
БИЗНЕС-ИНФОРМАТИКА

DOI: 10.34020/2073-6495-2021-1-245-253

УДК 336.7

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА В УСЛОВИЯХ СТАНОВЛЕНИЯ ЦИФРОВОЙ ЭКОНОМИКИ

Щербакова Н.В.

Алтайский государственный технический университет
им. И.И. Ползунова

E-mail: shcherbakova_nat@mail.ru

С развитием цифровизации общество сталкивается с новыми для себя угрозами и проблемами. В статье рассмотрены вопросы обеспечения информационной безопасности, актуальные для компаний, осуществляющих свою деятельность в любых секторах экономики; особое внимание уделено управлению рисками нарушения информационной безопасности в финансовых учреждениях. Приведены данные, отражающие уровень и динамику потерь от киберинцидентов, проанализирована структура киберинцидентов. Построение системы управления рисками нарушения информационной безопасности в кредитных организациях имеет первостепенное значение как основа предотвращения финансовых и репутационных потерь и должна выстраиваться с учетом наилучшей отечественной и зарубежной практики.

Ключевые слова: цифровая экономика, цифровые технологии, банк, риск, риск-менеджмент, киберинцидент, информационная безопасность.

ISSUES OF INFORMATION SECURITY OF SOCIETY UNDER THE CONDITIONS OF THE DEVELOPMENT OF DIGITAL ECONOMY

Shcherbakova N.V.

Polzunov Altai State Technical University

E-mail: shcherbakova_nat@mail.ru

Cybercrime is a growing industry around the world imposing significant costs on firms. Cyber threats have driven companies to build layers of defenses, resorting to a variety of products and services developed by different cybersecurity vendors. The financial sector is a major target for cybercriminals. The pace of cyberattacks is accelerating too quickly for banks to rely on manual threat analysis and response. The financial organizations face a growing threat from malicious cyber activity. In the financial sector, speed of response is critical to identify and block cyber threats. Regulators are taking notice of the increased risk of cyber threats. Paper draws our attention to information protection system of bank.

Keywords: digital economy, digital technologies, bank, risk, risk management, cyber incidents, information security.

Развитие экономики в условиях цифровой трансформации характеризуется рядом положительных трендов. В последние годы в России и зарубежных странах использование банкнот и монет в обществе сокращается; технологический прогресс в области электронных денег и способов оплаты идет быстрыми темпами. Одновременно с положительной тенденцией формируется и негативная: нарастают угрозы информационной безопасности для пользователей сетей, значительно увеличивается влияние киберпреступности на экономику во всем мире. Ее жертвами становятся крупные компании, малые и средние предприятия и отдельные потребители. Так, например, около 600 млрд долл. США, или почти один процент мирового ВВП, теряется в результате киберпреступности каждый год.

Наиболее важной областью в сфере обеспечения информационной безопасности общества является защита интеллектуальной собственности и конфиденциальной деловой информации. Кража интеллектуальной собственности, например, такой как дизайн продукта, для малого или среднего предприятия может стать непреодолимой проблемой. Кража интеллектуальной собственности составляет как минимум четверть стоимости киберпреступности и, когда речь идет о военных технологиях, также создает риски для национальной безопасности. По данным экспертов, более 22 000 предприятий во всем мире стали жертвами компрометации деловой электронной почты: взлом деловой электронной почты и кража личных данных позволяет киберпреступникам отправлять электронные письма, выдавая себя за руководителя компании, заказывая крупные переводы. Банкам, действующим по распоряжениям клиентов и осуществляющим расчеты по клиентским операциям, сложно обнаружить и предотвратить взлом электронной почты, поскольку транзакция осуществляется с согласия или непосредственно клиентом банка [7].

Потери общества от нарушения информационной безопасности складываются из различных элементов: утрата интеллектуальной собственности и конфиденциальной деловой информации; мошенничество в интернете и финансовые преступления, часто являющиеся результатом кражи личной информации; финансовые манипуляции с использованием украденной конфиденциальной информации (например, информация о потенциальных слияниях или предварительное знание отчетов об эффективности для публично торгуемых компаний); стоимость защиты сетей, покупки киберстрахования и оплаты восстановления после кибератак; репутационный ущерб для компании и ее бренда, включая временное падение стоимости акций [5]. Однако любая стоимостная оценка киберпреступности сталкивается с несколькими проблемами: недооценка жертвами своих потерь и недостаточный сбор данных правительствами стран, что усугубляется специфичностью правил отчетности. Например, в Великобритании, по оценкам экспертов, сообщается только о 13 % случаев киберпреступности. Неспособность собрать данные усугубляется нежеланием многих компаний сообщать, когда они стали жертвами. Сбор данных по проблемам в сфере информационной безопасности остается проблемой, и национальные оценки все еще являются весьма неточными. Сообщается только о части потерь, поскольку компании стремятся избежать рисков ответственности и ущерба репутации [6].



Рис. 1. Киберинциденты в финансовом и страховом секторе.

Источник: Консультативные данные о киберпотерях компании Advisen, июль 2019 г.

Информационные ресурсы компании Advisen, специализирующейся на исследованиях в области рисков, позволяют как выявлять общемировые тенденции, так и учитывать глобальные угрозы, в первую очередь затрагивающие финансовые учреждения. Компания Advisen разрабатывает собственные аналитические базы достаточно давно, самый ранний киберинцидент она зафиксировала в наборе данных киберинцидентов в 1973 г.; однако более 90 % киберинцидентов произошло после 2008 г. К июлю 2019 г. статистика компании включает более 90 000 киберинцидентов в различных секторах и отраслях промышленности по всему миру.

С учетом общемировой практики и с целью выявления специфичности киберрисков, киберинциденты в финансовом секторе можно разбить на категории: злонамеренные киберинциденты с применением вредоносных программ, также известные как кибератаки, когда субъект угрозы намеревается нанести вред (например, атаки с использованием вымогателей, кража данных сотрудниками); потеря конфиденциальности и личных данных, когда информация утеряна, использована не по назначению; ошибки внедрения и обработки ИТ, когда инцидент происходит в результате некорректного обновления или замены оборудования или программного обеспечения. Частота ошибок внедрения и обработки ИТ низка, в то время как потери от них намного превышают те, о которых сообщается для других типов киберинцидентов, что отражено на рис. 1. События, связанные с изменениями в ИТ, могут представлять высокий риск для финансовой организации и системы. Кибератаки на финансовую систему обычно бывают не сразу заметны; киберзлоумышленники, как правило, терпеливы, действуют осторожно.

Киберпреступники используют передовые технологии для определения целей, создания и доставки программного обеспечения и монетизации того, что получили преступным путем. Около двух третей пользователей в сети стали жертвами киберпреступников: у более двух миллиардов человек была украдена или взломана их личная информация. Несмотря на активную деятельность правоохранительных органов в области информа-

ционной безопасности, есть ряд факторов, способствующих росту киберпреступности: быстрое внедрение новых технологий киберпреступниками; увеличение числа новых пользователей в сети; растущая финансовая изоциренность среди киберпреступников, что облегчает им монетизацию украденных данных.

Монетизация украденных данных, ранее являющаяся проблемой для киберпреступников, стала менее трудной из-за использования цифровых валют. Цифровая валюта делает платежи менее отслеживаемыми. Киберпреступники не идентифицируют себя лично; использование и обмен биткойнов позволяет преступникам действовать практически безнаказанно, несмотря на тот факт, что все операции с биткойнами публично регистрируются. Пользователи биткойнов могут быть идентифицированы только в том случае, если их учетные записи будут привязаны к их реальной личности, чего большинство преступников стараются избегать. Однако связывание учетной записи с идентифицирующей информацией является необходимым компонентом конвертации биткойнов в реальные валюты через банки или биржи, создавая уязвимость для преступников.

Новые технологии делают людей и компании более эффективными и действенными, что справедливо может быть отнесено и к категории киберпреступников. Написание вредоносных программ автоматизировано, каждый день генерируются тысячи новых фрагментов. Многие исследователи отслеживают количество выпущенных новых вредоносных программ, по оценкам от 300 000 до 1 000 000 вирусов и других вредоносных программных продуктов, создаваемых каждый день. Большинство из них представляют собой автоматизированные сценарии, которые выполняют поиск в Интернете уязвимых устройств и сетей. Электронная почта по-прежнему является наиболее популярным средством взлома целевых компьютеров. Простота использования была главной движущей силой роста вымогателей. Инцидент с WannaCry показал, как работают подобные атаки. Поскольку интернет-активность перешла на мобильные платформы, за ней последовала киберпреступность, ожидается, что вымогатели будут все чаще нацеливаться на мобильные системы; киберпреступники стремятся воспользоваться огромным количеством незащищенных телефонов во всем мире.

Наиболее существенные потери для общества от наступления рисков в сфере информационной безопасности связаны с деятельностью финансовых учреждений. Финансовые учреждения во всем мире являются ведущими объектами кибератак. Банки работают с денежными средствами, и для киберпреступников, атакующих банки, есть множество способов получения прибыли за счет вымогательства, краж и мошенничества. Регуляторы внедряют новые средства контроля за киберрисками. При этом фишинг остается самым популярным и простым способом совершения киберпреступлений. Борьба с киберпреступностью предполагает большие финансовые затраты со стороны финансовых учреждений, поскольку они борются с мошенничеством и прямой кражей. По оценкам экспертов, банки тратят в три раза больше на кибербезопасность, чем нефинансовые институты, руководящие органы банков согласны с тем, что киберпреступность пред-

ставляет «систематический» риск для финансовой стабильности. Данные показывают, что киберинциденты чаще встречаются в финансовом секторе по сравнению со всеми остальными секторами экономики.

В финансовом секторе, по собранным статистическим данным, было зарегистрировано наибольшее количество киберинцидентов, а также киберпреступлений в части нарушения конфиденциальности и потери данных, второе место по количеству ошибок при внедрении и обработке ИТ занимает финансовый же сектор, что отражено на рис. 2.

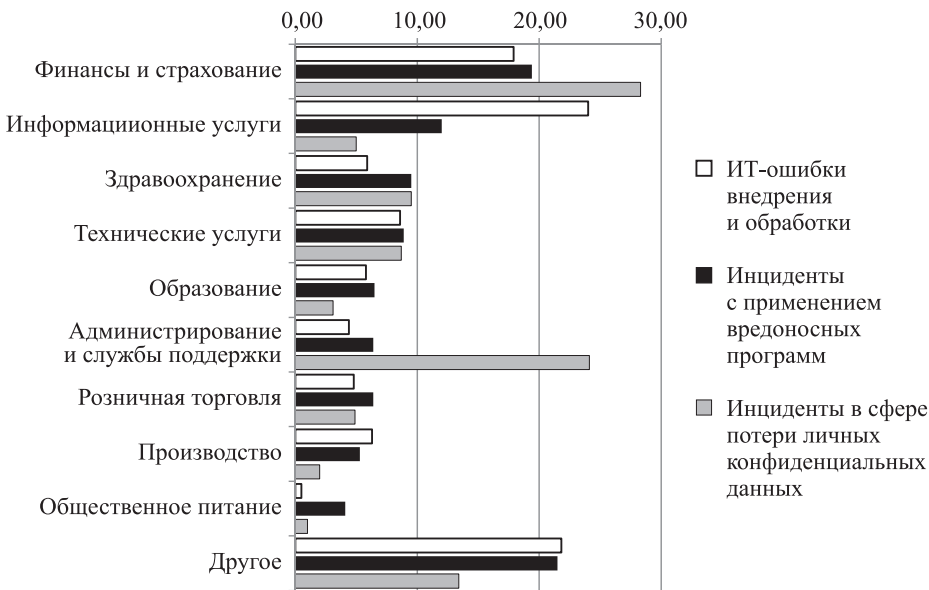


Рис. 2. Структура киберинцидентов по секторам, %.

Источник: Данные о потерях в киберпространстве компании Advisen, июль 2019 г.

Для целей управления рисками информационной безопасности важным является вопрос определения источника угрозы. Анализ статистики по киберинцидентам показывает, что наиболее распространенным источником угроз являются внешние субъекты. К внутренним источникам угроз можно отнести нынешних и бывших сотрудников компаний. Большинство преднамеренных киберинцидентов произошло из внешних источников, что отражено на рис. 3.

Финансовые потери выше существенно от угроз, исходящих из внешних источников. Такая ситуация характерна для всех секторов, в частности, и для финансового. Контроль за предотвращением, сопротивлением и сдерживанием внутренних рисков (например, проверка данных, политика доступа и уведомления о мониторинге) снижает частоту и потенциальный ущерб от этих источников киберинцидентов. Распространенность киберинцидентов с внутренним источником в финансовом секторе близка к средней по всем секторам и меньше, чем в других секторах, которые также обрабатывают большие объемы конфиденциальных данных (например, здравоохранение), что показывает диаграмма на рис. 4.

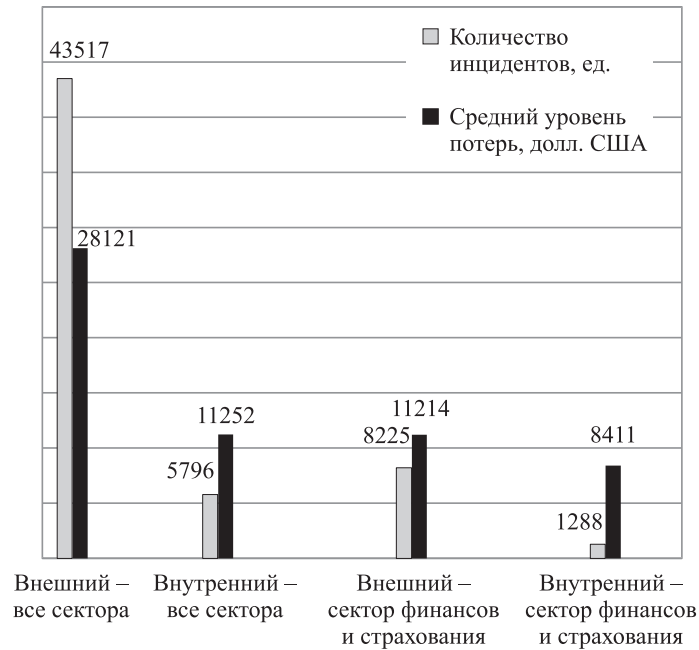


Рис. 3. Количество и средний уровень потерь от киберинцидентов по секторам и источнику угрозы.
Источник: Данные по кибернетическим потерям компании Advisen, июль 2019 г.

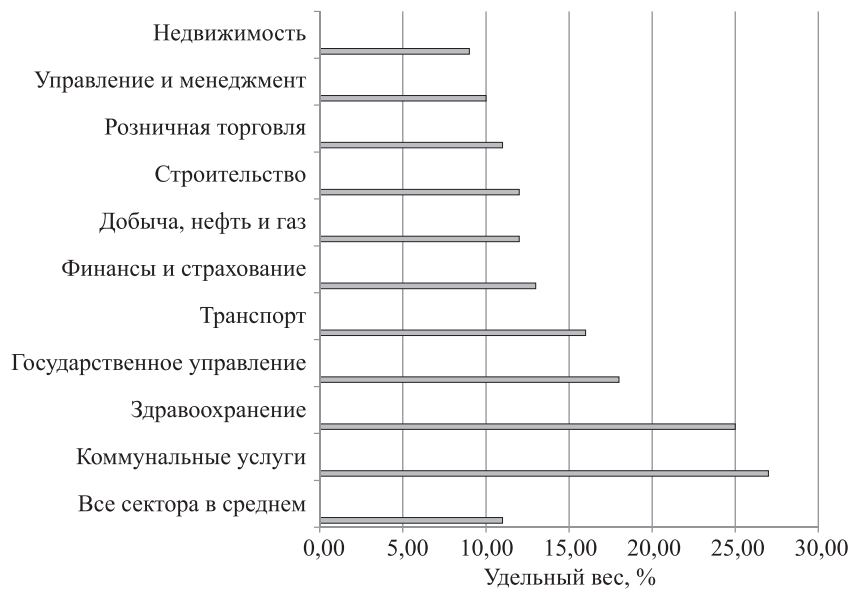


Рис. 4. Удельный вес киберинцидентов от внутренних источников по секторам, %.
Источник: Данные по потерям от киберинцидентов компании Advisen, июль 2019 г.

В финансовом секторе чаще происходят киберинциденты, и финансовые учреждения сталкиваются с более высокими прямыми издержками, чем фирмы в других секторах. Значительное количество этих киберинцидентов является злонамеренным, большинство из которых происходит от внешних субъектов. Но киберсобытия включают в себя не только злонамеренные киберинциденты. Неправильное обращение финансовой организации с информацией, находящейся под ее контролем, может нести аналогичную ответственность и может быть более частым, чем злоумышленные инциденты. Это усиливает необходимость расширения политики информационной безопасности финансовых учреждений за рамки ИТ-отделов, включение в регламент информационной безопасности кредитных учреждений не только злонамеренное использование информации.

Общемировые тенденции характерны и для ситуации в России. Так, в Российской Федерации объем несанкционированных операций со счетов юридических лиц по итогам 2018 г. составил 1,469 млрд руб. На территории России и за ее пределами объем несанкционированных операций с использованием платежных карт, эмитированных российскими кредитными организациями, в 2018 г. составил 1,384 млрд руб. Удельный вес таких операций в общем объеме операций с использованием платежных карт, эмитированных российскими кредитными организациями, в 2018 г. составил 0,0018 % [3]. В то же время в Российской Федерации не зарегистрированы инциденты, которые приводили бы к критичному ущербу в системно значимых организациях кредитно-финансовой сферы. Вместе с тем ряд инцидентов вызывал нарушение непрерывности предоставления финансовых услуг и, как следствие, рост социальной напряженности в обществе. В малых и средних финансовых организациях инциденты информационной безопасности могут являться причиной прекращения их деятельности. Результаты анализа покушений на хищение денежных средств кредитных организаций показывают, что риску хищения подвержены денежные средства в объеме, сопоставимом со средним дневным остатком по корреспондентскому счету кредитной организации, открытому в Банке России, суммированным со средним дневным приходом по соответствующему корреспондентскому счету. Рост киберрисков предопределяет необходимость разработки и широкого внедрения в банковскую практику новых инструментов защиты клиентов банков, в частности, страховых продуктов [2].

Повышение степени защищенности информационных систем кредитных организаций привело к тому, что фокус внимания преступников сместился на атаки на клиентов российских банков. В 2019 г. более 90 % хищений со счетов физических лиц и около 40 % хищений со счетов юридических лиц было совершено с использованием приемов социальной инженерии (злонамеренное введение в заблуждение путем обмана или злоупотребления доверием). Отличительная черта этого вида мошенничества – таргетированность на конкретные группы граждан: конечной целью злоумышленников является перевод средств жертв на их счета, при этом средства ее достижения варьируются. Так, для хищения денежных средств методом социальной инженерии мошенникам достаточно владеть информацией о фамилии, имени и отчестве, а также о номере телефона физического лица. При этом данные, относящиеся к банковской тайне, необязательны для со-

вершения противоправных действий, они лишь уточняют и дополняют необходимую информацию [3].

В условиях развития электронного банкинга в РФ организация системы управления информационной безопасностью в банке является основой его надежности, стабильности ресурсной базы, финансовой устойчивости; нарушения информационной безопасности влекут за собой финансовые и репутационные потери для кредитной организации. Управление и контроль риска информационной безопасности относится к компетенциям органов управления кредитной организации: совет директоров банка, правление банка, президент банка, вице-президент банка, структурные подразделения банка, служба внутреннего контроля. Система управления рисками нарушения информационной безопасности предполагает установление процедур, обеспечивающих оценку, контроль и управление риском на том уровне, который соответствует масштабам деятельности банка. Важные компоненты системы управления рисками нарушения информационной безопасности включают в себя: выделение в кредитной организации сотрудника или подразделения, ответственного за мониторинг и оценку риска нарушения информационной безопасности; степень независимости данного сотрудника (подразделения) от подразделений, осуществляющих банковские операции и сделки; полнота разработанности в банке внутренних нормативных актов по управлению рисками нарушения информационной безопасности; разработка в банке собственной аналитической базы данных об убытках, понесенных вследствие наступления риска нарушения информационной безопасности и случаях наступления данного риска; отражение во внутренней отчетности банка данных убытков [1].

Таким образом, ключевыми задачами в сфере развития цифровых технологий в РФ являются обеспечение безопасности общества, его защита от информационных угроз. Потери общества от наступления информационных рисков могут носить как частный характер, так и быть связанными с профессиональной деятельностью, функционированием компании. Наибольшие потери несет общество, если угрозы и риски связаны с деятельностью финансовых организаций и потреблением финансовых услуг. Устойчивость финансовых организаций определяется рядом мер: обеспечение операционной надежности и непрерывности их деятельности; противодействие компьютерным атакам, в том числе при использовании инновационных финансовых технологий; защита прав потребителей финансовых услуг. Борьба с информационными угрозами, киберпреступностью должна носить в ряде аспектов межгосударственный характер, поэтому необходимо расширять международное сотрудничество между правоохранительными органами других стран, их частным сектором. Инвестиции в защитные технологии являются критически важными для развития цифровой экономики и обеспечения информационной безопасности общества.

Литература

1. Бердюгин А.А. Управление риском нарушения информационной безопасности в условиях электронного банкинга // Вопросы кибербезопасности. 2018. № 1 (25). С. 28–38.

2. Щербакова Н.В., Ильиных Ю.М. Страхование в эпоху цифровых и интернет-технологий // Экономика. Профессия. Бизнес. 2019. № 1. С. 83–86.
3. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов. ЦБ РФ. [Электронный ресурс]. URL: http://www.cbr.ru/Content/Document/File/83253/onrib_2021.pdf (дата обращения: 5.07.2019).
4. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России 1.09.2018 – 31.08.2019. [Электронный ресурс]. URL: https://cbr.ru/Content/Document/File/84354/FINCERT_report_20191010.PDF (дата обращения: 5.07.2019).
5. Economic Impact of Cybercrime. Report. February 21, 2018. Отчет о результатах воздействия киберпреступности на мировую экономику от 21.02.2018. [Электронный ресурс]. URL: <https://www.csis.org/analysis/economic-impact-cybercrime> (дата обращения: 5.07.2019).
6. The Evolution of Cybersecurity Requirements for the U.S. Financial Industry. Report. July, 2015. Эволюция требований кибербезопасности для финансового сектора США. Отчет от июля 2015. [Электронный ресурс]. URL: <https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/financial-sector-cybersecurity> (дата обращения: 5.07.2019).
7. Cybersecurity and the Problem of Interoperability. Report. January 27, 2020. Кибербезопасность и проблема взаимодействия. Отчет от 27.01.2020. [Электронный ресурс]. URL: <https://www.csis.org/analysis/cybersecurity-and-problem-interoperability> (дата обращения: 5.07.2019).

Bibliography

1. Berdjugin A.A. Upravlenie riskom narushenija informacionnoj bezopasnosti v uslovijah jelektronного bankinga // Voprosy kiberbezopasnosti. 2018. № 1 (25). P. 28–38.
2. Shherbakova N.V., Il'inyh Ju.M. Strahovanie v jepohu cifrovyh i internet-tehnologij // Jekonomika. Professija. Biznes. 2019. № 1. P. 83–86.
3. Osnovnye napravlenija razvitija informacionnoj bezopasnosti kreditno-finansovoj sfery na period 2019–2021 godov. CB RF. [Jelektronnyj resurs]. URL: http://www.cbr.ru/Content/Document/File/83253/onrib_2021.pdf (data obrashhenija: 5.07.2019).
4. Otchet centra monitoringa i reagirovanija na komp'juternye ataki v kreditno-finansovoj sfere Departamenta informacionnoj bezopasnosti Banka Rossii 1.09.2018 – 31.08.2019. [Jelektronnyj resurs]. URL: https://cbr.ru/Content/Document/File/84354/FINCERT_report_20191010.PDF (data obrashhenija: 5.07.2019).
5. Economic Impact of Cybercrime. Report. February 21, 2018. Otchet o rezul'tatah vozdejstvija kiberprestupnosti na mirovuju jekonomiku ot 21.02.2018. [Jelektronnyj resurs]. URL: <https://www.csis.org/analysis/economic-impact-cybercrime> (data obrashhenija: 5.07.2019).
6. The Evolution of Cybersecurity Requirements for the U.S. Financial Industry. Report. July, 2015. Jevoljucija trebovanij kiberbezopasnosti dlja finansovogo sektora SShA. Otchet ot ijulja 2015. [Jelektronnyj resurs]. URL: <https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/financial-sector-cybersecurity> (data obrashhenija: 5.07.2019).
7. Cybersecurity and the Problem of Interoperability. Report. January 27, 2020. Kiberbezopasnost' i problema vzaimodejstvija. Otchet ot 27.01.2020. [Jelektronnyj resurs]. URL: <https://www.csis.org/analysis/cybersecurity-and-problem-interoperability> (data obrashhenija: 5.07.2019).