DOI: http://dx.doi.org/10.21686/2413-2829-2020-6-198-207

УПРАВЛЕНИЕ КИБЕРБЕЗОПАСНОСТЬЮ ВНУТРИБАНКОВСКОЙ ЭКОСИСТЕМЫ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

А. Д. Безделов
Евразийский банк развития, Москва, Россия
Е. В. Логинова
Российский экономический университет имени Г. В. Плеханова, Москва, Россия

Информационным технологиям (ИТ) принадлежит ключевая роль в корпоративной инфраструктуре. Именно они обеспечивают беспрецедентное экономическое развитие предприятий современной эпохи. Системы ИТ помогают экономить ресурсы и позволяют глубже проникать в сущность корпоративных операций. Рынок финансовых услуг активно развивается вследствие формирования цифровой экономики. Цифровые технологии уже проникли во все сферы жизни общества, и уровень оснащенности инновационными технологиями продолжает расти за счет мобильных технологий. Система управления внутрифирменным финансовым контролем входит в структуру функционала менеджмента как обязательный элемент современного механизма управления. Разработка программ внутрибанковского контроля является необходимой составляющей деятельности любой финансово-кредитной организации в соответствии с международным и национальным законодательством. В статье раскрывается структура единого внутрибанковского механизма контроля, целеориентированного на предотвращение легализации криминальных доходов и подготовку кадров для служб банковского внутреннего контроля. Проанализированы внутрибанковские программы по его организации и обоснованы функциональные обязанности сотрудников подразделений внутреннего контроля, интегрированного в систему мониторинга и управления банковскими рисками. Оценена роль дифференцированных по типам клиентов анкет, с помощью которых банк осуществляет идентификацию своих клиентов. Структурированы программы обучения сотрудников подразделений внутреннего контроля.

Ключевые слова: банковская сфера, бизнес-модель, эффективные инновационные бизнес-модели, цифровизация, банковское пространство, внутренний контроль, легализация доходов, конфиденциальность информации, идентификация клиентов, риски легализации преступных доходов, классификация клиентов, алгоритм действий персонала, программы обучения, дистанционное обучение.

MANAGING CYBER-SECURITY OF IN-BANK ECOSYSTEM IN CONDITIONS OF DIGITALIZATION

Anton D. Bezdelov
Eurasian Development Bank, Moscow, Russia
Elena V. Loginova
Plekhanov Russian University of Economics, Moscow, Russia

Information technologies (IT) play a key role in corporate infrastructure. They provide unprecedented economic development of enterprises in our era. IT systems help economize resources and give an opportunity to peep in the essence of corporate transactions. Finance service market develops energetically due to digital economy shaping. Digital technologies have penetrated all spheres of life and the level of innovation technology equipment keeps on growing at the expense of mobile technologies. The system of in-company finance control is included n the structure of management functioning as an obligatory element of the current mechanism of management. The development of programs of in-bank control is a necessary component of work of any finance and credit organization according to

international and national legislation. The article describes the structure of unique in-bank mechanism of control, oriented to preventing legalization of criminal incomes and raining personnel for services of internal bank control. The article analyzes in-bank programs aimed at its organization and grounds functional responsibilities of employees in divisions of internal control integrated in the system of monitoring and managing bank risks. The role of questionnaires differentiated by clients' types is assessed, with the help of which the bank can identify its clients. Programs of training employees of internal control divisions are structured.
Keywords: banking sphere, business-model, efficient innovation business-models, digitalization, banking space, internal control, legalization of income, information confidentiality, client identification, risk of criminal income legalization, algorithm of employees' steps, client classification, training program, distance study.

Введение

Для успешного внедрения в информационное общество и цифровую экономику банкам необходимо ускорить смену существующей бизнес-модели и перейти к формированию финансовой экосистемы на базе использования современных цифровых технологий. В докладе Global Risks Report 2019 («Глобальные риски 2019») Всемирного экономического форума отмечалось, что одной из главных общемировых проблем является киберпреступность, которая в основном и сдерживает потенциал применения цифровых технологий.

Кибербезопасность – это совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями. Теперь информация стала наиболее очевидным механизмом функционирования и двигателем эволюции общественных институтов. Однако с повышением уровня интеграции у человечества не только появилась возможность ускорить темпы собственного развития, но и возникли новые слабые места – новая сфера, безопасность которой ввиду столь глубокой интеграции в человеческую и общественную жизнь вышла на первый план для всего поколения. Угрозы безопасности информации и информационным ресурсам перешли в раздел угроз, определяющих безопасность и свободу человека. Поддержание конституционных прав на свободу и неприкосновенность, на защиту достоинства личности напрямую зависит от сохранения порядка в информационной среде.

По данным Министерства внутренних дел Российской Федерации, в первом квартале 2020 г. число киберпреступлений выросло почти вдвое по сравнению с аналогичным периодом 2019 г. Количество IT-преступлений выросло на 83,9%, а их удельный вес составил 19,9% от общего числа совершенных преступлений. Помимо исключительно «цифровых» преступлений, на фоне пандемии обостряются и ранее существовавшие проблемы, которые перешли в электронный формат. Злоумышленники очень быстро адаптировали известные схемы мошенничества к новым условиям, чтобы извлечь выгоду из кризиса, связанного с пандемией COVID-19.

Рост киберпреступлений является серьезным вызовом для страны. В конце февраля 2020 г. президент России Владимир Путин поддержал предложение о внесении в статью 71 Конституции Российской Федерации нормы по обеспечению кибербезопасности личности и государства, подчеркнув, что обеспечение безопасности личности, общества и государства чрезвычайно важно и востребовано.

Сегодня техническая база обеспечения кибербезопасности уже не та, которой она была пару лет назад. Выработка новых методов хищения, искажения и уничтожения информации и информационных ресурсов, задействованных в киберпространстве, требует принятия принципиально новых контрмер. С изменением среды происходит и изменение характера киберпространства, а потому большинство исследований, опубликованных в последнее десятилетие, теряют свою актуальность, оставаясь весомыми лишь в качестве анализа исторической ретроспективы, а предло-

женные в них модели прогрессивного развития феномена становятся неприменимыми. Кроме того, исследования прошлых лет уделяли мало внимания рассмотрению моделей международного контроля киберпространства, а именно созданию обособленного наднационального органа по поддержанию безопасного состояния среды.

Результаты исследования и обсуждения

Как отмечается в отчете Банка России о работе Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) за период с сентября 2018 по август 2019 г., основной проблемой в сфере информационной безопасности остается социальная инженерия. Банк России сосредоточил свое внимание на противодействии данной противоправной деятельности, в частности за счет блокировки ресурсов, используемых злоумышленниками для хищения средств граждан[1].

Для реализации программ внутреннего контроля в банках формируется подразделение внутреннего контроля, которое подчиняется президенту банка (первому заместителю), назначающему начальника аналитического отдела по работе с клиентами с функционалом разработки и реализации правил контроля в целях противодействия легализации преступных доходов и программ его осуществления, организационных мер по руководству отделом. В процессе систематического мониторинга действенности системы внутрибанковского контроля аналитический отдел по работе с клиентами осуществляет контроль как деятельности банка в целом, так и его отдельных сотрудников в соответствии с Федеральным законом от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», а также исполнение сотрудниками банка правил внутреннего контроля. В целях решения проблем, возникающих при реализации программ осуществления внутреннего контроля, сотрудники в свою очередь могут обращаться за консультациями к начальнику и специалистам аналитического отдела[2].

Российские банки и другие финансовые организации пока еще не научились управлять киберрисками: у 75 банков, проверенных в 2020 г. на соответствие требованиям кибербезопасности, были обнаружены нарушения. Об этом заявила глава Банка России Эльвира Набиуллина в ходе Международного конгресса по кибербезопасности, организованного СберБанком. Руководитель финансового регулятора отметила, что обнаруженные проблемы нельзя назвать критическими, но в любой момент они могут стать серьезными, если с ними не работать. Глава Центробанка указала, что зачастую руководители банков и компаний скидывают ответственность за киберриски на менеджеров.

С 2019 г. у регулятора появились полномочия осуществлять надзор за финансовыми институтами и контролировать выполнение ими требований по кибербезопасности. В свою очередь глава СберБанка Герман Греф заявил, что для защиты всех элементов современных систем нужно «не только иметь какую-то очень мощную компетенцию внутри, но для этого нужна очень серьезная кооперация»[3].

Кибербезопасность является огромной проблемой, которая должна делать руководителей крупных компаний параноиками. По данным киберкриминалистов из компании Group-IB, 74% российских банков не готовы к атакам хакеров. Причину они видят в низком уровне организации защиты. Кибератаки на финансовую сферу с лета 2017 по лето 2018 г. нанесли порядка 3 млрд рублей ущерба[4].

[1] URL: https://cbr.ru/Press/event/?id=3928

[2] URL: http://www.consultant.ru/document/cons_doc_LAW_49131/

[3] URL: https://www.samara.kp.ru/daily/26993.7/4053696/

[4] URL: https://www.rbc.ru/finances/21/06/2019/5d0cc0189a7947b221a9492d

Российская компания «ЮНИТ» специализируется на инновационных решениях, направленных на обеспечение безопасности данных в процессе их хранения и обмена, и тестирует свои разработки в США, Канаде и Восточной Европе. Компания ориентируется на создание комплексных решений для автоматизации широкого спектра бизнес-задач.

В целях централизации ответственности за эту работу президент банка назначает специальное должностное лицо – начальника аналитического отдела по работе с клиентами, который является ответственным за разработку и контроль правил и норм внутрибанковского контроля, обеспечивающих предотвращение деятельности клиентов по легализации криминальных доходов, и руководит аналитическим отделом по работе с клиентами [1].

Банк идентифицирует своего клиента при открытии счета, совершении банковских операций и других сделок с денежными средствами, руководствуясь соответствующими законами Российской Федерации. Для этого используется информация из Единого государственного реестра юридических лиц, сводного Государственного реестра аккредитованных филиалов, представительств иностранных юридических лиц, а также сведения об утерянных и недействительных паспортах, паспортах умерших физических лиц, их утраченных бланках. При этом банковский институт вправе не открывать банковский счет физического или юридического лица, если они не представили полный комплект документов, обеспечивающих их идентификацию, либо представили недостоверные документы [11].

К тому же в банк подаются подлинники всех документов, соответствующие установленным образцам, или заверенные нотариусом копии. При представлении этих копий банк может затребовать подлинники документов для их сравнения с копией. Необходимо подчеркнуть, что такие требования не предъявляются при открытии банковских счетов органами госвласти Российской Федерации или ее субъектов. Но муниципальные органы не относятся к государственным и поэтому подлежат соответствующей идентификации.

Идентификация банком своих клиентов производится с использованием дифференцированных анкет, соответствующих типам клиентов: юридических лиц, юридических лиц – участников рынка ценных бумаг, физических лиц и кредитных организаций. Заполнение сотрудником банка сведений, предусмотренных анкетой клиента, производится на основании документов юридических досье, а также других сведений и документов, полученных по запросу от клиента и вносимых в карточку клиента в автоматизированной банковской системе «Сапфир» (АБС «Сапфир»). При заполнении карточек клиентов при открытии ими расчетного счета автоматически создается анкета по всем клиентам банка.

Анкета клиента ведется в электронном виде в АБС «Сапфир» в подсистеме «Противодействие легализации доходов, полученных преступным путем – ПЛД». Персонал банка, ответственный за идентификацию клиентов, имеет непрерывный доступ к анкетам для проверки информации о клиенте. При этом электронная анкета переносится на бумажный носитель и заверяется подписью ответственного сотрудника[1].

Одним из инструментов повышения эффективности противодействия банковских институтов легализации криминальных доходов на основании всей собранной для достоверной идентификации клиентов информации является оценка рисков участия клиентов в различных схемах узаконивания нелегальных доходов с использованием соответствующих критериев [9].

Банк непрерывно обновляет информацию, собранную в процессе идентификации клиента, один раз в год переоценивая степень риска на основе поступления обновленной информации о ее изменении, если операция клиента идентифицируется как высокорискованная, в других случаях –

[1] URL: http://www.consultant.ru/document/cons_doc_LAW_80299/

один раз в три года [4; 10]. В целях обеспечения полноценного контроля операций клиентов с высоким уровнем риска банк классифицирует своих клиентов по степени риска на характеризующихся соответственно низкой и высокой степенью риска [6]. Основанием для отнесения клиента к одной из категорий степени риска является анализ совершаемых клиентом операций [3].

По упрощенному порядку идентификация физического лица включает проверку его фамилии, имени и отчества, а также всех данных о документе, удостоверяющем его личность, и осуществляется при наличии всех установленных банком условий.

Внутрибанковская программа по выявлению в деятельности клиентов банка подозрительных сделок включает следующий алгоритм:

1. Анализ сведений об операциях клиентов.

2. Выделение финансовых сделок, обязательных для контроля, т. е. подозрительных или необычных, определяемых как легализация криминальных доходов.

При приеме платежных и других документов от клиентов сотрудник банка, ответственный за ведение его банковского счета или проведение данной операции (куратор счета), анализирует денежную сумму, указанную в платежном документе, контрагентов клиента по данной сделке, содержание операции, соответствие данной операции характеру хозяйственной деятельности клиента в целях выявления операций клиентов, предусмотренных статьей 6 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

На каждую сделку, подлежащую обязательному внутрибанковскому контролю, или необычную, в отношении которой возникли соответствующие подозрения, ответственным исполнителем составляется особое сообщение [7]. Тексты сообщений, передаваемых подразделениями банка по операциям, сведения о которых направлены в уполномоченный орган (а также копии платежных документов по этим операциям, дающие основание считать данную сделку подлежащей обязательному контролю либо подозрительной), и тексты сообщений по сделкам, признанным экономически целесообразными, хранятся в отдельных досье.

В сообщении фиксируется достаточно полная информация, включающая следующие данные[1]:

– вид сделки и основания ее осуществления;

– дата проведения финансовой сделки;

– объем денежных средств по данной операции;

– информация, обеспечивающая достоверную идентификацию физического лица, распорядившегося о совершении подозрительной на отмывание денег операции;

– наименование, ИНН юридического лица, номер его госрегистрации, его место и адрес местонахождения;

– информация по полной идентификации физического или юридического лица, которое поручает от своего имени совершить подозрительную сделку;

– информация для идентификации представителя физического или юридического лица, который осуществляет финансовую сделку;

– информация по идентификации бенефициара (получателя) денежных средств по подозрительной на отмывание денег операции.

При выявлении необычной сделки клиента банка предпринимаются соответствующие установленному алгоритму действия (рис. 1).

Банк вправе приостановить операции своих клиентов в том случае, если у его работников формируется мнение о том, что соответствующая сделка подозрительна на легализацию криминальных доходов, или в случае, когда одной из ее сторон выступает юридическое или физическое лицо,

[1] URL: http://base.garant.ru/584330/

подозреваемое в осуществлении террористической деятельности, или юридическое лицо, находящееся в собственности или под контролем таких организаций или лиц [8]. Банк хранит по совершаемым клиентом подозрительным операциям все собранные в процессе расследования документы (рис. 2).

Рис. 1. Действия сотрудников банка
при фиксировании необычной сделки клиента

Рис. 2. Документы, сохраняемые банком
по подозрительным операциям клиентов [5]

Очевидно, что сотрудники, осуществляющие внутрибанковский контроль по противодействию криминальных доходов, должны обладать достаточно широким спектром необходимых компетенций, которые формируются как в процессе накопления опыта работы, так и на основе реализации банком дополнительных обра-

зовательных программ повышения квалификации и переподготовки своих сотрудников. Целью обучения сотрудников банка по программам противодействия отмыванию преступных доходов является получение знаний и формирование компетенций, необходимых для полноценного исполнения ими нормативных актов Российской Федерации в данной области и соответствующих внутренних документов банка.

Программа обучения, повышения квалификации и переподготовки сотрудников банка разрабатывается начальником аналитического отдела и периодически (один раз в год) обновляется ответственным сотрудником. Кроме того, обновление осуществляется при изменении действующих законов или принятии новых, а также в случае ввода в банке новых или изменении действующих регламентов внутреннего контроля.

Реализация программы совершенствования компетенций персонала банка в сфере противодействия легализации криминальных доходов и финансовой поддержке терроризма осуществляется по строго институционализированному алгоритму. Прежде всего президентом банка издается приказ о назначении ответственных сотрудников по организации и проведению обучения. Далее формально институционализируется (документируется) сама программа обучения, включая:

– порядок и формы проведения обучения сотрудников;

– систему мер, которые необходимо принимать в соответствующих условиях;

– порядок проверки полученных знаний сотрудников.

Вместе с тем планируется и утверждается президентом банка до 31 января текущего года ход реализации программы обучения на текущий и последующие годы, включая тематику и сроки проведения обучения, а также фамилии исполнителей, отвечающих за его организацию.

В завершении подготовки программы разрабатывается список подразделений, персонал которых направляется на обучение:

– отдел по противодействию легализации криминальных доходов;

– подразделения, осуществляющие финансовые операции и сделки;

– юридический отдел;

– служба безопасности;

– служба внутреннего контроля.

Обучение по данной программе является обязательным для всех специалистов, принимаемых в аналитический отдел или при их переводе в подразделения, осуществляющие финансовые операции и сделки, а также в течение дальнейшей трудовой деятельности сотрудника. Обучение сотрудников производится в форме вводного (первичного), целевого (внепланового) инструктажа, планового повышения квалификации или дистанционного обучения[1].

Дополнительные образовательные программы повышения квалификации и переподготовки сотрудников подразделений банков по внутреннему контролю должны отвечать таким требованиям, как:

– соответствие содержания программы обучения требованиям Банка России;

– реализация запланированных показателей по обучению за текущий и предшествующие годы;

– систематическая модернизация программы, а также ее обновление при изменении законодательства;

– адекватность регламентов и сроков проведения вводного, целевого инструктажа и планового повышения квалификации установленным требованиям Центрального банка;

– систематический контроль знаний и уровня сформированных компетенций сотрудников банка по соответствующей тематике.

Дистанционное обучение предполагает отправку сотрудникам из разных подразделений соответствующих нормативных документов, разъяснений, обзорных писем,

[1] URL: http://www.consultant.ru/document/cons_doc_LAW_49131/

проведение заочного консультирования. Такое обучение проводится с сотрудниками филиалов и дополнительных офисов.

По итогам обучения один раз в год осуществляется проверка знаний сотрудников через тестирование, собеседование или общую аттестацию.

Вывод

Таким образом, кибербезопасность является большой проблемой, которая только увеличивается по мере того, как с каждым днем растут попытки фишинга, вредоносного программного обеспечения, кражи личных данных и огромных утечек информации. Наличие системы внутреннего контроля в банке – это обязательное условие его успешного функционирования, поскольку она обеспечивает соблюдение действующего законодательства и нормативных актов, разработанной банком политики, внутренних правил и процедур, а также способствует снижению риска непредвиденных потерь или нанесения ущерба репутации банка.

Прогресс не стоит на месте, особенно в банковской системе. С момента становления информации как основополагающего фактора мирового развития банковской сферы появились и сопутствующие данному явлению угрозы, а там, где есть угрозы, есть и феномен безопасности.

Кибербезопасность – одно из ключевых направлений подготовки кадров автономной некоммерческой организации высшего образования «Университет Иннополис». Университет выпускает специалистов по кибербезопасности, а вопросами защиты от киберугроз занимаются многие резиденты. Так, французская компания Schneider Electric известна как производитель электронных компонентов. В Иннополисе она работает над цифровыми двойниками (цифровая копия объекта или процесса, созданная для сбора и повторного использования полученной о нем информации). Эта технология позволяет не только повысить эффективность реального объекта, но и улучшить его безопасность: механизмы защиты необходимо внедрять уже на стадии проектирования системы (security by design), и двойник помогает сделать это наиболее грамотно. Японская Soramitsu разрабатывает собственный подвид блокчейн-протокола для систем передачи цифровых активов. Распределенный реестр – один из способов обеспечить безопасность по умолчанию (security by default – способ изначальной настройки системы, в котором приоритет отдается ее безопасности).

Цифровая трансформация производства, появление киберфизических объектов и систем, формирование киберсреды – неизбежные следствия повсеместного использования программируемых контроллеров и компьютеризации процессов управления. Одновременно наблюдаются рост и изменение специфики атак на производственные системы. Банковская экосистема становится эффективной инновационной бизнес-моделью в менеджменте в условиях цифровой экономики. В результате внедрения IT-технологий (сетевые продукты, онлайн-платформы продвижения товаров и продаж и пр.) применяются новые подходы в управлении. Следует отметить немаловажную роль трансформации методов и подходов в HR-менеджменте.

С точки зрения управления персоналом в условиях перехода к инновационной бизнес-модели банковской экосистемы необходимо отработать механизм вовлеченности и глубокой всесторонней заинтересованности сотрудников в результативности бизнеса. И здесь, помимо материальных стимулов, необходимо подключить разного рода рычаги. В частности, важно организовать эффективное и точное ознакомление сотрудников с разработанной и внедряемой бизнес-моделью экосистемы, что позволит им лучше понять все нюансы развития бизнеса и повысить его конечную эффективность.

Список литературы

1. *Аль-Гаррави Мохаммед А. Д.* Структурные элементы банковского механизма внутреннего контроля // Форсайт «Россия»: будущее технологий, экономики и человека : сборник докладов V Санкт-Петербургского международного экономического конгресса (СПЭК–2019) / под общ. ред. С. Д. Бодрунова. – Т. 3. – СПб. : ИНИР, 2019.

2. *Арабян К. К.* Система финансового контроля //Аудитор. – 2013. – № 11. – С. 13–20.

3. *Бардина И. В., Затолокин И. В.* Сущность и значение финансового контроля в системе управления хозяйствующих субъектов // Вестник Университета. – 2015. – № 3. – С. 142–149.

4. *Самохина Н. Н., Готова С. Г.* Феномен идеологии экстремизма и терроризма в сети интернет: проблемы и пути их решения // Общество: политика, экономика, право. – 2016. – № 10. – С. 18–23.

5. *Свиридов О. Ю., Лысоченко А. А.* Банковское дело: 100 экзаменационных ответов. – Ростов н/Д. : Феникс, 2014.

6. *Семёнова Н. В.* Внутренний контроль и управление рисками. – М. : Проспект, 2007.

7. *Федоров А.* Проблемы информационной безопасности сегодня: алогизмы развития // Индекс безопасности. – 2013. – Т. 19. – № 1 (104). – С. 261–270.

8. *Ширяев П. С.* Корпоративный финансовый контроль: сущность, виды, стратегия развития (модель COSO) // Национальные интересы: приоритеты и безопасность. – 2010. – № 24 (81). – С. 54–60.

9. *Шушков Г. М., Сергеев И. В.* Концептуальные основы информационной безопасности Российской Федерации // Актуальные вопросы научной и научно-педагогической деятельности молодых ученых : сборник научных трудов III Всероссийской заочной научно-практической конференции. – М. : ИИУ МГОУ, 2016. – С. 69–76.

10. *Karaman M., Catalkaya H., Aybar C.* Institutional Cybersecurity from Military Perspective // International Journal of Information Security Science. – 2016. – N 1. – P. 1–7.

11. *Rohrig W.* Cyber Security and Cyber Defense in the European Union // Cyber Security Review. – 2014. – N 2. – P. 7–16.

References

1. Al-Garravi Mokhammed A. D. Strukturnye elementy bankovskogo mekhanizma vnutrennego kontrolya [Structural Elements of banking Mechanism of Internal Control]. *Forsayt «Rossiya»: budushchee tekhnologiy, ekonomiki i cheloveka, sbornik dokladov V Sankt-Peterburgskogo mezhdunarodnogo ekonomicheskogo kongressa (SPEK–2019)* [Foresight 'Russia': the Future of Technologies, Economy and Man. Collection of reports of the 5th St. Petersburg International Economic Congress (SPEC-2019)], edited by S. D. Bodrunov. Vol. 3. Saint Petersburg, INIR, 2019. (In Russ.).

2. Arabyan K. K. Sistema finansovogo kontrolya [The System of Finance Control]. *Auditor* [Auditor], 2013, No. 11, pp. 13–20. (In Russ.).

3. Bardina I. V., Zatolokin I. V. Sushchnost i znachenie finansovogo kontrolya v sisteme upravleniya khozyaystvuyushchikh subektov [The Essence and Importance of Finance Control in the System of Managing Business Entities]. *Vestnik Universiteta* [Bulletin of the University], 2015, No. 3, pp. 142–149. (In Russ.).

4. Samokhina N. N., Gotova S. G. Fenomen ideologii ekstremizma i terrorizma v seti internet: problemy i puti ikh resheniya [Ideology of Extremism and Terrorism in the Internet: Problems and Their Solution]. *Obshchestvo: politika, ekonomika, pravo* [Society: Policy, Economy, Law], 2016, No. 10, pp. 18–23. (In Russ.).

5. Sviridov O. Yu., Lysochenko A. A. Bankovskoe delo: 100 ekzamenatsionnykh otvetov [Banking: 100 Exam Answers]. Rostov-on-Don, Feniks, 2014. (In Russ.).

6. Semenova N. V. Vnutrenniy kontrol i upravlenie riskami [Internal Control and Risk Management]. Moscow, Prospekt, 2007. (In Russ.).

7. Fedorov A. Problemy informatsionnoy bezopasnosti segodnya: alogizmy razvitiya [Problems of Information Security Today: Algorithms of Development]. *Indeks bezopasnosti* [Security Coefficient], 2013, Vol. 19, No. 1 (104), pp. 261–270. (In Russ.).

8. Shiryaev P. S. Korporativnyy finansovyy kontrol: sushchnost, vidy, strategiya razvitiya (model COSO) [Corporate Finance Control: Essence, Types, Strategy of Development (COSO Model)]. *Natsionalnye interesy: prioritety i bezopasnost* [National Interests: Priorities and Security], 2010, No. 24 (81), pp. 54–60. (In Russ.).

9. Shushkov G. M., Sergeev I. V. Kontseptualnye osnovy informatsionnoy bezopasnosti Rossiyskoy Federatsii [Conceptual Basis of Information Security of the Russian Federation]. *Aktualnye voprosy nauchnoy i nauchno-pedagogicheskoy deyatelnosti molodykh uchenykh, sbornik nauchnykh trudov III Vserossiyskoy zaochnoy nauchno-prakticheskoy konferentsii* [Acute Issues of Academic and Research-Pedagogic Work of Young Scientists: collection of works f the 3rd All-Russian Distance Conference]. Moscow, IIU MGOU, 2016, pp. 69–76. (In Russ.).

10. Karaman M., Catalkaya H., Aybar C. Institutional Cybersecurity from Military Perspective. *International Journal of Information Security Science*, 2016, No. 1, pp. 1–7.

11. Rohrig W. Cyber Security and Cyber Defense in the European Union. *Cyber Security Review*, 2014, No. 2, pp. 7–16.

Сведения об авторах

Антон Дмитриевич Безделов
специалист клиентского блока
Евразийского банка развития.
Адрес: Евразийский банк развития,
119034, Москва, 1-й Зачатьевский пер.,
д. 3, стр. 1.
E-mail: antonbezdelov@mail.ru

Елена Вячеславовна Логинова
кандидат экономических наук, доцент,
старший научный сотрудник научной школы
«Теория и технологии менеджмента»
РЭУ им. Г. В. Плеханова.
Адрес: ФГБОУ ВО «Российский экономический
университет имени Г. В. Плеханова»,
117997, Москва, Стремянный пер., д. 36.
E-mail: elog495@gmail.com

Information about the authors

Anton D. Bezdelov
Client Unit Specialist
Eurasian Development Bank.
Address: Eurasian Development Bank,
1 building, 3 1st Zachatievsky Lane, Moscow,
119034, Russian Federation.
E-mail: antonbezdelov@mail.ru

Elena V. Loginova
PhD, Assistant Professor, Leading Researcher
of the Scientific School
"Theory and Technologies of Management"
of the PRUE.
Address: Plekhanov Russian University
of Economics, 36 Stremyanny Lane,
Moscow, 117997, Russian Federation.
E-mail: elog495@gmail.com