Московский экономический журнал. № 6 2023
Moscow economic journal. № 6 2023
Научная статья
Original article
УДК 339.5+339.94 (98)
doi: 10.55186/2413046X_2023_8_6_277

УПРАВЛЕНИЕ КИБЕРБЕЗОПАСНОСТЬЮ В НЕФТЕГАЗОВОЙ СФЕРЕ РОССИИ В УСЛОВИЯХ МЕЖДУНАРОДНЫХ САНКЦИЙ
CYBERSECURITY MANAGEMENT IN THE RUSSIAN OIL AND GAS SECTOR UNDER INTERNATIONAL SANCTIONS

Липатов Антон Борисович, аспирант, ФГАОУ ВО «Самарский государственный экономический университет», E-mail: ablipatov@gmail.com
Lipatov Anton Borisovich, graduate student, Educational institution: Samara State Economic University, Email: ablipatov@gmail.com

Аннотация. Научная статья посвящена анализу вопросов управления кибербезопасностью в нефтегазовой отрасли России и выработке рекомендаций по ее повышению в условиях международных санкций. В статье рассмотрены характеристикам видов кибератак на критическую инфраструктуру нефтегазовой отрасли; проведен количественный и качественный анализ киберинцидентов в отношении нефтегазовых бизнесов и структура целей атак; сформированы предложения по совершенствованию управления кибербезопасностью объектов критической инфраструктуры. Статья ориентирована на широкий круг читателей, интересующихся вопросами обеспечения кибербезопасности в нефтегазовой сфере, устойчивого развития и противодействия международных санкциям.

Abstract. Scientific article is devoted to the analysis of issues of cyber security management in the oil and gas industry of Russia and the development of recommendations to improve it in the context of international sanctions. The article con-

siders the characteristics of cyber attacks on critical infrastructure of the oil and gas industry; a quantitative and qualitative analysis of cyber incidents against oil and gas businesses and the structure of the targets of attacks; proposals for improving cyber security management of critical infrastructure were made. The article is intended for a wide range of readers interested in the issues of cybersecurity in the oil and gas sector, sustainable development and counteraction to international sanctions.
Ключевые слова: санкции, кибербезопасность, цифровая трансформация, нефтегазовая отрасль, критическая инфраструктура

Keywords: sanctions, cybersecurity, digital transformation, oil and gas industry, critical infrastructure

Введение. Обеспечение продуктивности и устойчивого инновационного развития российского нефтегазового сектора объективно невозможно без соответствующей критической инфраструктуры, включающей оборудование, системы управления и контроля за технологическими процессами, интегрированными в единое информационное пространство сети. По мере перехода к Индустрии 4.0 как новой парадигме технологического мироустройства, обеспечение кибербезопасности становится стратегической задачей для любого бизнеса. Принимая во внимание роль нефтегазового сектора в обеспечении доходов бюджета, вкладе в развитие территорий и колоссальном технологическом влиянии, важность защиты критической инфраструктуры от кибератак вкупе с растущим давлением международных санкций становится одной из фундаментальных задач интенсификации развития отрасли и противостояния вызовам и угрозам внешнего окружения в лице недружественных стран коллективного Запада, что обуславливает *актуальность и практическую значимость темы научной публикации*.

Методы. Подготовка научного исследования осуществлялась с использованием *общенаучных* (наблюдение, сравнение, измерение, анализ и синтез, метод логического рассуждения) и *специальных* (абстрагирование, анализ,

формализация, синтез, дедукция) методов. Для обеспечения объективности и беспристрастности научного исследования автором применялись верифицированные источники статистической *информации* и *аналитических материалов:* ежегодный статический сборник НИУ ВШЭ «Индикаторы цифровой экономики», «Индикаторы инновационного развития», публичные отчеты крупнейших российских нефтегазовых компаний, тематические публикации отечественных и зарубежных ученых и представителей бизнес-среды по указанной теме.

Ход исследования. *Цель научной публикации* выражается в оценке защищенности российского нефтегазового сектора от кибератак и выработке рекомендаций по совершенствованию управления кибербезопасностью объектов критической инфраструктуры. *Объектом* научного исследования является нефтегазовая отрасль России, *предметом* – процессы обеспечения кибербезопасности объектов критической инфраструктуры. Исходя из сформулированной выше цели были поставлены следующие задачи, определившие ход исследования: 1) подготовка теоретического раздела, посвященного характеристикам видов кибератак на критическую инфраструктуру нефтегазовой отрасли; 2) количественный и качественный анализ киберинцидентов в отношении нефтегазовых бизнесов и структура целей атак; 3) формирование предложений по совершенствованию управления кибербезопасностью объектов критической инфраструктуры.

Результаты и обсуждение. Генезис термина «кибербезопасность» восходит к научным работам американского аналитика Н. Негропонте, который, собственно, в 1995 г. и ввел его в научный оборот [1, С. 40]. Несмотря на длительность его применения, до сих пор существует плюрализм точек зрений касательно его сущности, что обусловлено наличием разрыва в технологическом и организационно-управленческом развитии в странах Запада и Востока, а также уровне проникновения информационно-компьютерных технологий в бизнес-процессы обеспечения нормального функционирования объектов инфраструктуры и управления ими. Так, в зарубежных академических

кругах кибербезопасность рассматривается преимущественно как самостоятельная ветвь корпоративной стратегии: например, П. Левинсон (*P. Levinson*) и Ф. Кристиано (*F. Cristiano*) определяют кибербезопасность как самостоятельный блок управления бизнес-моделью компании с целью обеспечения ее цифрового суверенитета [2, С. 171; 3, С. 29-30]. Р. Ж. Харкнет, М. Смит (*Harknett, R. J., & Smeets, M.*) трактуют кибербезопасность в энергетической сфере как системную работу по недопущению появления уязвимостей среди критически важных объектов инфраструктуры и оперативного устранения последствий уже свершившихся киберинцидентов [4, С. 38]. Согласно требованиям стандарта ISO/IEC 27032-2012 Руководство по кибербезопасности, это «сохранение конфиденциальности, целостности и доступности информации в киберпространстве». В отечественной академической литературе, например, в публикации М.Н. Дудина и С.В. Шкодинского, кибербезопасность трактуется как комплекс организационно-распорядительных и технических мер по недопущению киберинцидентов в отношении важнейших компонентов бизнес-модели компании [5, С. 58-59], т.е. в самом определении подчеркивается полная нетерпимость к рискам кибератак, что на практике маловероятно ввиду множественности их видов и очень быстрого эволюционирования. В публикациях А.Ю. Добродеева и Ю.А. Бекишева понятие «кибербезопасность» рассматривается как самостоятельная часть политики риск-менеджмента компании, направленная на анализ и управление киберрисками информационного пространства с целью недопущения их влияния на бизнес-процессы [6; 7], что еще раз подчеркивает отношение российского менеджмента к кибербезопасности как одному из многочисленных операционных рисков, управление которым возможно в рамках сложившейся модели риск-менеджмента.

Следующим этапом научного исследования является идентификация и описание наиболее значимых киберугроз для критической инфраструктуры нефтегазовой сферы на основе критического обзора аналитических публикаций авторитетных российских агентств в сфере кибербезопасности: Positive

Technologies и InfoWatch, а также Методических рекомендаций по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса (таблица 1).

Таблица 1. **Ключевые киберугрозы для критической инфраструктуры нефтегазовой отрасли**

Вид киберугрозы	Характеристика влияния на критическую инфраструктуру
1. Несанкционированный доступ к корпоративной информационной сети	Неавторизованный доступ третьих лиц в корпоративную информационную сеть может привести к изменению нормального функционирования бизнес-процессов, подмены управляющих сигналов, выведения из строя оборудования, утечку коммерческих и персональных данных, в особо сложных случаях – манипулирование комплексом операционных и управленческих бизнес-процессов.
2. Внедрение в ERP-систему компании вредоносных программных продуктов	Инкорпорация вредоносного программного обеспечения с целью нарушения работоспособности программ, хищения данных, блокирования работы и вымогательства вознаграждения приведет к нарушению ритмичности работы и возникновению финансовых потерь. В отдельных случаях возможно полное удаление данных, их кража или искажение с последующим проявлением в виде промышленных аварий.
3. Инфраструктурные атаки на IoT-сети (интернет вещей)	Киберугроза реализуется в отношении именно производственно-технологических процессов, направленных на провоцирование техногенных катастроф или манипулирование процессами управления т.н. «цифровыми двойниками» - виртуальными копиями месторождений и удаленного управления буровыми процессами.
4. Использование уязвимостей и «черных ходов» импортных программных продуктов	Импорт программного обеспечения из-за рубежа несет в себе скрытые риски наличия сознательно сделанных уязвимостей в программном коде для доступа санкционированных государством хакеров и нарушения нормального функционирования работы бизнес-процессов нефтегазовой компании. Масштаб негативного влияния колеблется от простого шпионажа и копирования данных до провокаций с целью создания промышленных аварий.
5. Продажа хакерских инструментов с открытым кодом для организации массовых индивидуальных атак	В сегменте DarkNet имеются в продаже конструкторы для создания хакерских программ или сценариев атак, реализуемых индивидуальными хактивистами в отношении государственных корпораций как форма выражения «гражданской позиции». При их как правило невысокой квалификации, основная опасность связана с их массовостью и сложностью идентификации, что приводит к перегрузке корпоративной системы информационной безопасности и распылению ресурсов на «ложные угрозы», в то время как может быть совершена мощная высококлассная и спланированная кибератака.

Особенностями отечественной бизнес-модели кибербезопасности в нефтегазовой сфере является одновременное сосуществование традиционных механистических процессов управления критической инфраструктурой (месторождения, буровая и нефтесервисная инфраструктура, логистические каналы) на старых месторождениях, введенных в эксплуатацию до принятия Правительством в 2017 г. национальной программы «Цифровая экономика» и масштабных процессов сквозной цифровизации на новых месторождениях, что создает значительные сложности по интеграции всех объектов в единую систему обеспечения кибербезопасности. *Во-вторых*, нефтегазовая отрасль является одним из ключевых объектов международных санкций, часть из которых направлена на запрет трансферта программного обеспечения, его обновления и пролонгации лицензий, что повышает его уязвимость ввиду отсутствия своевременного обновления. *В-третьих*, принятие Правительством Постановления «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» № 1236 от 16.11.2015 г. (в ред. от 28.12.2022 г.) создал существенные затруднения как для отечественной нефтегазовой, так и IT-сферы, которые оказались не готовы к столь масштабному импортозамещению: по данным на конец 2022 г. уровень импортозависимости составил от 80% в мидстриме (транспортировка и хранение) до 90% в разведочных и проектировочных процессах [8, С. 69-70; 9].

В составе аналитического раздела публикации автором был подготовлен обзор индикаторов для оценки уровня кибербезопасности в нефтегазовой сфере (таблица 2).

Таблица 2. **Индикаторы уровня кибербезопасности в нефтегазовой сфере в 2017 – 2022 гг.**

Индикаторы	2017г.	2018г.	2019г.	2020г.	2021г.	2022г.
1. Общее число зафиксированных кибератак на нефтегазовую отрасль, ед. *В том числе по объектам атак*:	27	40	125	239	208	223
1.1 Оборудование, оснастка, управляемая удаленно через Internet	3	4	29	86	48	29
1.2 ERP-системы управления бизнес-процессами	6	10	43	69	72	88
1.3 ЦОДы, инфраструктура связи и передачи данных	5	8	25	47	55	63
1.4 Расчетно-финансовая группа	9	11	9	14	18	21
1.5 Библиотеки данных и технологических решений, чертежей, инновационных разработок	4	7	19	23	15	22
2. Уровень успешности кибератак на объекты критической инфраструктуры, в % к общему количеству атак	16,2	13,4	10,2	19,4	25,7	30,3
3. Уровень защищенности крупнейших нефтегазовых бизнесов от кибератак, в % к итогу (*расчет по методологии пентестов PT Research)*	62,7	59,5	54,4	57,3	58,2	51,6
4. Оценочные потери нефтегазового бизнеса от кибератак, млрд. руб.	72,4	86,9	124,7	238,5	178,6	331,2
5. Расходы нефтегазового бизнеса на кибербезопасность, млрд. руб.	216,8	335,4	279,2	244,6	316,3	425,7
6. Индекс эффективности киберзащиты (стр.4 / стр.5)	0,33	0,26	0,45	0,98	0,56	0,78
7. Уровень инновационной активности в отрасли, % *В том числе*:	11,2	13,7	12,4	12,1	15,0	…
7.1 Создание организационных, процессных и управленческих инноваций	3,2	2,7	4,4	4,8	5,6	…

Как следует из приведенных в таблице расчетов, в анализируемом периоде отмечается рост количества кибератак на нефтегазовые бизнесы с 27 фактов в 2017 г. до 223 ед. в 2022 г., при этом в статистическую выборку попадают только те, о которых было официально заявлено менеджментом самих компаний, т.е. фактически их может быть больше. В части структуры атакуемых объектов основное внимание уделяется ERP-системам управления бизнес-процессами – среднее количество атак составило 48 ед., на втором месте – ЦОДы, инфраструктура связи и передачи данных (34 ед), на третьем – оборудование, оснастка, управляемая удаленно через Internet (33 ед), что

позволяет сделать вывод о целенаправленности атак именно на критическую производственную и управленческую инфраструктуру.

Негативным фактом следует отметить рост индикатора успешности кибератак на объекты критической инфраструктуры в % к общему количеству атак: в 2022 г. по сравнению с 2017 г. он вырос на 14,2 п.п. с 16,2 % до 30,4%, при этом уровень защищенности крупнейших нефтегазовых бизнесов от кибератак, рассчитанных на основе пентестов PT Research снизился с 62,7% до 51,6 %, при этом, несмотря на рост расходов на кибербезопасность (прирост составил 96,4%) индекс эффективности киберзащиты также увеличился: 0,78 против 0,33, что говорит о принятии большинства компаниями «антикризисных мер», направленных на устранение уже выявленных уязвимостей, но не работу на опережение с целью недопущения самого киберинцидента.

В заключительной части аналитического раздела автором был подготовлен обзор индикаторов прямого и косвенного влияния международных санкций на кибербезопасность нефтегазовой отрасли (таблица 3).

Таблица 3. **Индикаторы прямого и косвенного влияния международных санкций на кибербезопасность нефтегазовой отрасли в 2017 – 2022 гг.**

Индикаторы	2017г.	2018г.	2019г.	2020г.	2021г.	2022г.
1. Общее количество санкций против нефтегазового сектора, ед. *В том числе по видам, относящимся к кибербезопасности*:	39	51	24	72	72	489
1.1 Заморозка контрактов / запрет на поставку нефтесервисного оборудования и систем управления бизнес-процессами	9	18	24	39	27	216
1.2 Заморозка/ разрыв контрактов на трансферт ИКТ в сфере управления и киберзащиты	13	…	…	5	8	49
1.3 Заморозка информационно-технического обмена геоданными	…	4	…	…	5	11
1.4 Ограничение / запрет мобильности кадров, обмена управленческими компетенциями	7	9	5	…	…	26
2. Оценочная сумма недоинвестированного капитала в инфраструктурные и сервисные продукты, сервисы и решения, млрд. руб.	99,2	158,9	112,9	86,8	133,4	211,8
3. Удельный вес импортных ИКТ в	25,9	28,8	33,5	37,2	39,5	52,6

сфере безопасности, попавших под эмбарго, %						
4. Удельный вес технологий-субститутов, полученных в рамках импортозамещения, в % к итогу	4,8	5,9	11,7	16,8	19,2	25,3
4. Количество совместных инвестиционных проектов технологической направленности, приостановленных / замороженных в связи с санкциями, всего, ед. *В том числе*:	18	17	13	16	19	45
4.1 Группа проектов в сфере кибербезопасности и цифровой трансформации бизнес-процессов	…	…	5	7	9	16

Основываясь на полученных результатах, можно сделать следующие выводы о влиянии международных санкций на кибербезопасность нефтегазовой отрасли:

1) основное деструктивное влияние на показатели устойчивости отрасли к кибератакам вызвано заморозкой контрактов, запретом на поставку нефтесервисного оборудования и систем управления бизнес-процессами, что постепенно привело к ослаблению периметра информационного пространства и повысило его уязвимость перед внешней средой [10; 11];

2) несмотря на популярность суждения среди стран коллективного Запада о разрушительности влияния санкций на технологический трансферт и запрета доступа российским компаниям к геоданным, в реальности данный фактор оказался не ключевым, что связано как с активными процессами импортозамещения систем управления путем разработки сугубо отечественных аналогов (например, роботизированный комплекс «ЭРА.Оптима» для комплексного управления процессами нефтедобычи, программный комплекс «Когнитивный геолог»; пилотный запуск прототипа цифровой платформы, основанной на лучших практиках оптикализации промышленных объектов);

3) вопреки растущему удельному весу импортных ИКТ в сфере безопасности, попавших под эмбарго (52,6% против 25,9% соответственно), российскими субъектами инновационной инфраструктуры совместно с крупнейши-

ми высокотехнологичными государственными корпорациями: Ростех, Росатом, – достигнуты существенные успехи в области выпуска технологий-субститутов: 25,3% против 4,8% соответственно, что позволяет отметить системный характер, а главное продуктивность работы по обеспечению кибербезопасности в нефтегазовой отрасли страны;

4) важно отметить и «коварность корпоративной политики зарубежных компаний-поставщиков ИКТ в сфере кибербезопасности: вплоть до 2019 г. официальных заявлений об эмбарго на поставки данной группы технологий не было, что свидетельствует о высокой политизированности санкций и их неэтичности, которая ставит под угрозу экологическое и социальное благополучие не только огромных территорий России и проживающих на ней граждан, но в среднесрочной перспективе и целого евразийского региона, т.к. возможные техногенные аварии приведут к необратимым изменениям флоры и фауны [11; 12].

Исходя из проведенной оценки кибербезопасности в нефтегазовой сфере России в условиях международных санкций, автором были сформулированы следующие предложения по ее повышению и укреплению:

1) заключение государственным регулятором – Министерством энергетики – в рамках государственных закупок долгосрочных партнерских договоров в форме концессий на разработку, внедрение и комплексное обслуживание программных продуктов антивирусного назначения, а также специальной инфраструктуры для обеспечения кибербезопасности. Потенциальными партнерами могут стать: Positive Technologies, Лаборатория Касперского, ГК«Цитадель», СОРМ «МФИ Софт», АДМ Системс. Данное предложение направлено не только на импортозамещение программных продуктов для защиты объектов критической инфраструктуры, но и поощрения инновационной деятельности отечественных IT-компаний;

2) развитие межфирменной кооперации нефтегазовых компаний с субъектами инновационной инфраструктуры (технопарки, технополисы, венчурные фонды) для финансирования проектов в области информационной без-

опасности. Уже действующим кейсом является созданный корпоративный стартап-акселератор StartupDrive от «Газпром нефти», занимающийся отбором и финансированием стартап-проектов в сфере цифровой трансформации бизнес-процессов управления под запросы головной компании; вторым примером является созданный в составе нефтегазового холдинга дочерний бизнес – Центр управления информационной безопасности ООО «ЛУКОЙЛ-Технологии», отвечающий за разработку, внедрение и эксплуатацию программного обеспечения в сфере информационной безопасности;

3) создание отраслевого комплекса фильтрации информационных потоков – файервола – для обеспечения первичной защиты от кибератак всех бизнесов в отрасли, независимо от их размера и политики в сфере информационной безопасности. Реальным кейсом применения такого инструмента стала инициализация ARMA Industrial Firewall в нефтегазовом холдинге «Газпром», созданный российского компанией InfoWatch. Его рекомендуется масштабировать сначала для компаний, входящих в ТОП-10 крупнейших компаний, а в перспективе – на всю отрасль.

Область применения результатов. Результаты научного исследования проблемы обеспечения кибербезопасности в нефтегазовой сфере могут быть применены при формировании прогнозов и сценариев развития отрасли, а также нефтегазовыми бизнесами при разработке корпоративных стратегий устойчивого развития и противодействия вызовам и угрозам цифровой трансформации в условиях международных санкций.

Выводы. По результатам проведенного научного исследования управления кибербезопасностью в нефтегазовой сфере России в условиях международных санкций было установлено, что кибербезопасность рассматривается менеджментом как один из многочисленных операционных рисков, управление которым возможно в рамках сложившейся модели риск-менеджмента, что обусловлено одновременным сосуществованием традиционных механистических процессов управления критической инфраструктурой и масштабных процессов сквозной цифровизации на новых месторождениях, что созда-

ет значительные сложности по интеграции всех объектов в единую систему обеспечения кибербезопасности, введёнными запретами трансферта программного обеспечения, его обновления и пролонгации лицензий, существенными затруднениями обеспечения своевременного импортозамещения как для отечественной нефтегазовой, так и IT-сферы.

Исходя из проведенной оценки кибербезопасности в нефтегазовой сфере России в условиях международных санкций, автором были сформулированы следующие предложения по ее повышению и укреплению: заключение Министерством энергетики в рамках государственных закупок долгосрочных партнерских договоров в форме концессий на разработку, внедрение и комплексное обслуживание программных продуктов антивирусного назначения; развитие межфирменной кооперации нефтегазовых компаний с субъектами инновационной инфраструктуры (технопарки, технополисы, венчурные фонды) для финансирования проектов в области информационной безопасности; создание отраслевого комплекса фильтрации информационных потоков – файервола – для обеспечения первичной защиты от кибератак всех бизнесов в отрасли, независимо от их размера и политики в сфере информационной безопасности.

Список источников

1. Алпеев, А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 5. С. 39 – 43.
2. Levinson P. Micro-cyberwar vs. macro-cyberwar: towards the beginning of a taxonomy. *Digital War*. 2020, 1(1–3):171–172. DOI:10.1057/s42984-020-00020-z
3. Cristiano F. From Simulations to Simulacra of War: Game Scenarios in Cyberwar Exercises. *Journal of War and Culture Studies*, 2018, 11(1):22–37. DOI: 10.1080/17526272.2017.1416761
4. Harknett R. J., & Smeets M. Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, 2020, 4:36–42. DOI:10.1080/01402390.2020.1732354

5. Дудин М. Н., Шкодинский С. В. Вызовы и угрозы цифровой экономики для устойчивости национальной банковской системы. Финансы: теория и практика. 2022;26(6):52-71. DOI: 10.26794/2587-5671-2022-26-6-52-71

6. Добродеев, А.Ю. Кибербезопасность в Российской Федерации. модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века // Вопросы кибербезопасности. 2021. № 4. С. 61 – 72. DOI: 10.21681/2311-3456-2021-4-61-72

7. Бекишев, Ю.А., Куликов, Д.А., Писаренко, Ж.В. Риски кибератак на предприятия, входящие в реальный сектор экономики стран // Московский экономический журнал. 2022. № 4. С. 616 – 628. DOI: 10.55186/2413046X_2022_7_4_247.

8. Малых, О.Е., Ходковская, Ю.В. Влияние цифровых технологий на капитализацию нефтегазового бизнеса // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика. 2020. № 4. С. 66 – 71.

9. Разманова С.В. Нефтесервисные компании в рамках цифровизации экономики: оценка перспектив инновационного развития / С.В.Разманова, О.В.Андрухова // Записки Горного института. 2020. Т. 244. С. 482-492. DOI: 10.31897/PMI.2020.4.11

10. Субботин А.С. Вопросы информационной безопасности вертикально-интегрированных нефтяных компаний в условиях цифровизации // Креативная экономика. 2021. Т.15. № 12. С. 5005-5014. DOI:10.18334/ce.15.12.114004.

11. Лившиц, И.И. Практика управления киберрисками в нефтегазовых проектах компаний холдингового типа // Вопросы кибербезопасности.2020. № 1. С. 42 – 51.

12. Biro M., Mashkoor A., Sametinger J., Seker R. Software Safety and Security Risk Mitigation in Cyber-physical Systems // IEEE Software. 2018. vol. 35. no. 1. pp. 24-29. DOI: 10.1109/MS.2017.4541050

References

1. Alpeev, A.S. Security terminology: cybersecurity, information security // Issues of cybersecurity. 2014. No. 5. P. 39 – 43.

2. Levinson P. Micro-cyberwar vs. macro-cyberwar: towards the begin-ning of a taxonomy. digital war. 2020, 1(1–3):171–172. DOI:10.1057/s42984-020-00020-z

3. Cristiano F. From Simulations to Simulacra of War: Game Scenarios in Cyberwar Exercises. Journal of War and Culture Studies, 2018, 11(1):22–37. DOI: 10.1080/17526272.2017.1416761

4. Harknett R. J., & Smeets M. Cyber campaigns and strategic outcomes. Journal of Strategic Studies, 2020, 4:36–42. DOI:10.1080/01402390.2020.1732354

5. Dudin M. N., Shkodinsky S. V. Challenges and threats of the digital economy for the sustainability of the national banking system. Finance: theory and practice. 2022;26(6):52-71. DOI: 10.26794/2587-5671-2022-26-6-52-71

6. Dobrodeev, A.Yu. Cybersecurity in the Russian Federation. fashionable term or priority technological direction of ensuring national and international security of the 21st century // Issues of cybersecurity. 2021. No. 4. P. 61 – 72. DOI: 10.21681/2311-3456-2021-4-61-72

7. Bekishev, Yu.A., Kulikov, D.A., Pisarenko, Zh.V. Risks of cyber attacks on enterprises that are part of the real sector of the economy of countries // Moscow Economic Journal. 2022. No. 4. P. 616 – 628. DOI: 10.55186/2413046X_2022_7_4_247.

8. Malykh, O.E., Khodkovskaya, Yu.V. The impact of digital technologies on the capitalization of the oil and gas business. Vestnik UGNTU. Science, education, economics. Series: Economy. 2020. No. 4. P. 66 – 71.

9. Razmanova S.V. Oilfield service companies within the digitalization of the economy: assessment of the prospects for innovative development / S.V. Razmanova, O.V. Andrukhova // Notes of the Mining Institute. 2020. V. 244. S. 482-492. DOI: 10.31897/PMI.2020.4.11

10. Subbotin A.S. Issues of information security of vertically integrated oil companies in the context of digitalization // Creative Economy. 2021. V.15. No. 12. S. 5005-5014. DOI:10.18334/se.15.12.114004.

11. Livshits, I.I. Cyber risk management practice in oil and gas projects of holding companies // Issues of cybersecurity.2020. No. 1. S. 42 - 51.

12. Biro M., Mashkoor A., Sametinger J., Seker R. Software Safety and Security Risk Mitigation in Cyber-physical Systems // IEEE Software. 2018.vol. 35 no. 1.pp. 24-29. DOI: 10.1109/MS.2017.4541050

Для цитирования: Липатов А.Б. Управление кибербезопасностью в нефте-газовой сфере России в условиях международных санкций // Московский экономический журнал. 2023. № 6. URL: https://qje.su/otraslevaya-i-regionalnaya-ekonomika/moskovskij-ekonomicheskij-zhurnal-6-2023-24/