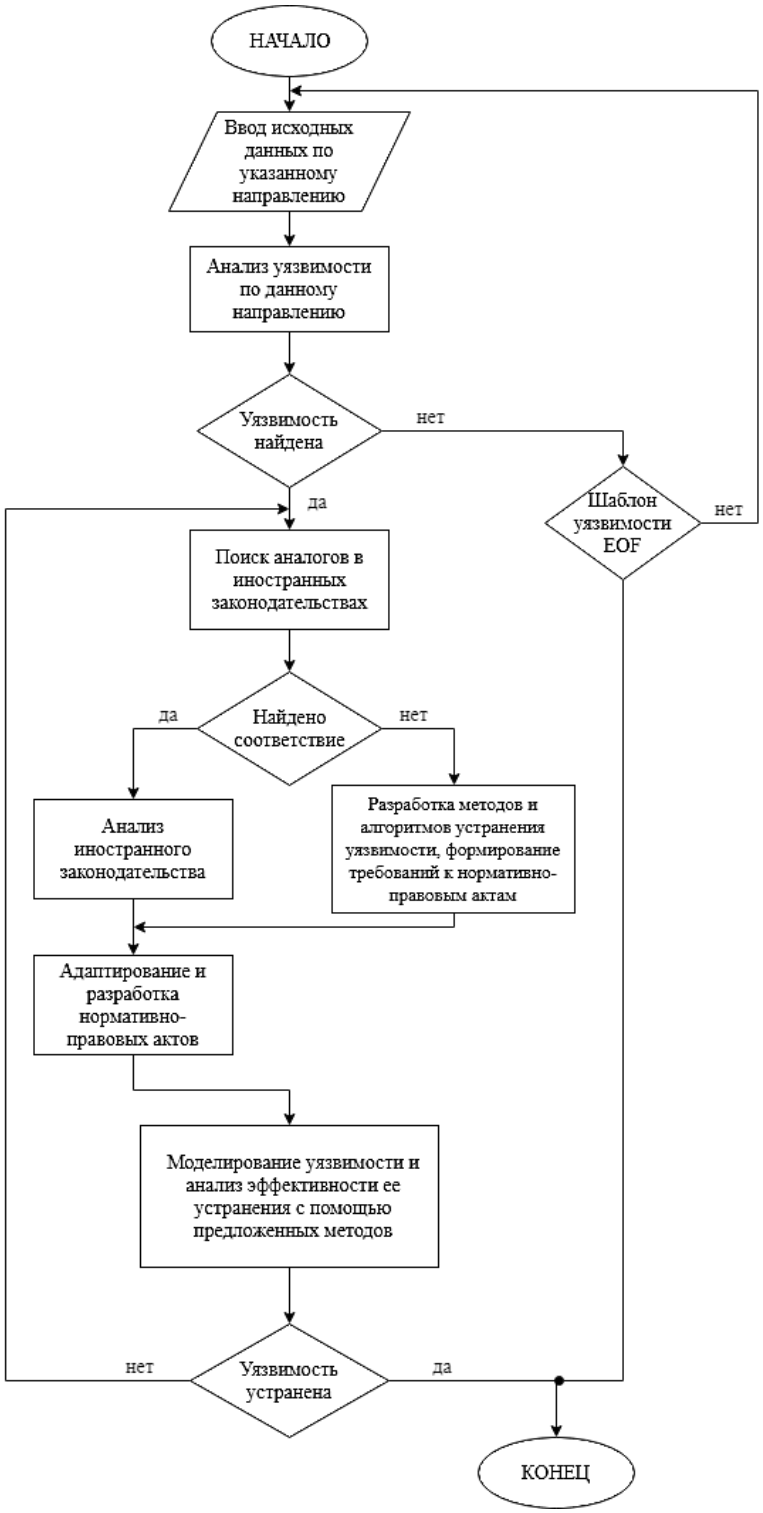

Рис. 1. Алгоритм устранения уязвимостей в информационной безопасности Российской Федерации

Fig. 1. Algorithm of elimination of vulnerabilities in information security of the Russian Federation

Ниже представлены результаты моделирования, воспроизведенные с помощью метода иерархий Саати (табл., рис. 2).

Расчет интегральных показателей

Calculation of integral indicators

Критерии		Веса	Расширение границ сотрудничества в данной сфере	Развитие в РФ производства средств и систем информатизации	Борьба с информационными преступлениями	Улучшение законодательства в данной сфере	Персональные данные, государственная и коммерческая тайна	Базовые значения
Конфиденциальность	A_1	1,00	3	5	7	6	7	5,60
Целостность	A_2	0,90	4	4	6	5	6	5,00
Доступность	A_3	0,80	6	5	4	5	3	4,60
Аутентичность	A_4	0,50	5	2	6	6	4	4,60
Аппелируемость	A_5	0,50	5	2	5	6	4	4,40
Интегральный показатель Q, (%)			**16,40**	**14,60**	**21,10**	**20,50**	**18,80**	

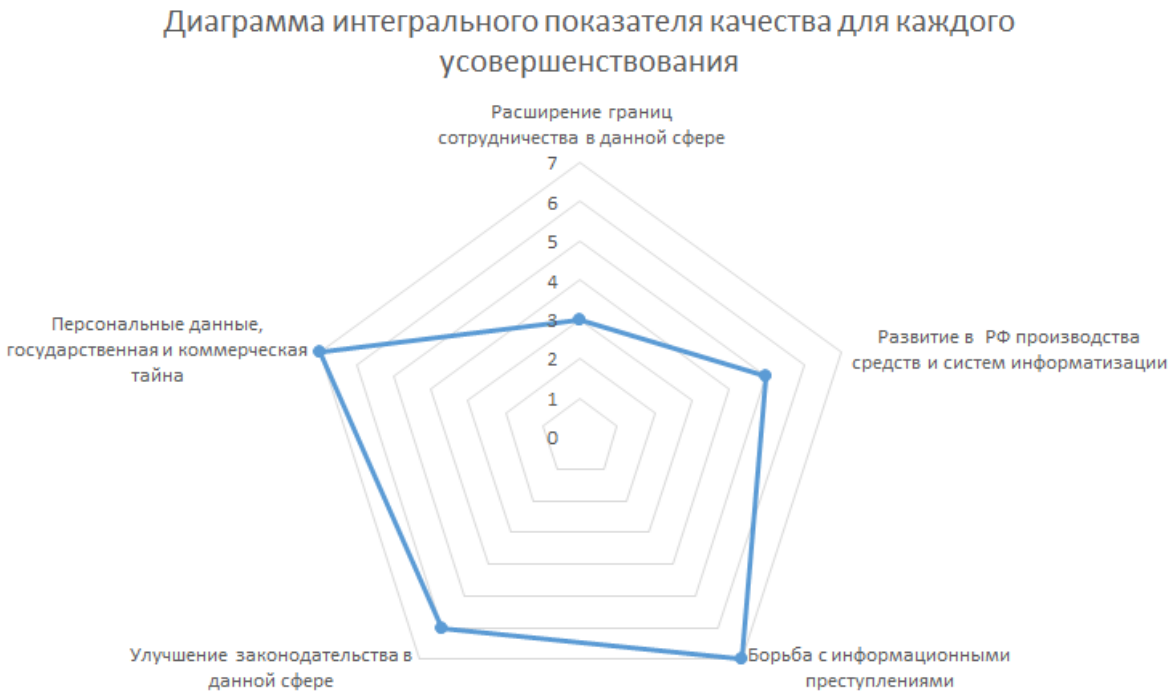

Рис. 2. Результат расчетов, представленный в виде диаграммы

Fig. 2. The result of the calculations is presented in the form of a diagram

Выводы

В качестве подведения итогов проведенного анализа можно сказать следующее: информационной безопасности в России уделяется значительное внимание, для ее обеспечения проведены многие меры, принят целый ряд законодательных актов, действуют специ-

альные федеральные органы. Однако имеются и существенные недостатки. По-прежнему несовершенно обеспечение защиты персональных данных, требуют серьезной доработки статьи 280 и 282 УК РФ, устанавливающие уголовную ответственность за высказывания в социальных сетях. Сравнивая уровень развития данной сферы с другими странами, можно сказать, что оно, в целом, началось в них гораздо раньше и, следовательно, имеет более установившуюся базу. Многие методы и концепции защиты данных, принятые в перечисленных странах, являются более результативными. У России есть перспективы развития в направлении защиты информации, поэтому следует улучшать ее законодательную, организационную и технологическую основу.

Список источников

1. Панищев В.С., Таныгин М.О., Информационная безопасность. Курск, 2017. 196 с.

2. Карта киберугроз в режиме реального времени. URL: https:// cybermap.kaspersky.com/ru/ (дата обращения 22.11.2018).

3. «Консультант Плюс» - законодательство РФ: кодексы, законы, указы, постановления правительства РФ. URL: http:// www.consultant.ru/ (дата обращения 23.11.2018).

4. Евсеева А.А., Калуцкий И.В., Спеваков А.Г. Сравнительный анализ российского и китайского законодательства в области обработки и защиты персональных данных// Известия Юго-Западного государственного университета. 2016. №7. С.78-84.

5. Система защиты информации в ведущих зарубежных странах. URL: http://webkonspect.com/?room= profile&id=11572&labelid= 162322. (дата обращения 23.11.2018).

6. Попыкин А.В. Информационная безопасность России в системе многополярного сотрудничества // Актуальные проблемы международных отношений в условиях формирования мультиполярного мира. Курск, 2015. С.129-131.

7. Аверченков В. И. Системы защиты информации в ведущих зарубежных странах. Брянск, 2007. 225 с.

8. Остроцкая С.В., Калуцкий И.В. Модель интерактивного справочного ресурса сведений и рекомендаций в области безопасности субъектов персональных данных// Известия Юго-Западного государственного университета. 2018. №2. С.73-81.

9. Общие сведения о стандартах серии ISO 27000. URL: http://www.iso27000.ru/standarty/iso-27000-mezhdunarodnye-standarty-upravleniya-informacionnoi-bezopasnostyu-1/iso-27000-mezhdunarodnye-standarty-upravleniya-informacionnoi-bezopasnostyu (дата обращения 24.11.2018).

10. Добрица В.П., Спеваков А.Г., Губорев А.А. Алгоритм исключающего преобразования данных // Известия Курского государственного технического университета. 2010. №1 (30). С. 49-54.

11. Graham J. Cyber Security Essentials. 2010. 331 p.

References

1. Panishev V.S., Tanygin M.O. Informacionnaya bezopanost’ [Information security]: Kursk, 2017, 196 p. (In Russ.).

2. Karta kiberugroz v regime realnogo vremeni [Real-time cyber threat map] (In Russ.). Available at: https://cybermap.kaspersky.com/ru. (accessed: 22.11.2018).

3. "Konsultant Plus" - zakonodatelstvo RF: kodeksy, zakony, ukazy, postanovleniya pravitelstva RF [“Consultant Plus” - the legislation of the Russian Federation: codes, laws, decrees, decrees of the government of the Russian Federation]. (In Russ.) Available at: http://www.consultant.ru/. (accessed: 23.11.2018).

4. Evseeva A.A., Kaluckiy I.V., Spevakov A.G. Sravnitelniy analiz rossiiskogo i kitaiskogo zakonodatelstva v oblasty obrabotki i zashity personalnyh dannyh [Comparative analysis of Russian and Chinese legislation in the field of processing and protection of personal data]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*, 2016, no.7, pp.78-84 (In Russ.).

5. Systema zashity informacij v vedushih zarubegnih stranah [Information security system in leading foreign countries]. Available at: http:// webkonspect.com/?room= profile&id=11572&labelid=162322. (accessed: 23.11.2018).

6. Popykin A.V. Informatsionnaya bezopasnost’ Rossij v sisteme mnogopolyarnogo sotrudnichestva [Information security of Russia in the system of multipolar cooperation]. *Aktualnye problem megdunarodhyh otnosheniy v usloviyah formirovaniya multipolyarnogo mira = Actual problems of international relations in the context of the formation of a multipolar world*. Kursk, 2015, pp.129-131 (In Russ.).

7. Averchenkov V.I. Sistemy zashity informatsij v vedushih zarubegnih stranah [Information security systems in leading foreign countries]. Bryansk, 2007, 225 p. (In Russ.).

8. Ostrockaya S.V., Kaluckiy I.V. Model’ interactivnogo spravochnogo resursa svedeniy i rekomendaciy v oblasty bezopasnosty subjektov personalnyh dannyh [A model of an interactive reference resource of information and recommendations in the field of security of personal data subjects]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University,* 2018, no.2, pp.73-81 (In Russ.).

9. Obshiye svedeniya o standartah serij ISO 27000 [General information on the standards of the ISO 27000 series] (In Russ.). Available at: http://www.iso27000.ru/standarty/iso-

27000-mezhdunarodnye-standarty-upravleniya-informacionnoi-bezopasnostyu-1/iso-27000-mezhdunarodnye-standarty-upravleniya-informacionnoi-bezopasnostyu. (accessed 24.11.2018).

10. Dobritsa V.P., Spevakov A.G., Guborev A.A. Algoritm iskluchaushego preobrazovaniya dannyh [Exclusion data conversion algorithm]. *Izvestiya Kurskogo gosudarstvennogo tekhnicheskogo universiteta = Proceedings of the Kursk State Technical University*, 2010, no.1 (30), pp. 49-54 (In Russ.).

11. Graham J. Cyber Security Essentials. 2010, 331 p.

Информация об авторах / Information about the Authors

Ханис Андрей Леонидович, кандидат военных наук, доцент кафедры информационной безопасности, ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Российская Федерация, e-mail: hanis.a_@mail.ru

Andrey L. Hanis, Candidate of Military Sciences, Associate Professor, Information Security Department, Kursk, Russian Federation, e-mail: hanis.a_@mail.ru

Щедрина Екатерина Игоревна, студент, ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Российская Федерация, e-mail: cat.shhedrina05061999@yandex.ru

Yekaterina I. Shhedrina, student, Kursk, Russian Federation, e-mail: cat.shhedrina05061999@yandex.ru

Спевакова Светлана Викторовна, аспирант кафедры вычислительной техники, ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Российская Федерация, e-mail: sspev@yandex.ru

Svetlana V. Spevakova, Post-Graduate Student, Computer Engineering Department, Kursk, Russian Federation, e-mail: sspev@yandex.ru