Список использованных источников:
1. Федеральная служба государственной статистики [Электронный ресурс]. – Режим доступа: http://www.gks.ru.
2. Адушев М.Н., Лоткова Е.П. Девальвация рубля: возможные преимущества и последствия для российской экономики // Международный журнал прикладных и фундаментальных исследований. 2015. № 7 С. 86-92 2.
3. Божко Е.И., Шитиков С.Э. Роль нефти в бюджете Российской Федерации // Актуальные проблемы авиации и космонавтики . 2011. №7. С.15-16. 3.
4. Мухаметшин М.Ф., Хасанова А.Ш. Факторы роста конкурентоспособности нефтехимических предприятий // Научное обозрение. 2015. № 1. С. 230-233.

ВЗАИМОСВЯЗЬ КАДРОВОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБУЧЕНИИ СОТРУДНИКОВ ОАО «РЖД»

Дужан Татьяна Юрьевна[1]
Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара

Аннотация. В статье проанализирована проблема обеспечения информационной и кадровой безопасности при реализации электронного обучения сотрудников ОАО «РЖД». Определены причины взаимосвязи кадровой безопасности организации с информационной безопасностью. Описаны методы обеспечения кадровой и информационной безопасностей, оказывающие влияние на систему обучения персонала компании.

Ключевые слова*:* кадровая безопасность, информационная безопасность, электронное обучение, система обучения персонала.

В настоящее время в каждой крупной компании актуальной проблемой является обеспечение кадровой и информационной безопасности. Особую значимость данная проблема имеет в тех компаниях, которые осуществляют приоритетные направления реализации государственной политики

При реализации государственной программы «Цифровая экономика» в компании ОАО «РЖД» была разработана концепция «Цифровая железная дорога», подразумевающая разработку единого информационного пространства для реализации грузовых и пассажирских перевозок, встраивание Интернет-системы обработки больших объемов данных, создание новых мобильных

[1]Студент 1 курса магистратуры Института экономики и управления Самарского университета. Научный руководитель: Дмитриев Д.С., кандидат педагогических наук, доцент кафедры математики и бизнес-информатики Самарского университета.

рабочих мест и электронный документооборот во всех процессах, выполняемых компанией, а также использование сквозных информационных технологий при выполнении поставленных перед холдингом задач [2, с. 80-81].

С 2016 года в компании отмечаются кадровые риски, связанные с недостаточным количеством квалифицированного персонала, вследствие низкой конкурентоспособности на рынке труда. В связи с этим в компании принимаются усилия, направленные на создание такой среды, в которой работник может профессионально совершенствоваться и эффективно выполнять задачи на своем рабочем месте. При реализации социальной политики ОАО «РЖД» одной из основных задач является непрерывное развитие персонала [2, с. 101].

Для повышения квалификации сотрудников в созданном в 2009 году корпоративном университете с каждым готом появляются новые курсы и направления переподготовки и повышения квалификации персонала. Также для развития персонала реализованная система дистанционного и электронного обучения персонала с использование web-технологий, позволяющая проходить обучение по различным курсам, осуществлять плановое обучение сотрудников, а также проводить тестирование по оценке компетенций без отрыва от производства. Это позволяет пройти очередное обучение большему количеству сотрудников за меньшее количество времени, в отличии от обучения персонала с командированием в корпоративный университет.

Согласно стандарту ОАО «РЖД» «Управление информационной безопасностью. Общие положения» под информационной безопасностью понимается состояние защищенности информации, при котором обеспечиваются такие ее характеристики, как конфиденциальность, целостность и доступность [3, с. 4].

В связи с реализацией электронного обучения проблема обеспечения информационной безопасности при использовании сети Интернет и Интранет становится одной из ключевых. В качестве угроз информационной безопасности организации при использовании электронного обучения можно выделить следующие:

- вероятность получения несанкционированного доступа к электронной информационно-образовательной среде;
- атаки на информационные службы и сервисы, задействованные при работе системы электронного обучения;
- изменения, вносимые в назначенные курсы, и механизмы тестирования;
- изменение персональных данных в личном кабинете сотрудника;
- утечка информации от сотрудников;

Для обеспечения информационной безопасности в компании ОАО «РЖД» создана служба безопасности, отвечающая за контроль и мониторинг состояния всех информационных ресурсов, проведение внешнего и внутреннего

аудита информационной безопасности, а также создания условий для обеспечения высокого уровня безопасности при выполнении работ согласно должностным инструкциям сотрудников.

При управлении информационной безопасностью в ОАО «РЖД» выделяются следующие принципы: законность, достаточность и нормирование защиты, базирование на рисках, надежность, соразмерность затрат на защиту, контроль доступа, открытость, приемлемость, многоуровневая защита и разделение привилегии [3].

В качестве мер по минимизации проявления угроз информационной безопасности на всех предприятиях холдинга проводится мониторинг и анализ мер обеспечения информационной безопасности, периодический анализ и переоценка рисков, внутренний и внешний аудит (как в запланированные сроки, так и внепланово, с целью оценки эффективности системы управления информационной безопасности и разработки рекомендаций по ее совершенствованию). Виды мониторинга, проводимого в ОАО «РЖД», представлены на рисунке 1 [3].

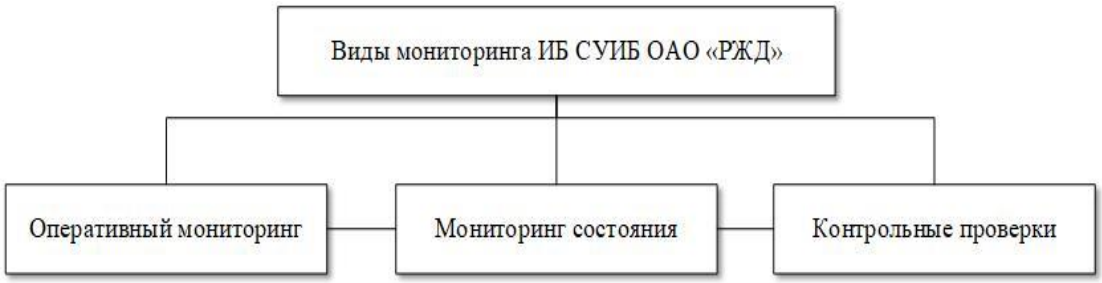

Рисунок 1 – Виды мониторинга информационной безопасности в ОАО «РЖД»

Под кадровой безопасностью организации понимается процесс предотвращения негативных воздействий на экономическую безопасность и другие виды безопасности предприятия за счет рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом [1].

В компании разработана и внедрена система управления рисками и внутреннего контроля, предназначенная для обеспечения разумной уверенности в достижении целей холдинга, а также защиты стоимости и активов компании. Структура процесса управления рисками, являющегося частью корпоративного управления представлена на рисунке 2 [2, с. 133-134].

Рисунок 2 – процесс управления рисками в ОАО «РЖД»

В связи с ежегодным развитием корпоративного университета, при обучении сотрудников ОАО «РЖД» возникают следующие кадровые риски:

- риск увольнения сотрудника, получившего высокую квалификацию и повысившего свою компетентность;
- риск незаинтересованности в обучении;
- риск не усвоения материала;
- риск непонимания важности обучения сотрудником;
- риск утечки информации при обучении;
- риск подделки документов о прохождении обучения;
- риск получения неполного объема информации;
- риск получения ошибочной программы обучения и т.п..

В качестве методов предотвращения данных кадровых рисков организации необходимо поддерживать конкурентоспособный уровень на рынке труда, также обеспечивать оплату труда на уровне выше общероссийского. Большое внимание должно уделяться не только способам достижения поставленных целей, но и мотивации персонала к долговременному сотрудничеству, а также появлению желания получать новые знания и использовать их в своей профессиональной деятельности.

Таким образом, источниками угроз как для информационной, так и для кадровой безопасности являются сотрудники компании. Для обеспечения безопасности организации в целом необходимо тесное взаимодействие политик кадровой и информационной безопасности, так как при реализации электронного обучения с доступом к глобальной сети Интернет состояние безопасности становится уязвимым. При использовании методов минимизации кадровой безопасности сотрудники должны знать какими средствами обеспечивается защита информации, а также как реагировать нарушение информационной безопасности ОАО «РЖД». Обеспечение как кадровой, так и информационной безопасности в первую очередь, подразумевает состояние защищенности

компании от внешнего и внутреннего воздействия на информацию со стороны персонала организации и внешних источников угроз.

Список использованных источников:

1. Кибанов А.Я. HR-Portal [Электронный ресурс]: Кадровая безопасность в системе безопасности организации «Кадровик. Кадровый менеджмент», № 10, 2010 – Режим доступа: http://znanium.com/catalog/product/452694 (Дата и время доступа: 30.11.2019 14:20)
2. Годовой отчет 2018 «Новый взгляд» [Электронный ресурс] // – Режим доступа: https://ar2018.rzd.ru (Дата и время доступа: 30.11.2019 15:20)
3. Стандарт ОАО «РЖД» // «Управление информационной безопасностью. Общие положения» // СТО РЖД 1.18.002-2009

ЭКОНОМИКА СОВМЕСТНОГО ПОТРЕБЛЕНИЯ ИЛИ ШЕРИНГ-ЭКОНОМИКА

Жугалёв Иван Игоревич[1]
Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара

Аннотация*:* Статья посвящена исследованию основных элементов экосистемы ЭСП, анализу мотиваций пользователей шеринг-сервисов, созданию обобщенного портрета пользователя и выявлению ключевых трендов развития ЭСП в России.

Ключевые слова*:* ЭСП, экосистема, преимущества, демография, модели, тренды.

Что такое «шеринг-экономика»? Шеринговая экономика (от анг. to share – делиться), или экономика совместного потребления – новая культура и социально-экономическая модель, где происходит осознанный отказ от частной собственности в пользу собственности коллективной, причем отказ этот связан не с недостатком денег, а с желанием расширить свои возможности.

Укрепление горизонтальных связей в обществе позволяет людям оптимизировать потребительские расходы и существенно повысить качество жизни, используя принципы совместного потребления. Благодаря онлайн-сервисам потребителям нет необходимости приобретать товар для получения

[1]Студент 3 курса бакалавриата Института экономики и управления Самарского университета. Научный руководитель: Гоман И.В., кандидат экономических наук, доцент, доцент кафедры экономики инноваций Самарского университета.