УДК 004.056

А.А. Бутин [1]

[1] *Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация*

АНАЛИЗ УЯЗВИМОСТЕЙ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ДИСТАНЦИОННОМ РЕЖИМЕ РАБОТЫ ОРГАНИЗАЦИИ

Аннотация. Рассмотрены преимущества и недостатки удаленной работы, как для самих сотрудников, так и для работодателей. Определены основные риски утечки корпоративных данных в режиме удаленной работы организации. Проведен анализ уязвимостей инфраструктуры автоматизированной системы и угроз информационной безопасности в режиме удалённой работы.

Ключевые слова: дистанционный режим работы, информационные технологии, корпоративные данные, удаленная работа, защита информации, информационная безопасность.

A.A. Butin[1]

[1] *Irkutsk State Transport University, Irkutsk, Russian Federation*

ANALYSIS OF INFORMATION SECURITY VULNERABILITIES AND THREATS DURING REMOTE OPERATION OF THE ORGANIZATION

Abstract. The advantages and disadvantages of remote work, both for the employees themselves and for employers, are considered. The main risks of corporate data leakage in the mode of remote work of the organization are identified. An analysis of the vulnerabilities of the infrastructure of the automated system and threats to information security in the remote work mode was carried out.

Key words: telecommuting, information technology, corporate data, remote work, information security, information security.

Введение. В настоящее время происходит стремительный рост информационно-телекоммуникационных технологий. Их быстрое развитие и внедрение позволило различным предприятиям и организациям модифицировать классическую форму трудовых отношений. Вследствие этого все большее распространение получил дистанционный режим работы, когда сотрудник выполняет трудовую функцию физически вне места нахождения работодателя.

Удаленный режим работы – это такой формат работы, который не подразумевает наличие сотрудника на территории работодателя. Это позволяет выполнять трудовые обязанности из любого доступного места. Для сотрудников и организаций такой формат работы является выгодным, поскольку и те и другие сокращают свои затраты по обеспечению рабочего процесса как прямо, так и косвенно.

Цифровизация бизнеса и использование современных информационных технологий позволяет организациям увеличивать свою эффективность и продуктивность за счет снижения издержек на взаимодействие между сотрудниками, например, экономить временные и финансовые ресурсы на дорогу в офис компании.

Удаленный формат работы для самих организаций в свою очередьтоже позволяет экономить на обустройстве рабочих мест в офисах и возможности нанять большое количество сотрудников, не платя за увеличенную аренду и уборку большого офиса, электричество, канцеляриюи не тратить деньги на покупку мебели, офисной технички и т.д. К тому же компания может нанимать удаленных специалистов из регионов и таким образом экономить на зарплатах.

Текущий уровень информационных технологий позволяет работнику и работодателю не только связываться между собой на удаленном расстоянии в режиме реального времени, но и оперативно обмениваться результатами своего труда. Учитывая возможности

компьютерной техники и Интернета, во многих случаях отпадает необходимость нахождения работника в офисе компании.

Однако, не смотря навсе преимущества, такой формам трудовых отношений имеет и ряд значительных недостатков. Именно, на любом предприятии практически каждый сотрудник становится носителем ценных сведений, которые представляют интерес для конкурентов. При дистанционном режиме работы службы информационный безопасности (ИБ) могут допустить различные ошибки и открыть доступ не тем сотрудникам ко всей внутренней инфраструктуре компании, что в свою очередь в случае утечки корпоративных данных может привести к возникновению различных инцидентов. В связи с этим возникает необходимость защиты информации организации.

С точки зрения компании сотрудник, работающий из дома, находится в ненадежной и неконтролируемой среде. Небрежное использование сотрудником корпоративных данных может привести к их утечке или краже. Для того, чтобы сотрудники осознали необходимость защиты критической информации, необходимо регулярно и в максимально доступной форме информировать их о том, как правильно организовывать работу с корпоративными данными.

Данная статья будет полезна тем организациям,которые функционируют в удаленном режиме работыи хотят защитить свои данные от утечки со стороны своих сотрудников (см.[1, 2]).

Основные сложности перехода на удаленный режим работы. Ключевая проблема при переходе на удаленный режим работы для всех компаний заключалась в том, насколько быстро и эффективно необходимо было обеспечить работу сотрудников из дома. Большинство предприятий столкнулись с некоторыми трудностями при организации удаленной работы. Во-первых, усложняет скорость и качество перевода сотрудников на удалённый режим работы (УРР) отсутствие аппаратно-технической базы, начиная с корпоративного ноутбука и домашнего рабочего места и заканчивая сложностями доступа и подключения к корпоративным ресурсам компаний, обеспечением безопасности и коммуникации между сотрудниками. Во-вторых, для многих людей удаленная работа стала новым опытом в работе. Фактически, до сих пор она ограничивалась лишь несколькими днями в году во время командировок или больничных, но мало кто из сотрудников был морально готов к тому, что придется нескольких месяцев работать из дома.

Основной проблемой, обострившейся при массовом переводе сотрудников на удаленную работу, является неподготовленность значительной части организаций к полному переходу на УРР. Реальность показала, что для этого перехода недостаточно одного управленческого решения, необходима специально подготовленная инфраструктура. Удаленная работа – эта вынужденная мера, которую ввели компании. Ведь до пандемии в организациях, как правило, было всего несколько сотрудников, которые работали удаленно, а процесс взаимодействия с ними выстраивался практически вручную. Но когда значительная часть сотрудников перешла на удаленную работу, многие компании практически утратили контроль над деятельностью своего персонала.

Массовый и стремительный переход компаний на УРР существенно обострил проблемы информационной безопасности. Большинство организаций столкнулись с подобной задачей впервые, так как ранее они не работали в таком режиме работы, а потому переход на удаленный режим вызвал у них немало сложностей.

Многие компании для оперативного реагирования на сложившуюся ситуацию просто открыли доступ к своим внутренним корпоративным ресурсам, разрешили сотрудникам забирать домой офисные компьютеры, закупили ноутбуки и средства удаленной работы. Все эти факторы создали ряд проблем при переходе на удаленную работу:

1) отсутствие аппаратно-технической базы и информационной инфраструктуры предприятия (корпоративные ноутбуки, телефоны, планшеты, программы удаленного доступа);

2) невозможность использовать некоторые технические средства защиты информации, применяемых в офисе;
3) отсутствие коммуникации и взаимодействия между сотрудниками (корпоративная почта, корпоративные месседжеры, электронный документооборот);
4) некоторые бизнес-процессы не настроены на работу в онлайн-режиме или не автоматизированы вообще;
5) их непрозрачность и невозможность контролировать сотрудников (программы для отслеживания рабочего времени и продуктивности сотрудника);
6) уменьшение продуктивности сотрудника из-за семейного окружения и домашней атмосферы;
7) использование сотрудниками для работы личных незащищенных устройств;
8) низкий уровень защиты домашних сетей;
9) обмен информацией с помощью публичных сервисов с низким уровнем защиты;
10) недостаточная подготовленность пользователей в области информационной безопасности при УРР.

Таким образом, при работе с удаленными сотрудниками существует множество уязвимых мест, через которые может произойти утечка конфиденциальной информации. Следовательно, важно выявить эти уязвимости и разработать эффективные меры для обеспечения защиты корпоративных данных.

Анализ уязвимостей при удаленной работе сотрудников. Переводя своих работников на удаленный режим работы, службы ИБ допускают различные ошибки безопасности и случайно открывают доступ ко всей внутренней инфраструктуре компании, что в свою очередь приводит к возникновению различных уязвимостей. Приведём перечень основных уязвимостей при удаленной работе сотрудников
(см. также [3-8]):

1) Отсутствие контроля над личными устройствами сотрудников, обрабатывающих корпоративную информацию.

Многие предприятия используют личные компьютеры на рабочих местах, а быстрая закупка, настройка и выдача ноутбуков всем сотрудникам оказалась непосильной задачей даже для крупных компаний. Поэтому организации были вынуждены разрешить сотрудникам использовать свои собственные компьютеры и устройства для работы из дома с установленным неизвестным набором программного обеспечения (ПО) и средств защиты.

Вместо безопасных офисных рабочих мест сотрудники перешли на домашние компьютеры, на которых не используется весь комплекс корпоративных средств защиты, кроме того, сотрудник стал не единственным пользователем своего рабочего места –вся семья пользуется домашним компьютером, а это пользователи, не прошедшие соответствующие инструктажи и не несущие никакой ответственности за свои действия перед предприятием.

На персональном компьютере сотрудник может выполнять как рабочие, так и личные задачи одновременно, иногда конфиденциальные документы и файлы часто остаются незакрытыми, это повышает риск случайных утечек информации. Ноутбук идеально подходит для комфортной работы в этом режиме, однако следует понимать, что наряду с ноутбуками периметр контролируемой зоны предприятия пересекает большое количество критической информации, ведь почти наверняка такая информация будет обрабатываться в ненадежной среде домашних сетей или общедоступных точек доступа. У большинства домашних роутеров не обновлены стандартные прошивки, так как обычному пользователю просто незачем это делать, также люди используют стандартные пароли и в большинстве случаев не пользуются лицензионными ОС и антивирусами. Вследствие этого сильно повышаются риски атаки на корпоративные сети через удаленные рабочие места сотрудников и особенно через их личные устройства. Поэтому компаниям приходится

вносить серьезные изменения в свою сетевую архитектуру, увеличивать производительность и пропускную способность сетей и внедрять дополнительные меры защиты своих сетей. При режиме удаленной работы защита личных устройств сотрудников никогда не была так актуальна.

2) Отсутствие контроля каналов коммуникации и использование общедоступных сервисов.

Следующая уязвимость – массовое использование сотрудниками публичных облачных сервисов. Во-первых, к примеру, сотрудникам службы ИБ срочно потребовалось перенастроить систему защиты информации от утечек, чтобы отследить новые каналы коммуникаций, которые появились у сотрудников при переходе на удаленную работу, и доступ к которым был ограничен при работе в офисном режиме. Таким образом, сотрудники, находящиеся вне периметра организации, могут активно использовать не облачные хранилища компании, а общедоступные сервисы Google или Яндекс-диск для обмена рабочей, в том числе конфиденциальной информацией. Пока службы ИБ компании занимались настройкой удаленного доступа к корпоративным ресурсам, сотрудники начали передавать данные через свои личные аккаунты на публичных файлообменных ресурсах. Это может стать серьезным инцидентом для бизнеса, в случае взлома бесплатного облачного хранилища. Кроме того, сотрудники гораздо чаще стали копировать корпоративные данные и документы на съемные носители. Если в компании не использовалась DLP-система в режиме блокировки, и тем более если компания не обеспечила всех сотрудников корпоративными ноутбуками, то задача по защите от утечек оказывалась практически невыполнимой.

Во-вторых, службам ИБ пришлось срочно задумываться о системе управления и контроля почтового трафика и терминальных серверов. Что касается мониторинга корпоративной почты, то компании были вынуждены внедрять технологии, которые позволяют контролировать почтовый сервер без использования агентов на рабочих станциях. Именно использование терминальных серверов для организации безопасного удаленного доступа к корпоративным ресурсам применяли большинство компаний. Те, кто смог быстро реализовать терминальный доступ для сотрудников, смогли решить первую проблему, описанную выше.

3) Построение режима удаленной работы в сжатые сроки и отсутствие контроля утечки данных.

При быстром переходе на УРР появляется уязвимость небрежного использования данных, их утечка или кража. Конечно, быстрый переход на УРР крайне сложен для сотрудников службы ИБ. Даже те предприятия, на которых имелась возможность удаленного доступа к корпоративным системам, столкнулись с необходимостью быстрого перевода большого количества сотрудников на удаленную работу. В настоящее время существует достаточное число подходов и средств защиты информации, способных обеспечить полноценную работу сотрудников удаленно без существенного увеличения уровня угроз корпоративных систем. Если у организации достаточно много времени и средств, можно создать безопасную систему удаленного доступа для сотрудников. Однако большинству компаний приходилось крайне быстро перестраивать свои системы и бизнес-процессы, и при этом вопросам ИБ уделялось очень мало внимания, т.к. они не были приоритетными. При этом большинство предприятий не смогли перейти на УРР и сохранить тот же уровень безопасности и контроля над действиями пользователей, который обеспечивался в стандартном режиме работы. Кроме того, некоторые компании никогда не собирались когда-либо использовать удаленный доступ для полноценной работы своих сотрудников. Тогда им приходилось с нуля создавать системы для удаленной работы. Все это привело к тому, что созданные и работающие в данный момент системы удаленного доступа не отвечают всем требованиям по информационной безопасности. Даже сейчас многие компании не внедрили все необходимые средства защиты и не выстроили свои процессы для обеспечения

безопасного удаленного доступа сотрудников. Со временем это может привести к крупным утечкам корпоративных данных и к атакам злоумышленников на корпоративные системы.

4) Невысокая компетенция сотрудников в вопросах ИБ при удаленной работе.

С точки зрения компании сотрудник, который работают из дома, располагается в ненадежной и неконтролируемой среде. Для того чтобы сотрудники поняли необходимость защиты информации, следует регулярно и в легкодоступной форме оповещать их, как правильно организовывать работу с корпоративной информацией, проводить учебные фишинговые атаки и онлайн-уроки по обучению информационной безопасности. Следует сформировать инструкции для удаленных сотрудников по информационной безопасности. Необходимо включить в них правила о чистом столе (в случае если сотрудник уходит с рабочего места, он убирает с рабочего стола все без исключения носители с конфиденциальными данными) и чистом экране (блокировке компьютера, если пользователь прекратил работу). Следует напомнить касательно политики формирования паролей, а также о высоких рисках утечки корпоративной информации в случае использования публичных месседжеров, электронной почты и общедоступных файло-обменных ресурсов.

5) Отсутствие контроля над поставщиком услуг.

Доверяя коммерческую информацию сторонним компаниям аутсорсерам, организация должна быть полностью уверена в её безопасности. Аутсорсеры сейчас работают в тех же условиях, что и компании-клиенты, и также испытывают сбои во внутренних процессах. Поэтому необходимо проводить полноценный аудит таких поставщиков услуг. Это можно сделать путем запроса подтверждающих документов и проверки процессов и средств безопасности, которые они применяют для защиты информации, которую им доверила компания. Конечно, лучше пользоваться услугами известных и уже проверенных аутсорсеров.

6) использование домашних (личных) незащищенных устройств:

- отсутствие или использований слабых паролей на устройстве;
- хранение конфиденциальной информации на рабочем столе персонального компьютера или на незащищенных внешних USB-накопителях;
- при неактивности устройства отсутствует автоматическая блокировка;
- отсутствие последних обновлений безопасности как ОС, так и прикладного ПО;
- отсутствие антивирусной программы.

7) наличие публичных незащищенных каналов связи:

- при использовании беспроводных сетей – недостаточное шифрование или полное его отсутствие;
- при использовании домашней сети – уязвимости маршрутизирующих устройств (слабые пароли, уязвимые прошивки, ненастроенный брандмауэр);
- использование уязвимых протоколов передачи данных.

8) режим публичных сервисов для обмена файлами:

- использование для обмена и хранения файлов публичные сервисы (Google диск, Яндекс диск, Облако Mail.ru и т.п.);
- если есть открытая ссылка на файл в облаке, то он может быть проиндексирован поисковыми машинами, после чего конфиденциальный документ может стать доступным в поиске, что в свою очередь, может привести к его утечке в общедоступную сеть.

Обзор актуальных угроз информационной безопасности предприятия при переходе на удаленный режим работы. При переходе на удаленный режим работы сотруднику необходим удаленный доступ к корпоративным серверам организации. На практике любой удаленный доступ – это расширение периметра, так как в инфраструктуре компании появляются новые подключения извне. Персональные устройства, на которых работают сотрудники и с которых подключаются к корпоративным системам, могут быть недостаточно защищены, скомпрометированы или вовсе утеряны или украдены.

Типичными угрозами удаленного доступа являются взлом и заражение сети. Они возможны при наличии следующих обстоятельств:

– ошибки конфигурации устройств доступа (компьютеров), в результате которых они частично или полностью незащищены;
– использование устройств не по назначению, когда сотрудники подключаются со своих не доверенных устройств к корпоративным ресурсам или используют корпоративные компьютеры дома;
– недостаточная защита конечных устройств пользователей, в том числе в случае их кражи или потери;
– ошибки в настройке шлюза, используемого для доступа в корпоративную сеть, неправильные решения, связанные с публикацией корпоративных сервисов, использование небезопасных облачных сервисов, вне доверенной среды;
– отсутствие контроля доступа к ресурсам организации, когда нет доверия только к логину и паролю пользователя и нет возможности различить, кто именно работает;
– недостаточно строгая политика информационной безопасности по контролю трафика пользователей при работе с конфиденциальными документами, а также ненадежные пароли для удаленного доступа;
– недостаточный контроль над трафиком, который передается с рабочих устройств обратно в корпоративную среду, так как существует возможность проникновения с использованием программных средств и несанкционированного воздействия;
– отсутствие системы контроля утечек на случай несанкционированного копирования информации умышленно или случайно из корпоративной системы и передача информации злоумышленникам.

Типичными угрозам непосредственно на домашнем рабочем месте сотрудника являются:

– проникновение вирусов в офисную сеть из домашней сети, сетевая или вирусная атака на корпоративные системы в периметре;
– заражение документов, обрабатываемых на домашних рабочих местах сотрудников;
– заражение компьютеров пользователей в связи с недостаточностью установленных СЗИ на местах и работа с потенциально открытой или потенциально зараженной информацией;
– утечка данных из корпоративной сети через рабочие места пользователей, даже если контролируется их копирование на внешние носители (фотографирование экрана);
– недостаточно строгая аутентификация пользователей (доступ без пароля или с простым паролем);
– потеря/кража конечных устройств или данных;
– нарушение периметра (случайное изменение документов компании третьими лицами, которые имеют доступ к компьютеру сотрудника, например члены его семьи);
– проблемы связи, необходима хорошая пропускная способность канала связи и возможности устройств, для того чтобы не возник инцидент «отказ в облуживании»;
– распространение персональных данных и личной информации сотрудников, где они находятся и их рабочие часы, присутствия и возможностей – информация становится доступной для мониторинга и может использоваться людьми, для которых она не предназначена.

Актуальность всех перечисленных выше угроз многократно возрастает при использовании персонального компьютера, смартфона или другого домашнего (личного) устройства для доступа к корпоративным ресурсам.

Поэтому при выходе сотрудников с удаленного режима работы, службам ИТ и ИБ приходится учитывать ряд новых угроз, и адаптироваться к новым условиям, ведь недостаточно просто восстановить ранее существовавшие процессы, а необходимо проверить все устройства, которые вернулись в корпоративную инфраструктур, на наличие вредоносного ПО, которое не всегда выявляется стандартными антивирусами. К тому же следует обновить все без исключения пароли сотрудников. Да и сам периметр организации теперь не тот, что прежде, и нужно оперативно проверить корпоративную сеть на предмет доступных из интернета сервисов.

Таким образом, при переходе на удаленные режим работы возникает множество новых угроз, которых ранее не существовало при функционировании предприятия в штатном режиме. К тому же неправильно настроенный удаленный доступ к корпоративным ресурсам может привести к крупным утечкам данных и атакам злоумышленников, как на корпоративные информационные системы коммерческих предприятий, так и на государственные информационные системы и даже на системы КИИ.

Заключение. Дистанционный режим работы организации может привести как к утечке корпоративных данных, так и к нарушению работы целых функциональных систем предприятийвследствие неосторожности самих сотрудников, также и в случае кражи или утечки значимой информации по их вине.

В действительности, используя богатый арсенал технологий обеспечения защиты информации, имеется возможность избежать большинства угроз, соответствующих рисков и инцидентов, связанных с обеспечением безопасности корпоративных данных предприятия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Базаров Р.С. Удаленная работа как новая реальность // Журнал «Трибуна ученого». – 2020. –№11. – С. 14-18.

2. Босова Е.Д. Селищев В.А. Информационная безопасность: современные реалии // Известия Тульского государственного университета. Технические науки. Вып. 9. – 2020. – С. 296-300.

3. Асс Е.С., Бутин А.А. Методические аспекты защиты информации при дистанционном режиме работы организации // Информационные технологии и математическое моделиро-вание в управлении сложными системами. –2022. – № 2 (14). – С. 65-76.

4. Носков С.И., Бутин А.А. Экспертно-статистическая модель уровня защищённости данных // Электронный сетевой политематический журнал "Научные труды КубГТУ". – 2022. – № 1. – С. 117-127.

5. Носков С.И., Бутин А.А. Применение экспертных данных при построении регрессионной модели оценки уровня защищённости носителей информации // Инженерный вестник Дона. –2022. – № 8 (92) .– С. 186-195.

6. ISO 27001 Риски информационной безопасности при переходе на удаленную работу [Электронный ресурс]. – Режим доступа: https://www.sgs.ru/ru-ru/news/2020/04/iso-27001-i-riski-informacionnoj-bezopasnosti-pri-perehode-na-udalennuyu-rabotu. – Заглавие с экрана. – (дата обращения: 20.09.2022).

7. Как защитить корпоративные данные при удаленной работе [Электронный ресурс]. – Режим доступа: https://www.vedomosti.ru/management/blogs/2020/06/08/832180-zaschitit-korporativnie. – Заглавие с экрана. – (дата обращения: 20.09.2022).

8. Носков С.И., Бутин А.А. Методическое обеспечение оценки уровня уязвимости объектов информатизации //Информационные технологии и проблемы математического моде-лирования сложных систем. – 2015. – № 14. – С. 38-48.

REFERENCES

1. Bazarov R.S. Udalennaj rabota rar novaj realnost // Jurnal "Tribuna uchenogo". – 2020. – No. 11. – pp. 14-18.

2. Bosova E.D. Selishchev V.A. Informazionnaj bezopasnost: sovremtnnie realii // Izvestij Tulskovo gosudarsnvennogo univtrsiteta. Tehnicheskie nauki. Vip. 9. – 2020. – pp. 296-300.

3. Ass E.S., Butin A.A. Metodicheskie asptkti zacsiti informacii pri distancionnom regime raboti organizacii // Informacionnie tehnologii i matematicheskoe modelirovanie v upravlenii slognimi sistemami. – 2022. – No. 2 (14). – pp. 65-76.

4. Noskov S.I., Butin A.A. Expertno-statistichescaj model urovnij zashishennosti dannih // Elektronnii setevoi politematicheskii gurnal KubGTU". – 2022. – No. 1. – pp. 117-127.

5. Noskov S.I., Butin A.A. Primenenie ekspertnih dannih pri postroenii regressionnoi modeli ocenki urovnij zashishennosti nositeltq informacii // Ingenernii vestnik Dona. – 2022. – No. 8 (92). – pp. 186-195.

6. ISO 27001 Riski informacionnoi bezopasnosti pri perehode na udalennuj rabotu [Electronic resource]. – Regim dostupa: https://www.sgs.ru/ru-ru/news/2020/04/iso-27001-i-riski-informa-cionnoj -bezopasnosti-pri-perehode-na-udalennuyu-rabotu. - Zaglavie s ekrana. – (data obracseniaj: 20.09.2022).

7. Kak zachsititt korporativnie Dannie pri udalennoi rabote [Electronic resource]. – Regim dostupa: https://www.vedomosti.ru/management/blogs/2020/06/08/832180-zaschitit-korporativnie. - Zaglavie s ekrana. – (data obracseniaj: 20.09.2022).

8. Noskov S.I., Butin A.A. Metodicheskoe obespechenie ocenki urovniaj uajzvomosti obektov informatixacii // Informacionnye tekhnologii i problemi matematicheskogo modelirovania slozhnih system. – 2015. – No. 14. – pp. 38-48.

Информация об авторе

Александр Алексеевич Бутин – доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: butin_aa@mail.ru

Author

Alexander Alekseevich Butin – Associate Professor of the Department of Information systems and information protection, Irkutsk State University of Railways, Irkutsk, e-mail: butin_aa@mail.ru

Для цитирования

Бутин А.А. Анализ уязвимостей и угроз информационной безопасности при дистанционном режиме работы организации // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2022. – №3(15). – С.39-46– DOI: 10.26731/2658-3704.2022.3(15).39-46 – Режим доступа: http://ismm-irgups.ru/toma/315-2022, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 15.10.2022)

For citations

Butin A.A. Analysis of information security vulnerabilities and threats during remote operation of the organization // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2022. No. 3(15). P. 39-46. DOI: 10.26731/2658-3704.2022.3(15).39-46 [Accessed 15/10/22]