Шумилина В.Е., к.э.н., доцент кафедры «Экономическая безопасность, учет и право» ДГТУ, Ростов-на-Дону, Россия;

Shumilina.vera@list.ru

Аистова А.А.,студент 4 курса кафедры «Экономическая безопасность, учет и право» ДГТУ, Ростов-на-Дону, Россия;

nasty2640@icloud.com

Асташова О.В., студент 4 курса кафедры «Экономическая безопасность, учет и право» ДГТУ, Ростов-на-Дону, Россия;

astashova-olga@mail.ru

Управление информационными рисками в организации

Аннотация. В статье рассматриваются понятие и классификация информационных рисков, разъясняются возможности управления рисками в различных организациях, предлагаются основные меры управления рисками в коммерческих организациях. Особое внимание уделяется вопросам управления информационными рисками в организациях.

Ключевые слова: информационные риски, управление рисками, информационные технологии, информационная безопасность, инфраструктура управления рисками, цифровой помощник.

ShumilinaV. E., Ph. D., associate Professor of the Department "Economic security, accounting and law" DSTU, Rostov-on-don, Russia;
Shumilina.vera@list.ru

Aistova A. A.,4 nd year student of the Department of economic security, accounting and law of the DSTU, Rostov-on-Don, Russia;

dsemerninova@gmail.com

Astashova O. V.4 nd year student of the Department of economic security, accounting and law of the DSTU, Rostov-on-Don, Russia;

astashova-olga@mail.ru

Information risk management in the organization

Annotation. The article discusses the concept and classification of information risks, explains the possibilities of risk management in various organizations, and suggests the main measures of risk management in commercial organizations. Special attention is paid to the issues of information risk management in organizations.

Keywords: information risks, risk management, information technology, information security, risk management infrastructure, digital assistant.

В настоящее время информационные технологии стали частью большинства политических, экономических и социальных процессов, активно помогая им развиваться.

Очевидно, что сектор информационных технологий является двигателем развития многих национальных экономик, а также лидером капитализации мировой экономики в условиях глобализма. При этом в новом веке ситуация с информационной безопасностью меняется так же стремительно, как цифровизация экономики, общества и всех основных жизненных процессов.

В свою очередь, поскольку создание, внедрение и использование информационных технологий тесно связано с угрозами информационной безопасности, задача эффективного управления рисками информационной безопасности стоит на первом месте [1, с.1].

Риски присущи каждой сфере человеческой деятельности. Информационная безопасность рассматривает информационные риски, которые понимаются как возможность того, что данная конкретная угроза может использовать уязвимость актива или группы активов и тем самым нанести ущерб организации.

Риски информационной безопасности напрямую влияют на активы организации. Менеджер по рискам должен работать над улучшением

ключевых показателей во всех трех областях, что позволяет специалистам по информационной безопасности быстрее выявлять угрозу и устранять ее с меньшими затратами [2, с.3].

Как показывает практика крупных бизнес-организаций, основным подходом к успешному решению этих задач являются методы стратегического уровня, а не уровня оперативного управления. С ростом интеграции информационных технологий во все области бизнеса менеджеры не уделяют достаточно внимания анализу рисков информационной безопасности.

Эти меры необходимо принимать в обязательном порядке, потому что, например, в крупных банках информация является самым важным активом, и вопросы информационной безопасности, безусловно, находятся на первом месте. В случае инцидента информационной безопасности организация понесет ущерб, включая значительные непредвиденные расходы и возможную потерю клиентов [2, с.4].

Успех управления рисками зависит от эффективности инфраструктуры управления, которая обеспечивает структуру и действия, которые должны применяться в организации на всех уровнях.

Эффективное управление рисками должно соответствовать принципам, показанным на рисунке 1.1.

Рисунок 1.1 – Принципы управления рисками[3,с.6]

Эти принципы можно объяснить следующим образом:

1) адаптируемость – структура и процесс управления рисками настраиваются в соответствии с деятельностью организации;

2) интегрируемость – это неотъемлемая часть деятельности организации;

3) основанный на максимальной доступности информации – используемая информация должна быть актуальной, ясной и доступной для заинтересованных сторон;

4) инклюзивный – своевременное вовлечение заинтересованных сторон с учетом их знаний, мнений и точек зрения, которые приводят к повышению и обоснованности управления рисками;

5) динамический – менеджмент риска предвидит, обнаруживает, распознает и реагирует на изменения в рисках информационной безопасности надлежащим и своевременным образом;

6) основанный на максимальной доступности информации – используемая информация должна быть актуальной, ясной;

7) постоянно совершенствуется – управление рисками постоянно улучшается благодаря обучению и опыту [3,с.7].

Целью структуры управления рисками является помощь организации во внедрении инфраструктуры управления рисками информационной безопасности. Эта эффективность будет зависеть от степени интеграции в систему менеджмента организации, включая принятие решений. Это требует поддержки заинтересованных сторон, особенно высшего руководства [4].

Структура управления рисками включает внедрение (интеграцию), разработку, оценку и улучшение управления рисками в организации. Чтобы эффективно управлять информационными рисками, организация должна оценить свои существующие методы и процессы, выявить пробелы в структуре и устранить их. Компоненты структуры и их взаимодействие должны быть адаптированы к потребностям организации.

На рисунке 1.2 показаны компоненты структуры управления рисками.

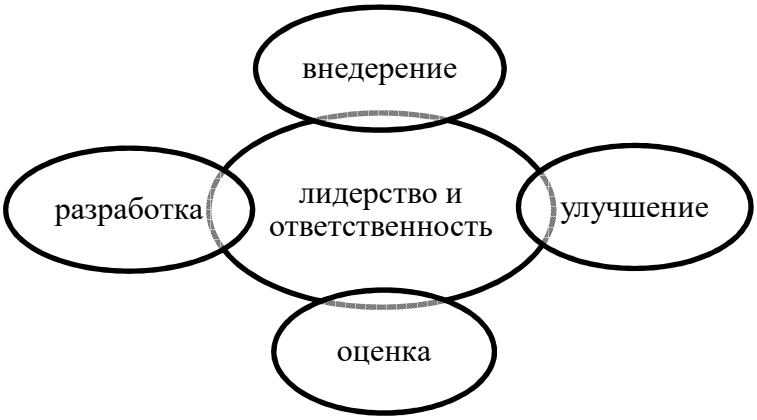

Рисунок 1.2 – Структура риск-менеджмента[5, с.2]

Процесс управления рисками включает систематическое применение политик, процедур и практик для обеспечения связи и консультаций, оценки, управления и мониторинга рисков, анализа и документации, а также отчетности о рисках, поэтому на рисунке 1.3 показан сам процесс риск-менеджмента.

Рисунок 1.3 – Процесс риск-менеджмента[6]

В условиях действия различных внешних и внутренних факторов риска могут использоваться различные методы снижения риска, влияющие на конкретные аспекты деятельности предприятия [9, с.11]:

Все методы управления рисками принято делить на 4 группы:

– методы предотвращения риска;

– методы локализации риска;

– методы диверсификации рисков;

– методы компенсации рисков.

В предпринимательстве часто используются методы предотвращения рисков, что означает выработку стратегических и тактических решений, исключающих возникновение рискованных ситуаций.

Методами локализации рисков пользуются в тех редких случаях, когда есть возможность четко определить источники возникновения рисков и идентифицировать их. Эти методы позволяют выделить в отдельные структурные подразделения наиболее опасные этапы бизнес-процессов, тем самым увеличив возможность контроля над ними. Примером могут служить:создание специальных структурных подразделений, венчурных предприятий; заключение договоров о совместной деятельности для реализации рискованных проектов.

Методы диверсификации рисков заключаются в распределении общего риска и делятся на:

1) разделение ответственности между участниками проекта;

2) диверсификация продаж и поставок;

3) диверсификация инвестиций.

Методы компенсации риска основаны на результатах более обширных аналитических работ. Они наиболее трудоемки и нацелены на создание механизмов предотвращения рисков (прогнозирование внешней обстановки на предприятии; стратегическое планирование деятельности; обучение персонала и его инструктирование)[9, с.12].

Очень часто в организациях наблюдается разрозненное взаимодействие по поводу информационных угроз между руководством и техническими специалистами, включая IT-директоров. У каждой стороны свои цели: в подавляющем большинстве случаев руководство заинтересовано в экономии денег, а отдел рисков называет вопросы информационной безопасности, не имеющие к нему никакого отношения, потенциальными критическими

угрозами. Для решения этих проблем IT-специалистам необходимо дополнительное финансирование, но эти риски часто можно принять, не нанося ущерба существованию бизнеса[7, с.8].

Чтобы считать цифровую трансформацию успешной, компании недостаточно купить лицензию, установить новое программное обеспечение или перенести определенные бизнес-процессы в онлайн.

Внедрение новых технологий – это, конечно, необходимый первый шаг, но он должен сопровождаться серьезными изменениями в процессах принятия решений, корпоративной культуре и подходах к управлению и обучению сотрудников.

Цифровые помощники помогают компаниям более плавно ориентироваться в этих изменениях с максимальной выгодой для бизнеса.

Функционал цифровых помощников может корректироваться в зависимости от выбора конкретной платформы, но в целом можно выделить четыре больших блока [10, с.2]:

1. Единое окно для пользователей. Цифровой помощник с помощью диалогового сервиса обучает сотрудников работе с IT-системами, отвечает на вопросы, предлагает решения и подсказки. Как правило, цифровые помощники могут работать как в популярных публичных мессенджерах (Telegram, Viber, FB Messenger и др.), так и встраиваться в любые закрытые корпоративные инструменты и каналы связи;

2. Выполнение рутинных операций. Благодаря интеграции с корпоративной ERP-системой цифровой помощник может выполнять действия за пользователя. Например, самостоятельно создавать стандартные приложения и контракты, отслеживать статус документов, организовывать командировки, запрашивать информацию и формировать отчеты;

3. Частичная замена техподдержки. Цифровые помощники способны решить большинство проблем пользователей и оказать техническую поддержку 24 часа в сутки. Сотруднику не нужно никуда звонить, писать запросы и ждать ответа – услуга доступна в режиме реального времени. Если

цифровой помощник не справляется с задачей, он сам подключает оператора или отправляет запрос в IT-отдел, предоставляя всю необходимую информацию о проблеме сотрудника.

В конечном итоге использование цифровых помощников – это вопрос прямой коммерческой выгоды. Есть несколько областей, где экономятся ресурсы или оптимизируются бизнес-процессы [11, с.5]:

а) с помощью цифровых помощников можно организовать обучение сотрудников без дополнительных финансовых затрат или необходимости выделять на это отдельное время – сотрудник осваивает сложное программное обеспечение прямо в процессе, в режиме онлайн;

б) сотрудники получают значительную экономию времени и повышают продуктивность: им больше не нужно искать информацию в 100-страничных инструкциях, спрашивать коллег или ждать ответа от службы поддержки;

в) автоматизация массовых рутинных операций сводит потенциальные ошибки практически к нулю. Например, номер контракта будет введен правильно, даты и сумма счета будет правильной. Кроме того, создание или проверка статуса документа, отправка заявки или создание отчета с помощью цифрового помощника происходит намного быстрее;

г) в результате решения технических проблем пользователей цифрового помощника нагрузка на IT-поддержку значительно снижается, а значит, и затраты на оплату высококвалифицированного персонала.

Фактически, бизнес получает возможность построить полноценную дорожную карту цифровой трансформации на основе конкретных, индивидуальных для каждой компании аналитических данных.

Подводя итог, можно констатировать следующее – любая организация осуществляет свою деятельность для достижения каких-либо коммерческих целей, однако важно понимать, что в настоящее время становится практически невозможно вести коммерческую деятельность без гарантии собственной безопасности посредством управления рисками [8.с.1].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бабич, А.М.Управление информационными рисками в организации.[Текст]: учебник / А.М. Бабич. – М.: 2017.- С.1.

2. Брусянин В. Е., Махмутов Я. И., Сковронская Я. В., Цыбульский А. В. Риски информационной безопасности // Молодой ученый. - 2018. - №49. - С.3-4.

3. Горелов А.Б.Принципы управления рисками/ А.Б. Горелов//Анализ информационных рисков в организации.- 2018.- №5.-С.6-7.

4. Шумилина, В. Е. Экономические риски и угрозы безопасности бизнеса / В. Е. Шумилина, А. А. Попова, Л. Е. Овчинникова // Управление безопасностью бизнеса в современных условиях. – Москва : AUSPUBLISHERS, 2021. – С. 23-30.

5. Коровина А.Б. Компоненты структуры управления рисками[Текст] /А. Б. Коровина, Е. Новик // Риски компании. - 2017. - №4. - С.2.

6.Красницкий В.А. Процесс управления рисками [Текст] /В. А. Красницкий // Экономика.- 2018. - №7.

7. Шумилина, В. Е. Управление предпринимательскими рисками в системе экономической безопасности / В. Е. Шумилина, Т. В. Сушкова, К. Е. Шегеря // : Современные проблемы экономической безопасности, учета и права в Российской Федерации. Том 2, 11 января 2018 года – 31 2019 года, 2019. – С. 9. – DOI 10.26526/conferencearticle_5c50608381edb3.56789250.

8. Мельникова Ю.А. Информационные риски организации [Текст] / Ю.А. Мельникова //Экономика РФ. - М., 2017. №9. - С.1.

9. Шумилина, В. Е. Информационная безопасность как фактор обеспечения экономической безопасности / В. Е. Шумилина, К. Н. Абдуллаева, Ю. А. Топор // Актуальные вопросы обеспечения экономической безопасности в Российской Федерации в условиях цифровой экономики. – Мельбурн : AUS PUBLISHERS, 2018. – С. 1-7.

10. Тимошенко В.А. Цифровые помощники для компаний. //Информационные риски на предприятии. - № 5. – 2018. – С.2.

11. Шумилина, В. Е. Анализ и оценки рисков для обеспечения экономической безопасности / В. Е. Шумилина, Е. Н. Богуслав // Управление безопасностью бизнеса в современных условиях. – Москва : AUSPUBLISHERS, 2021. – С. 31-37.

References:

1. Babich, A.M. Information risk management in the organization. [Text]: textbook / A.M. Babich. - M .: 2017.- P.1.

2. Brusyanin VE, Makhmutov Ya. I., Skovronskaya Ya. V., Tsybulsky AV Information security risks // Young scientist. - 2018. - No. 49. - P.3-4.

3. Gorelov AB Principles of risk management. Gorelov // Analysis of information risks in the organization. - 2018.- №5.-C.6-7.

4. Shumilina, V. E. Economic risks and threats to business security / V. E. Shumilina, A. A. Popova, L. E. Ovchinnikova // Business security management in modern conditions. - Moscow: AUSPUBLISHERS, 2021 .-- S. 23-30.

5. Korovina A.B. Components of the risk management structure [Text] / A. B. Korovina, E. Novik // Company risks. - 2017. - No. 4. - C.2.

6.Krasnitsky V.A. Risk management process [Text] / B. A. Krasnitsky // Economy. - 2018. - №7.

7. Shumilina, V. E. Management of entrepreneurial risks in the system of economic security / V. E. Shumilina, T. V. Sushkova, K. E. Shegerya //: Modern problems of economic security, accounting and law in the Russian Federation. Volume 2, January 11, 2018 - 31 2019, 2019 .-- P. 9. - DOI 10.26526 / conferencearticle_5c50608381edb3.56789250.

8. Melnikova Yu.A. Information risks of the organization [Text] / Yu.A. Melnikova // Economy of the Russian Federation. - M., 2017. No. 9. - C.1.

9. Shumilina, V. E. Information security as a factor in ensuring economic security / V. E. Shumilina, K. N. Abdullayeva, Yu. A. Topor // Topical issues of ensuring economic security in the Russian Federation in the digital economy. - Melbourne: AUS PUBLISHERS, 2018 .-- S. 1-7.

10. Timoshe nko V.A. Digital assistants for companies. // Information risks at the enterprise. - No. 5. - 2018. - P.2.

11. Shumilina, V. E. Analysis and assessment of risks to ensure economic security / V. E. Shumilina, E. N. Boguslav // Business security management in modern conditions. - Moscow: AUSPUBLISHERS, 2021 .-- S. 31-37.