МРНТИ 82.01.33
УДК 65.012.8
https://doi.org/10.47649/vau.2021.v60.i1.06

Д.Ж.Битманов[1], **Н.А.Урузбаева**[2*]

[1]Алматы Менеджмент университет
050060 г. Алматы, Республика Казахстан
[2]Евразийский Национальныйуниверситет им. Л.Н. Гумилева
010000 г. Нур-Султан, Республика Казахстан
*e-mail: nazym_amen@mail.ru

РАЗРАБОТКА МЕХАНИЗМОВ КИБЕРБЕЗОПАСНОСТИ НА ФАРМАЦЕВТИЧЕСКИХ КОМПАНИЯХ КАЗАХСТАНА И ВЫГОДЫ ОТ ИХ ВНЕДРЕНИЯ (НА ПРИМЕРЕ ТОО «СК-ФАРМАЦИЯ»)

Данное исследование проведено нами с целью определения эффективных механизмов использования кибербезопасности для совершенствования системы дистрибуции в ТОО «СК-Фармация». Установлено, что для обеспечения эффективности системы единой дистрибуции в РК требуется более эффективная система кибербезопасности. Предложено дополнить систему, имеющую SIEM, сканером уязвимостей, а также выработать стратегию развития кибербезопасности. В рамках стратегии следует использовать более перспективный механизм по обеспечению кибербезопасности. Основными приоритетами эффективного механизма кибербезопасности определены: сохранение активов предприятия, снижение рисков, установление эффективной системы управления киберрисками и постоянное усовершенствование средств контроля и процессов за безопасностью. Такие механизмы по обеспечению киберустойчивости, как: поддержка высшего руководства, создание систем структурного подразделения и системы риск-менеджмента, проведение постоянного и всестороннего мониторинга, системы независимого аудита, оценка уровня зрелости и системы менеджмента в области киберустойчивости – должны помочь предприятию решить все поставленные стратегией задачи. А также получить выгоды при использовании новых цифровых технологий, в виде баланса риска и доходности, так как именно они позволяют в современных условиях нивелировать последствия от киберугроз.

Ключевые слова: кибербезопасность, механизмы безопасности, стратегия безопасности, защищённость.

Введение

Одной из актуальнейших задач достижения стабильного и успешного функционирования казахстанских фармацевтических компаний является наличие эффективных механизмов кибербезопасности их деятельности. В данной статье нами отражены результаты по исследованию выбора наиболее перспективных механизмов обеспечения кибербезопасности в ТОО «СК-Фармация». При этом мы основываемся на том, что, как таковой кибербезопасностью на данном предприятии никто не занимается (отсутствует постоянно действующий консультирующий орган и нет стратегии развития кибербезопасности). Такое положение в области кибербезопасности характерно и для многих казахстанских предприятий.

Ранее нами было установлено, что специфика механизма кибербезопасности в казахстанских фармкомпаниях, занимающихся дистрибуцией, определена принципами процесса дистрибуции фармацевтических средств, предусмотренных правилами GDP ЕАЭС. А типовые механизмы (принципы) обеспечения кибербезопасности в дистрибуторских фармацевтических компаниях предусмотрены стандартом ISO/IEK 27032:2012, который раскрывает основные стороны обеспечения кибербезопасности и дает предприятиям рекомендации, как решать имеющиеся проблемы в данной области [1]. На этих условиях и было основано наше исследование.

Основная часть

Прежде, чем приступать к определению перспективных механизмов по обеспечению

кибербезопасности в ТОО «СК-Фармация», нужно было обозначить, что официально принятого понятия механизма кибербезопасности нет. Оно не определено ни наукой, ни нормами законов. Краткое руководство по обеспечению безопасного киберпространства CyberLaw предлагает для внедрения некоторые довольно строгие стратегии относительно «создания механизмов для информационной безопасности», в которую входит, по нашему мнению, и механизм кибербезопасности. Исходя из этого руководства, основными механизмами обеспечения безопасности ИТ признаны меры безопасности, которые, в первую очередь, ориентированы на обеспечение связи, а также включают комплексные меры по обеспечению кибербезопасности [2, с.114].

Изученные научные и практические материалы [3; 4; 5; 6] позволяют нам понимать под механизмом кибербезопасности на предприятии систему, состоящую из совокупности имеющихся ресурсов и характеристики всего осуществляемого процесса, направленного на управление киберр искамии обеспечение кибербезопасности (методы, нормы, средства, формы и способы функционирования или воздействия на состояние ресурсов и объектов, входящих в систему). А также механизм определяется как система элементов, взаимосвязанных между собой и функционально «настроенных» на исполнение работ общего процесса по обеспечению кибербезопасности.

При определении эффективного механизма кибербезопасности нужно помнить, что на практике используются различные уровни опасности при киберугрозах. Основнымиявляются три уровня киберопасности (терроризма), которые выделены по версии агентства «Monterey») [7]. Обозначим их схематично (рисунок 1).

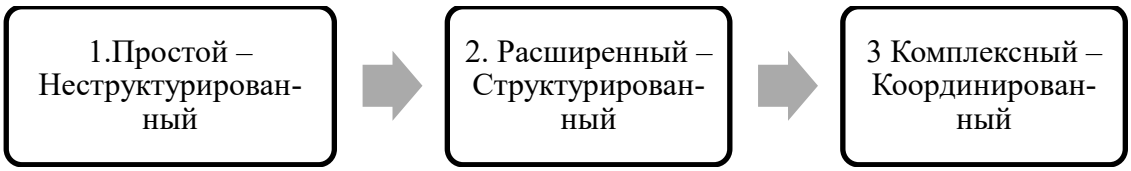

Рисунок 1. Уровни кибербезопасности

Ими являются: Простой – Неструктурированный; Расширенный – Структурированный и Комплексный – Координированный.

В результате исследования нами установлено, что механизм кибербезопасности в современных условиях должен быть комплексным и предполагающим активное взаимодействие всех его элементов. К тому же он должен быть адаптивным как к системе угроз, так и особенностям отрасли (в нашем случае дистрибуции). Основными приоритетами эффективного механизма кибербезопасности определены: сохранение активов предприятия; снижение рисков; установление эффективной системы управления киберрисками и постоянное усовершенствование средств контроля за процессами безопасности.

Для обеспечения эффективности всего механизма кибербезопасности рекомендовано разработать концепцию ее формирования и развития. Основной задачей концепции кибербезопасности предприятия является, в первую очередь, защита информации, в частности: обеспечение конфиденциальности имеющихся данных; обеспечение доступности данных; обеспечение целостности данных; обеспечение аутентичности данных.Исходя из этого, защита информации как средство контроля включает в себя следующее: распространение документов в электронной форме; недопущение несанкционированных рассылок от удаленных пользователей; обеспечение аутентичности документов от удаленных пользователей и другие вопросы.

Концепция стратегии кибербезопасности для ТОО «СК-Фармация», которая действует на медицинском и фармацевтическом рынках, в системе дистрибуции в форме стратегии

развития кибербезопасности имеет следующее содержание:

- актуальность разработки;
- место кибербезопасности в структуре ИС;
- понятийный аппарат;
- место в общей стратегии предприятия и в действующем законодательстве;
- цель;
- принципы, направления деятельности и меры по реализации.

Актуальность разработки для ТОО «СК-Фармация» определена, в первую очередь, все возрастающими киберугрозами на предприятиях медицинской и фармацевтической отрасли, особенно тех, что активно действует в системе дистрибуции. А также основана на понимании со стороны руководства того, что только на государственном уровне решить проблемы в области кибербезопасности невозможно. Кибербезопасность в современных условиях требует интеграции усилий и со стороны предприятия, региональной и национальной координации и различных форм сотрудничества. Актуальность определена и тем, что на данном предприятии еще не разрабатывалась подобная стратегия.

Кибербезопасность обычно описываться тремя составляющими, раскрывающими ее содержание и место в ИС: информационные ресурсы; компьютерная и сетевая инфраструктура; способы взаимодействия всех пользователей. Создаваемая система кибербезопасности призвана защищать активы предприятия и деятельность людей, которые отправляют информацию или получают ее из распространяемой технической инфраструктуры ИС и ИКТ. При этом нужно отметить, что в настоящее время на предприятии нет соответствующих структур, отвечающих за данный блок. Исходя из этого, его следует создать.

Важнейшими элементами мер реализации стратегии кибербезопасности на предприятии определены: мониторинг и обнаружение киберугроз; профилактика киберугроз и их предотвращение; быстрое реагирование на угрозы.

В рамках предложенной стратегии предложено внедрить на предприятиях «Концепцию по улучшению критической инфраструктуры кибербезопасности» (KPMG). Данный документ выступает в виде практического руководства для предприятий, желающих сформировать более эффективный механизм кибербезопасности, улучшив, тем самым, комплексные программы по общей безопасности. Данная концепция была сформирована Федеральным Правительством США для поддержки предприятий промышленности противостоять киберугрозам и атакам [8].

Основными ее этапами являются: идентификация; защита; ответные действия и восстановление. Данная концепция предусматривает трехэтапный подход, как логическая последовательность всех действий:

- сбор информации – ее результаты;
- анализ – его результаты;
- стратегия – ее результаты;
- дорожная карта – ее результаты.

На каждом этапе обозначены получаемые результаты, что важно для определения эффективности. К тому же такой подход гарантирует проведение на каждой фазе проверку результатов. Кроме сверки данных, в процессе модернизации инфраструктуры обеспечивается также участие всех заинтересованных сторон.

В рамках KPMG предлагается внедрить новую операционную модель IT. Данный механизм основан на технологическом прорыве, который направляет предприятие на мотивацию к постоянным изменениям. Новая операционная система ИТ предприятия ориентирована на потребителей (медицинские организации) и все заинтересованные стороны

(государство и поставщики).Основными компонентами новой операционной системы являются: сервисы, процессы, организация, управление, сорсинг и локация, управление эффективностью, персонал и компетенция. Роли IT реализуются в трех направлениях: Посредничество, Интеграция и Руководство в виде возможностей и решения.

Также предлагаются и другие механизмы по обеспечению кибербезопасности:

– проведение аудита информационной безопасности;

– проведение тестирование на киберпроникновение;

– механизм этичного взлома и расследования кибератак;

– механизм обеспечения качества, основан на обеспечении соответствия стандартам и протоколам по кибербезопасности;

– механизм обеспечения непрерывности бизнеса.

Последний базируется на анализе всех бизнес-процессов и разработке планов в формате BCP/DRP (см. рисунок 2).

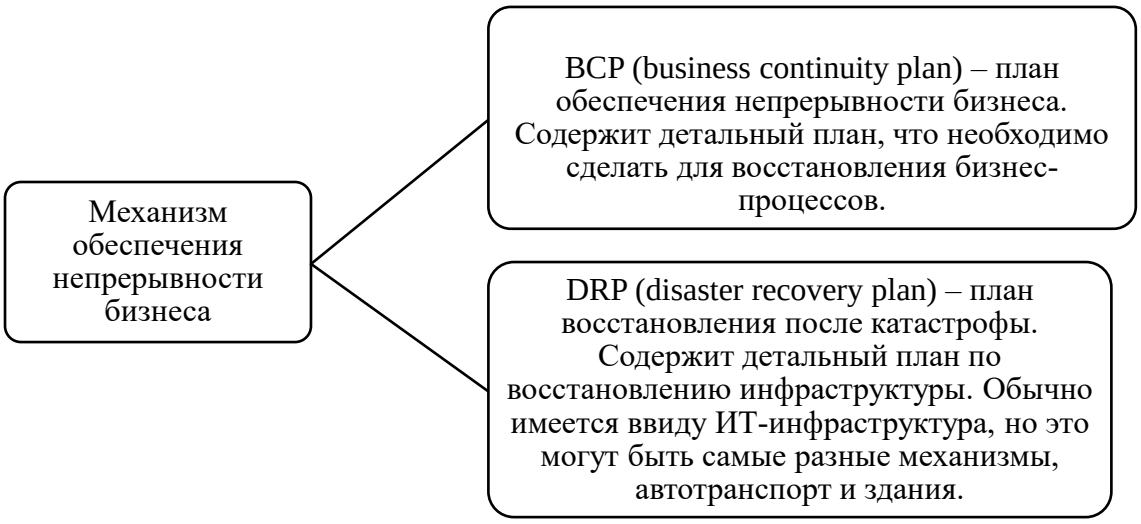

Рисунок2. Механизм обеспечения непрерывности бизнеса
Примечание: составлено согласно источника [9].

В рамках данного механизма проводится обучение всех специалистов, которые ответственны за реализацию планов, проводится тестирование на знание планов BCP/DRP.

Также предложена более универсальная и эффективная методика по оценке уровня зрелости киберустойчивости предприятия. Она предлагается компанией AXELOS, основана на 145 вопросах, относительно 5 доменов [10]. Также компания может применять как вопросы, предлагаемые методикой AXELOS, так и вопросы, разработанные специалистами компании или руководством компании.

Основной выгодой от предложенной стратегии и механизмов обеспечения кибербезопасности является условие, что предприятие признается киберустойчивым. Киберустойчивое предприятие работает стабильно, не имеет перерывов в основной деятельности, не несет дополнительных затрат на восстановление и так далее. При этом важно понимать, что обеспечить киберустойчивость возможно только при ее высоком уровне зрелости и успешности механизмов по обеспечению кибербезопасности. Будут реально достигнуты выгоды и при реализации следующих предложенных нами мероприятий (рисунок 3).

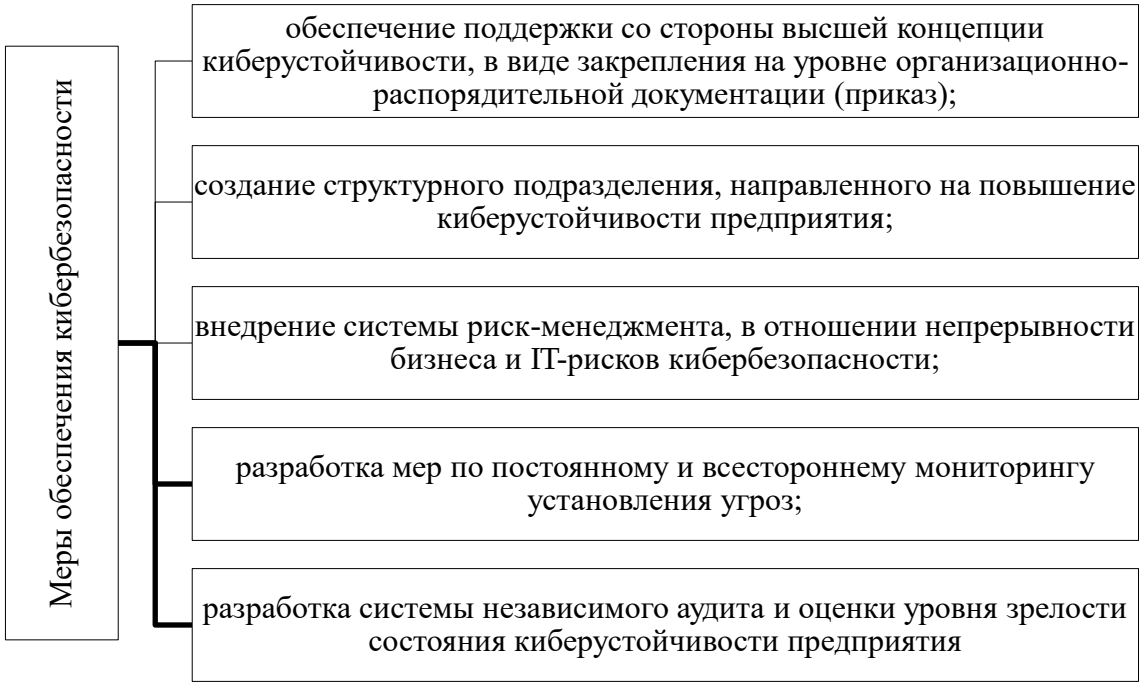

Рисунок 3. Меры обеспечения кибербезопасности

Важным является то, что эти меры способны позволить предприятию реагировать своевременно на угрозы и восстанавливаться при их реализации, а также непрерывно совершенствовать систему менеджмента предприятия в области киберустойчивости.Таким образом, мы установили, что механизм кибербезопасности для ТОО «СК-Фармация» должен характеризоваться комплексностью, что предполагает активное взаимодействие всех его элементов, а также является адаптивным к системе всех угроз и особенностям отрасли (в нашем случае дистрибуции).

Выводы

1. Предлагаемый новый подход позволил выделить более перспективные механизмы по обеспечению кибербезопасности в ТОО «СК-Фармация». Они направлены на обеспечение более эффективного использования ресурсов по обеспечению кибербезопасности и на недопущение существенных перебоев в операционной деятельности предприятия. Важно, чтобы они позволяли постепенно вырабатывать только успешные киберстратегии, с опорой на комплексное управление киберрисками (с учетом понимания важных бизнес-процессов и образа мыслей потенциальных злоумышленников).

2. Концепция по обеспечению кибербезопасности направлена на то, чтобы обеспечить предприятию успешную деятельность в условиях постоянного воздействия киберугроз на ее системы. Стратегия кибербезопасности, выработанная в рамках концепции, позволяет ей сформировать такие механизмы, которые позволяют своевременно предвидеть угрозы, противостоять (отражать) их, а также восстанавливаться в случае их происхождения.

3. Внедрение механизмов по обеспечению киберустойчивости, в рамках стратегии (от поддержки высшего руководства, структурного подразделения; системы риск-менеджмента; постоянного и всестороннего мониторинга; системы независимого аудита; оценки уровня зрелостии системы менеджмента предприятия) в области киберустойчивости) должно позволить решить предприятию все поставленные стратегией задачи. А также дает возможность получить выгоды, при использовании новых цифровых технологий, в виде

баланса риска и доходности, так как именно они позволяют в современных условиях нивелировать последствия от киберугроз. При этом выгоды от элементов по обеспечению кибербезопасности на предприятии во многом зависят от эффективности проводимого мониторинга по обнаружению киберугроз, профилактике и предотвращению киберугроз, быстрому реагированию на киберугрозы и возможностях предприятия на восстановление.

Список литературы

1 Руководящие указания по кибербезопасности в контексте ISO 27032.https://s3r.ru/wp-content/uploads/2014/03/iso27032.pdf

2 Новый подход к обеспечению кибербезопасности в сетевом мире. Исследование McKinsey, 2018. https://informburo.kz/stati/novyy-podhod-k-obespecheniyu-kiberbezopasnosti-v-setevom-mire-issledovanie-mckinsey.html

3 Горбунов Ю.В. О понятии «механизм» в экономических науках. – Барнаул. – С. 16-21

4 Энциклопедический словарь: современная версия / Ф. А. Брокгауз, И. А. Ефрон. – М. :Эксмо, 2002. – 672 с.

5 Райзберг Б. А. Современный экономический словарь / Райзберг Б.А., Лозовский Л. Ш., Стародубцева Е. Б. - 4-е изд. - М.: Инфра-М, 2004. – 478 с.

6 Теория систем и системный анализ в управлении организациями: справочник: учебное пособие / под ред. А. Н. Волковой и А. А. Емельянова. М.: Финансы и статистика, 2006. – 848 с.

7 Кибербезопасность (2017 – 2018): цифры, факты, прогнозы https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2017-2018/

8 Схема построения стратегии кибербезопасности KPMG –https://www.kbtu.kz/images/KPMG.pdf

9 BCP и DRP. Разница иногда не очевидна – https://habr.com/ru/post/312518/

10 Как разработать план аварийного восстановления (DisasterRecoveryPlan)https://mcs.mail.ru/blog/plan-avariynogo-vosstanovleniya-disaster-recovery-plan

ҚАЗАҚСТАНДАҒЫ ФАРМАЦЕВТИКАЛЫҚ КОМПАНИЯЛАРДАҒЫ КИБЕРҚАУІПСІЗДІК МЕХАНИЗМДЕРІН ДАМЫТУ ЖӘНЕ ОНЫ ЖҮЗЕГЕ АСЫРУДЫҢ ПАЙДАСЫ («СК-ФАРМАЦИЯ» ЖШС МЫСАЛЫНДА)

Бұл зерттеуді біз «СК-Фармация» ЖШС-да дистрибьютерлік жүйені жақсарту үшін киберқауіпсіздікті пайдаланудың тиімді механизмдерін анықтау мақсатында жүргіздік. Қазақстан Республикасында бірыңғай дистрибуция жүйесінің тиімділігін қамтамасыз ету үшін киберқауіпсіздіктің анағұрлым тиімді жүйесі қажет екендігі анықталған болатын. Жүйені осалдықтар сканерімен SIEM-мен толықтыру, сондай-ақ, киберқауіпсіздікті дамыту стратегиясын әзірлеу ұсынылатын болады. Стратегияда киберқауіпсіздіктің болашағы бар механизмі қолданылуы керек екендігі көрстеліген. Киберқауіпсіздіктің тиімді механизмінің негізгі басымдықтары айқындалды, осылар болып табылады: кәсіпорын активтерін сақтау, тәуекелдерді азайту, кибер тәуекелдерін басқарудың тиімді жүйесін құру, қауіпсіздікті бақылау мен процестерді үнемі жетілдіру сияқты. Кибер-тұрақтылықты қамтамасыз ету тетіктері осылар болып табылады, мысалы: топ-менеджментті қолдау, құрылымдық блоктар жүйесін құру және тәуекелдерді басқару жүйесін құру, үздіксіз және жан-жақты мониторинг, тәуелсіз аудит жүйесі, жетілу деңгейін бағалау және осы саладағы басқару жүйесі кибер тұрақтылығы кәсіпорынға стратегиямен қойылған барлық міндеттерді шешуге көмектесуі керек. Сондай-ақ, тәуекел мен кірістің тепе-теңдігі түрінде жаңа цифрлық технологияларды пайдалану кезінде артықшылықтарға қол жеткізуге болады, себебі дәл қазіргі кезде олар киберқауіптің салдарын бейтараптандыруға мүмкіндік береді.

Негізгі сөздер: киберқауіпсіздік, қауіпсіздік тетіктері; қауіпсіздік стратегиясы, қауіпсіздік.

DEVELOPMENT OF CYBERSECURITY MECHANISMS AT PHARMACEUTICAL COMPANIES IN KAZAKHSTAN AND BENEFITS FROM THEIR IMPLEMENTATION (ON THE EXAMPLE OF SK-PHARMACY LLP)

This study is carried out by us in order to determine effective mechanisms for using cyber security to improve the distribution system in SK-Pharmacy LLP. It has been established that a more effective cyber security system is required to ensure the effectiveness of the unified distribution system in the Republic of Kazakhstan. It is proposed to supplement the system with SIEM with a vulnerability scanner, as well as to develop a strategy for the development of cybersecurity. The strategy should use a more promising cyber security mechanism. The main priorities of an effective

cybersecurity mechanism are identified: preserving enterprise assets, reducing risks, establishing an effective cyber risk management system, and improving security controls and processes continuously. Mechanisms for ensuring cyber resilience, such as: support of top management, the creation of structural unit systems and a risk management system, continuous and comprehensive monitoring, an independent audit system, an assessment of the level of maturity and a management system in the field of cyber resilience should help the enterprise to solve all the tasks set by the strategy. And also to get benefits when using new digital technologies, in the form of a balance of risk and profitability, since it is they that allow, in modern conditions, to level the consequences of cyber threats.

Key words: cyber security, security mechanisms, security strategy, protection.

References

1 Rukovodjashhie ukazanija po kiberbezopasnosti v kontekste ISO 27032.https://s3r.ru/wp-content/uploads/2014/03/iso27032.pdf

2 Novyj podhod k obespecheniju kiberbezopasnosti v setevom mire. Issledovanie McKinsey, 2018. https://informburo.kz/stati/novyy-podhod-k-obespecheniyu-kiberbezopasnosti-v-setevom-mire-issledovanie-mckinsey.html

3 Gorbunov Ju.V. O ponjatii «mehanizm» v jekonomicheskih naukah. – Barnaul. – S. 16-21

4 Jenciklopedicheskij slovar': sovremennaja versija / F. A. Brokgauz, I. A. Efron. – M. :Jeksmo, 2002. – 672 s.

5 Rajzberg B. A. Sovremennyj jekonomicheskij slovar' / Rajzberg B.A., Lozovskij L. Sh., Starodubceva E. B. - 4-e izd. - M.: Infra-M, 2004. – 478 s.

6 Teorija sistem i sistemnyj analiz v upravlenii organizacijami: spravochnik: uchebnoe posobie / pod red. A. N. Volkovoj i A. A. Emel'janova. M. : Finansy i statistika, 2006. – 848 s.

7 Kiberbezopasnost' (2017 – 2018): cifry, fakty, prognozy https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2017-2018/

8 Shema postroenija strategii kiberbezopasnosti KPMG –https://www.kbtu.kz/images/KPMG.pdf

9 BCP i DRP. Raznica inogda ne ochevidna – https://habr.com/ru/post/312518/

10 Kak razrabotat' plan avarijnogo vosstanovlenija (Disaster Recovery Plan)https://mcs.mail.ru/blog/plan-avariynogo-vosstanovleniya-disaster-recovery-plan

Information about authors:

Didar Bitmanov, Master of Business Administration, Adviser to the Minister, Ministry of healthcare of the Republic of Kazakhstan, Mangilik el 8 Ave., House of Ministries, 5nd entrance, c. Almaty, Republic of Kazakhstan 050060, dida_b@bk.ru, +7 (7172) 74-28-19, +77000078777 ORCID: 0000-0002-5321-2029

Nazym Uruzbaeva**,** Doctor of Economics, Professor of the Department of Tourism, L. GumilyovEurasian National University, 2Satbayev street, c. Nur-sultan, Republic of Kazakhstan 010000, nazym_amen@mail.ru, +7 (7172) 70-95-00 (32-607), +77017789864, ORCID:0000-0003-2072-0788