ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 338.14

УПРАВЛЕНИЕ РИСКАМИ В ИНФОРМАТИЗАЦИИ

Синогеев Иван Сергеевич
Министерство обороны Российской Федерации, Военнослужащий.
Краснодарский край, Анапский район, хутор Усатова Балка, улица Полевая, дом 21 (индекс 353435)
sinogeev76@yandex.ru

Аннотация

Текущий период развития общества связан с массовой информатизацией. Процесс информатизации затронул все без исключения сферы бизнеса, народного хозяйства, науки, социально-экономического развития и т.д. Но вместе с той несомненной пользой, которую информатизация несет обществу, существуют так же определенные риски. Эти риски связаны, прежде всего, с необходимостью защиты информации. Так же определенные риски несет использованием информационных технологий в преступных целях. В связи с вышеизложенным, автором настоящей статьи, предпринята попытка научного анализа и критического осмысления процесса управления рисками в современной системе информатизации.

Ключевые слова: развитие общества, информатизация, риски информатизации, управление рисками.

RISK MANAGEMENT IN INFORMATIZATION

Sinogeev Ivan Sergeevich
Ministry of Defense of the Russian Federation, Serviceman.
Krasnodar Territory, Anapa District, Usatov Balka farm, Polevaya street, house 21 (zip code 353435)

ABSTRACT

The current period of development of society is associated with mass informatization. The informatization process has affected all spheres of business, the national economy, science, socio-economic development, etc. without exception. But along with the undoubted benefits that informatization brings to society, there are also certain risks. These risks are associated primarily with the need to protect information. There are also certain risks associated with the use of information technology for criminal purposes. In connection with the foregoing, the author of this article made an attempt to scientific analysis and critical understanding of the risk management process in the modern informatization system.

Keywords: development of society, informatization, risks of informatization, risk management.

Основой указанной проблемы является несовершенный процесс управления рисками в информатизации (технологическими, организационными, финансовыми и человеческими рисками).

На конфиденциальность, целостность и доступность информации влияют многие угрозы, пытающиеся использовать уязвимость. В зависимости от вероятности возникновения угроз, использующих уязвимости, и размера эффектов, которые угроза может вызвать, возникает риск.

Конфиденциальность, целостность и доступность информации подвержены риску. Увеличение риска угроз напрямую влияет на систему. Угрозы, использующие уязвимости системы. Уязвимость системы также увеличивает риск. Уязвимость системы позволяет подвергать риску активы (информацию в данном контексте). Свойство имеет определенную систему ценностей, которая влияет на всю организацию. Риск напрямую влияет на стоимость имущества, уменьшая ее. [2, с. 6]

К организациям предъявляются особые требования безопасности. Эти требования безопасности выполняются с помощью специальных средств контроля. Средства контроля необходимы для снижения риска (удовлетворение требований конфиденциальности, целостности и доступности информации). Контроль помогает защитить систему от угроз. Система защиты замыкается на этом.

Элементы управления: [6, с. 215]

1. Детектирующие – выявляют атаку на систему;

2. Предотвращение – защищает систему от уязвимостей, уменьшает количество вторжений в систему и может быть стартером (драйвером) для обнаружения элементов управления;

3. Корректирующий контроль – уменьшение вторжений в систему в результате уязвимости.

4. Технологические/эксплуатационные

- все риски, связанные с оборудованием, программным обеспечением, сетью и выполнением повседневных задач;

- недоступность сервисных рисков (инфраструктурные риски - эти риски связаны с ошибками, связанными с архитектурой системы (зависимость надлежащей производительности приложений и ИТ-сервисов от оборудования, сети и операционной системы).

Самый большой риск здесь связан с инвестиции в инфраструктуру риски приложений - недостаточная функциональность приложения, плохой контроль версий ... риски данных - отсутствие хороших процедур для манипулирования данными, низкое качество резервного копирования, риск потери данных, риски безопасности ИКТ - несанкционированный доступ к данным (отсутствие физической или логической защиты данных и приложений, невнимательность к целостности данных, доступности для них, невнимательность к точности и достоверности данных, несанкционированный доступ к основным серверам и сетевому оборудованию). [8, с. 956]

Эти риски наиболее многочисленны, но не столь фатальны для функционирования организации, хотя при длительном характере могут сказаться на эффективном функционировании.

Финансовые риски: [4, с. 76]

1. Выключение плана информатизации из финансовых планов;

2. Перерасход средств;

3. Анализ низкого качества или отсутствия анализа бизнес-отчетов (из-за прогнозов затрат на реализацию проекта или внедрения бизнес-процессов);

4. Отсутствие разработки сценариев обеспечения непрерывности бизнеса в случае реализации угрозы;

5. Отсутствие страхования основного оборудования.

Организационные / стратегические риски: [9, с. 66]

1. невозможность выполнения ключевых бизнес-процессов, функций;

2. нехватка ресурсов для процесса как ключевого звена между ними;

3. неспособность определить ключевые неблагоприятные события, влияющие на достижение важнейших бизнес-целей;

4. неспособность распознать способности и способности, необходимые для управления воздействиями, которые позволяют восстановить организацию на удовлетворительном уровне производительности.

Эти риски тесно связаны с реализацией бизнес-стратегий. Обнаружение, анализ и снижение этих рисков должны быть неотъемлемой частью стратегического плана организации.

Сотрудники являются значительным источником рисков, а также стабильности и успеха компании. Из-за этих фактов риски, связанные с работниками, очень важны. Эти риски могут возникать преднамеренно или непреднамеренно. Некоторые из них: [1, с. 51]

- недостаточная подготовка ИТ-персонала и вытекающие из этого ошибки;

- умышленное создание ошибок и проблем («утечка» конфиденциальной информации);

- неспособность ключевых сотрудников выполнять свои задачи (например, болезнь);

- зависимость только от одного работника (замены нет, знания не структурные, а интеллектуальные);

- забастовка сотрудников...

Эти риски можно преодолеть постоянным обучением сотрудников, обеспечением условий для удовлетворения сотрудников (зарплата, заработная плата, хорошая рабочая атмосфера), признанием нетрудоспособности, знакомством сотрудников через постоянное общение с ними, подачей личного примера.

Процесс управления рисками в целом одинаков во всех подходах, которые можно найти в литературе. Основными этапами процесса управления рисками являются: [5, с. 28]

Определение риска.

Оценка риска

Идентификация риска

Реагирование на риск

Эти шаги должны быть реализованы на всех уровнях организации. Единственная разница заключается в том, рассматриваются ли риски на стратегическом уровне, тактическом или оперативном. На стратегическом уровне владельцы бизнеса обсуждают риски, на тактическом уровне руководители (руководители, директора), управление операционными рисками осуществляют непосредственные исполнители (рабочие). Все они в своем сегменте должны следовать вышеуказанным шагам в процессе управления рисками. Здесь очень кратко о каждом из шагов. [7, с. 301]

Определение контекста

Здесь определяется область, на которой мы фокусируемся в управлении рисками.

Идентификация риска - это критический этап, поскольку он необходим для выявления всех угроз системе и каждой уязвимости, которую может использовать угроза. Наконец, в результате пар угроз и уязвимостей и их вероятности может быть определен риск. Здесь возникает проблема, как объективно идентифицировать угрозы и уязвимости.

Анализ рисков - на этом этапе система анализирует выявленные риски, оценивает вероятность возникновения рисков, их влияние на результативность. На основании полученных результатов риску присваивается определенная значимость.

Оценка риска - ранжированные риски оцениваются в соответствии с определенными критериями. Критерии оценки должны быть определены заранее. Это могут быть: характер и тип последствий, которые могут возникнуть, а также поддающиеся измерению последствия, как определяется вероятность, как долго будут существовать последствия, снижается ли вероятность возникновения с течением времени, метод определения уровня риска, уровень толерантности к риску, какой уровень риска требует реагирования на риск, какие наиболее важные риски требуют немедленных действий.

Реагирование на риск - здесь определяется реакция на риск с целью его устранения или снижения до приемлемого уровня. Ответами на риск могут быть: избежание риска (не предпринимать действий, которые могут привести к возникновению риска), принятие риска (принятие мер независимо от риска), уничтожение источников риска, передача риска (переключение риска на другой – например, страхование), снижение вероятности негативных событий.

В процессе управления рисками при информатизации возникает вопрос, какие средства контроля в ответ на риск (при обработке риска) должны существовать? Что необходимо: включить дублирование ресурсов, повысить уровень отказоустойчивости всей системы, запасной набор ИТ-сервисов (которые бы временно взяли на себя роль тех, что простаивают). Важно составить план действий на случай реализации риска, необходимо расставить приоритеты (какие ИТ-услуги необходимо доставлять, а без каких можно). План необходим для разработки возможных сценариев достижения риска, сценарии должны выявлять существенные риски ИТ-услуг и превентивно реагировать на них. [3, с. 82]

Управление рисками в целом и, следовательно, в информатизации представляет собой важные управленческие навыки для повышения безопасности и защиты внутри организации (также и в области ИКТ). Управление рисками для качества позволяет сделать результаты информатизации приемлемыми для пользователей, а руководство воспринимает ИТ как важного партнера для лучшего и более эффективного принятия решений.

Список литературы:

1. Алферова, В. В. Роль it-специалистов в эпоху информатизации современного общества / В. В. Алферова, Р. Э. Акопян // Международный журнал гуманитарных и естественных наук. – 2022. – № 5-4(68). – С. 50-52.
2. Бойченко, О. В. Информатизация систем управления бизнес-процессами / О. В. Бойченко, М. Э. Баталова // МедиаVектор. – 2022. – № 4. – С. 4-7.
3. Гайсина, Р. Р. Концептуальные основы информатизации предпринимательской деятельности / Р. Р. Гайсина // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика. – 2022. – № 2(40). – С. 78-84.
4. Гнездилова, Н. А. Исследование стратификационных рисков в развитии обучающихся в условиях информатизации образования / Н. А. Гнездилова, Т. А. Щучка, О. В. Рыжкова // Балтийский гуманитарный журнал. – 2021. – Т. 10. – № 2(35). – С. 75-78.

5. Гуров, Ф. Н. Информатизация образования: основные проблемы и вызовы / Ф. Н. Гуров, Е. В. Иноземцева // Тенденции развития науки и образования. – 2022. – № 86-6. – С. 27-30.
6. Лапина, Т. И. Оценка рисков проекта информатизации управления образованием / Т. И. Лапина, О. С. Прокопенко // Будущее науки - 2019: сборник научных статей 7-й Международной молодежной научной конференции, Курск, 25–26 апреля 2019 года. – Курск: Юго-Западный государственный университет, 2019. – С. 214-218.
7. Морковина, С. С. Риски, факторы риска и их приоритизация / С. С. Морковина, Т. Ю. Дзичковская // Актуальные вопросы современной экономики. – 2022. – № 6. – С. 299-303.
8. Серебрякова, Т. А. Информатизация общества / Т. А. Серебрякова, В. В. Зинченко // Вопросы устойчивого развития общества. – 2022. – № 5. – С. 955-958.
9. Товченник, Д. С. Система управления рисками на предприятии: риск-менеджмент / Д. С. Товченник, Д. В. Павлов // Парадигма. – 2022. – № 1. – С. 65-68.

References:

1. Alferova, V. V. The role of IT-specialists in the era of informatization of modern society / V. V. Alferova, R. E. Akopyan // International Journal of Humanities and Natural Sciences. - 2022. - No. 5-4 (68). – P. 50-52.
2. Boychenko, O. V. Informatization of business process management systems / O. V. Boychenko, M. E. Batalova // Media Vector. - 2022. - No. 4. – P. 4-7.
3. Gaisina, R. R. Conceptual foundations of informatization of entrepreneurial activity / R. R. Gaisina // Vestnik UGNTU. Science, education, economics. Series: Economy. - 2022. - No. 2(40). – P. 78-84.
4. Gnezdilova, N. A., Shchuchka, T. A., Ryzhkova, O. V. Study of stratification risks in the development of students in the context of informatization of education // Baltic Humanitarian Journal. - 2021. - T. 10. - No. 2 (35). – P. 75-78.
5. Gurov, F. N. Informatization of education: main problems and challenges / F. N. Gurov, E. V. Inozemtseva // Trends in the development of science and education. - 2022. - No. 86-6. – P. 27-30.
6. Lapina, T. I. Risk assessment of the education management informatization project / T. I. Lapina, O. S. Prokopenko // Future of science - 2019: collection of scientific articles of the 7th International Youth Scientific Conference, Kursk, April 25–26 2019. - Kursk: Southwestern State University, 2019. – P. 214-218.
7. Morkovina, S. S. Risks, risk factors and their prioritization / S. S. Morkovina, T. Yu. Dzichkovskaya // Actual issues of modern economics. - 2022. - No. 6. – P. 299-303.
8. Serebryakova, T. A. Informatization of society / T. A. Serebryakova, V. V. Zinchenko // Issues of sustainable development of society. - 2022. - No. 5. – P. 955-958.
9. Tovchennik, D. S., Pavlov, D. V. Risk management system at the enterprise: risk management / Paradigm. - 2022. - No. 1. – P. 65-68.