**УДК 004** **Информационные технологии**

***Сапега Александр Валерьевич,*** *студент, ДГТУ Ростов-на-Дону, РФ*

# АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

**Аннотация:** Риски безопасности информационной системы должны подвергаться непрерывному мониторингу и контролю с целью определения и поддержания актуального состояния уровня рисков и влияния на предприятие. Рискменеджер/сотрудник дополнительно осуществляет анализ эффективности системы управления риском кибербезоасности и результатов оценки внутреннего/внешнего аудита и, при необходимости, формирует план по внедрению мер, направленных на совершенствование и повышение эффективности системы управления риском кибербезоасности со сроками и ответственными.

**Ключевые слова:** риск, информационная безопасность, кибербезопасность, менеджмент, управление рисками.

**Abstract:** Information system security risks should be subject to continuous monitoring and control in order to determine and maintain an up-to-date state of risk level and impact on the enterprise. The risk manager/employee additionally analyzes the effectiveness of the cyber security risk management system and the results of the internal/external audit evaluation and, if necessary, forms a plan for the implementation of measures aimed at improving and increasing the efficiency of the cyber security risk management system with deadlines and responsible persons.

**Keywords:** risk, information security, cybersecurity, management, risk management.

## Введение

Предприятие обеспечивает проведение непрерывного мониторинга рисков с учетом следующих факторов:

- новых активов, которые были включены в область применения менеджмента риска;
- изменение ценности активов, например, вследствие изменившихся бизнестребований;
- изменение ландшафта угроз применительно к сектору экономики;
- актуальных уязвимостях и вероятности их использования;
- изменение влияния или последствий в случае реализации риска;
- мониторинг потоков информации;
- эффективности существующих мер защиты;
- статистики инцидентов и событий риска кибербезоасности, в том числе причин возникновения событий риска и потерь от их реализации [1; 2].

Предприятие осуществляет деятельность по мониторингу и переоценке риска на регулярной основе. По умолчанию срок переоценки риска устанавливается как ежегодный. Досрочная переоценка риска осуществляется в случае реализации инцидентов и событий риска кибербезоасности, изменении критичности актива, реализации плана обработки рисков или выявлении новых условий, существенно влияющих на уровень риска.

При достижении срока переоценки риска риск-менеджер/работник проводит анализ изменений в области оценки, актуальных угроз, уязвимостей и реализованных мер защиты. В случае отсутствия актуальных угроз и уязвимостей риск переносится в неактуальный и считается обработанным. В случае подтверждения актуальности или выявлении новых угроз, уязвимостей, инцидентов, рискменеджер/работник проводит повторную оценку уровня риска, контроль выполнения ранее предложенных мероприятий и их эффективности. Владелец риска принимает решение по обработке риска с учетом обновленного уровня [1].

Риск-менеджер/сотрудник осуществляет контроль выполнения мероприятий, направленных на уменьшение негативного влияния от реализации

риска кибербезоасности или вероятности реализации угроз кибербезоасности в соответствии с установленными сроками в плане обработки рисков. Рискменеджер/сотрудник запрашивает необходимую информацию о выполнении плана обработки рисков у владельца рисков и ответственных за реализацию мер. В случае невыполнения плана обработки в установленный срок осуществляется эскалация на руководителя структурного подразделения владельца риска/коллегиальный орган по рискам/кибербезопасности [3].

Риск-менеджер/сотрудник осуществляет контроль соблюдения выбранного варианта обработки риска.

В целях повышения эффективности функционирования системы управления риском кибербезопасности Управление внутреннего аудита/внешний аудит проводит независимую оценку эффективности функционирования системы управления риском кибербезопасности на ежегодной основе, в том числе оценку полноты и качества выполнения мероприятий, направленных на уменьшение негативного влияния от риска кибербезоасности. Управление внутреннего/внешнего аудита формирует отчет о результатах оценки эффективности системы управления риском кибербезоасности и предлагаемые рекомендации для повышения качества функционирования процессов и доводит их до коллегиального органа по рискам/кибербезопасности для принятия решения о необходимости совершенствования системы управления риском [4].

Организация и выполнение деятельности по повышению эффективности функционирования системы управления риском кибербезоасности включает, но не ограничивается:

- пересмотр политики управления риском кибербезоасности в части уточнения установленных в ней целей, состава участников и распределения функций;
- пересмотр области применения системы управления риском кибербезоасности;
- пересмотр и доработка методологии оценки риска кибербезоасности;

- пересмотр объемов ресурсного обеспечения в рамках управления риском кибербезоасности.

Управление внутреннего аудита осуществляет контроль за реализацией мер, направленных на улучшение системы управления риском кибербезоасности. **Формирование отчетности.** Разработка отчетности является важным этапом для:

- предоставления информации владельцам рисков для принятия решения по его обработке и дальнейшего развития бизнес-систем;
- повышения осведомленности бизнес-подразделений и руководства;
- принятия управленческих решений руководств;
- мониторинга и контроля рисков.

С целью обмена информацией о деятельности и результатах управления риском КБ, а также для принятия управленческих решений на уровне предприятия предусмотрены следующие виды отчетности:

1. Отчетность по результатам проведения оценки рисков. Формируется по результатам оценки каждого риска, направляется владельцу риска;
2. Отчетность (дашборды) по уровням риска безопасности предприятия, включая детализацию по владельцам риска, вариантам обработки, видам рисков и т.д. Формируется по результатам отчетного периода – ежемесячно. Направляется руководителю, руководству структурных подразделений.
3. Отчетность по инцидентам, событиям риска КБ (в т.ч. возникающих после запуска нового продукта/процесса). Формируется по результатам отчетного периода – ежемесячно. Направляется руководителю, руководству структурных подразделений предприятий

**Риск-культура.** Риск-культура — это устоявшиеся в организации нормы поведения работников, направленные на выявление рисков и управление ими.

Каждый работник предприятия должен действовать в соответствии с принципами риск культуры, а именно:

- знать и соблюдать требования безопасности предприятия;

- сообщать о подозрениях или фактах реализации риска, так как своевременное обнаружение потенциальных проблем или признание ошибок позволяют минимизировать возможные негативные последствия. Работники предприятия информируют риск-чемпиона/риск-менеджера/работника о потенциально возможных рисках КБ или реализовавшихся событиях риска;
- содействовать в проведении расследований события риска КБ. При расследовании событий работники предприятия по запросу предоставляют всю необходимую информацию риск-менеджеру/работнику.

Формирование риск-культуры в предприятие происходит через три основных канала:

- личный пример руководителя;
- общие коммуникации. В предприятие систематически направляются информационные рассылки, памятки, освещающие вопросы рисков;
- обучение работников.

**Заключение (выводы).** В целях поддержания высокого уровня риск-культуры при трудоустройстве новых работников и на регулярной основе в предприятие обеспечивается обучение работников по теме управления рисками.

Формирование обучающих материалов для сотрудников предприятия возлагается на рискменеджера/сотрудника.

Выстраивание и поддержание риск-культуры в предприятие способствует: раннему обнаружению или предотвращению реализации событий риска; минимизации потерь предприятия в случае реализации событий риска.

**Библиографический список:**

1. Галатенко, В.А. Стандарты информационной безопасности. Интернет-университет информационных технологий. ИНТУИТ.ру, 2005.

2. Лопатин, В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества. М.: 2000.

3. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные

методы и средства. М.: ДМК Пресс, 2008.

4. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир, 2009.