РЕЗЮМЕ

В статье проанализированы основные проблемы, определяющие формирования рынка объектов интеллектуальной собственности, учет которых требует особого отношения государства и общества в целом к задаче становления и развития подобного рынка как основы активизации интеллектуального потенциала инновационного фактора экономического роста.

SUMMARY

The article analyzes the main problems that determine the formation of the market of intellectual property objects, the consideration of which requires a special attitude of the state and society as a whole to the task of establishing and developing such a market as the basis for enhancing the intellectual potential of the innovation factor of economic growth.

МРНТИ: 06.54.51
JEL: O33

CYBER RISK MANAGEMENT IN BANKS

S.D. Tashenova,
Doctor of economic science,
Central-Asian University,
Almaty, Kazakhstan

G.M. Berdikulova,
Candidate of economic science,
International IT University,
Almaty, Kazakhstan

M.K. Tuleubayeva
Candidate of economic science,
Egyptian University of Islamic Culture “Nur-Mubarak”,
Almaty, Kazakhstan

ABSTRACT

The aim of the research is to determine the most effective methods of managing cyber risks in the banking sector.

We used *the methods* of analysis and synthesis, statistical and factor analyzes, on the basis of which the cyber risks were evaluated, and conclusions were drawn that reflected the progress of implementation and the results of work to reduce these risks.

Despite the fact that many studies are devoted to cyber risks, especially recently, these processes in the Kazakhstan economy remain insufficiently studied.

The study revealed the main directions of reducing cyber risks. First of all, it is necessary to increase awareness of information security threats. In order to eliminate cyber risks in terms of country security, the number of domestic information security specialists should be increased. It is also necessary to increase the share of domestic ICT software products used in the state and quasi-state sectors.

Keywords: banking risks, informatization, cybersecurity, cyberrisk, digitalization

УПРАВЛЕНИЕ КИБЕРРИСКАМИ В БАНКОВСКОЙ СИСТЕМЕ

Ташенова С.Д.,
доктор экономических наук, профессор,
Центрально-Азиатский университет,
г. Алматы, Казахстан

Бердыкулова Г.М.,
кандидат экономических наук,
International IT University,
г. Алматы, Казахстан

Тулеубаева М.К.,
кандидат экономических наук,
Египетский университет исламской культуры Нур-Мубарак,
г. Алматы, Казахстан

АННОТАЦИЯ:
Целью исследования является определение наиболее эффективных методов управления киберрисками в банковской сфере.
В работе использовались методы анализа и синтеза, статистический и факторный анализы, на основе которых была произведена оценка киберрисков, и сделаны выводы, отображающие ход реализации и результаты работы по снижению этих рисков.
Несмотря на то, что киберрискам посвящены многие исследования, особенно в последнее время, остаются недостаточно изученными данные процессы в казахстанской экономике.
В результате исследования выявлены основные направления снижения киберрисков. В первую очередь, необходимо повышение осведомленности об угрозах информационной безопасности. В целях устранения киберрисков в плане страновой безопасности следует увеличивать количество отечественных специалистов в сфере информационной безопасности. Также необходимо увеличение доли отечественных программных продуктов в сфере ИКТ, используемых в государственном и квазигосударственном секторах.
Ключевые слова: банковские риски, информатизация, кибербезопасность, киберриски, цифровизация

ВВЕДЕНИЕ

Статья посвящена опыту и практике коммерческих банков в управлении киберрисками. Киберриски возникли в эпоху цифровизации и компьютеризации с появлением современной техники и информационных технологий. Проблема киберпреступности была обозначена как одна из глобальных мировых проблем. Инциденты, связанные с утечкой данных, как правило, вызывают цепную реакцию и значительный репутационный и финансовый ущерб. Трансформация бизнеса организаций в направлении создания цифровой среды ведет к росту киберугроз и рисков. «Киберриск» означает любой риск финансовых потерь, разрушения или ущерба для репутации организации в результате какого-либо сбоя в работе систем информационных технологий [1].

Банк является коммерческой организацией, деятельность которой функционирует под постоянными рисками. Наряду с традиционными финансовыми и нефинансовыми рисками в цифровой среде возник новый тип риска – как киберриск. Киберриск представляет собой риск, связанный с использованием компьютерного оборудования и программного обеспечения, как в локальной, так и в глобальной

сети Интернет, а также риски, связанные с накоплением, хранением и использованием персональных данных. Риски такого рода связаны с функционированием расчетно-платежных систем, системы интернет-торговли и систем управления производством. Как отмечают эксперты, угрозы, связанные с информационными рисками, столь же опасны, как и угрозы физическим активам компании или банка.

Для решения вопросов управления рисками и предотвращения угроз киберрисков поставлены следующие задачи:

- Раскрыть сущность, угрозы и вызовы киберрисков в банках;
- Цели оценки киберрисков;
- Ключевые проблемы Казахстана в кибербезопасности;
- Определение возможностей предотвращения киберрисков.

ОСНОВНЫЕ УГРОЗЫ И ВЫЗОВЫ КИБЕРРИСКОВ

На Всемирном экономическом форуме в Давосе проблема киберпреступности была обозначена как одна из глобальных мировых проблем. Как отмечают эксперты, угрозы, связанные с информационными рисками, столь же опасны, как и угрозы по физическим активам компании. Инциденты, связанные с утечкой данных, как правило, вызывают цепную реакцию и наносят значительный ущерб репутации и финансовому ущербу.

Преобразование бизнеса организаций в создание цифровой среды вызывает рост киберугроз и рисков. Согласно исследованиям Allianz, киберугрозы увеличились с 1% в 2011 году до 28% в 2016 году [2].

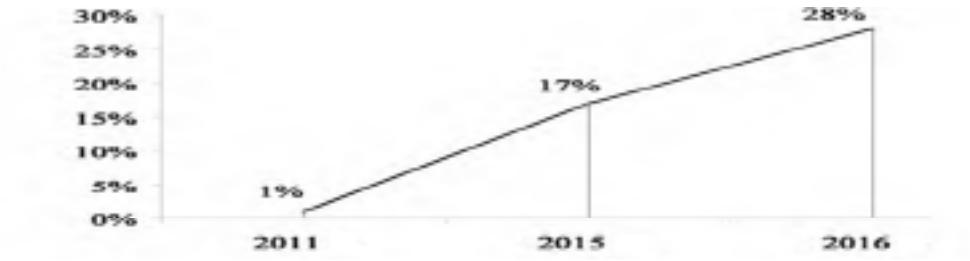

Рисунок 1 – Киберугрозы в мире за 2011-2016 гг.
Примечание: составлено авторами по источнику [2]

Нередко компании осознают риск, связанный с незаконным доступом к данным, но не располагают достаточными ресурсами для эффективного реагирования на действия преступников. В этом случае система страхования от кибер-рисков становится мощным барьером на пути киберпреступности.

Киберпреступность - это реальность рынка, так как индустрия мировой киберпреступности развивается большими темпами, особенно в финансовой сфере. Сейчас основным риском финансовой сферы является кибер-риск, вследствие концентрации финансовых средств в банках и других финансовых организациях [3].

Сейчас атака хакерских банков является международной проблемой и Казахстан также находится в тренде и зоне риска. За последние 10 лет технические возможности хакеров все время росли, в том числе через мобильные приложения.

Согласно исследованиям, проведенным «Лабораторией Касперского» и B2B International в 2014 году, DDoS-атаки на интернет-ресурсы компании могут привести к значительным убыткам - в среднем от 52 до 444 тысяч долларов в зависимости от размера предприятия. Такие непредвиденные обстоятельства для многих организаций являются серьезным препятствием. Атаки хакеров также могут нанести вред репутации предприятия из-за длительного отсутствия доступа к его онлайн-ресурсам и вылиться в дополнительные еще более серьезные финансовые потери [4].

Казахстанское правительство нацелено на цифровизацию и информатизацию ощества, в соответствии с чем разрабатывает программы, включающие в себя также вопросы кибербезопасности [5]. Исследование угроз киберрисков проведено по данным «Kaspi Bank», который использует максимальное количество приложений для осуществления своей деятельности и предоставления услуг населению. В результате исследования были определены критические риски для «Каспи Банка» и рассмотрена модель управления киберрисками. Данная модель нацелена на выяснение уровня рисков по процедурам целей, оценки и оценки рисков.

«Каспий Банк» является казахстанским розничным банком и занимает третье место по объему депозитов от физических лиц, 6-е место по размеру собственного капитала среди казахстанских банков на дату января 2017 года [6].

По данным Digital Kazakhstan-2020, любой хозяйствующий субъект трансформирует свою деятельность и бизнес-процессы. Kaspi Bank разработал три онлайн-сервиса на Kaspi.kz: «Платежи», «Мой Банк», «Магазин», благодаря которым можно оплачивать счета за различные услуги и осуществлять покупки [7].

С момента запуска «Kaspi Shop» казахстанцы купили более 115 тысяч товаров, в мае 2016 года было сделано более 15 тысяч покупок, что в 7 раз больше, чем в предыдущем году. Пользователи онлайн-сервисов «Kaspi.kz» могут осуществлять платежи без комиссий и покупки в кредит через приложение «Магазине», для которой предусмотрен «Кредит на покупки» [7].

Платежный оборот за время работы сайта составил более 33 миллиона платежей без комиссий на сайте «Kaspi.kz» с экономией более 3 миллиардов тенге национальной валюты.

Рисунок 2 – Динамика онлайн-платежей на «Kaspi.kz»
Примечание: составлено авторами по источнику [7]

Однако, увеличение электронной торговли и онлайн-сервисов увеличивает угрозы киберрисков для банка и его клиентов. «Каспи Банк» может обеспечить управление киберрисками на всех этапах жизненного цикла банковских процессов, чтобы обеспечить скорость, удобство и безопасность бизнес-процессов.

Модель управления киберрисками включает пять целей, три этапа оценки и определение уровня риска [8].

Таблица 1 – Цели оценки киберрисков

Цели	Содержание
Для построения модели оценки это даст объективное представление об уровне киберрисков.	Основная цель внедрения модели - не тратить ресурсы на снижение незначительных рисков, а направить усилия на обработку допустимого уровня рисков.
Построить простой и удобный процесс оценки.	Это особенно актуально для экспертов в области кибербезопасности, где процессы разработки и развертывания значительно ускоряются, требования к конечному продукту могут меняться каждую неделю, и нет возможности выделить более пяти минут для оценки рисков.
Учитывать мнения нескольких экспертов из разных областей.	Для получения объективных результатов предусмотрена возможность привлечения экспертов к оценке рисков для разных профилей, включая безопасность, бизнес и ИТ.

Создать универсальную модель, подходящую для разных видов деятельности.	Модель единообразия в оценке всех выявленных кибер-рисков. При практическом применении такой подход позволит объединить результаты всех оценок в единый рейтинг киберрисков и сравнить их, чтобы выяснить приоритетность рисков.
Предоставить возможность отслеживать динамику уровня риска при изменении внутренних или внешних факторов.	Уровни рисков изменяются одновременно с трансформацией угроз, условий защиты и роста бизнеса. Для понимания динамики изменения уровней риска планируется оценить влияние принимаемых решений на риск и изучить закономерности связи между изменениями размера риска и зарегистрированным фактическим ущербом.
Примечание: составлено авторами по источнику [8]	

Оценка кибер-риска происходит в три этапа.

Шаг 1. Формирование системных факторов риска. Эксперты определяют список соответствующих угроз, уязвимостей и мер защиты для каждого типа кибер-риска.

Шаг 2. Оценка факторов риска экспертами. Независимо друг от друга эксперты оценивают каждый фактор риска как четырехуровневую шкалу (рисунки 2 и 3). Критерии критичности разработаны с учетом масштабов бизнеса «Каспий Банк».

		Риск фактор		
Угроза (частота дополнения)	Уязвимость (частота дополнения)	Потенциал злоумышленника	Эффективность защитных мер	Вероятность
1 раз в день и чаще	1 раз в день и чаще	Как пользователи Как администрация Спецназ Террористические и криминальные группировки Хакеры	Незначительный	Событие обязательно произойдет
От 1 раза в день до 1 раза в месяц	От 1 раза в день до 1 раза в месяц	Конкурирующий Организации Разработчики программного обеспечения и технологий	Низкий	Событие, скорее всего, произойдет
От 1 раза в год до 1 раза в месяц	От 1 раза в год до 1 раза в месяц	Бывший сотрудник Третьи стороны Участие в контакте	Высокий	Событие может случиться
Меньше чем 1 раза в год	Меньше чем 1 раза в год	Стороны без квалификации	Очень высокий	Событие не произойдет

Рисунок 3 – Четырехуровневая шкала оценки риска угрозы

Примечание: составлено авторами

На этом же этапе определяется вес каждого фактора риска, чтобы уменьшить влияние на факторы риска, некритические для него. Пример: для риска утечки информации оценка ущерба от нарушения процессов может не учитываться, а параметр «категория информации» действует как решающий, и его вес должен быть увеличен. Вес факторов оценивается по шкале от одного до девяти.

Шаг 3. Расчет рейтинга киберрисков. Ключевое отличие модели от существующих качественных методов заключается в возможности объединить большое количество полученных мнений и шкал в одно значение рейтинга риска. В то время как классический табличный метод не позволяет оперировать таким количеством мнений экспертов. Для расчета рейтинга суммарного риска рекомендуется использовать матричный метод расчетов, который объединяет все качественно оцененные факторы в одно количественное значение для «Kaspi Bank». Это позволяет учесть участие экспертов и разброс их мнений, а также различие в шкалах, что повышает объективность оценки (рисунок 3).

			Риск фактор			
Категория информации	Критичность	Нарушение процессов	Клиенты и партнеры	Регуляторы	Репутация	Ущерб
Коммерческий секрет	Очень Критично	Сбои в нескольких процессах Минимизировать процессы и направления	Потеря доверия значительной части клиентов и партнеров. Возникновение судебных исков	Внеплановая проверка. Большие штрафы вплоть до прекращения действия лицензии	Федеральный и международный уровень	Высокое влияние
Банковская тайна, SPI	Высокая критичность	Сбои в одном процессе	Массовое недовольство клиентов. Отток части клиентов и партнеров	Штрафы. Повышенное внимание в виде писем и запросов	Интернет	Среднее влияние
Служебная информация	Критично	Будет влиять на скорость процессов, но не будет вызывать сбои	Недовольство клиентов не приводит к оттоку	Инструкция при проверке без наложения штрафов	Региональный уровень	Низкое влияние
Публичная информация	Не критично	Не повлияет	Недовольство единичных клиентов	Без последствий	Не произойдет	влияние

Рисунок 4 – Четырехуровневая шкала оценки информационного риска
Примечание: составлено авторами

Результатом оценки является оценка риска R, выраженная числом от 0 до 1 и соответствующая уровню риска, представленному на рисунке 4:

Уровень риска	Низкий	Средний	Высокий	Критичный
R	R<0,25	0,25≤R<0,5	0,5≤R<0,75	0,75≤R

Рисунок 5 – Результаты оценки риска
Примечание: составлено авторами

Пример результата оценки: рейтинги риска потери доступности сервиса и риска утечки информации равны 0, 61 и 0, 73 соответственно. Уровень риска обоих типов высокий, но риск утечки информации более критичен.

Убыток				
Высокий			критично	
Средний		высокий		
Низкий	средний			
Незначительный	низкий			
Возможность	Событие не произойдет	Событие может произойти	Событие скорей всего произойдет	Событие действительно произойдет

»

критично			
высокий			
средний			
низкий			
Событие не произойдет	Событие может произойти	Событие скорей всего произойдет	Событие действительно произойдет

Рисунок 6 – Модель оценки рисков для «Каспий Банка»
Примечание: составлено авторами

Таким образом, предлагаемая модель управления киберрисками, разработанная для Kaspi Bank», может быть использована в других казахстанских банках, с учетом особенностей каждого хозяйствующего субъекта. Наиболее важным ресурсом банков является информация, несанкционированное изъ-

ятие которой может нанести ущерб репутации банка и навредить клиентам и пользователям сервисов. В этих условиях предпочтительнее усилить работу по обеспечению сохранности информации, снизить влияние человеческого фактора и улучшить работу по предупреждению кибератак.

КЛЮЧЕВЫЕ ПРОБЛЕМЫ КАЗАХСТАНА В КИБЕРБЕЗОПАСНОСТИ

Как уже отмечалось, кибербезопасность является актуальной для Казахстана, поэтому основные проблемы в вопросах кибербезопасности можно сформулировать следующим образом [9]:

- Увеличение пользователей интернета;
- Недостаточная защита и информация по предотвращению киберугроз;
- Отсутствие достаточного количества отечественных разработок в области ИТ;
- Недостатки в защите информации о клиентах со стороны государственных органов;
- Транснациональный и трансграничный характер многих продуктов ИКТ;
- Милитаризация сферы ИКТ;
- Нехватка специалистов в области ИТ.

В Республике Казахстан с 2010 по 2016 год плотность пользователей интернета увеличилась с 36,1% до 75%, а количество пользователей мобильного интернета с 3 млн. 694 тыс. Практически утроилось и достигло 10 млн. 567 тыс. , Такое экспоненциальное увеличение числа пользователей Интернета повышает критичность и приводит к более заметным последствиям в случае отказа или вредного воздействия на технические средства.

Недостаточная осведомленность о методах защиты информации и недостаточное снабжение в системах защиты информации предприятий малого и среднего бизнеса, в том числе занятых в сфере оказания информационно-коммуникационных услуг, которые зачастую даже не могут оценить состояние принадлежащей информации и связи. Инфраструктура приводит к большому количеству не проанализированных событий и инцидентов информационной безопасности, усложняющих как предотвращение технологических уязвимостей, так и борьбу с преступниками, использующими ИКТ в качестве средства для совершения взлома.

Отечественный сектор ИТ-индустрии не вносит существенного практического вклада в программу диверсификации национальной экономики (менее 5 процентов продукции, используемой в государственном секторе, имеет казахстанское происхождение), а также культуру кибербезопасности, в том числе Производственная культура в сфере разработки и использования продукции не всегда является определяющей.

Меры, связанные с автоматизацией государственных функций и предоставлением государственных услуг в электронном виде, а также продолжающейся цифровизацией доступа к информации о деятельности органов государственной власти, несут в себе определенные риски. Низкокачественные услуги и приложения, предоставляемые гражданам и частным организациям в рамках «электронного правительства», включая машиночитаемые открытые данные, могут привести к нарушению прав и законных интересов граждан.

Транснациональный и трансграничный характер многих продуктов ИКТ и международная согласованность сетей общественных телекоммуникаций используются преступлением для совершения незаконных действий в отношении пользователей и операторов услуг ИКТ и владельцев интернет-ресурсов, размещенных в национальном сегменте. а также информационные системы, взаимодействующие с Интернетом.

Милитаризация сферы ИКТ, трудности, навязываемые некоторыми странами в доказательство участия государств в использовании ИКТ вопреки принципам международного права, вызванные в значительной степени стихийно развитым характером существующей международной системы контроля над Интернет, сохраняющийся цифровой разрыв между странами, препятствует формированию в мировом сообществе надежных международно-правовых инструментов предотвращения военного использования достижений в сфере информатизации и телекоммуникаций.

Существующая казахстанская модель школьного, среднего специального, высшего и послевузовского образования в области ИКТ, включая специализацию в сфере информационной безопасности, требует постоянного и тщательного анализа от всех заинтересованных лиц (включая Министерство образования и науки Республика Казахстан, высшие учебные заведения и потенциальные работодатели) на предмет соответствия современным требованиям общества и тенденциям обеспечения безопасного развития информационных технологий в типе динамичного развития этой области.

Концепция кибербезопасности «Cyber Shield Kazakhstan» («Кибер-щит») была выпущена в 2017 году. Целью Концепции является достижение и поддержание уровня безопасности электронных информационных ресурсов, информационных систем, информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, обеспечивающих устойчивое развитие Республики. Казахстан в условиях глобальной конкурентоспособности [10].

Таблица 2 – Ожидаемые результаты Cyber Shield в Казахстане в 2017-2022 гг.

Индикатор	2018	2019	2020	2021	2022
Глобальный индекс кибербезопасности	0,300	0,400	0,500	0,550	0,600
Повышение осведомленности об угрозах информационной безопасности		5%,	10%,	15%,	20%
Количество подготовленных специалистов в сфере информационной безопасности	300	500	600	700	800
Увеличение доли отечественных программных продуктов в сфере ИКТ, используемых в государственном и квазигосударственном секторах	10%	20%	30%	40%	50%
Доля использования отечественных сертификатов безопасности при передаче закодированных данных интернет-ресурсами с доменом. Казахстан и Азербайджан	20%	40%	60%	80%	100%
Доля использования отечественных сертификатов безопасности при передаче закодированных данных интернет-ресурсами с доменом. Казахстан и Азербайджан	20%	40%	60%	80%	100%
Примечание: составлено по данным источника [10]					

Обновленный Глобальный индекс кибербезопасности сделал 2017 год Международным союзом электросвязи (таблица 2). Рейтинг представляет собой опрос, основанный на пяти ключевых показателях: законодательная база, технические характеристики, организационные вопросы, улучшение качества и сотрудничество. На их основе Международный союз электросвязи составляет список по уровню приверженности государств вопросам обеспечения кибербезопасности [9].

Всего в Глобальном индексе кибербезопасности было рассмотрено 193 страны, из которых Казахстан занял 83-е место в рейтинге по определению уровня кибербезопасности. Республика получила 0,352 балла и улучшила свои позиции по сравнению с предыдущим рейтингом 2014 года (0,177 балла).

Среди государств Евразийского экономического союза (ЕАЭС) позиции распределились следующим образом [9]:

- Россия - 10 место (0,788 балла);
- Беларусь - 39-е место (0,592);
- Казахстан - 83-е (0,352);
- Кыргызстан - 97-е место (0,27);
- Армения - 111-е место (0,196).

В ТОП-5 вошли Сингапур, США, Малайзия, Оман и Эстония. Центральноафриканская Республика, Йемен и Республика Экваториальная Гвинея закрыли рейтинг [9].

Таким образом, Казахстан в сфере кибербезопасности сталкивается с такими серьезными угрозами, как:

− низкая правовая грамотность населения, работников сферы ИКТ и руководителей организаций по информационной безопасности;

− нарушение информатизации государственными и негосударственными субъектами и пользовате-

лями услуг в сфере ИКТ установленных требований, технических стандартов и правил сбора, обработки, хранения и передачи информации в электронном виде;

− непреднамеренные человеческие ошибки и технологические сбои, оказывающие негативное влияние на информационные системы, программное обеспечение и другие элементы информационно-коммуникационной инфраструктуры;

− действия международных преступных групп, сообществ и частных лиц по осуществлению хищений в финансово-банковской сфере, вредное воздействие за нарушение работы автоматизированных систем управления процессами промышленности, энергетики, связи и в сфере информационно-коммуникационных услуг;

− деятельность политических, экономических, террористических структур, спецслужб и спецслужб иностранных государств направлена против интересов Республики Казахстан путем оказания разведывательного и взрывного воздействия на информационно-коммуникационную инфраструктуру.

Помимо перечисленных задач, определенную озабоченность вызывают операции с электронными деньгами, механизм которых не исследован до конца. Казахстанские коммерческие банки еще не так активно работают на этом рынке, так как законодательством предусмотрен выпуск электронных денег только под руководством Национального банка. Также остается немало вопросов в межгосударственном регулировании операций с электронными деньгами [11; 12].

Казахстан в своей деятельности по снижению рисков или предотвращению проявления их негативных последствий опирается на опыт других стран, которые также делают акцент на повышении корпоративной социальной ответственности [13]. В первую очередь это проявляется в ведении бизнеса с пользой для общества, в том числе при внедрении и использовании инновационных технологий и техники. Развитие инноваций следует проводить в соответствии с общеэкономическими целями не только отдельных стран, но и всего мирового сообщества [14].

Работа по предотвращению киберрисков проводится практически всеми организациями, так как связана не только с материальным ущербом, но и потерей репутации или имиджа. Каждая организация выбирает свой путь, но общие рекомендации, приведенные в данной статье, призваны обобщить опыт противодействия киберрискам в банковской системе и определить наиболее общие методы борьбы с киберпреступлениями.

СПИСОК ЛИТЕРАТУРЫ

1 Cyber risk and risk management. (2018).Institute of Risk Management. https://www.theirm.org

2 Allianz Risk Barometer (2016). Reports. http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2016/

3 Клеменкова К. Кибератаки на казахстанские банки (2017). https://ru.sputniknews.kz/economy/2017

4 Кремер К. Кибер риски – это серьезно (2016). https://www.aig.ru/content/dam/aig/emea/russia/documents/brochures/sst-aig-or-5-brochure.pdf

5 Государственная программа «Цифровой Казахстан». Постановление Правительства Республики Казахстан от 12 декабря 2017 года № 827. // http://www.akorda.kz/ru/official_documents/strategies_and_programs

6 Сведения о финансовых показателях (2017). Финансовые показатели банков второго уровня по состоянию на 01.01.2017. http://stat.gov.kz/faces/homePage

7 Клиенты Kaspi Bank выбирают online сервисы (2016). https://forbes.kz/finances/finance/klientyi_kaspi_bank_vyibirayut_onlayn-servisyi/

8 Симачевская Н. Как сберечь миллионы: модель оценки киберрисков (2017). // https://bosfera.ru/bo/kak-sberech-million-model-ocenki-kiberriskov

9 Global Cybersecurity Index (GCI) .(2017). // https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

10 Об утверждении Концепции кибербезопасности («Киберщит Казахстан»). Постановление Правительства Республики Казахстан от 30 июня 2017 года №407. // https://zakon.uchet.kz/rus/docs/P1700000407

11 T.Ashimbayev, S. Tashenova, Prospects for Using Cryptocurrency in the Economy of Kazakhstan and the Attitude of the National Bank // European Research Studies Journal Volume XXI, Issue 4, 2018 pp. 524-532.

12 T.Ashimbayev, S. Tashenova, Y.Sadvakassov, A. Karshalova, (2018) Trends in developing financial innovations in the course of the economic development in Russia // «Academic Research Publishing Group» Germany-Pakistan, pp. 44-51.

13 Юрасов И. А., Бондаренко В. В., Юдина В. А., Кузнецова Т. А. Корпоративная социальная ответственность. Учебник. - М.: Инфра-М, 2015. - 234 с.

14 Бердалиев К. Б. Управляемое прогнозирование и развитие экономики // КазЭУ Хабарщысы / Вестник КазЭУ (Специальный выпуск). – 2013. – с. 28-37.

REFERENCES

1. Cyber risk and risk management. (2018).Institute of Risk Management. https://www.theirm.org

2. Allianz Risk Barometer (2016). Reports. http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2016/

3. Klemenkova K. Kiberataki na kazahstanskie banki (2017). https://ru.sputniknews.kz/economy/2017

4. Kremer K. Kiber riski – eto ser'ezno (2016). https://www.aig.ru/content/dam/aig/emea/russia/documents/brochures/sst-aig-or-5-brochure.pdf

5. Gosudarstvennaya programma «Cifrovoj Kazahstan». Postanovlenie Pravitel'stva Respubliki Kazahstan ot 12 dekabrya 2017 goda № 827. // http://www.akorda.kz/ru/official_documents/strategies_and_programs

6. Svedeniya o finansovyh pokazatelyah (2017). Finansovye pokazateli bankov vtorogo urovnya po sostoyaniyu na 01.01.2017. http://stat.gov.kz/faces/homePage

7. Klienty Kaspi Bank vybirayut online servisy (2016). https://forbes.kz/finances/finance/klientyi_kaspi_bank_vyibirayut_onlayn-servisyi/

8. Simachevskaya N. Kak sberech' milliony: model' ocenki kiberriskov (2017). // https://bosfera.ru/bo/kak-sberech-million-model-ocenki-kiberriskov

9. Global Cybersecurity Index (GCI) .(2017). // https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

10. Ob utverzhdenii Koncepcii kiberbezopasnosti («Kibershchit Kazahstan»). Postanovlenie Pravitel'stva Respubliki Kazahstan ot 30 iyunya 2017 goda №407. // https://zakon.uchet.kz/rus/docs/P1700000407

11. T.Ashimbayev, S. Tashenova, Prospects for Using Cryptocurrency in the Economy of Kazakhstan and the Attitude of the National Bank // European Research Studies Journal Volume XXI, Issue 4, 2018 pp. 524-532.

12. T.Ashimbayev, S. Tashenova, Y.Sadvakassov, A. Karshalova, (2018) Trends in developing financial innovations in the course of the economic development in Russia // «Academic Research Publishing Group» Germany-Pakistan, rr. 44-51.

13. Yurasov I. A., Bondarenko V. V., YUdina V. A., Kuznecova T. A. Korporativnaya social'naya otvetstvennost'. Uchebnik. - M.: Infra-M, 2015. - 234 s.

14. Berdaliev K. B. Upravlyaemoe prognozirovanie i razvitie ekonomiki // KazEU Habarshchysy / Vestnik KazEU (Special'nyj vypusk). – 2013. – s. 28-37.

ТҮЙІН

«Банк жүйесіндегі киберқауіптерді басқару» мақаласында ақпараттық қауіпсіздік пен кибершабуылға байланысты тәуекелдер көрсетілген. Бұл проблема ақша және әртүрлі мәселелер бойынша ақпарат

шоғырланған банк жүйесі үшін әсіресе өзекті. Материалдық және материалдық емес активтердің қауіпсіздігі мәселелері «адам факторы» ескеріле отырып, басқарудың және орындалудың барлық деңгейлерінде шешіледі.

РЕЗЮМЕ

В статье «Управление киберрисками в банковской системе» представлены риски, связанные с информационной безопасностью и кибератаками. Данная проблема особенно актуальна для банковской системы, в которой сконцентрированы денежные средства и информация по различным вопросам. Вопросы сохранности материальных и нематериальных средств решаются в на всех уровнях управления и исполнения, учитывая также «человеческий фактор».

SUMMARY

The article “Cyber Risk Management in the Banking System” presents the risks associated with information security and cyber-attacks. This problem is especially relevant for the banking system, in which money and information on various issues are concentrated. The safety issues of tangible and intangible assets are resolved at all levels of management and execution, taking into account also the “human factor”.