УДК 336:004.056
ББК 65.050
JEL G21, G32, L86

Источники киберрисков в условиях функционирования экосистем

Ревенков Павел Владимирович, доктор экономических наук,
профессор Департамента информационной безопасности,
Финансовый университет при Правительстве Российской Федерации,
Адрес: 4-й Вешняковский проезд, д. 4, корп. 2, г. Москва, 109456, Россия.
ORCID: 0000-0002-0354-0665
E-mail: pavel.revenkov@mail.ru
Чебарь Александр Геннадьевич, аспирант Департамента информационной безопасности,
Финансовый университет при Правительстве Российской Федерации,
Адрес: 4-й Вешняковский проезд, д. 4, корп. 2, г. Москва, 109456, Россия.
ORCID: 0000-0002-2661-3580
E-mail: chebar.alex@gmail.com
Бердюгин Александр Александрович, младший научный сотрудник Департамента информационной безопасности,
Финансовый университет при Правительстве Российской Федерации,
Адрес: 4-й Вешняковский проезд, д. 4, корп. 2, г. Москва, 109456, Россия.
ORCID: 0000-0003-2301-1776
E-mail: a40546b@gmail.com

Аннотация: В статье дается характеристика понятия «Цифровая экосистема», под которой подразумевается совокупность продуктов одной группы компаний или компании и её партнёров (а иногда и конкурентов), предоставляющая набор финансовых и нефинансовых сервисов. Получению коммерческой выгоды-прибыли и повышению уровня эффективности бизнеса способствует использование цифровых платформ. Авторами применены общенаучные методы проведения исследований: анализ, синтез, дедукция, индукция, аналогия, а также графическое отображение информации. В статье приведены наиболее распространенные модели построения цифровых экосистем в нашей стране и основные источники рисков для них, дана характеристика основных типов кибератак на цифровые экосистемы и «цифровой профиль клиента», уделено внимание возрастанию рисков кибермошенничества при использовании клиентами «цифровых помощников».

Ключевые слова: цифровые экосистемы; бигтех-компании; GAFA; цифровой профиль клиента; киберриски; атака; кибербезопасность

Sources of cyber risks in the context of ecosystem functioning

Revenkov Pavel V., Doctor of Economic sciences, Professor of the Department of Information Security, Financial University under the Government of the Russian Federation
Address: 4th Veshnyakovsky passage, 4, bldg. 2, Moscow, 109456, Russia.
ORCID: 0000-0002-0354-0665
E-mail: pavel.revenkov@mail.ru
Chebar Aleksandr G., graduate student of the Department of Information Security, Financial University under the Government of the Russian Federation
Address: 4th Veshnyakovsky passage, 4, bldg. 2, Moscow, 109456, Russia.
ORCID: 0000-0002-2661-3580
E-mail: chebar.alex@gmail.com
Berdyugin Alexander A., junior researcher of the Department of Information Security, Financial University under the Government of the Russian Federation

Address: 4th Veshnyakovsky passage, 4, bldg. 2, Moscow, 109456, Russia.
ORCID: 0000-0003-2301-1776
E-mail: a40546b@gmail.com

Abstract: The article describes the concept of “Digital ecosystem”, which means a set of products of one group of companies or a company and its partners (and sometimes competitors), providing a set of financial and non-financial services. The use of digital platforms contributes to obtaining commercial benefits-profits and increasing the level of business efficiency. The authors applied general scientific methods of research: analysis, synthesis, deduction, induction, analogy, as well as graphical display of information. The article presents the most common models of building digital ecosystems in our country and the main sources of risks for them, describes the main types of cyber attacks on digital ecosystems and the “digital client profile”, pays attention to the increasing risks of cyber fraud when using «digital assistants» by clients.

Keywords: digital ecosystems; bigtech companies; GAFA; digital client profile; cyber risks; attack; cybersecurity

Преимущества цифровых экосистем

Цифровые экосистемы не только приносят инновации в экономику, но и создают дополнительные преимущества для потребителей[1].

На сегодняшний день крупнейшими интернациональными цифровыми экосистемами являются четыре технологические компании из США: Google, Apple, Facebook, Amazon и иногда Microsoft (так называемая GAFA или GAFAM), а также две китайские: Alibaba и Tencent. Успешно используя цифровые платформы и включая в зону обслуживания смежные сегменты рынка эти компании привлекли массу клиентов и добились значительных финансовых успехов[2].

GAFA действуют в США на основании лицензий (полученных в рамках группы) поставщиков услуг по денежным переводам, а в Европейском союзе эти же глобальные игроки (за исключением Apple) имеют статус поставщиков платежных услуг.

В Российской Федерации можно выделить три модели построения цифровых экосистем:

1. Основой является технологическая компания и для её нужд есть (или создается) дочерний банк. Примером может служить симбиоз компании «МТС» и «МТС-Банк»;

2. Модель строится на равноправных (партнерских) отношениях банка и других участников цифровой экосистемы (например, коммерческий банк «Тинькофф Банк»);

3. Ядром выступает кредитная организация. Наиболее известный пример такой модели – крупнейший универсальный банк Восточной Европы и России – ПАО Сбербанк[3] (рис. 1).

[1] На сегодняшний день большинство ежедневных покупок можно совершать онлайн, быстро и в несколько кликов с устройства, имеющего доступ к Интернету и с установленным на нем необходимым web-приложением.

[2] При этом китайские игроки сфокусированы в первую очередь на национальном рынке в силу его масштаба и количества населения, их международная экспансия менее выражена по сравнению с американскими технологическими гигантами. В отличие от глобальных бигтех-компаний китайские экосистемы при выходе на иностранные рынки сохраняют национальный фокус: оказание услуг китайским туристам за рубежом и продвижение китайских производителей товаров.

[3] Инициатива превращения банка в экосистему уровня Google и Amazon предусмотрена «Стратегией-2020». См. подробнее [1] и «Стратегия 2020: как Г.О. Греф обещал “отобрать свой завтрак” у Google и Amazon». URL: https://www.rbc.ru/finances/14/12/2017/5a3298649a79479b6882a13a (дата обращения 23.02.2022).

Рис. 1. / Fig. 1. **Структура цифровой экосистемы Сбербанка / The structure of Sberbank's digital ecosystem**

Государственная поддержка развития российских цифровых платформ является стратегической задачей на ближайшие годы. В указе Президента Российской Федерации «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», отражена необходимость обеспечения внедрения платформенных решений в ряде отраслей экономики, социальной сферы, госуправления и сферы оказания госуслуг, в том числе в интересах населения, индивидуальных предпринимателей и субъектов малого и среднего бизнеса[4].

Цифровой профиль клиента – почему его надо защищать

Успешное функционирование цифровых экосистем возможно только при хорошо отлаженной системе поиска и накопления разнообразной информации о пользователях. Эта совокупность цифровых записей способствует формированию «цифрового профиля клиента» (ЦПК), который включает в себя не только сведения о месте жительства, роде деятельности, любимом отдыхе и развлечениях, но и данные о расходах, гастрономических предпочтениях (исходя из истории покупок в супермаркетах, ресторанах, кафе, продуктовых магазинах), вкусах в одежде и т.п.

Эта информация становится краеугольным камнем фундамента успешного функционирования цифровых экосистем [2]. Порядок её сбора, накопления, хранения, использования, как и способы реализации потребителем права распоряжения принадлежащими ему сведениями (т.е. управление данными), являются одними из

[4] Указ Президента РФ от 07.05.2018 № 204 (ред. от 21.07.2020) «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года». URL: http://www.kremlin.ru/acts/news/57425 (дата обращения 10.02.2022).

центральных вопросов в государственной регуляторной политике[5]. При формировании цифровых экосистем персональные данные клиентов покупаются и продаются вместе с входящими в неё сервисами, причем зачастую клиенты об этом даже не догадываются.

Рассмотрим структуру потоков информации, которая формируется в рамках функционирования обобщенной цифровой экосистемы. На рис. 2 структура цифровой экосистемы схематично представлена четырьмя направлениями обслуживания:

1. Финансы (платежи, управление активами, страхование, сбережения, ипотека, кредитование);

2. Образ жизни (социальные сети и мессенджеры, игры, видео/кинотеатры, музыка, книги, онлайн-обучение, такси/автопрокат, аренда/продажа недвижимости, другие сервисы);

3. Информационные технологии (операционная система, телеком сервисы, поисковый сервис, голосовой помощник, облачные сервисы);

4. Электронная коммерция (онлайн-магазины электронной торговли).

Всевозможная информация о клиентах из сервисов поступает в единое хранилище данных, где, при помощи алгоритмов машинного обучения, и формируется ЦПК. В результате использования ЦПК интернет-сервисы могут спрогнозировать модель поведения пользователя и немало удивить его[6].

Рис. 2. / Fig. 2. **Структура информационных потоков в цифровой экосистеме / Structure of information flows in the digital ecosystem**

Цифровая экосистема оперирует информацией о ЦПК в нескольких направлениях, которые на рис. 2 скомпонованы в отдельные блоки:

- Аналитика;
- Учет;
- Управление рисками;
- Внутренний контроль.

В реальности, для работы с этими данными (в зависимости от архитектуры цифровой экосистемы) могут быть организованы как маленькие отделы, так и крупные департаменты. Все зависит от поставленных задач.

---

[5] Регулирование рисков участия банков в экосистемах и вложений в иммобилизованные активы: Доклад для общественных консультаций. Банк России, июнь 2021 г. – 33 с. URL: https://cbr.ru/Content/Document/File/123688/Consultation_Paper_23062021.pdf (дата обращения 14.03.2022).

[6] Правда или миф, что смартфоны нас подслушивают? URL: https://www.kaspersky.ru/blog/smartphones-eavesdropping/23201/ (дата обращения: 02.03.2022).

Защита цифровых экосистем от киберугроз

Данные о своих клиентах собирают все организации, и в той мере, в какой они способны обеспечить адекватную защиту от киберугроз, они выполняют свои обязательства и обеспечивают кибербезопасность. Данная задача существенно усложняется, когда они участвуют в цифровой экосистеме. В этой среде участники цифровой экосистемы больше не могут контролировать ситуацию. Им приходится полагаться на гарантии безопасности своих партнеров: поставщиков облачных сервисов, компонентов, товаров и услуг, клиентов, продавцов, – и, конечно, они самостоятельно не способны в полной мере контролировать их.

Основные типы кибератак, с которыми сталкиваются цифровые экосистемы, следующие:

1. Атаки через поставщиков услуг – состоят во взломе подрядчиков или дочерних организаций, с последующей атакой на связанную с ними целевую организацию.

Такие атаки делятся на два вида:

– supply chain[7] – атака на цепочку поставок;

– trusted relationship[8] – атака через доверительные отношения.

Эти виды атак похожи, но реализуются они по-разному [3].

Атака на цепочку поставок реализуется с помощью изменений в программном, аппаратном и микропрограммном обеспечении поставляемых программных или аппаратно-программных средств. В программное обеспечение поставленного средства либо в его обновление внедряется вредоносный код или производится изменение конфигурации. Данные манипуляции обеспечивают в ходе эксплуатации предоставление прямого доступа к атакуемой системе, или соединение её с центром управления атакой (Command & Control, C&C) [4].

Атака на цепочку поставок, в большинстве случаев, не является целенаправленной, т.к. для её успеха необходимо одновременное свершение маловероятных событий:

а) атакуемая компания установит скомпрометированное обновление или устройство загрузит вредоносную конфигурацию;

б) атакуемое устройство, для которого подготовлено скомпрометированное обновление, имеет доступ во внешние сети и сконфигурировано на автоматическое обновление.

Атаки через доверительные отношения связаны с компрометацией каналов взаимодействия инфраструктур двух организаций. Как правило, организации, взаимодействующие в рамках цифровой экосистемы, пользуются услугами подрядчиков, в том числе небольших организаций или экспертов. При этом подрядчики работают удаленно с устройств неконтролируемых организацией. Сначала злоумышленники получают несанкционированный доступ к инфраструктуре подрядчиков, а в дальнейшем проникают в целевую инфраструктуру атакуемой организации, развивая атаку и маскируя свои действия. По статистике, подвергшиеся такой атаке организации не ожидали вредоносных действий со стороны доверенных партнеров и не считали необходимым применять к ним защитные меры.

Кроме того, злоумышленники могут задействовать различные сопутствующие виды атак, например, «внутренний» фишинг [5]. Анализ таких инцидентов показывает, что в большинстве случаев внутренняя инфраструктура атакованных организаций была менее защищена, чем внешний периметр, что существенно облегчало действия злоумышленников.

2. Утечки информации – актуальны как для традиционных систем хранения данных организаций, так и для единых хранилищ данных цифровых экосистем подверженных схожим векторам атак.

Зачастую значительное количество ресурсов обрабатываемой информации, её объема, используемых публичных облачных сервисов и хостинг-провайдеров подвергает риску кибератак хранилища этой информации. Уровень вероятных угроз и ущерба пропорционален преимуществам, которые обретет злоумышленник, завладев этой информацией.

[7] в классификации MITRE ATT&CK – ID:1195

[8] в классификации MITRE ATT&CK – ID:1199

Значительный ущерб репутации цифровой экосистемы может нанести утечка персональных данных, данных, составляющих коммерческую тайну, интеллектуальной собственности или иной информации ограниченного доступа. При выявленной утечке цифровую экосистему неизбежно ожидают штрафные санкции и иски, но не только они. В современной чрезвычайно конкурентной среде также неизбежен моральный ущерб, причем как для отдельного бренда, так и для всей цифровой экосистемы в целом. К сопутствующему ущербу можно отнести долгие и тяжелые процедуры восстановления имиджа.

3. Атаки на программы лояльности цифровых экосистем и бонусные программы.

Программы лояльности задействуют в мировом масштабе значительные цифровые финансовые активы. Поэтому они привлекают внимание как профессиональных киберпреступников, так и мелких мошенников, которые пользуются данной возможностью как дополнительным источником дохода.

Киберпреступники не останавливаются перед относительно небольшими суммами денег и ограниченной ликвидностью баллов – большинство программ имеет возможность предоставления баллов третьим лицам или их конвертации в более ликвидные баллы партнерской программы, приобретения подарочных сертификатов, которые в дальнейшем можно обменять на реальные деньги. Небольшой размер хищений компенсируется меньшей сложностью мошенничества, меньшим риском поимки и, как правило, меньшими последствиями при разоблачении преступной схемы [6].

Наиболее распространенный тип кибератаки заключается в получении несанкционированного доступа к аккаунту программы. Реальный пользователь аккаунта может не догадываться о возможности доступа к его учетной записи через интернет или не пользоваться данной опцией. Начальная компрометация может быть вызвана вирусной атакой на пользовательское устройство или утечкой данных из инфраструктуры компании.

Зачастую данная информация перепродается киберпреступниками так же, как и данные банковских карт, персональные данные и учетные записи банк-клиентов.

По причине откровенно слабой системы защиты во многих бонусных программах процветает внутреннее мошенничество: массовый выпуск фиктивных карт, произвольное списание бонусов, фарминг[9] бонусов через покупку и возвратный платеж (чарджбэк – от англ. chargeback). Иногда возможно непосредственное изменение баланса баллов в системе учета по причине отсутствия систем проверки целостности [7].

Внимания заслуживает злонамеренное использование программы лояльности: когда клиенты находят уязвимость в логике работы системы – самостоятельно или же через инсайдеров. Перед компанией встает вопрос, стоит ли признавать баллы недобросовестных пользователей или подвергаться репутационным рискам, обнуляя баллы честных пользователей.

Итак, мы видим, что цифровые экосистемы подвержены множеству киберугроз, и в случае реализации таких угроз злоумышленник получает вполне ощутимый материальный выигрыш, а все участники цифровой экосистемы несут потери.

Поэтому, прежде чем подключиться к цифровой экосистеме, организации следует провести тщательную проверку потенциальных партнеров (особенно конкурентов) аналогичную проверке при совершении сделки слияния и поглощения. В случае если в рамках цифровой экосистемы организация предоставляет поставщикам доступ к своим IT-системам, ей следует провести оценку соответствующих рисков. Эти мероприятия состоят в изучении деловой активности поставщика и оценки её на предмет возможного риска, который она представляет для организации. Организации могут использовать тот же подход к своим взаимодействиям в рамках цифровой экосистемы: оценить риски, связанные с любыми сущностями цифровой экосистемы, которая технически связана с организацией или делится с ней данными.

[9] Фарминг (от англ. pharming) – процедура скрытного перенаправления жертвы на ложный IP-адрес.

Поскольку в основе любой цифровой экосистемы лежит информационное взаимодействие, это предъявляет повышенные требования по кибербезопасности: зачастую обычные пароли и даже двухфакторная аутентификация не обеспечивают надежную защиту в среде цифровой экосистемы, где использование искусственного интеллекта и машинного обучения позволяет недобросовестным участникам добиваться конкурентного преимущества. Поэтому для обеспечения безопасности автоматизированного обмена данными с потенциальными партнерами организациям следует соблюдать меры предосторожности.

Выбранные меры предосторожности имеют большое значение для защиты организации. Вместе с тем, партнеры и клиенты организации хотят гарантии того, что организация внедрила все средства защиты, необходимые для безопасности конфиденциальных данных.

Поэтому, руководство организации должно организовать проведение периодического внешнего аудита уровня информационной безопасности в своей организации [8, 9] – обеспечения доступности, целостности и конфиденциальности обрабатываемой информации.

Цифровые экосистемы – это путь в будущее, поэтому организациям необходимо активно взаимодействовать с ними, чтобы не остаться в прошлом.

При должной осмотрительности, надлежащей защите и независимом аудите, обеспечивающем контроль эффективности защитных мер, организация может обеспечить достаточный уровень защиты от киберугроз в цифровых экосистемах. Однако, в реальности, как бы организация ни старалась обеспечить безопасность своих сведений, часть из них неизбежно потеряет свою конфиденциальность.

Дополнительные риски использования «цифровых помощников»

Возможности цифровых экосистем позволяют максимально приблизить различные информационные и финансовые услуги к потребителям. Для этого клиентам достаточно иметь подключенный к Интернету компьютер или смартфон и установить на эти устройства необходимое программное обеспечение.

Компьютерные сети становятся быстрее, мобильные устройства оснащаются новыми датчиками, а методы моделирования человеческого поведения становятся более точными и детализированными. Все это превращает смартфоны в центры персональной информации о своих пользователях.

Современные смартфоны позволяют не только извлекать информацию о местонахождении и шаблонах звонков пользователя, но также отображать социальные сети, участником которых он является, и даже оценивать настроение владельца, анализируя повседневное виртуальное общение. Потребители уже могут делать покупки, сканируя товары при помощи своих смартфонов, и добавлять к виртуальном биографиям, состоящим из мобильного трафика, информацию о финансах и выборе продуктов.

Именно эти данные и называют сегодня «нефтью экономики»[10]. С помощью них владельцы данной информации (особенно в условиях функционирования цифровых экосистем) могут влиять на выбор клиента и предлагать ему «умные» услуги и целевой контент[11].

Учитывая критичность данных, которые будут скапливаться в хранилищах цифровых экосистем (а в действующих уже скапливаются), вопросы обеспечения кибербезопасности (включая мероприятия по предотвращению кибермошенничества) становятся основными,

[10] Что такое Big Data и почему их называют «новой нефтью». URL: https://trends.rbc.ru/trends/innovation/5d6c020b9a7947a740fea65c (дата обращения 27.02.2022).

[11] Абдрахманова Г.И., Вишневский К.О., Гохберг Л.М. и др. Цифровая экономика 2019: краткий статистический сборник. Национальный исследовательский университет «Высшая школа экономики». М.: НИУ ВШЭ, 2019. – 96 с. URL: https://www.hse.ru/data/2018/12/26/1143130930/ice2019kr.pdf (дата обращения 05.03.2022).

т.к. от их решения будет зависеть уровень доверия не только к отдельно взятой цифровой экосистеме, но и к кредитно-финансовой сфере в целом[12].

Кибератакам могут подвергаться все участники цифровых экосистем (включая самых незащищенных – клиентов организаций, участниц цифровых экосистем), поэтому можно предположить повышение активности кибермошенничества с помощью методов социальной инженерии и особенно фишинга. Ведь выбором в большинстве случаях будут заниматься роботы с использованием машинного обучения. И если пользователи привыкнут доверять своим «цифровым помощникам», то риски кибермошенничества с использованием манипулятивных техник и фишинговых схем значительно возрастут.

Одной из самых опасных киберугроз являются атаки на web-приложения, которыми будут пользоваться клиенты организаций, входящих в состав участников цифровых экосистем.

Технология работы современных web-приложений обычно не ограничивается функцией доставки информации пользователю в форме обычных web-страниц. Обработка основных компонентов динамически изменяемого интерфейса, обработка и хранение данных, бизнес-логика выносится разработчиками на серверы приложений и баз данных, которые осуществляют как промежуточную обработку данных, так и используются для генерации и вывода специфических данных пользователям. Данные компоненты обычно размещаются и выполняются в центрах обработки данных, в т.ч. облачных, и могут либо разделять, либо не разделять хранилища данных между собой. В программном коде сложного web-приложения могут быть задействованы сервисы различных компаний, которые могут иметь географически распределенную инфраструктуру [10].

Хакеры используют уязвимости переходов и с помощью злонамеренного исправления web-приложений направляют пользователя по поддельному адресу на незащищенный ресурс. Данные атаки вызывают значительные проблемы с общей безопасностью участника цифровой экосистемы, так как пользователи с низким уровнем соблюдения кибергигиены доверяют таким переходам, что приводит к утечке конфиденциальных данных и(или) потере денежных средств (рис. 3).

Рис. 3. / Fig. 3. **Обобщенная схема атаки на клиентские web-приложения в условиях функционирования цифровых экосистем / Generalized scheme of attack on client web applications in the conditions of functioning of digital ecosystems**

[12] Эта статья посвящена организациям кредитно-финансовой сферы, поэтому упоминается именно она. Очевидно, что распространение экосистем в других отраслях будет ставить эти же задачи и перед ними.

Принцип атаки заключается в том, что хакеры создают видимость легального перехода на интерфейс получения подарков или оформления доставки (интерфейс максимально замаскирован под известные сервисы, чтобы сбивать с толку пользователя) и вынуждают пользователя самостоятельно ввести необходимую злоумышленнику информацию.

Добавим, что уже сейчас выявляется достаточно большое количество фишинговых сайтов, выдающих себя за web-представительства различных организаций, в том числе входящих в состав кредитно-финансовой сферы.

Для эффективного противодействия фишингу и кибермошенничеству требуется повышение уровня критического мышления, киберграмотности и финансовой грамотности населения. Что касается критического мышления, интерес представляет простая формула 5W+H из [11], которая раскрывается так: “Who? What? When? Why? Where? How?” или «Кто? Что? Когда? Почему? Где? Как?» (рис. 4).

Рис. 4. / Fig. 4. **Формула 5W+H. См. подробнее в [11] / Formula 5W+H. See details in [11]**

Эти задачи необходимо решать не только самостоятельно, но и:

а) силами организаций, в том числе входящих в состав цифровых экосистем;

б) на государственном уровне (Министерство науки и высшего образования России, Министерство просвещения России, Роскомнадзор, Росфинмониторинг, Банк России).

Век цифровых технологий рождает не только преимущества получения качественных цифровых услуг, но и киберугрозы, последствия проявления которых становятся все более значительными.

Заключение

Развивающееся регулирование инновационных платформ и цифровых экосистем, должно не только стимулировать их дальнейшее развитие, но также решать задачу снижения вероятности реализации сопутствующих рисков, оценки возможного ущерба и сокращения негативных последствий от их реализации.

Для предотвращения части рисков желательно начать разработку кодексов и нормативно-правовых актов, регулирующих поведение человека в информационных сетях и процессах. Вопросы обеспечения кибербезопасности и управления киберрисками на протяжении всего жизненного цикла цифровых экосистем выходят на первый план.

Список литературы

1. Греф Г.О. Лидерство – это ответственность за свою жизнь // Прямые инвестиции. 2013. № 12 (140). С. 5–6. ISSN: 1727-1304.

2. Скиннер К. ValueWeb. Как финтех-компании используют блокчейн и мобильные технологии для создания интернета ценностей. М.: Манн, Иванов и Фербер, 2018. – 416 с. ISBN 978-5-00100-948-1.

3. Ivanyuk V., Slovesnov E., Soloviev V. Credit risk assessment in the banking sector based on neural network analysis // Lecture Notes in Computer Science. 2021. Vol. 12855 LNAI. Pp. 267–277. ISSN: 0302-9743, eISSN: 1611-3349. DOI: 10.1007/978-3-030-87897-9_25.

4. Osipov A., Pleshakova E., Gataullin S., Korchagin S., Ivanov M., Finogeev A., Yadav V., Deep Learning Method for Recognition and Classification of Images from Video Recorders in Difficult Weather Conditions. Sustainability. 2022, vol. 14(4), no. 2420. 16 p. ISSN: 2071-1050. DOI: 10.3390/su14042420.

5. Прокопайло А.А. Целевой фишинг // StudNet. 2021. Т. 4. № 7. С. 1645-1650. ISSN: 2658-4964. URL: https://cyberleninka.ru/article/n/tselevoy-fishing (дата обращения 03.03.2022).

6. Diogenes Y., Ozkaya E. Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Birmingham – Mumbai: Packt Publishing, 2018. – 384 p. ISBN: 978-1-78847-529-7.

7. Дудка А.Б., Ревенков П.В., Силин Н.Н. и др. Кибербезопасность в условиях электронного банкинга: практическое пособие. М.: Прометей, 2020. – 522 с. ISBN: 978-5-907244-61-0.

8. Славин Б.Б. Зачем и кому необходим ИТ-аудит? // БИТ. Бизнес & Информационные технологии. 2021. № 2 (105). С. 32–35. ISSN: 2313-8718.

9. Ревенков П.В., Бердюгин А.А., Чебарь А.Г. Экосистемы: преимущества платформенных моделей, особенности построения и сопутствующие киберриски // Банковское дело. 2022. № 1. С. 65–72. ISSN: 2071-4904

10. Королёва Е.В., Солган Л.А. Экосистема в экосистеме: развитие финансовых технологий в России // Финансы и кредит. 2021. Т. 27. № 5 (809). С. 1116–1131. DOI: 10.24891/fc.27.5.1116. ISSN: 2071-4688, eISSN: 2311-8709. DOI: 10.24891/fc.27.5.1116.

11. Лукацкий А.В. Обзор мировых трендов по промышленной кибербезопасности // Релейщик. 2020. № 1 (36). С. 60–62.

References

1. Gref G.O. Leadership is a responsibility for your life. *Direct investment.* 2013;12(140):5-6. ISSN: 1727-1304.

2. Skinner C. ValueWeb. *How Fintech firms are using mobile and blockchain technologies to create the Internet of Value.* Moscow. Mann, Ivanov and Ferber, 2018. 416 p. ISBN 978-5-00100-948-1.

3. Ivanyuk V., Slovesnov E., Soloviev V. Credit risk assessment in the banking sector based on neural network analysis. *Lecture Notes in Computer Science.* 2021;12855:267-277. ISSN: 0302-9743, eISSN: 1611-3349. DOI: 10.1007/978-3-030-87897-9_25.

4. Osipov A., Pleshakova E., Gataullin S., Korchagin S., Ivanov M., Finogeev A., Yadav V., *Deep Learning Method for Recognition and Classification of Images from Video Recorders in Difficult Weather Conditions. Sustainability.* 2022;14(4);2420:16. ISSN: 2071-1050. DOI: 10.3390/su14042420.

5. Prokopailo A.A. Target phishing. *StudNet.* 2021;4(7):1645-1650. ISSN: 2658-4964. URL: https://cyberleninka.ru/article/n/tselevoy-fishing (date of access 03.03.2022).

6. Diogenes Y., Ozkaya E. *Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics.* Birmingham – Mumbai: Packt Publishing. 2018. – 384 p. ISBN: 978-1-78847-529-7.

7. Dudka A.B., Revenkov P.V., Silin N.N. et al. *Cybersecurity in the conditions of electronic banking.* Practical guide. Moscow. Prometei, 2020. 522 p. ISBN: 978-5-907244-61-0.

8. Slavin B.B. Why and who needs an IT audit? *BIT. Business & Information Technology.* 2021;2(105):32-35. ISSN: 2313-8718.

9. Revenkov P.V., Berdyugin A.A., Chebar A.G. Ecosystems: advantages of platform models, features of construction and related cyber risks // Bankovskoye delo = Banking. 2022, no. 1. Pp. 65–72.

10. Koroleva E.V., Solgan L.A. Ecosystem in ecosystem: development of financial technologies in Russia // Finance and Credit. 2021, vol. 27, no. 5 (809). Pp. 1116–1131. DOI: 10.24891/fc.27.5.1116. ISSN: 2071-4688, eISSN: 2311-8709. DOI: 10.24891/fc.27.5.1116.

11. Lukatsky A.V. Overview of global trends in industrial cybersecurity // Releyshchik = Relayer. 2020, no. 1 (36). Pp. 60–62.