УДК 004.056
ББК 65.050
JEL G29, G32, L86

Аутсорсинг информационной безопасности финансовых организаций: основные подходы и сопутствующие риски

Водоватов Максим Сергеевич, магистрант 2 курса,
Финансовый университет при Правительстве Российской Федерации
Адрес: 4-й Вешняковский проезд, д. 4, корп. 2, г. Москва, 109456, Россия
Ревенков Павел Владимирович, доктор экономических наук, доцент,
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: PVRevenkov@fa.ru

Аннотация: Статья затрагивает вопросы аутсорсинга информационной безопасности в финансовых организациях. Подробно рассматривается значимость определения рисков и разработки Service Level Agreements (SLA) в контексте аутсорсинга, подчеркивая необходимость тщательного планирования и учета специфических требований финансовых организаций. Выделены ключевые аспекты аутсорсинга информационной безопасности. Особое внимание уделяется вопросам мониторинга и контроля параметров оценки услуг, включая процедуры мониторинга, уведомления, регулярного контроля и хранения данных для проверки. Также статья обращает внимание на особенности российского рынка услуг информационной безопасности и важность адаптации стратегии аутсорсинга к этим особенностям. Статья предоставляет ценные рекомендации для финансовых организаций, стремящихся обеспечить надежную информационную безопасность.

Ключевые слова: аутсорсинг; параметры оценки; управление; оценка услуг; рекомендации; финансовые организации.

Outsourcing information security of financial organizations: main approaches and associated risks

Maxim S. Vodovatov, 2nd year master's student,
Financial University under the Government of the Russian Federation
Address: 4th Veshnyakovsky passage, 4, bldg. 2, Moscow, 109456, Russia
Pavel V. Revenkov, Doctor of Economics, Associate Professor,
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: PVRevenkov@fa.ru

Abstract: The article covers important aspects of information security outsourcing in financial organizations. The importance of risk identification and development of Service Level Agreements (SLA) in the context of outsourcing is considered in detail, emphasizing the need for careful planning and consideration of specific requirements of financial organizations. The article highlights the key aspects of information security outsourcing. Particular attention is paid to the monitoring and control of the parameters of the evaluation of services, including monitoring procedures, notification, regular monitoring and storage of data for verification. The article also draws attention to the features of the Russian information security services market and the importance of

adapting the outsourcing strategy to these features. The article provides valuable recommendations for financial organizations seeking to ensure reliable information security.

Keywords: outsourcing; evaluation parameters; management; evaluation of services; recommendations; financial organizations.

Введение

Увеличение скорости внедрения цифровых технологий и автоматизации в области финансовых услуг, более глубокое разделение труда и специализация в сфере деятельности, а также необходимость адаптации финансовых рынков к современной геополитической обстановке создают ситуацию, в которой совершенствование информационной безопасности (ИБ) становится одной из главных задач для финансовых организаций (ФО). Однако, далеко не все участники финансового рынка способны качественно и эффективно обеспечивать, и поддерживать собственное подразделение ИБ. Это, в свою очередь, неминуемо ведет к снижению уровня обеспечения ИБ (включая невыполнение требований нормативно-правовых документов на должном уровне). Одним из вариантов решения данной проблемы можно выделить передачу данных функций (которые в противном случае должны были бы выполняться самостоятельно ФО) на аутсорсинг[1] внешней стороне – специализированной организации, которая уже наработала экспертизу в предоставлении данного вида услуг.

Краткий анализ аутсорсинга информационной безопасности в финансовых организациях

Как следует из статистики[2], к аутсорсингу какой-либо функции прибегают половина опрошенных ФО. Распределение функций, передаваемых на аутсорсинг представлено на рис. 1.

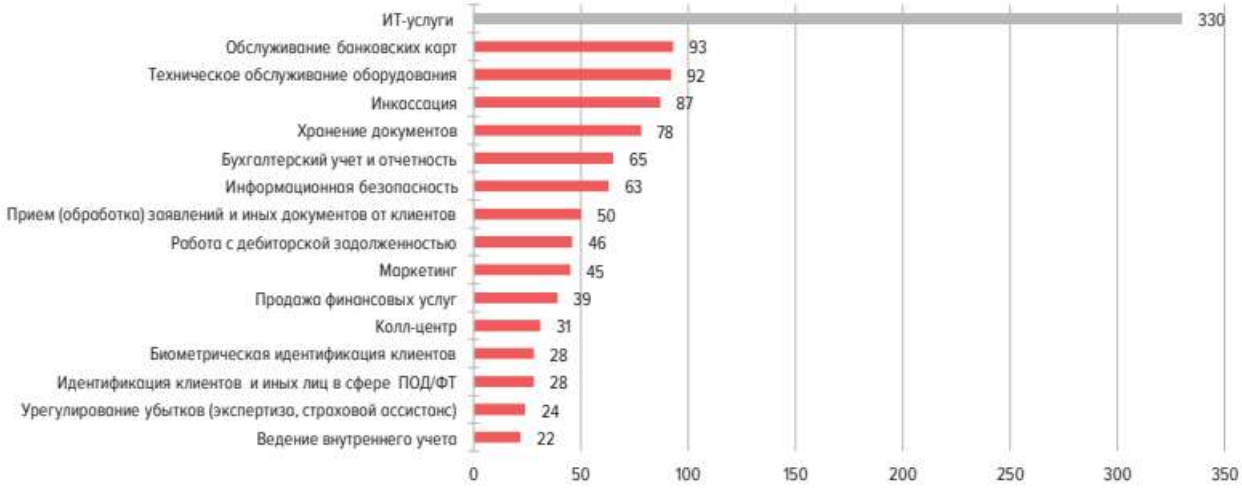

Рис. 1. / Fig. 1. **Основные функции, при осуществлении которых применяется аутсорсинг (по количеству лицензий опрошенных финансовых организаций) / Main functions for which outsourcing is used (by the number of licenses of surveyed financial organizations)**

[1] Аутсорсинг (от анг. outsoursing, out – внешний, source – ресурс) представляет собой передачу определенных бизнес-процессов или производственных функций компании-заказчика на обслуживание узкоспециализированной организации-исполнителю (поставщику услуг). Поставщиками услуг в данном случае могут выступать как сторонние организации, не связанные с участником финансового рынка, так и иные организации, которые могут быть как аффилированы, так и образовывать с ним одну банковскую или финансовую группу.

[2] См. подробнее «Управление рисками аутсорсинга на финансовом рынке. Доклад для общественных консультаций. Москва 2022» URL: http://www.cbr.ru/Content/Document/File/142481/Consultation_Paper_06122022.pdf (дата обращения 13.11.2023).

Аутсорсинг может быть, как полным, так и частичным, а также может осуществляться как внутри ФО, так и вовне.

Основная особенность аутсорсинга в области ИБ заключается в том, что полностью передать все функции этой области внешнему исполнителю практически невозможно. Это объясняется наличием определенных функций обеспечения ИБ, которые невозможно делегировать третьей стороне при любых обстоятельствах, особенно в контексте процессов обеспечения ИБ в ФО.

Современный аутсорсинг ИБ в большинстве случаев предоставляется по модели Managed Security Service Provide (MSSP), при которой поставщик услуг удалённо контролирует или администрирует файрволы, системы предотвращения вторжений (IPS) и другие средства защиты информации (СЗИ), которые находятся внутри ФО, а также обеспечивает их круглосуточное сопровождение. При этом услуги аутсорсинга, как правило, предоставляются на основе специального документа – внутреннего соглашения о предоставлении услуг, известного как Service Level Agreement (SLA). В первую очередь, это связано с важностью обработки информации в области ИБ для наиболее эффективного управления бизнес-процессами ФО.

Обсуждение

Аутсорсинг предоставляет набор стратегических выгод, среди которых ключевой пункт заключается в возможности фокусироваться на основной бизнес-деятельности и экономии ресурсов, которые ранее расходовались на задачи, не относящиеся к получению прибыли. Основываясь на рекомендациях [1], представленных Центральным банком Российской Федерации (Банк России), для ФО имеет смысл рассмотреть возможность аутсорсинга следующих аспектов обеспечения ИБ:

1. Кадровое обеспечение:

– гарантирование безопасности данных при отсутствии внутри ФО необходимого количества сотрудников с требуемой квалификацией;

– освобождение ключевых сотрудников ФО от рутинных задач для их привлечения в более приоритетные проекты.

2. Экономическая эффективность:

– обеспечение стабильности и прозрачности финансовых затрат на обеспечение процессов ИБ при использовании аутсорсинга;

– оптимизация расходов на организацию и эксплуатацию систем обеспечения ИБ ФО.

3. Техническое и технологическое обеспечение:

– повышение уровня общей ИБ с применением современных инструментов, систем и технологий;

– поддержка реализации критически важных процессов в обеспечении ИБ в режиме круглосуточной доступности;

– возможность оперативной реализации и усовершенствования отдельных процессов в сфере обеспечения ИБ.

Таким образом, обычно аутсорсинг включает в себя передачу управления над технически сложными СЗИ, администрирование которых требует значительных финансовых и временных затрат, а также высокой квалификации персонала. Однако тут важно отметить – разработка политики ИБ всегда остается в компетенции ФО, в то время как поставщик услуг занимается только настройкой СЗИ на основе разработанной политики.

Риски аутсорсинга ИБ в ФО

Существует ошибочное мнение, что использование аутсорсинга для ФО автоматически перекладывает все риски в области ИБ на поставщика услуг. Это в корне неверно, на самом же деле организация имеет возможность передать поставщику услуг только часть ответственности за конкретные меры по обеспечению ИБ, и даже это, в конечном счете никак

не освобождает ее от общей ответственности за возможные инциденты нарушения ИБ. Например, существуют такие риски, которые могут быть напрямую связаны с защитой персональных данных, и они априори не могут полностью перекладываться на поставщика услуг. Банк России, в свою очередь, четко указывает [1], что передача выполнения бизнес-функций на аутсорсинг не снимает обязанности и не переносит ответственности с ФО, включая вопросы ИБ. Более того, использование услуг поставщика, первоначально предназначенных для снижения рисков ИБ в ФО, часто сопровождается появлением новых рисков, связанных с передачей критически важных функций в области ИБ третьей стороне.

Риски, связанные с аутсорсингом ИБ, по большей части обладают всеми теми же характерными чертами рисков, что присущи и любому аутсорсингу в целом, однако, они имеют ряд своих особенностей. Так, можно выделить следующие:

– полная или частичная утрата доверия к поставщику услуг. При осуществлении работ по обеспечению ИБ, поставщик услуг имеет постоянный доступ к чувствительной информации, будь то конфиденциальная информация или даже банковская тайна, раскрытие которой может значительно сказаться на репутации ФО [4];

– операционная зависимость от поставщика услуг. Так, полагаясь на услуги конкретного поставщика, ФО неминуемо увеличивает свою зависимость от выбранного поставщика в вопросах стабильности и надежности бизнеса, например, уход поставщика с рынка может критично сказаться на уровне ИБ ФО;

– скрытые расходы. Возможно, некоторые издержки не будут учтены при определении стоимости услуги в аутсорсинговом соглашении на момент его подписания, поскольку они еще не могут быть четко определены на данном этапе;

– нарушение соглашений с поставщиком услуг. Одним из основных рисков является неправильное планирование взаимодействия между ФО и поставщиком услуг. Именно поэтому, договор с поставщиком услуг должен быть всеобъемлющим, учитывать всевозможные сценарии развития событий в процессе аутсорсинга, например, обязательно включая в себя условия досрочного расторжение соглашения аутсорсинга, процедуры изменения, либо расширения услуг, а также пересмотр текущих тарифов и условия обеспечения непрерывности предоставления услуг в чрезвычайных ситуациях;

– разделение «рабочего пространства» поставщика услуг между несколькими своими клиентами. Наличие такого пространства у поставщика услуг увеличивает вероятность несанкционированного доступа к конфиденциальной информации одной ФО со стороны других клиентов этого же поставщика услуг;

– правовые риски. ФО и поставщик услуг должны четко и заблаговременно определить возможные юридические последствия инцидентов в сфере ИБ, в которые они обе могут быть втянуты.

«Качественный» SLA должен содержать прозрачные параметры предоставляемых услуг, только тогда, SLA может принести выгоду обеим сторонам аутсорсинга – для ФО оно дает возможность контролировать уровень предоставляемых ей услуг, а поставщику услуг, в свою очередь, поможет эффективно планировать необходимые ресурсы и нагрузку.

В подходах к разработке SLA, регламентирующего аутсорсинг в области ИБ, рекомендуется обращаться к общепринятым методам и стандарты. К примеру, стандарт СТО БР ИББС-1.4-2018, может служить хорошим примером, поскольку описывает существующие риски аутсорсинга ИБ, зоны ответственности, особенности мониторинга и контроля риска нарушения ИБ, а также требования к поставщику услуг и оценку SLA.

Более того, структура, описанная в данном стандарте, может помочь определить области, в которых следует устанавливать показатели для оценки качества предоставляемых услуг аутсорсинга.

Здесь также важно отметить, какие именно преимущества получает ФО:

– во-первых, это помогает ФО определить четкие области ответственности как для самой организации, так и для поставщика услуг;

– во-вторых, это помогает точно идентифицировать и описать основные параметры, использующиеся для оценки услуги предоставления аутсорсинга;

– в-третьих, это помогает грамотно устанавливать и документировать процедуры оценки и контроля этих параметров. Сюда можно отнести, например, периодические независимые аудиты. Результатом такого подхода будет значительное уменьшение предпосылок возникновения различных угроз в области ИБ.

Параметры оценки услуг аутсорсинга ИБ

Прежде чем приступить к определению состава параметров, которые требуется периодически контролировать при использовании аутсорсинга в области ИБ, необходимо отметить – такой состав может значительно различаться от организации к организации, в зависимости от предоставляемых услуг, политики ФО и целей самого аутсорсинга. Также целесообразно определять эти параметры на основе анализа рисков конкретной ФО. Такой подход позволяет значительно сократить количество контролируемых параметров и увеличить эффективность всего процесса управления услугами аутсорсинга.

Так, важно учитывать следующие факторы:

– специфичные риски, которые могут быть присущи только конкретной ФО;

– предыдущий опыт аутсорсинга, возможно, опыт сбоев и инцидентов в области ИБ;

– риски, связанные с самой процедурой аутсорсинга как таковой.

Современные методологии, системы и инфраструктуры ИБ стремительно развиваются в наши дни, и в значительной степени зависят от особенностей как самой ФО, так и спектра услуг, переданных на аутсорсинг. По этой причине, какого-либо "универсального" набора параметров оценки услуг аутсорсинга, подходящих для всех ФО не существует. Эффективным подходом здесь будет определение таких параметров методом "от общего к частному" для конкретной ФО, начиная с общих целей и задач программы обеспечения ИБ организации и заканчивая выработкой специфических параметров, характеризующих, например, конкретную деятельность поставщика услуг.

К общим требованиям можно отнести:

– обеспечение экономической эффективности, включая оценку расходов на предоставление конкретных служб в области ИБ и контроль за их правильным функционированием;

– согласованность с целями компании, такими как повышение операционной эффективности, улучшение управляемости, обеспечение гибкости и другие;

– сосредоточенность на обеспечение конфиденциальности, целостности и доступности данных конкретной организации;

– соблюдение требований стандартов и нормативных актов, таких как, PCI DSS, 152-ФЗ, СТО БР ИББС-1.4-2018 и другие.

– применение S.M.A.R.T.-критерий (конкретность, измеримость, достижимость, повторяемость, ограниченность по времени).

По мнению авторов, можно выделить ряд типичных параметров (табл. 1).

Таблица 1. Параметры управления уровня услуг аутсорсинга

Параметр	Описание	Пример
Экономическая эффективность услуги		
Стоимость	Оценка ежегодных расходов на услуги аутсорсинга ИБ.	Стоимость аутсорсинга ИБ в год составляют 3000000 руб.
Расходы на каждый успешно предотвращенный инцидент	Расчет стоимости на каждый успешно предотвращенный инцидент безопасности.	Средние расходы на предотвращение одного инцидента составляют 50000 р.

Уровень угроз и инцидентов		
Количество обнаруженных инцидентов безопасности в месяц	Количество обнаруженных инцидентов безопасности в определенный период.	10 инцидентов в месяц.
Уровень серьезности инцидентов	Оценка серьезности инцидентов и их влияния на организацию.	95% инцидентов имеют низкий уровень серьезности.
Операционная эффективность услуги		
Время реагирования на инциденты	Среднее время, необходимое для реагирования на инциденты безопасности и устранения уязвимостей.	Среднее время реагирования на инциденты составляет 30 минут.
Процент успешно расследованных инцидентов	Процент инцидентов, которые успешно расследованы и устранены.	95% всех инцидентов безопасности успешно расследованы.
Уровень обеспечения конфиденциальности, целостности и доступности информации компании		
Уровень защиты данных	Оценка уровня защиты данных и информации от утечек и несанкционированного доступа.	Ни одна утечка данных не была зарегистрирована за последний год
Уровень доступности услуг ИБ	Оценка доступности услуг ИБ и их способности обеспечивать непрерывность бизнес-процессов.	Уровень доступности услуг - 99,9%.
Уровень доступности поддержки		
Время доступности службы поддержки	Процент времени, в течение которого служба поддержки ИБ доступна для клиентов.	Служба поддержки доступна 24/7.
Время ожидания ответа службы поддержки	Среднее время ожидания ответа от службы поддержки при обращении клиента.	Среднее время ожидания ответа - менее 10 минут.

Эти параметры помогут более полно оценить уровень услуг аутсорсинга ИБ и удостовериться в их эффективности, безопасности и операционной эффективности.

Важно понимать, что определение параметров для оценки качества услуг аутсорсинга не сможет гарантировать надежность работы поставщика услуг и доверие к качеству предоставляемых услуг. Поэтому крайне важно обращать особое внимание на выстраивание эффективного процесса мониторинга контроля таких параметров. Если обобщить, то суть такого мониторинга заключается не только в своевременном обнаружении, но и в предвидении превышения пороговых значений определенных параметров – это может позволить вовремя принять соответствующие меры для предотвращения или компенсации возможных отклонений (в том числе и штрафные санкции).

Для объективной оценки качества услуг ИБ, особенно когда параметры рассчитываются поставщиком услуг, необходимо учесть следующие аспекты:

– формат представления данных, содержащих информацию о текущих показателях параметров ФО. Это важно для возможности проведения всесторонней ретроспективной оценки и сравнения;

– установление точного времени, когда ФО будет уведомлена о последних значениях параметров. Это позволяет определить регулярность обновлений (например, еженедельно в определенное время);

– определение временного интервала для мониторинга параметров, который минимизирует эффект «статистического усреднения». Разумным выбором является ежемесячный или еженедельный контроль;

– заключение обязательств со стороны поставщика услуг по надежному и долгосрочному хранению статистических данных, используемых при расчете параметров. Эта информация должна быть доступна независимым аудиторам для проверки правильности расчетов.

Выводы

При переходе на аутсорсинг важно также учитывать текущую обстановку на рынке услуг ИБ в России при разработке параметров и определении условий SLA.

Рынок услуг ИБ имеет свои особенности:

– нехватка высококвалифицированных специалистов как в области ИБ, так и в информационных технологиях;

– высокая стоимость услуг в этой области, обусловленная опытными специалистами и современным оборудованием;

– проблемы взаимного доверия и деловой репутации поставщиков услуг, особенно когда речь идет об обеспечении ИБ ФО;

– недостаточное развитие нормативной и правовой базы в данной области.

Среди преимуществ использования аутсорсинга ИБ можно выделить более высокий уровень экспертизы и качества услуг, который часто недостижим без серьезных инвестиций, а также минимизацию затрат собственных ресурсов на выполнение непрофильных задач. Однако в большинстве случаев невозможно полностью передать все функции ИБ ФО на аутсорсинг, и некоторые задачи, включая разработку и мониторинг параметров для оценки качества аутсорсинга ИБ, придется выполнять самостоятельно.

Список источников

1. Стандарт Банка России СТО БР ИББС-1.4-2018 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге. Дата введения: 2018-07-01 Издание официальное. Москва, 2018. URL: https://www.cbr.ru/statichtml/file/59420/st-14-18.pdf.

2. Аникин Б.А., Рудая И.Л. Аутсорсинг и аутстаффинг: высокие технологии менеджмента: учебное пособие / Б.А. Аникин, И.Л. Рудая. — 4-е изд., испр. и доп. — Москва: ИНФРА-М, 2022. – 313 с. – ISBN 978-5-16-016979-8.

3. Канашевский В.А. Банковская тайна и использование банками услуг аутсорсинга информационной безопасности / В. А. Канашевский // Lex Russica (Русский закон). – 2018. – № 7(140). – С. 92-97. – DOI 10.17803/1729-5920.2018.140.7.092-097. – EDN XULFVZ. – ISSN 1729-5920 (Print). – ISSN 2686-7869 (Online).

4. Неизвестный С.И. Риски аутсорсинга и привлечения подрядчиков к внедрению системы информационной безопасности / С.И. Неизвестный // Информационная безопасность: вчера, сегодня, завтра: Сборник статей по материалам VI Всероссийской научно-практической конференции, Москва, 12 апреля 2023 года. – Москва: Российский государственный гуманитарный университет, 2023. – С. 43-46. – EDN QFIYTV. – ISBN: 978-5-7281-3105-2.

5. Ревенков П.В. Кибербезопасность в условиях электронного банкинга / Практическое пособие под ред. П.В. Ревенкова. М.: Прометей. 2020. – 522 с. – ISBN: 978-5-907244-61-0.

6. Ревенков, П.В., Чебарь, А.Г., Бердюгин, А.А. Источники киберрисков в условиях функционирования экосистем. *В центре экономики*. 2022;3(1):1-11. URL: https://vcec.ru/index.php/vcec/article/view/53. – ISSN 2713-2242.

7. Cezar Asunur, Cavusoglu Huseyin, Raghunathan, Srinivasan Outsourcing Information Security: Contracting Issues and Security Implications. *Management Science*. 2010;60(3): 638-657. DOI 10.1287/mnsc.2013.1763.

8. Jacques Touma Conventional versus Unconventional Outsourcing. *American Journal of Industrial and Business Management*. 2020;10(12);1812-1822. URL: https://www.scirp.org/journal/paperinformation.aspx?paperid=106052. DOI: 10.4236/ajibm.2020.1012112. ISSN 2164-5167. eISSN 2164-5175.

9. Jiangping Wan, Dan Wan, Hui Zhang Case Study on Business Risk Management for Software Outsourcing Service Provider with ISM. *Technology and Investment*. 2010;1(4):257-266. URL: https://www.scirp.org/journal/paperinformation.aspx?paperid=3213. DOI: 10.4236/ti.2010.14033. ISSN 2150-4059. eISSN 2150-4067

10. Teng Qian, Kouyate Boh Aisaata, Miao Miao Human Resource Outsourcing in Banking Sector: Case Study of UBA Bank-Guinea. *Open Journal of Business and Management*. 2019;7(1):245-262. URL: https://www.scirp.org/journal/paperinformation.aspx?paperid=89943. DOI: 10.4236/ojbm.2019.71017. ISSN 2329-3284. eISSN 2329-3292

11. Xinyuan Xi, Yingyu Xu, Hiroyushi Todo The Present Situation of IT Outsourcing and Countermeasure. Journal of Software Engineering and Applications. 2013;6(8):426-430. URL: https://www.scirp.org/journal/paperinformation.aspx?paperid=35254. DOI: 10.4236/jsea.2013.68052. ISSN 1945-3116. eISSN Online: 1945-3124.

Reference

1. Bank of Russia standard STO BR IBBS 1.4-2018 Ensuring information security of organizations of the banking system of the Russian Federation. Managing the risk of information security violations during outsourcing. Date of introduction: 2018-07-01 Official publication. Moscow, 2018. URL: https://www.cbr.ru/statichtml/file/59420/st-14-18.pdf.

2. Anikin B.A., Rudaya I.L. *Outsourcing and outstaffing: high technology managemen*t: textbook. 4th ed., rev. and additional. Moscow: INFRA-M, 2022. 313 p. ISBN 978-5-16-016979-8

3. Kanashevsky V.A. Bank secrecy and the use of information security outsourcing services by banks. *Lex Russica (Russian Law)*. 2018;7(140):92-97. DOI 10.17803/1729-5920.2018.140.7.092-097. EDN XULFVZ. ISSN 1729-5920 (Print). ISSN 2686-7869 (Online)

4. Unknown S.I. Risks of outsourcing and attracting contractors to implement an information security system. *Information security: yesterday, today, tomorrow*: Collection of articles based on the materials of the VI All-Russian Scientific and Practical Conference, Moscow, April 12, 2023. Moscow: Russian State University for the Humanities, 2023. pp. 43-46. EDN QFIYTV. ISBN: 978-5-7281-3105-2.

5. Revenkov P.V. *Cybersecurity in electronic banking*. Practical guide, ed. P.V. Revenkova. M.: Prometheus. 2020. – 522 p. – ISBN: 978-5-907244-61-0.

6. Revenkov P.V., Chebar A.G., Berdyugin A.A. Sources of cyber risks in the context of ecosystem functioning. *In the Center of Economy*. 2022;3(1):1-11. URL: https://vcec.ru/index.php/vcec/article/view/53. ISSN 2713-2242.

7. Cezar Asunur, Cavusoglu Huseyin, Raghunathan, Srinivasan Outsourcing Information Security: Contracting Issues and Security Implications. *Management Science*. 2010;60(3): 638-657. DOI 10.1287/mnsc.2013.1763.

8. Jacques Touma Conventional versus Unconventional Outsourcing. *American Journal of Industrial and Business Management*. 2020;10(12);1812-1822. URL:

https://www.scirp.org/journal/paperinformation.aspx?paperid=106052. DOI: 10.4236/ajibm.2020.1012112. ISSN 2164-5167. eISSN 2164-5175.

9. Jiangping Wan, Dan Wan, Hui Zhang Case Study on Business Risk Management for Software Outsourcing Service Provider with ISM. *Technology and Investment*. 2010;1(4):257-266. URL: https://www.scirp.org/journal/paperinformation.aspx?paperid=3213. DOI: 10.4236/ti.2010.14033. ISSN 2150-4059. eISSN 2150-4067

10. Teng Qian, Kouyate Boh Aisaata, Miao Miao Human Resource Outsourcing in Banking Sector: Case Study of UBA Bank-Guinea. *Open Journal of Business and Management*. 2019;7(1):245-262. URL: https://www.scirp.org/journal/paperinformation.aspx?paperid=89943. DOI: 10.4236/ojbm.2019.71017. ISSN 2329-3284. eISSN 2329-3292

11. Xinyuan Xi, Yingyu Xu, Hiroyushi Todo The Present Situation of IT Outsourcing and Countermeasure. Journal of Software Engineering and Applications. 2013;6(8):426-430. URL: https://www.scirp.org/journal/paperinformation.aspx?paperid=35254. DOI: 10.4236/jsea.2013.68052. ISSN 1945-3116. eISSN Online: 1945-3124.