Журнал "Мировые цивилизации" / Scientific journal "World civilizations" https://wcj.world

2021, №1, Том 6 / 2021, No 1, Vol 6 https://wcj.world/issue-1-2021.html

URL статьи: https://wcj.world/PDF/02ECMZ121.pdf

**Ссылка для цитирования этой статьи:**
Захаров А.Н. Корпоративная безопасность фирмы в контексте развития Арктических регионов России // Мировые цивилизации, 2021 №1, https://wcj.world/PDF/02ECMZ121.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

**For citation:**
Zakharov A.N. (2021). Corporate security of the company in the context of the development of the Arctic regions of Russia. *World civilizations*, [online] 1(6). Available at: https://wcj.world/PDF/02ECMZ121.pdf (in Russian)

**УДК 338.24**

**Захаров А.Н.**
ФГБОУ ВО «Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации», Москва, Россия
Доктор экономических наук
Профессор кафедры «Мировой и национальной экономики»
E-mail: azakharov@vavt.ru

# Корпоративная безопасность фирмы в контексте развития Арктических регионов России

**Аннотация.** В условиях трансформации глобальной экономической среды службы корпоративной безопасности фирм, активная часть деятельности которых проходит в Арктическом регионе России, должны быть способны пересмотреть и обновить традиционный подход к процессу обеспечения корпоративной безопасности. В эпоху сверхбыстрых преобразований, происходящих во всех секторах мировой экономики, система корпоративного управления, а значит и система корпоративной безопасности не могут работать по старым сценариям. Внедрение современных тенденций в оптимизацию бизнес-процессов на основе технологий цифровизации открывает широкие возможности для роста, но вместе с тем значительно усложняет процесс обеспечения безопасности фирм.

**Ключевые слова:** Арктические регионы России, корпоративная безопасность, кибербезопасность, архитектура корпоративной безопасности, ландшафт угроз

Мировой тренд цифровой трансформации оказывает значительное влияние на бизнес-среду Арктической зоны России. С постоянным увеличением потоков данных в компаниях Арктического региона возникает потребность в более совершенной инфраструктуре, способной соответствовать росту цифрового сектора. Кибертехнологии и цифровые инструменты все чаще заменяют существующие традиционные механизмы, а информация, услуги и данные перемещаются в цифровую сферу в соответствии с тенденцией цифровизации. При этом компании, имеющие центры обработки данных, объекты энергетической инфраструктуры, расположенные в Арктическом регионе, должны обеспечить надежный контроль состояния, физической и информационной безопасности своих объектов. На современном этапе взаимосвязанные вопросы цифровизации и безопасности в Арктическом регионе становятся одними из приоритетных и оказывают значительное влияние на расширение ландшафта угроз безопасности компаний, находящихся в стадии цифровой трансформации. В этих условиях решение задачи долгосрочного экономического роста фирмы

невозможно без обеспечения надежной защиты критически важной информационной инфраструктуры и информационной безопасности.

Изменение ландшафта угроз корпоративной безопасности и связанная с этим необходимость трансформации системы безопасности компании обусловливает важность не только расширения инструментария управления безопасностью, но и расстановки приоритетов внутри уже сформировавшихся направлений корпоративной безопасности: информационной безопасности, экологической, экономической (финансовой) безопасности, правовой безопасности, физической и личной безопасности сотрудников, физической безопасности инфраструктуры, управления рисками, кадровой безопасности, репутационной безопасности.

Среди угроз корпоративной безопасности в Арктическом регионе следует выделить: оказание направленного физического воздействия (в том числе, удаленно) на объекты критической инфраструктуры компании; высокая вероятность возникновения техногенных катастроф вследствие сложных климатических условий региона; повышение рисков возникновения киберинцидентов из-за перехода компаний в цифровой контур; многоэтапность хакерских атак на информационную инфраструктуру (центры обработки данных, каналы связи), объекты критической инфраструктуры фирм; рост утечек данных вследствие человеческого фактора; промышленный шпионаж; террористические атаки на объекты компании.

Роль подразделения корпоративной безопасности компании заключается в защите активов, сотрудников, технологий, технических ресурсов и данных компании и клиентов от внутренних и внешних угроз для обеспечения надлежащего непрерывного функционирования фирмы и снижения производственных, коммерческих и финансовых рисков. Согласно прогнозам, общемировые расходы на безопасность будут только возрастать и превысят 100 млрд долл. ежегодно. Компании тратят большие суммы денег на предотвращение нарушений безопасности, защиту финансовых данных и раннее обнаружение кибератак.

Для эффективного управления безопасностью в условиях новых бизнес-реалий предприятиям целесообразно использовать проактивный подход к обеспечению безопасности, ядром которого является способность подразделения корпоративной безопасности прогнозировать влияние различных событий на возникновение и развитие угроз и работать на их предупреждение. Одна из самых важных задач, которую постоянно должны решать подразделения корпоративной безопасности с проактивной моделью поведения – анализ и прогноз ситуации на предмет выявления потенциальных угроз и оценки их возможного влияния на компанию. В частности, подразделениям коммерческих организаций, работающим в Арктических регионах России, в целях снижения вероятности возникновения различного рода инцидентов [1], способных привести к резонансным проблемам, в том числе связанным с возможным нарушением экологической обстановки в регионе, проактивный подход необходим в первую очередь. Структуры безопасности должны отслеживать новые тренды, моделировать возможные сценарии поведения злоумышленников, выявлять изменения в их подходах и методах.

В этих условиях важна оперативность адаптации к происходящим изменениям не только стратегии управления компанией, но и процесса обеспечения корпоративной безопасности на всех основных направлениях, основанного на понимании значимости процессов, оказывающих наибольшее воздействие на состояние безопасности фирмы и оценку потенциальных источников атак или уязвимостей. Предотвращение угроз нарушения безопасности предприятия следует считать наиболее стратегически важным элементом системы защиты, как

[1] https://tass.ru/obschestvo/9637329.

показывает практический опыт, недопущение инцидентов значительно удешевляет процесс обеспечения безопасности из-за отсутствия дополнительных издержек на восстановление функционирования и критичности простоев.

Переход к цифровизации бизнеса значительно увеличивает объемы данных, генерируемых компаниями, их партнерами и клиентами. Информация стала очень важным элементом современной интегрированной экосистемы бизнеса и ее ценность для коммерческих организаций, как и для злоумышленников, постоянно растет. Цифровизация бизнеса сделала компании уязвимыми перед новыми угрозами, что, разумеется, способствует актуальности проблемы эффективного обеспечения кибербезопасности и конфиденциальности данных. Идеология цифровой трансформации бизнеса предполагает необходимость одновременного преобразования системы безопасности и управления рисками в режиме реального времени.

Привычная архитектура безопасности фирмы работает лишь до тех пор, пока угрозы или факторы риска остаются традиционными. В связи с изменением ландшафта угроз для достижения необходимого уровня безопасности и цифровой трансформации компании необходимо расширить взгляд на процесс обеспечения безопасности предприятия, сделав его более интеллектуальным и всеобъемлющим. В частности, необходима систематизация мер защиты объектов инфраструктуры компаний от новых видов угроз, например, БПЛА (беспилотников, дронов), которые могут с успехом использоваться недобросовестными конкурентами и террористическими группировками. Как показывает анализ практического опыта обеспечения корпоративной безопасности, одиночные противоправные действия против организаций трансформировались в форму многоэтапных кампаний, и аналитики “в ручном режиме” часто не способны увидеть всю картину и распознать цепочку шагов атакующей стороны, поэтому для эффективного отражения современных киберугроз требуется внедрение автоматической системы раннего распознавания инцидентов с использованием технологий искусственного интеллекта.

В условиях, когда для устойчивости бизнеса особенно важно сохранение целостности и конфиденциальности информации, обеспечение необходимого уровня корпоративной безопасности должно подкрепляться поддержкой инициатив в области кибербезопасности на уровне принятия стратегических решений. Способность компании противостоять кибератакам является ключевым фактором корпоративной безопасности, а одной из важнейших задач является оптимизация системы корпоративной безопасности, повышение ее гибкости и оперативности реакции на угрозы и вызовы цифровой трансформации.

Одной из тенденций, характерных для современной ситуации, является необходимость опережающего обновления и расширения принятых подходов к обеспечению безопасности, как правило, сфокусированных на текущих задачах фирмы. В частности, спровоцированный эпидемиологической ситуацией в мире форсированный массовый переход компаний к дистанционному формату работы сотрудников вызвал необходимость оперативного учета множества проблем безопасности. Для обеспечения непрерывности бизнеса в сложившейся ситуации организациям необходимо обеспечить комплексную защиту расширяющейся в реальном времени архитектуры безопасности. Помимо решения технических задач формирования доступных коммуникационных каналов между корпоративными сетями и удаленными устройствами, должны решаться задачи по развертыванию надежной защиты от современных угроз и методов противодействия киберпреступности на всех этапах функционирования предприятия. Конвергенция физической и информационной безопасности, в совокупности со все более усложняющимися и развивающимися технологиями цифровизации, приводит к ситуации, когда процесс обеспечения безопасности фирмы становится междисциплинарной областью деятельности и включает в себя технологии искусственного интеллекта, методы социальной инженерии и новейшие информационные

технологии. Современная система физической и инфраструктурной безопасности строится на технологиях биометрии, радиочастотной идентификации, спутниковых системах наблюдения и слежения, а специалисты подразделения обеспечения безопасности должны использовать эти технологии и ориентироваться в возникающих проблемных ситуациях. По мере перехода общества к Индустрии 4.0. и парадигме цифровизации развития, проблема обеспечения безопасности организаций становится все более критической. Введение профессиональных стандартов может помочь выкристаллизовать понимание возникающих проблем, а также определить область ответственности подразделений безопасности в рамках уменьшения возможного ущерба и управлении рисками.

Представляется очевидным, что при освоении арктического шельфа риски, связанные с разведкой запасов нефти и газа, здесь выше, чем где бы то ни было, поскольку это необходимый результат развития отрасли в сложных условиях северной природно-климатической среды, требующей применения уникальных технологий и оборудования, а инфраструктура остается недостаточно развитой, все это может приводить к различным негативным последствиям, к осложнениям экологической ситуации в Арктическом регионе [2] . В этих условиях подразделению, отвечающему за безопасность фирмы, необходимо развивать направление аналитического обеспечения процессов оценки и прогнозирования широкого спектра угроз, а также разрабатывать сценарии реагирования на инциденты нарушения безопасности. Кроме того, важной составляющей повышения эффективности решения вопросов обеспечения безопасности как на национальном уровне, так и на уровне корпораций, является налаженное взаимодействие между государственными органами и частными компаниями. Такое взаимодействие способно значительно повысить взаимную результативность решения вопросов безопасности на всех уровнях на различных направлениях: экологической, транспортной, финансовой, экономической, информационной.

Таким образом, к основным задачам подразделений корпоративной безопасности в Арктическом регионе можно отнести:

- мониторинг, анализ и прогноз развития ситуации на предмет выявления потенциальных угроз и оценки их возможного влияния на безопасность компании;
- систематизацию мер защиты объектов инфраструктуры компаний от новых видов угроз, например, БПЛА (беспилотников, дронов);
- разработку методологических рекомендаций по оценке рисков, управленческих инструментов и технологических методов защиты критически важной инфраструктуры в суровых погодных условиях;
- аналитическое обеспечение процессов оценки и прогнозирования широкого спектра угроз, разработка сценариев реагирования на инциденты нарушения безопасности;
- взаимодействие с государственными органами и частными компаниями по предупреждению и снижению возможных последствий инцидентов.

Как представляется, эффективность деятельности подразделения, отвечающего за безопасность фирмы в Арктическом регионе, зависит от своевременности и точности оценки угроз, правильности расстановки приоритетов защиты. Комплексная стратегия управления безопасностью компании в регионе должна выходить за рамки локальных угроз, должен осуществляться постоянный мониторинг угроз и их систематизация. Корпоративная

[2] https://www.rbc.ru/society/03/06/2020/5ed7dadc9a79472475bc4f62.

безопасность в Арктическом регионе является областью, подвергающейся непрерывным изменениям, и требует от специалистов по корпоративной безопасности высокопрофессионального подхода к работе на опережение возникающих угроз, предполагающего объединение знаний последних передовых практик и тенденций.

## ЛИТЕРАТУРА

1. Стратегия развития Арктической зоны России и обеспечения национальной безопасности до 2035 года. Указ Президента Российской Федерации от 26 октября 2020 г. № 645. URL: http://static.kremlin.ru/media/events/files/ru/J8FhckYOPAQQfxN6Xlt6ti6XzpTVAvQy.pdf (дата обращения: 20.11.2020).
2. Zandee D., Kruijver K., Stoetman A. The future of Arctic security The geopolitical pressure cooker and the consequences for the Netherlands. URL: https://www.clingendael.org/sites/default/files/2020-04/Report_The_Future_of_Arctic_Security_April_2020.pdf. (дата обращения: 20.11.2020).
3. Degeorges D. EU Arctic Policy 2.0: A call for responsible investments in the Arctic? URL: https://thebarentsobserver.com/en/opinions/2020/11/eu-arctic-policy-20-call-responsible-investments-arctic (дата обращения: 22.11.2020).
4. Klimenko E. The Geopolitics of a Changing Arctic. The geopolitics of a changing Arctic. SIPRI. December, 2019. URL: https://www.sipri.org/sites/default/files/2019-12/sipribp 1912_geopolitics_in_the_arctic.pdf (дата обращения: 15.03.2020).

**Zakharov A.N.**
Russian foreign trade academy Ministry of economic development of the Russian Federation, Moscow, Russia
E-mail: azakharov@vavt.ru

# Corporate security of the company in the context of the development of the Arctic regions of Russia

**Abstract.** In the context of the transformation of the global economic environment, companies corporate security services should be able to review and update the traditional approach to the corporate security process, especially those companies operating in the Arctic regions of Russia. In an era of ultra-rapid transformations taking place in all sectors of the world economy, the corporate governance system, and therefore the corporate security system, cannot work according to the old scenarios. The introduction of modern trends in business process optimization based on digitalization technologies opens up wide opportunities for growth, but at the same time significantly complicates the process of ensuring company security

**Keywords:** Russian Arctic regions, corporate security, cybersecurity, corporate security architecture, threat landscape

## REFERENCES

1. Strategiya razvitiya Arkticheskoy zony Rossii i obespecheniya natsional′noy bezopasnosti do 2035 goda. Ukaz Prezidenta Rossiyskoy Federatsii ot 26 oktyabrya 2020 g. № 645. URL: http://static.kremlin.ru/media/events/files/ru/J8FhckYOPAQQfxN6Xlt6ti6XzpTVAvQy.pdf (data obrashcheniya: 20.11.2020).
2. Zandee D., Kruijver K., Stoetman A. The future of Arctic security The geopolitical pressure cooker and the consequences for the Netherlands. URL: https://www.clingendael.org/sites/default/files/2020-04/Report_The_Future_of_Arctic_Security_April_2020.pdf. (data obrashcheniya: 20.11.2020).
3. Degeorges D. EU Arctic Policy 2.0: A call for responsible investments in the Arctic? URL: https://thebarentsobserver.com/en/opinions/2020/11/eu-arctic-policy-20-call-responsible-investments-arctic (data obrashcheniya: 22.11.2020).
4. Klimenko E. The Geopolitics of a Changing Arctic. The geopolitics of a changing Arctic. SIPRI. December, 2019. URL: https://www.sipri.org/sites/default/files/2019-12/sipribp 1912_geopolitics_in_the_arctic.pdf (data obrashcheniya: 15.03.2020).