УДК 004.056

Дроздова Д.В.
студент магистратуры
РГУ нефти и газа (НИУ) им. И.М. Губкина
Россия, г. Москва

УПРАВЛЕНИЕ РИСКАМИ В РАМКАХ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ ТЭК

Аннотация. Управление рисками в рамках обеспечения кибербезопасности становится необходимостью для компаний ТЭК, чтобы минимизировать возможные угрозы и последствия хакерских атак, вредоносного программного обеспечения или утечек конфиденциальной информации.

Целью данной работы является исследование управления рисками в рамках обеспечения кибербезопасности предприятий ТЭК. Для достижения этой цели были проанализированы подходы и методы компаний в области управления рисками и обеспечения кибербезопасности. Основываясь на опыте «Газпром», сможем выделить ключевые принципы и рекомендации для успешного управления рисками.

В результате работы были выявлены основные риски, связанные с кибербезопасностью предприятий ТЭК, такие как хакерские атаки, утечка конфиденциальных данных и проблемы с защитой от вредоносного программного обеспечения.

Ключевые слова: риски, кибербезопасность, предприятия, топливно-энергетический комплекс, Газпром.

Drozdova D.V.
Master's degree student
Gubkin Russian State University of Oil and Gas (NRU)

Russia, Moscow

RISK MANAGEMENT IN THE FRAMEWORK OF ENSURING CYBERSECURITY OF FUEL AND ENERGY COMPANIES

Annotation. Risk management within the framework of cybersecurity is becoming a necessity for fuel and energy companies in order to minimize possible threats and consequences of hacker attacks, malicious software or leaks of confidential information.

The purpose of this work is to study risk management in the framework of ensuring cybersecurity of fuel and energy companies. To achieve this goal, the approaches and methods of companies in the field of risk management and cybersecurity were analyzed. Based on Gazprom's experience, we will be able to identify key principles and recommendations for successful risk management.

As a result of the work, the main risks associated with the cybersecurity of TCE enterprises were identified, such as hacker attacks, leakage of confidential data and problems with protection against malicious software.

Keywords: risks, cybersecurity, enterprises, fuel and energy complex, Gazprom

Введение. Предприятия топливно-энергетического комплекса относятся к числу критически важных объектов, требующих наиболее серьезных мер защиты от современных кибератак. Однако, наряду с критичностью и актуальностью защиты предприятий ТЭК, существуют трудности в организации интегрированной системы информационной безопасности.

Количество атак на российские компании неуклонно растет с каждым годом, но в 2023 году темпы роста были рекордными. По данным экспертного центра безопасности Positive Technologies, количество

проектов по расследованию инцидентов в 2022 году увеличилось на 50% по сравнению с 2021 годом, в то время как за первые девять месяцев 2023 года, по сравнению с показателями за весь прошлый год, их количество увеличилось еще на 76%. Таким образом, данная тема является актуальной, т.к. атакам подвергаются крупнейшие компании с хорошей защитой, что может наносить вред компании, а через компании и государству, исследователи связывают такое явление с геополитической обстановкой, а также экономическими составляющими страны.

Современные предприятия ТЭК сталкиваются с угрозами кибератак.

Кибербезопасность — это защита подключенных к Интернету устройств и служб от вредоносных атак хакеров, спамеров и киберпреступников. Эта практика используется компаниями для защиты от фишинговых схем, атак программ-вымогателей , кражи личных данных, утечки данных и финансовых потерь.[1]

На сегодняшний день, можно сказать, что компании больше зависят от технологий, чем когда-либо прежде. Преимущества этой тенденции варьируются от почти мгновенного доступа к информации в Интернете до современных удобств, предоставляемых технологиями.

Учитывая пользу, исходящую от технологий, трудно поверить, что потенциальные угрозы скрываются за каждым устройством и платформой. Тем не менее, несмотря на радужное восприятие компаниями современных достижений, угрозы кибербезопасности, представляемые современными технологиями, представляют собой реальную опасность.

Устойчивый рост киберпреступности подчеркивает недостатки устройств и услуг, от которых компании стали зависеть.

Хотя некоторые компоненты кибербезопасности созданы для того, чтобы наносить удар первыми, большинство современных специалистов

1 What is Cybersecurity and Why It is Important? - https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security (Дата обращения: 13.12.23).

больше внимания уделяют определению наилучшего способа защиты всех активов — от компьютеров и смартфонов до сетей и баз данных — от атак.

Кибербезопасность использовалась в средствах массовой информации как всеобъемлющий термин для описания процесса защиты от всех форм киберпреступности, от кражи личных данных до международного цифрового оружия. К сожалению, они не отражают истинную природу кибербезопасности для тех, кто не имеет степени в области компьютерных наук или опыта работы в цифровой индустрии.

Cisco Systems, технологический конгломерат, специализирующийся на сетевых технологиях, облачных технологиях и безопасности, определяет кибербезопасность как «...практику защиты систем, сетей и программ от цифровых атак. Данные кибератаки обычно направлены на доступ, изменение или уничтожение конфиденциальной информации; вымогательство денег у пользователей; или прерывание обычных бизнес-процессов».[2]

В современном цифровом мире нельзя игнорировать кибербезопасность. Одно-единственное нарушение безопасности может привести к раскрытию личной информации миллионов людей. Данные нарушения оказывают сильное финансовое влияние на компании, а также теряют доверие клиентов. Следовательно, кибербезопасность очень важна для защиты предприятий и частных лиц от спамеров и киберпреступников.

По мнению Forbes , 2022 год преподнес множество разнообразных и ужасающих проблем в области кибербезопасности: от сбоев в цепочках поставок до увеличения рисков для интеллектуальных устройств, до продолжающейся нехватки специалистов в области кибербезопасности.

По данным журнала Cybercrime Magazine , к 2025 году киберпреступность будет стоить миру 10,5 триллионов долларов

2 What is Cybersecurity and Why It is Important? - https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security - (Дата обращения: 13.12.23)

ежегодно. Более того, согласно прогнозам, глобальные издержки от киберпреступности будут расти почти на 15 процентов ежегодно в течение следующих четырех лет.

Такие концепции, как пандемия, криптовалюта и рост удаленной работы, объединяются, чтобы создать богатую среду, которой могут воспользоваться преступники. Кибербезопасность включает в себя технологии, процессы и методы защиты компьютерных систем, данных и сетей от атак.

Таким образом, атаки могут привести к серьезным последствиям (нарушения работ оборудования, поставка энергии, потеря информации). В 2023 году основными целями атак были правительственные учреждения и объекты критической инфраструктуры. Топливно-энергетические компании, наряду с транспортными и финансовыми, являются одними из крупнейших географически распределенных объектов.

В 2024 году эксперты советуют не ждать снижения остроты ситуации, так как атаки станут более сложными. По прогнозам исследователей, в 2024 году, мы по-прежнему будем наблюдать нехватку экспертов, обладающих необходимыми знаниями для получения описания ситуаций.

Организации топливно-энергетического комплекса относительно недавно начали пользоваться плодами Индустрии 4.0: автоматизацией производства, использованием Интернета вещей, внедрением технологий «больших данных», которые приводят не только к повышению эффективности производства, но и к результативности целенаправленных атак. Обратимся к определениям понятия риск и управление рисками.

Риск – неопределенное событие или условие, наступление которого отрицательно или положительно сказывается на целях проекта[3].

[3] PMI (Project Management Institute) — URL: https:// https://www.defence.lk/upload/ebooks (Дата обращения: 09.11.2023)

Управление рисками – это процессы, связанные с идентификацией, анализом рисков и принятием решений, которые включают максимизацию положительных и минимизацию отрицательных последствий наступления рисковых событий.

В случае кибербезопасности, риски связаны с возможностью нарушений информационной безопасности и потенциальными угрозами для инфраструктуры технической безопасности. Каждая компания ставит перед собой цель управления такими рисками: уменьшить ущерб, который могут нанести кибератаки.

В целях стратегического планирования в сфере обеспечения национальной безопасности в отраслях ТЭК в мае 2019 года Президент России утвердил новую Доктрину энергетической безопасности страны, которая разрабатывалась с участием Минэнерго России и других ведомств.[4]

В процессе написания статьи были применены такие методы исследования, как теоретический анализ, системный подход, а также метод прогнозирования (подходы и методы компаний в области управления рисками и обеспечения кибербезопасности).

Были проанализированы исследования и материалы по данной тематике, рассмотрена система управления рисками информационной безопасности, а также изучены популярные системы защиты ТЭК в работах, Курило А.П.[5], Агафонова В.А[6], Столбова А.Г.[7].

Для защиты критической информационной инфраструктуры можно выделить несколько этапов:

[4] Доктрина энергетической безопасности Российской Федерации от 13 мая 2019 года №216
[5] Курило А.П. Управление рисками информационной безопасности: учебное пособие для вузов – 2-е изд., испр. М.: Горячая линия – Телеком, 2015. – 130 с.
[6] Агафонов В.А. Стратегическое управление и экономическая безопасность: монография. – М.: НИЦ ИНФРА-М, 2006. – 257 с.
[7] Столбов А.Г. Организационно-экономическое обоснование системы управления энергетической безопасностью Мурманской области. – М.: Издательство «Спутник+», 2011. – 183 с.

1. Выбор нового ПО – проводится анализ рынка и на основе маркетинговой информации выбирается ПО. Важно подчеркнуть, что работа идет исключительно с маркетинговой информацией.

2. Пилотирование – пробное внедрение и опытная эксплуатация выбранного ПО в рамках небольшого участка информационной информации, для проработки и установления безопасности.

3. Проектирование – разработка технического проекта замены старого ПО на выбранное новое (желательно отечественное).

4. Закупка и внедрение – подготовка конкурсной документации и закупка. Установка и настройка нового ПО. В ряде случаев установке и настройке будет предшествовать удаление старого ПО.

5. Испытания и опытная эксплуатация – приемочные испытания, в рамках которых проверяется работоспособность и функциональность ПО, а также защита КИИ.

6. Обучение персонала – обучение работы с новым ПО и его администрирование.

Для того, чтобы ускорить переход на отечественные ПО, необходимо исключить некоторые этап, либо сократить срок введения нового ПО.

ПАО «Газпром» — глобальная энергетическая компания. Основные направления деятельности — геологоразведка, добыча, транспортировка, хранение, переработка и реализация газа, газового конденсата и нефти, реализация газа в качестве моторного топлива, а также производство и сбыт тепло- и электроэнергии. Большое количество данных и информации хранится на серверах компании, что делает ее значительной целью для кибератак.

Система управления рисками и внутреннего контроля «Газпрома» — совокупность взаимосвязанных организационных мероприятий и процессов, организационная структура, локальные нормативные акты ПАО «Газпром» и организаций Группы «Газпром», другие документы, методы и

процедуры (положения, регламенты, стандарты и методические рекомендации), нормы корпоративной культуры и действия сотрудников структурных подразделений ПАО «Газпром» и организаций Группы «Газпром», направленные на предоставление достаточных гарантий для достижения целей и задач, а также поддержка сотрудников структурных подразделений «Газпрома» и организаций Группы «Газпром» в принятии решений в условиях неопределенности.

Таким образом, каждой компании ТЭК необходимо разработать стратегии для защиты корпорации. Для этого можно выделить несколько шагов стратегии:

1. Заменить устаревшие системы защиты (для защиты производства от внешних атак используются как специализированные промышленные брандмауэры, так и современные средства защиты доступа в Интернет – брандмауэры следующего поколения (NGFW);
2. Повысить требования к специалистам информационной безопасности (только 13% компаний внедряют современные технологии);
3. Сотрудничество с поставщиками средств информационной безопасности (одной из стратегий противодействия хакерству является формирование целостного представления об объекте и применение комплексного подхода к обеспечению безопасности).

Методика. Анализ угроз и уязвимостей в обеспечении безопасности ТЭК является основной частью процесса управления рисками. В данном разделе мы рассмотрим аспект анализа угроз и уязвимостей.

Топливно-энергетические компании в Российской Федерации чаще всего сталкиваются с утечками информации в результате хакерских атак. Исследование проводилось среди сотрудников компаний на сайте Positive Technologies.

Проанализировав данные по атакам ТЭК, можно прийти к выводу, результаты которого представлены в таблице 1:

Таблица 1 – Результаты опроса

Ответы	Проценты (%)
Утечка информации	30
Уничтожение или подмена информации	26
Атака с простоями инфраструктуры	25
Нарушение технологического процесса	12
Репутационный ущерб	9

Таким образом, отсюда можно выделить ряд причин атак на ТЭК:

1. Нарушение производственного процесса;

2. Вывод из строя инфраструктуры;

3. Шпионаж;

4. Нанесение ущерба и репутации компании;

5. Кража имущества и денежных средств.

6.Человеческий фактор (наиболее популярная субъективная причина) - безответственный сотрудник или же «Вирус со стороны».

В схематичной форме можно отразить причины так, как представлено на Рисунке 1:

Рисунок 1 – Причины атак на ТЭК

Таким образом, в современном информационном пространстве существует множество потенциальных угроз, которые могут нанести значительный ущерб компаниям ТЭК. Основными угрозами являются атаки (хакерские атаки), программы и другие методы злоумышленников для получения несанкционированного доступа к информации или нарушения работы систем предприятий или нефтегазовых объектов:

1. Потери в случае преднамеренной дискредитации, вскрытие файловой системы компьютера;

2. Сбои аппаратного и программного компонентов в ресурсах для пользователей;

3. Электронная блокировка в каналах, компьютерах или другом подобном устройстве нарушает их функционал из-за вирусной инфекции;

4. Промышленный шпионаж (например, перехват данных).

Проведя анализ угроз, можно определить приоритеты исправления ошибок и угроз. Можно выделить два способа:

1. Технические изменения (установка новых продуктов, которые могут приводить к обновлению оборудования).

2. Организационные меры (обучение и повышение квалификации персонала).

Важным этапом анализа является оценка последствий возможного инцидента в случае успешной эксплуатации уязвимости или осуществления угрозы. Таким образом, оцениваются как прямые финансовые потери, так и непосредственное влияние на бизнес-процессы компании. Например, утечка конфиденциальной информации может привести к финансовым потерям или ухудшению репутации предприятия.

На примере ПАО «Газпром нефть» создана система защиты нефтегазовых компаний. Рассмотрим некоторые направления защиты:

а) Обеспечение безопасности цифрового двойника: кибериммунитет, модели зрелости (защиты от киберугроз), профиль зрелости (безопасность IoT для цифровых двойников);

б) Внедрение и развитие беспилотных летательных аппаратов (БПЛА). Можно с помощью БПЛА осуществлять мониторинг и защиту объекта;

в) Разработка и внедрение ИТ-проектов.

В рамках повышения информационной защиты рассмотрим пример создания цифровых моделей в Таблице 2.

Таблица 2 – Процесс оказания услуги по созданию цифровых моделей месторождений и карьеров

№ п/п	Услуги	Описание
1	Согласование технического задания и стоимости	Создание и согласование технического задания, в т.ч. определение состава работ, выходные конечные данные, утвержденные стоимости.
2	Оформление документов	Получение разрешения на выполнение авиационных работ и установление временного или местного режима для проведения полетов в центре ЕС ОрВД.
3	Выполнение полевых материалов	Осуществление планово-высотного обоснования территории и аэрофотосъемочные работы

4	Обработка полевых материалов	Преобразование снимков в плотное облако точек, на основе которого строится цифровая модель месторождения/карьера.
5	Передача материала Заказчику	Передача данных на проверку Заказчику, по принятию подписание акта приемки выполненных работ.

Группа компаний «Газпром» разработала противоборствующие схемы. На официальном сайте «Газпрома» имеется следующая информация: “ПАО «Газпром» не имеет никакого отношения к интернет-сайтам и мобильным приложениям, предлагающим различные схемы обогащения от имени «Газпрома», его должностных лиц или дочерних компаний. ПАО «Газпром» не располагает информацией о содержании информации, распространяемой через такие интернет-сайты,” - таким образом Газпром обезопасило себя и своих клиентов. Были случаи проведения мошеннических атак от имени Газпрома. После вывода денежных средств мошенники не выходили на связь.

Компанией были разработаны рекомендации по распознаванию типовых мошеннических схем в сфере ТЭК:

1. Вы получите предложение о приобретении продукции от «Газпром» или его аффилированных лиц по электронной почте. К письму может прилагаться проект соглашения или образец заполнения заявки на покупку товара (ICPO) вместе с образцом банковской выписки. ПАО «Газпром» не инициируют отправку таких предложений по почте и не предоставляют гарантий доставки товаров заочно через Интернет и электронную почту, а также не наделяют аналогичными полномочиями других лиц;

2. Параметры сделки существенно отличаются от рыночных: вам предлагаются очень большие объемы по очень выгодной цене;

3. Перед официальным подписанием контракта от вас требуется перевести деньги для оплаты каких-либо услуг, например, для оформления различных документов (виз, приглашений, разрешений), для легализации

или активации контракта в департаментах и министерствах Правительства России (внимание: данная процедура не предусмотрена законодательством Российской Федерации) и т.д.;

4. Перевод денег на счет физического лица.

В заключение следует отметить, что анализ угроз и уязвимостей является важным этапом процесса управления рисками в рамках обеспечения кибербезопасности топливно-энергетических компаний.

Таким образом, данный анализ позволяет выявить потенциальные риски для информационной безопасности, на примере ПАО «Газпром» определить приоритеты устранения выявленных проблем и разработать соответствующий план действий. Таким образом, это помогает предотвращать инциденты и минимизировать негативные последствия для компании.

Результаты. Управления рисками в области кибербезопасности являются важным элементом обеспечения безопасности ТЭК. ПАО «Газпром» разработал механизм безопасности компании, чтобы минимизировать риски необходим комплексный подход к решению проблем. Проведя анализ, можно выделить несколько этапов управления рисками:

1. Идентификация рисков - определение внутренних и внешних событий, которые оказывают влияние на достижение целей организации, с учётом их разделения на риски и возможности;

2. Оценка рисков - анализ рисков с учётом вероятности их возникновения и влияния, по результатам которого определяются необходимые действия в их отношении;

3. Управление рисками - процессы, связанные с идентификацией, анализом рисков и принятием решений, которые включают максимизацию

положительных и минимизацию отрицательных последствий наступления рисковых событий;[8]

4. Анализ средств контроля - на постоянной основе. Оцените, насколько эффективны средства контроля для снижения рисков, и при необходимости добавьте или скорректируйте средства контроля.

Стратегия управления рисками признает, что организации не могут полностью устранить все уязвимости системы или заблокировать все кибератаки. Проведя анализ, были выявлены несколько стратегий:

1. Превентивное действие (предотвращение угроз, с помощью проведения анализов);

2. Мониторинг системы безопасности (возможны несанкционированные атаки).

Результат анализа информационной безопасности ПАО «Газпром» свидетельствует о высоком уровне защиты предприятия. На предприятии используют превентивные методы защиты, а за обеспечение системы информационной безопасности отвечает компетентный персонал.

В заключение можно сказать, что стратегии и методы управления рисками в области кибербезопасности являются неотъемлемой частью деятельности предприятий ТЭК, таких как ПАО «Газпром» и ПАО «Газпром нефть». Таким образом, использование комплексного подхода, включая превентивные меры, оперативное реагирование, автоматизацию процессов, обучение персонала и партнерские отношения с другими организациями, помогает минимизировать риски, связанные с киберугрозами, и обеспечить безопасность информационной инфраструктуры предприятий ТЭК.

Обсуждение. Нефтегазовые компании продолжают активно внедрять собственные стратегии цифровой трансформации. Использование новых технологий в нефтегазовой отрасли призвано обеспечить не только

[8] COSO Enterprise Risk Management - Integrated Framework. 2004.

дальнейший рост прибыли, но и выживание на высококонкурентном рынке. Таким образом, использование цифровых технологий повышает конкурентоспособность предприятий нефтегазовой отрасли и эффективность управленческой деятельности. В Таблице 3 рассмотрим примере ПАО «Газпром нефть».

Таблица 3 – Проект и цель ПАО «Газпром»

№ п/п	Проект	Цель
1	Когнитивная геология	Сокращение продолжительности цикла ГРР за счет инструментов поддержки принятия решений, цифровых двойников и интеллектуальных помощников для интерпретации данных.
2	Создание центров управления проектами	Ускорение ввода месторождений посредством внедрения IT-решений, формирования единой системы информационного моделирования объектов строительства, создания общих требований к моделям данных и использования беспилотных летательных аппаратов (БПЛА) для мониторинга строительства.
3	Актив будущего	Создание и ведение цифровых двойников, интегрированное управление производством и управление надежностью оборудования.

Большинство проектов цифровой трансформации компании находятся в стадии разработки или завершения, поэтому ПАО «Газпром» еще необходимо направлять не малые усилия для внедрения цифровых технологий в систему обеспечения экономической безопасности.

На основе результатов анализа разрабатывается стратегия по управлению рисками, которая включает в себя набор мероприятий по превентивной защите и реагированию на возможные инциденты:

Во-первых, компания активно применяет принцип «защиты в глубину». Предприятия ТЭК устанавливают несколько уровней защиты, чтобы минимизировать атаки. При этом необходимо контролировать сетевой трафик;

Во-вторых, ПАО «Газпром» развивает культуру безопасности среди своих сотрудников, с помощью тренингов, мастер-классов и повышения

квалификации. Также стимулируется ответственное поведение сотрудников при работе с информацией и осуществлении операций в информационных системах;

В-третьих, компания активно взаимодействует с другими организациями и экспертами в области кибербезопасности.

Также ПАО «Газпром» активно участвует в разработке стандартов и нормативных документов по кибербезопасности.

Важным аспектом является также постоянное мониторинг состояния информационной безопасности предприятия. Регулярно проводятся аудиты и проверки систем, чтобы выявить потенциальные риски и недостатки. На основе результатов аудита принимаются соответствующие корректирующие меры для устранения выявленных уязвимостей.

Таким образом, особенности управления цифровыми потоками в нефтегазовой отрасли заключаются в оптимизации бизнес-процессов нефтегазовых компаний на основе применения цифровых технологий, методов, решений.

Заключение. Практическая реализация управления рисками в области кибербезопасности осуществляется через систематический анализ уязвимостей, применение принципа «защиты в глубину», развитие культуры безопасности информации среди сотрудников, взаимодействие с другими организациями и экспертами, а также постоянное мониторинг состояния информационной безопасности.

Таким образом, рассмотренные практики помогают обеспечить эффективную защиту от киберугроз и минимизировать возможные риски для предприятия ТЭК.

Использованные источники:

1. Доктрина энергетической безопасности Российской Федерации от 13 мая 2019 года №216.

2. Абалкин Л.И. Экономическая безопасность России: угрозы и их отражение// Вопросы экономики. – 2013.- №12.

3. Агафонов В.А. Стратегическое управление и экономическая безопасность: монография. – М.: НИЦ ИНФРА-М, 2006. – 257 с.

4. Васильков А.В. Безопасность и управление доступом в информационных системах. - М.: Форум, -2015. – 368с.

5. Гриднева Е.В., Шаповалов В.И. Подходы к оценке уровня экономической безопасности предприятия // Экономика и бизнес: теория и практика. – 2019. – № 12-1. – С. 113-115.

6. Кибербезопасность в нефтегазовой отрасли: путь к надежной защите//[Электронный ресурс] — URL: https://axoftglobal.ru/news/kiberbezopasnost (дата обращения: 11.11.2023)

7. Котенко И.В. Методы оценивания уязвимостей: использование для анализа защищенности компьютерных систем // Защита информации. Инсайд. – СПб.: Афина. – 2011. – № 4. – С. 74–81.

8. Курило А.П. Управление рисками информационной безопасности: учебное пособие для вузов – 2-е изд., испр. М.: Горячая линия – Телеком, 2015. – 130 с.

9. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. - М.: ГЛТ, 2016. – 280с.

10. Основы киберугрозы, типы угроз, 2017 // [Электронный ресурс] — URL: https://itsecforu.ru/2017/03/08/основы-киберугрозы-типы-угроз/ (дата обращения: 09.11.2023)

11. Официальный сайт ПАО «Газпром нефть» // [Электронный ресурс] — URL: https://www.gazprom-neft.ru (дата обращения: 09.11.2023)

12. Официальный сайт ПАО «Газпром» // [Электронный ресурс] — URL: https://www.gazprom.ru (дата обращения: 09.11.2023)

13. Столбов А.Г. Организационно-экономическое обоснование системы управления энергетической безопасностью Мурманской области. – М.: Издательство «Спутник+», 2011. – 183 с.

14. COSO Enterprise Risk Management - Integrated Framework, 2004 // [Электронный ресурс] — URL: https://www.coso.org/guidance-erm.

15. PMI (Project Management Institute) // [Электронный ресурс] — URL: https:// https://www.defence.lk/upload/ebooks (дата обращения: 09.11.2023)

16. What is Cybersecurity and Why It is Important // [Электронный ресурс] — URL: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security - (дата обращения: 11.11.2023)