УДК 33 **DOI: 10.34670/AR.2022.87.87.038**

Кадровая безопасность в системе обеспечения информационной безопасности нефтегазового комплекса

Уразова Кристина Александровна

Старший преподаватель,
кафедра экономической теории и национальной экономики,
Тихоокеанский государственный университет,
680035, Российская Федерация, Хабаровск, ул. Тихоокеанская, 136;
e-mail: 010555@pnu.edu.ru

Дикарева Ольга Сергеевна

Студент,
Тихоокеанский государственный университет,
680035, Российская Федерация, Хабаровск, ул. Тихоокеанская, 136;
e-mail: 2019101518@pnu.edu.ru

Аннотация

В статье рассмотрена позиция нефтегазовой сферы в структуре общей системы экономической безопасности государства, факторы обеспечения экономической безопасности нефтегазовых предприятий. На основе проведенного анализа подходов к определению термина «информационная безопасность», выявлены основные критерии информационной безопасности с точки зрения обеспечения экономической безопасности предприятий нефтегазовой сферы. Статья посвящена исследованию кадровой безопасности в системе обеспечения информационной безопасности нефтегазового комплекса. Проведен анализ угроз информационной безопасности, на основании которого определена структура информационной безопасности нефтегазового комплекса, выявлены основные причины нарушений, вызывающих операционные риски, сделан вывод о последствиях использования незащищенной информационной системы и значимости мероприятий по обеспечению безопасности. Рассмотрено влияние кадровой безопасности нефтегазовых компаний на информационную безопасность. Предложен ряд мер по совершенствованию системы кадрового обеспечения нефтегазового комплекса для предотвращения угроз информационной безопасности.

Для цитирования в научных исследованиях

Уразова К.А., Дикарева О.С. Кадровая безопасность в системе обеспечения информационной безопасности нефтегазового комплекса // Экономика: вчера, сегодня, завтра. 2022. Том 12. № 5А. С. 425-431. DOI: 10.34670/AR.2022.87.87.038

Ключевые слова

Кадровая безопасность, информационная безопасность, экономическая безопасность, нефтегазовый комплекс, угроза, кибербезопасность, киберсреда.

Введение

Нефтегазовый комплекс по праву занимает первое место в формировании национальной экономики каждой страны. Нефтегазовый комплекс формируется не только за счет добычи углеводородного сырья из почвы, не малую долю занимают процессы по очистке ресурсов и изготовлению из нефти и газа готовой продукции.

Для России нефтегазовый комплекс является одним из основополагающих направлений экономики, так как формирует основную долю государственного бюджета, что напрямую влияет на благосостояние всего населения страны и национальную безопасность. В нефтегазовом комплексе России наибольшей конкурентоспособностью обладает сфера добычи сырья, так как нефть и газ – один из приоритетных экспортных товаров. Развитие нефтегазового комплекса России зависит от наличия специализированного оборудования, своевременного принятия технологических решений и, как следствие, наличия высококвалифицированных кадров.

Основная часть

Основные принципы формирования стратегии развития нефтегазового комплекса включают: разработку интегрированной системы фискальных и экономических инструментов, адаптированной к существующим реалиям современного мира, создание стабильной налоговой среды; перенос основной налоговой нагрузки на период выхода производства на проектную мощность; снижение косвенных административных расходов; максимальное использование инструментов для снижения рисков.

Информационные технологии сократили время принятия технологических решений, как внутри отдельных компаний, так и на государственном и международном уровне. Упрощение процесса внутренних и внешних коммуникаций влечет за собой рост угроз кибератак. Киберугрозы с каждым днем становятся все более изощренными и настойчивыми. Особое опасение у государств вызывают кибермоделированные атаки на важные энергетические объекты, как основополагающие элементы экономической стабильности и национальной безопасности.

В последние годы число атак на организации нефтегазового комплекса с точки зрения информационной безопасности значительно увеличилось. В связи с этим возросла доля инвестиций в технологические решения, направленные на предотвращение угроз информационной безопасности.

Наиболее распространенной угрозой информационной безопасности для предприятий нефтегазового комплекса является промышленный шпионаж, начиная от кибератак шпионажа с помощью вредоносных программ и заканчивая вторжением высокопоставленных злоумышленников с целью нарушения оперативного контроля.

Возросшая роль информационной безопасности как для нефтегазового комплекса в частности, так и для России в целом влечет за собой необходимость переосмысления значимости информационной безопасности, как важнейшего фактора жизни, влияющего на формирование национальной безопасности. Информационная безопасность нефтегазового комплекса содержит информацию о плановых, материально-финансовых, договорных условиях деятельности, данные финансового и управленческого учета, а также другие типы данных. Такая коммерческая информация является строго конфиденциальной, и ее потеря может иметь

решающее значение для работы всего предприятия: привести к серьезным экономическим спадам или в будущем из-за разливов или утечек нефти.

Зачастую осведомленность сотрудников и надежность информационной безопасности воспринимается как должное, даже в таких хорошо защищенных областях, как нефтегазовый комплекс. Учитывая тот факт, что большинство атак на информационную безопасность происходят из-за халатного отношения внутренних сотрудников к политике информационной безопасности организации, возникает необходимость совершенствования системы кадровой безопасность предприятий нефтегазового комплекса. По данным отчета Symantec об атаках на информационную безопасность, организации нефтегазового комплекса входят в пятерку самых подверженных информационным атакам организаций. Следовательно, растет необходимость уделять внимание информационной безопасности, поскольку нефтегазовые компании стремятся защитить свои активы от кибератак.

Наиболее яркими примерами угроз информационной безопасности являются:

Использование вредоносного компьютерного червя – «Stuxnet», для угона промышленных систем управления по всему миру в 2010 году. Данной атаке были подвержены и предприятия нефтегазового комплекса, в частности нефтеперерабатывающие заводы и газопроводы. Огромный урон червь нанес ядерной отрасли Ирана, уничтожив пятую часть иранских ядерных центрифуг. Червь был доставлен с помощью большого пальца рабочего.

В августе 2012 года одна из ведущих мировых компаний подверглась атаке компьютерного вируса Shamoon, уничтожившего 30000 корпоративных персональных компьютеров компании, что привело к немедленному отключению внутренней сети компании. Вирус был запущен одним из сотрудников, имевших привилегированный доступ к системе управления компании.

В январе 2015 г. онлайновые злоумышленники могли получать удаленный доступ к устройству, которое использовалось для контроля уровня бензина на заправочных станциях в Соединенных Штатах – так называемый автоматический датчик уровня топлива в баке или ATG, манипулировать им, вызывать оповещения и даже отключать поток топлива [Грошева, Невмержицкий, 2017].

Таким образом, целенаправленный контроль безопасности сотрудниками компаний может сократить риски информационной безопасности. Важную роль для формирования информационной безопасности занимают технические средства контроля, состоящие из корректирующих и превентивных мер. К таким мерам относят: мониторинг контента, антивирус, сетевую безопасность, брандмауэры. В организациях, уделяющих особое внимание поведенческому контролю, социально-организационный аспект определяется как жизненно важный элемент управления информационной безопасностью. По данным исследования кибербезопасности Price Waterhouse and Coopers за 2020 год, самым серьезным нарушением безопасности на предприятиях нефтегазового комплекса является халатность персонала, в отчете указано, что «сотрудник — это все, что нужно для компрометации системы организации и безопасности данных» [там же]. К основным ошибкам, допускаемым сотрудниками, которые наносят ущерб организации, относят: утечку конфиденциальных данных, несоблюдение правил защиты информации и несанкционированный доступ к данным, относящимся к коммерческой тайне.

Одной из основных причин нарушений, провоцирующих операционные риски, можно назвать низкую осведомленность об информационной безопасности. Постоянное обновление и разработка систем по предупреждению угроз кибербезопасности сопровождается появлением новых улучшенных инструментов для взлома, что обуславливает необходимость систематического обновления программного обеспечения с точки зрения брандмауэра.

Для предотвращения угроз и снижения рисков информационной безопасности, связанных с киберсредой, необходимо внедрение специализированных мер, таких как:

– Запрет применения личных цифровых носителей для хранения и передачи данных, ограничение использования приложений на ПК;

– Применение средств для защиты данных, таких как антивирусы, firewall, proxy или разработка своих антивирусных программ;

– Формирование системы поэтапного контроля за доступом к информации компании.

Однако, учитывая сложную инфраструктуру нефтегазового комплекса, подверженную влиянию информации и напрямую связана с персоналом организации, можно говорить о том, что данных мер будет недостаточно. Возникает новая угроза – угроза кадровой безопасности предприятий нефтегазового комплекса. Сотрудник компании – это человек, не только владеющий данными, относящимися к коммерческой тайне, но и подверженный многим другим рискам, например, здоровья и безопасности [Кузнецова, 2011].

Угрозы кадровой безопасности для предприятий нефтегазового комплекса можно классифицировать на внешние и внутренние.

Внешние угрозы подвержены воздействию экзогенных факторов, влекущие за собой нанесение ущерба, которым можно отнести:

– Конкурентные преимущества оппонентов;

– Инфляция на рынке;

– Хантинг.

Внутренние угрозы формируются под влиянием эндогенных факторов и также приводят к ущербу:

1. Низкая квалификация сотрудников копании, несоответствующая занимаемой должности;

2. Отсутствие системы мотивации персонала в повышении квалификации;

3. Неграмотное взаимодействие с техническим и высокотехнологическим оборудованием;

4. Промышленный шпионаж в корыстных целях.

Человеческий фактор играет гораздо большую роль для информационной безопасности компании, чем технические угрозы, поскольку предотвратить кибератаку при помощи технических средств легче, чем идентифицировать человеческие угрозы. Для обеспечения информационной безопасности и контроля за поведением работников предприятия эффективнее использовать физические меры безопасности. Анализ систем управления информационной безопасностью предприятий нефтегазового комплекса выявил низкую эффективность в системах управления информационной безопасностью предприятий. Это обуславливает необходимость включение в состав стратегий организационного управления предприятиями, таких программ как программы повышения осведомленности, оценка посредством мониторинга и соблюдения политик, для защиты ценных записей и активов.

Для предотвращения угроз необходимо четко регламентировать защиту и контроль персонала предприятия, а также принять ряд мер по совершенствованию кадровой отрасли:

1. Участие в формировании кадровой стратегии компании, процессе планирования человеческих ресурсов, финансовой, финансовой деятельности, развития и оценки персонала;

2. Проведение аттестации сотрудников, которая впоследствии показывает уровень знаний и квалификации сотрудника, соответствующую должность;

3. Привлечение молодых специалистов: организация стажировок студентов и школьников в нефтегазовой отрасли, развитие в них качества лидеров и высококвалифицированных рабочих, т.е. привлечение новых людей с их идеями и способностями;

4. Создать эффективную систему мотивации сотрудников, возможность повышения квалификации, семинаров с топ-менеджерами и начальством;

5. Создание комфортных условий труда и проведение общественных мероприятий, мероприятий по выплате пенсий и премий работникам за выслугу лет или за вклад в производство [Бобылев, 2016].

Существенное влияние на соблюдение политики информационной безопасности предприятия оказывает что привязанность, приверженность и личные нормы сотрудника. Эффективное организационное управление может повысить приверженность, привязанность, вовлеченность и личные нормы человека. Мониторинг физической безопасности может улучшить приверженность, вовлеченность и личные нормы человека, а также может дать лучшие результаты для соблюдения политики информационной безопасности. Практическая оценка и анализ рисков также оказывают этическое влияние на обязательства и участие.

Заключение

Обеспечение экономической безопасности нефтегазового комплекса связано с множеством проблем, решение которых зависит от наличия ресурсов и средств, оценки состояния предприятия, качества проводимых мероприятий, осведомленности сотрудников и уровня кадрового состава. менеджмент в целом. От эффективного обеспечения зависят не только финансовые показатели нефтегазовых компаний, но и жизнь и здоровье людей.

Библиография

1. Бобылев Ю. Возможности и ограничения развития нефтяного сектора // Экономическое развитие России. 2016. № 4. С. 23.
2. Богомолов В.А. Экономическая безопасность. URL: https://biblioclub.ru/index.php?page=book&id=118282
3. Грошева Е.К., Невмержицкий П.И. Информационная безопасность: современные реалии // Бизнес-образование в экономике знаний. 2017. № 3 (8). С. 35-38.
4. Захаров А.Э., Жариков В.В. Экономическая безопасность России // Экономинфо. 2012. № 18. С. 40-42.
5. Кузнецова Н.В. Безопасность персонала: терминологический аспект // Известия Байкальского государственного университета. 2011. №. 5. С. 102.
6. Лысенко А.О. Кадровая безопасность в системе обеспечения экономической безопасности предприятия // Международный журнал гуманитарных и естественных наук. 2018. № 3. С. 213-216.
7. Перминов О.Г., Глущенко Н.В. О системе экономической безопасности предприятий нефтегазовой отрасли // Проблемы экономики и юридической практики. 2016. № 6. С. 347-350.
8. Шободоева А.В. Развитие понятия «информационная безопасность» в научно-правовом поле России // Известия Байкальского государственного университета. 2017. Т. 27. №. 1. С. 74.

Personnel security in the information security system of the oil and gas complex

Kristina A. Urazova

Senior Lecturer,
Department of Economic Theory and National Economy,
Pacific National University,
680000, 136, Tikhookeanskaya str., Khabarovsk, Russian Federation;
e-mail: 010555@pnu.edu.ru

Ol'ga S. Dikareva

Graduate Student,
Pacific National University,
680000, 136, Tikhookeanskaya str., Khabarovsk, Russian Federation;
e-mail: 2019101518@pnu.edu.ru

Abstract

The research in economics presented in this article considers the position of the oil and gas sector in the structure of the general system of economic security of the state, the factors for ensuring the economic security of oil and gas enterprises. Based on the analysis of approaches to the definition of the term information security; the main criteria for information security were identified in terms of ensuring the economic security of oil and gas enterprises. The article is devoted to the study of personnel security in the information security system of the oil and gas complex. An analysis of information security threats was carried out, on the basis of which the information security structure of the oil and gas complex was determined, the main reasons of violations that cause operational risks were identified, a conclusion was made about the consequences of using an unprotected information system and the importance of security measures. The influence of personnel security of oil and gas companies on information security is considered in this study. A number of measures have been proposed by the authors to improve the system of personnel support for the oil and gas complex in order to prevent threats to information security.

For citation

Urazova K.A., Dikareva O.S. (2022) Kadrovaya bezopasnost' v sisteme obespecheniya informatsionnoi bezopasnosti neftegazovogo kompleksa [Personnel security in the information security system of the oil and gas complex]. Экономика: вчера, сегодня, завтра. 2022. Том 12. № 5A. С. 425-431. DOI: 10.34670/AR.2022.87.87.038

Keywords

Personnel security, information security, economic security, oil and gas complex, threat, cyber security, cyber environment.

References

1. Bobylev Yu. (2016) Vozmozhnosti i ogranicheniya razvitiya neftyanogo sektora [Opportunities and limitations of the development of the oil sector]. *Ekonomicheskoe razvitie Rossii* [Economic development of Russia], 4, p. 23.
2. Bogomolov V.A. *Ekonomicheskaya bezopasnost'* [Economic security]. Available at: https://biblioclub.ru/index.php?page=book&id=118282 [Accessed 05/05/2022]
3. Grosheva E.K., Nevmerzhitskii P.I. (2017) Informatsionnaya bezopasnost': sovremennye realii [Information security: modern realities]. *Biznes-obrazovanie v ekonomike znanii* [Business education in the knowledge economy], 3 (8), pp. 35-38.
4. Kuznetsova N.V. (2011) Bezopasnost' personala: terminologicheskii aspekt [Personnel safety: terminological aspect]. *Izvestiya Baikal'skogo gosudarstvennogo universiteta* [Bulletin of the Baikal State University], 5, p. 102.
5. Lysenko A.O. (2018) Kadrovaya bezopasnost' v sisteme obespecheniya ekonomicheskoi bezopasnosti predpriyatiya [Personnel security in the system of ensuring the economic security of an enterprise]. *Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk* [International Journal of the Humanities and Natural Sciences], 3, pp. 213-216.
6. Perminov O.G., Glushchenko N.V. (2016) O sisteme ekonomicheskoi bezopasnosti predpriyatii neftegazovoi otrasli [On the system of economic security of oil and gas industry enterprises]. *Problemy ekonomiki i yuridicheskoi praktiki* [Problems of Economics and Legal Practice], 6, pp. 347-350.

7. Shobodoeva A.V. (2017) Razvitie ponyatiya «informatsionnaya bezopasnost'» v nauchno-pravovom pole Rossii [Development of the concept of information security in the scientific and legal field of Russia]. *Izvestiya Baikal'skogo gosudarstvennogo universiteta* [Bulletin of the Baikal State University], 27, 1, p. 74.
8. Zakharov A.E., Zharikov V.V. (2012) Ekonomicheskaya bezopasnost' Rossii [Economic security of Russia]. *Ekonominfo* [Econominfo], 18, pp. 40-42.