УДК 334.024
МРНТИ 06.81.12

Ибыжанова А.Д., к.э.н., https://orcid.org/0000-0001-7552-8203
НАО «Западно-Казахстанский аграрно-технический университет имени Жангир хана», г. Уральск, ул. Жангир хана 51, 090009, Казахстан, iaizhan02@mail.ru

Ibyzhanova A.D., c.e.s., https://orcid.org/0000-0001-7552-8203
NJSC «West Kazakhstan Agrarian and Technical University named after Zhangir khan», Uralsk, st. Zhangir khan 51, 090009, Kazakhstan, iaizhan02@mail.ru

ИНФОРМАЦИОННЫЕ РИСКИ В ФОРМИРОВАНИИ ПОЛИТИКИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ
INFORMATION RISKS IN THE FORMATION OF THE ORGANISATION'S ECONOMIC SECURITY POLICY

Аннотация

Статья рассматривает различные подходы к формированию политики безопасности в организациях с учетом их разработки в крупных мировых компаниях: IBM, Sun Microsystems, Cisco Systems и Microsoft. Подход IBM основан на использовании международного стандарта ISO/IEC 17799 и включает этапы определения информационных рисков, разработки политики безопасности, выработки стратегий для чрезвычайных ситуаций и оценки остаточных рисков. Sun Microsystems предпочитает стратегический подход, начиная с разработки проекта политики безопасности организации и заканчивая поддержанием режима информационной безопасности. Cisco Systems сосредотачивается на оценке рисков в сети и рекомендует создание специальной рабочей группы по реагированию на инциденты. Microsoft предлагает свою стратегию, основанную на управлении информационными рисками и включающую оценку рисков, разработку политики безопасности, внедрение средств защиты и аудит безопасности. Указанные подходы подчеркивают важность анализа и управления информационными рисками в обеспечении безопасности организаций.

ANNOTATION

The article considers different approaches to the formation of security policy in organisations, taking into account their development in large global companies: IBM, Sun Microsystems, Cisco Systems and Microsoft. IBM's approach is based on the international standard ISO/IEC 17799 and includes the stages of information risk identification, security policy development, development of strategies for emergency situations and residual risk assessment. Sun Microsystems prefers a strategic approach from drafting an organisation's security policy to maintaining an information security regime. Cisco Systems focuses on network risk assessment and recommends a dedicated incident response task force. Microsoft offers its strategy based on information risk management, which includes risk assessment, security policy development, security implementation and security auditing. These approaches highlight the importance of information risk analysis and management in securing organisations.

Ключевые слова: *информационная безопасность, экономическая безопасность, риск, управление рисками, управление информацией*

Key words: *information security, economic security, risk, risk management, information management*

Введение. Характеризуя современное состояние внешней среды большинства казахстанских и зарубежных предприятий, из числа факторов, влияющих на выбор системы управления, в первую очередь, на наш взгляд, следует выделить фактор нестабильности и высокой динамики изменений. Влияние этого фактора постоянно нарастает на протяжении последних десятилетий и влечет за собой необходимость использования в формируемой на предприятии системе управления различных методов и инструментов, связанных с

менеджментом рисков. Также следствием этой тенденции является глобальное нарастание информационных потоков и выделение информационного менеджмента в отдельную область управления. На смену индустриальному способу производства приходит информационно-технологический. Информация становится ведущей производительной силой, так как информационное производство определяет на сегодняшний день пути и темпы развития экономических систем, диктует характер технических, организационных и структурных изменений.

Повышение эффективности управления информацией и рисками особенно актуально для наукоемких и инновационных предприятий. Объясняется это прежде всего тем, что в условиях стремительного увеличения мощности информационных потоков ни одно инновационное предприятие не может успешно работать без системы управления знаниями, интегрированной в корпоративную информационную систему. При этом построение и использование корпоративной информационной системы требует концентрации больших объемов обобщенной и систематизированной информации, что ведет к увеличению вероятности утечки секретных и конфиденциальных сведений, а значит, и к необходимости управления рисками информационной безопасности. Поэтому корпоративная информационная система должна, с одной стороны, способствовать эффективной организации информационных потоков внутри предприятия, с другой – создавать условия для решения комплекса задач по обеспечению безопасности информационных ресурсов предприятия. В случае, если корпоративная информационная система не обеспечивает выполнения указанных функций, для инновационного предприятия помимо традиционных возникают новые виды рисков, связанные с потреблением такого специфического фактора производства, как информация.

В связи с этим в системе управления предприятием ее неотъемлемой частью становится риск-менеджмент. Оценивая уровень развития отечественных научных школ риск-менеджмента, можно сделать вывод, что они существенно уступают зарубежным в силу специфической истории развития рыночной экономики в стране. Поэтому на сегодняшний день задача создания фундамента научного риск-менеджмента, его теоретико-методологической основы, в которой оптимальным образом интегрированы адаптированные элементы зарубежных источников и лучшие образцы отечественной теории и практики, в данной области имеет высокую актуальность.

В целом можно сделать вывод об актуальности и недостаточной степени разработанности проблемы управления информационными и экономическими рисками на теоретическом и методологическом уровнях, что обусловило выбор направления данного исследования и определило его цели и задачи.

Материалы и методы исследования. Для проведения данного исследования были использованы как источники литературы, так и данные из практического опыта исследователей в области управления рисками и информационной безопасности. Статьи, книги, научные публикации и стандарты по управлению рисками и информационной безопасности предоставили базовый фундамент для проведения анализа и выработки рекомендаций. Кроме того, были рассмотрены стандарты и методики, разработанные ведущими мировыми компаниями, такими как IBM, Sun Microsystems, Cisco Systems, Microsoft.

Анализ существующих методик оценки рисков в системах обработки информации был основан на систематическом обзоре литературы и стандартов в данной области. Это включало в себя изучение методов анализа рисков, применяемых в различных сферах, а также анализ эффективности этих методов в контексте управления информационными рисками. Характеристика выборки включала в себя широкий спектр источников, включая научные статьи, книги, отчеты, а также стандарты и руководства по информационной безопасности. Это обеспечило достаточное покрытие различных аспектов управления рисками и информационной безопасности, позволяя получить комплексное представление о текущем состоянии и перспективах развития этой области.

В настоящее время существующие методы и средства управления рисками предприятия не объединены в рамках единой методологии и, соответственно, могут применяться только при решении отдельных задач и проблем. В связи с этим одной из наиболее перспективных концепций управления рисками является контроллинг, так как он дает широкие возможности интегрированного объединения и развития научных представлений различных школ

менеджмента, акцентируя внимание на инструментальном и информационном обеспечении управленческих процессов.

Результаты исследования. Проблеме риск-менеджмента, в том числе в сфере информационной безопасности (ИБ), посвящено большое число работ преимущественно, зарубежных ученых, например, А.М. Астахова [1], И.В. Бородушко [2], В.И. Завгороднего [3-5], А.О. Калашникова [6-7], Н.Г. Милославской [8], Г.А. Остапенко [9], С.А. Петренко [10-11], Г.И. Золотаревой [12]; разработано значительное количество стандартов в данной области [13-20].

Вместе с тем необходимо отметить, что, несмотря на то, что в большинстве теоретических работ по управлению информационными рисками декларируется необходимость комплексного подхода сбалансировано сочетающего в себе как методы технологического, так и экономического управления, на практике экономическим методам управления уделяется значительно меньше внимания [21, с. 14].

Любой экономический риск включает в себя информационную составляющих, то есть является и косвенным информационным риском. Соотношение информационной и экономической составляющей для разных рисков вариативно и определяется главным образом значением информации для определенных видов экономической деятельности предприятий и особенностями технологических и управленческих процессов [21, с. 67].

Управление информационными рисками выходит на одно из первых мест среди проблем обеспечения экономической безопасности предприятия. Придание информационному риску экономического смысла позволяет применять экономические методы управления этим риском.

Анализ существующих методик оценки рисков, применяемых в системах обработки информации, показывает, что теоретическая база, необходимая для разработки методик оценки и управления информационными рисками в условиях действия ограничений, является слабо изученной.

Таким образом, возникает объективная необходимость исследования математических методов моделирования рисков в информационных системах и разработки на их основе методических рекомендаций по управлению информационными рисками в различных системах обработки информации.

Метод управления информационными рисками на уровне информационной системы, направленный, в том числе, и на деятельность участвующих в обработке информации этой системой людей, рассмотрен в научной работе зарубежных исследователей Christopher A., Schmidt, M., Owusu K., Althonayan and A. Andronache, Asamoah, D., Luo, Y., Lund, S., Legowo N. [22-29]. В научных исследованиях основной акцент делается на универсальность управления рисками, однако, не содержит подходов к своему применению при управлении информационными рисками для множества угроз информационной безопасности и наличия дополнительных ограничений на выбор средств обеспечения информационной безопасности.

В настоящее время теория и практика информационной безопасности получили интенсивное развитие ввиду широкого распространения информационных технологий. Соответственно при определении целей, задач и механизмов управления защитой информации на уровне организации в качестве основополагающего документа используется политика безопасности. Поэтому отдельного рассмотрения заслуживают подходы к формированию политик безопасности, разработанные ведущими мировыми компаниями: IBM, Sun Microsystems, Cisco Systems, Microsoft. Рассмотрим некоторые из этих подходов.

С точки зрения компании IBM политика безопасности представляет собой составную часть процесса управления информационными рисками, реализуемого на основе международного стандарта ISO/IEC 17799.

В разработке политики безопасности IBM выделяет следующие этапы:

– определение информационных рисков организации, которые способны нанести наибольший ущерб, что необходимо для определения процедур и мер по предупреждению их возникновения;

– разработка политики безопасности, которая будет декларировать меры защиты информационных ресурсов, соответствующие целям и задачам бизнеса;

– выработка стратегий для чрезвычайных ситуаций, а также для случаев, когда выбранные контрмеры не помогли предотвратить потенциальные негативные воздействия в области информационной безопасности;

– оценка остаточных информационных рисков, на основе анализа которых руководство может принять решение о дополнительных инвестициях в средства обеспечения безопасности [5].

Компания Sun Microsystems дает понятию политики безопасности определение стратегического документа, в котором требования и ожидания руководства организации к режиму информационной безопасности выражаются в определенных постоянно контролируемых целях и задачах. При этом предпочтительным считается подход «сверху-вниз», в котором предварительно разрабатывается проект политики безопасности организации, за которым реализуется соответствующая ему структура системы защиты информации предприятия.

Под основной задачей политики безопасности понимается информирование руководства компании и ее сотрудников о требованиях по защите информационных ресурсов компании. Политика безопасности должна применяться ко всем компонентам информационной системы организации. При этом компания Sun Microsystems выделяет в ней следующие разделы:

– структура информационных ресурсов организации и их состав;

– классификация информационных ресурсов;

– определение владельцев информационных ресурсов;

– анализ информационных рисков;

– выработка требований к обеспечению защиты конфиденциальной информации;

– определение методики организации режима информационной безопасности;

– реализация требуемого режима информационной безопасности;

– поддержание режима информационной безопасности организации.

Компания Cisco Systems при построении сетевой политики безопасности рекомендует производить оценку рисков в сети и организовывать специальную рабочую группу по реагированию различных инцидентов, происходящих в ИС. Анализ рисков необходимо производить для того, чтобы классифицировать информационные ресурсы компании и определить среди них наиболее «опасные» угрозы и уязвимости для этих ресурсов. В дальнейшем это будет служить обоснованием выбора соответствующих мер локализации выделенных угроз и уязвимостей. Предполагается, что такой подход способствует нахождению и поддержанию баланса между требуемым уровнем доступа к сети и необходимым уровнем безопасности. В терминологии Cisco Systems политика безопасности определяет следующие уровни информационных рисков:

низкий уровень риска. Доступ для изучения, повреждение или уничтожение неавторизованными лицами информационных систем и данных (компрометирование) не приносит серьезного ущерба, финансовых проблем или проблем другого характера;

средний уровень риска. Компрометирование информационных систем и данных приносит умеренный ущерб, умеренные финансовые проблемы или небольшие проблемы другого характера. Также становится возможным получение несанкционированного доступа к другим частям системы. Восстановление скомпрометированных систем и информации требует умеренных усилий;

высокий уровень риска. Компрометирование информационных систем и данных приносит значительный ущерб или тяжелые финансовые проблемы другого характера. Возможно нанесение ущерба безопасности здоровью и жизни сотрудников. Восстановление скомпрометированных систем и информации требует существенных усилий.

Компания Microsoft предлагает собственную стратегию безопасности, в которой можно выделить следующие составляющие:

– миссия корпоративной безопасности; – принципы информационной безопасности; – модель управления рисками.

– Обеспечение информационной безопасности достигается путем управления информационными рисками, под которым понимается процесс определения, оценки и уменьшения рисков на постоянной основе. Управление рисками позволяет найти разумный баланс между стоимостью средств и мер информационной безопасности и требованиями бизнеса.

– Модель управления информационными рисками, предложенная компанией Microsoft, включает в себя этапы:

– оценка информационных рисков;

– разработка политики безопасности по предупреждению, минимизации, уклонению и локализации рисков;

– внедрение средств защиты (интеграция персонала, бизнес-процессов и технологий для снижения рисков, основанная на соотношении эффективность/стоимость);

– аудит безопасности, оценка действующего уровня защищенности ИС [29].

Национальным банком Республики Казахстан введены в действие Требования к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах.

С целью обеспечения и поддержания высокого уровня информационной безопасности организаций банковской системы данный стандарт определяет регулярную оценку уровня информационной безопасности. Степень необходимой защищенности информационной сферы при этом рассчитывается путем анализа рисков информационной безопасности, которые сопоставляются с характерными для деятельности организации банковской системы РК рисками. По результатам указанного анализа разрабатывается комплекс мероприятий, направленный на управление рисками. Для минимизации информационных рисков создается политика безопасности организации, которая разрабатывается на основе прогнозирования инцидентов информационной безопасности. Для этого составляются модели угроз, уязвимостей и нарушителя, осуществляется идентификация требующих защиты ресурсов, производится оценка рисков, учитывающая особенности применяемых технологий, деятельности организации, а также требований собственников. В соответствии с построенной политикой безопасности формируется и внедряется система менеджмента информационной безопасности (СМИБ) организаций банковской системы.

Обеспечение информационной безопасности организаций банковской системы РК реализуется в соответствии с «процессным подходом» к внедрению, эксплуатации, контролю, сопровождению и модернизации СМИБ.

Деятельность по управлению информационной безопасности организации банковской системы должна обеспечивать достижение целей этой организации в условиях:

– штатного функционирования;

– возникновения локальных инцидентов и проблем информационной безопасности;

– возникновения широкомасштабных катастроф и аварий раз-личной природы, последствия которых имеют или могут иметь отношение к информационной безопасности организации.

На основании стандарта РК ISO/IEC 27031-2013 «Информационные технологии. Методы обеспечения безопасности» разработана методика оценки соответствия информационной безопасности, которая определяет показатели информационной безопасности, способы их оценивания и способы определения степени соответствия стандарту [30].

Отличительной особенностью данного подхода является учет каждого этапа цикла управления, в отличие от методов, осуществляющих непосредственную работу только по разделу «Выполнение». Таким образом, подсчет рисков слабо отличается от применяемого так называемого «заплаточного» метода. Только полностью осуществленный цикл управления, последующее его циклическое повторение с корректировкой, пересмотром рисков позволяет обеспечить информационную безопасность с помощью анализа рисков.

Проведенный анализ различных подходов к построению политики безопасности организации показывает, что центральное место при обеспечении режима информационной

безопасности занимает проблема анализа и управления информационными рисками. Установлено, что перечисленные стандарты в области информационной безопасности и принятые в различных организациях нормативные документы по обеспечению режима информационной безопасности имеют декларативный характер и не позволяют создать универсальную, единую для всех организаций методику управления рисками, в силу чего построение и реализация политик безопасности пока не стали во многих организациях нашей страны общей практикой. Вследствие этого необходимо рассмотреть существующие методы и программные средства анализа и управления рисками.

СПИСОК ЛИТЕРАТУРЫ

1 Астахов А. М. Искусство управления информационными рисками. М. : ДМК «Пресс», 2020. 312 с.

2 Бородушко И. В., Васильева Э. К. Стратегическое планирование и контроллинг: Теория и практика стратегического планирования на предприятии. СПб. : Питер, 2016. 192 с.

3 Завгородний В. И. Информационные риски и экономическая безопасность предприятия. М. : Финакадемия, 2018. 160 с.

4 Завгородний В. И. Информационные риски : сущность, концепция управления. М. : Экономика, 2017. 175 с.

5 Завгородний В. И. Управление информационными рисками предприятия. М. : ИНИОН РАН, 2019. 174 с.

6 Калашников А. О. Модели и методы организационного управления информационными рисками корпораций : монография. М. : Эгвес, 2021. 312 с.

7 Калашников А. О. Управление информационными рисками организационных систем: базовая модель // Системы управления и информационные технологии : научно-технический журнал. 2018. № 1.3(31). С. 366–371.

8 Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Управление рисками информационной безопасности : учеб. пособие для вузов. 2-е изд., испр. М. : Горячая линия-Телеком, 2021. 130 с.

9 Остапенко О. А. Методика оценки параметров риска с применением непрерывных распределений вероятности ущерба // Информация и безопасность. 2016. Т. 9, № 1. С. 55–58.

10 Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность. М. : Компания АйТи ; ДМК Пресс, 2021. 348 с.

11 Петренко С. А. Особенности организации защиты информации в корпоративных системах Internet/Intranet // Экспресс– электроника. 2001. № 12. С.50–83.

12 «Риск-контроллинг информационной и экономической безопасности : монография / Г. И. Золотарева, С. В. Филько, И. В. Филько, И. В. Федоренко. — Красноярск : СибГУ им. академика М. Ф. Решетнёва, 2018. — 192 с. — ISBN 978-5-86433-759-2

13 ISO/IEC 27031:2011 "Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса" (Information technology – Security techniques – Guidelines for information and communications technology readiness for business continuity). Библиотека нормативной документации https://files.stroyinf.ru/Index/55/55334.htm

14 СТ РК ISO/IEC 27031-2013 "Информационные технологии. Методы обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий для обеспечения непрерывности бизнеса". ИС «Юрист» https://online.zakon.kz/Document/?doc_id=36259376

15 ISO/IEC 15408-1:2009 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 1. Введение и общая модель" (Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model).

16 СТ РК ISO/IEC 15408-1-2017 "Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель".

17 ISO/IEC 15408-2:2008 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 2. Функциональные требования

безопасности" (Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components).

18 СТ РК ISO/IEC 15408-2-2017 "Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности".

19 ISO/IEC 15408-3:2008 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 3. Требования к обеспечению защиты" (Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components).

20 СТ РК ISO/IEC 15408-3-2017 "Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования обеспечению защиты".

21 Калашников А. О. Модели и методы организационногоуправления информационными рисками корпораций : монография.М. : Эгвес, 2021. 312 с.

22 Christopher, A., Audrey, D. (2002) Managing Information Security Risks: The OCTAVE Approach Addison-Wesley Professional, ISBN: 0-321-11886-3

23 Schmidt, M. Information security risk management terminology and key concepts. Risk Manag 25, 2 (2023). https://doi.org/10.1057/s41283-022-00108-8

24 Owusu Kwateng, K., Amanor, C. and Tetteh, F.K. (2022), "Enterprise risk management and information technology security in the financial sector", Information and Computer Security, Vol. 30 No. 3, pp. 422-451. https://doi.org/10.1108/ICS-11-2020-0185

25 Althonayan and A. Andronache, "Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management Alignment," 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Oxford, UK, 2019, pp. 1-9, doi: 10.1109/CyberSA.2019.8899445

26 Asamoah, D., Nuertey, D., Agyei-Owusu, B. and Acquah, I.N. (2022), "Antecedents and outcomes of supply chain security practices: the role of organizational security culture and supply chain disruption occurrence", International Journal of Quality & Reliability Management, Vol. 39 No. 4, pp. 1059-1082. https://doi.org/10.1108/IJQRM-01-2021-0002

27 Luo, Y. A general framework of digitization risks in international business. J Int Bus Stud 53, 344–361 (2022). https://doi.org/10.1057/s41267-021-00448-9

28 Lund, S., DC, W., & Manyika, J. (2020). Risk, resilience, and rebalancing in global value chains.

29 Nilo Legowo, Yoyo Juhartoyo. Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001. ISSN 1816-6075 (Print), 1818-0523 (Online). Journal of System and Management Sciences. Vol. 12 (2022) No. 3, pp. 181-199. DOI:10.33168/JSMS.2022.0310

30 Анализ и управление рисками в информационных системах на базе операционных систем Microsoft [Электронный ресурс] //Интуит: [сайт]. URL: http://www.intuit.ru/studies/courses/531/387/lecture/8996 (дата обращения: 26.12.2023).

REFERENCES

1 Astahov A. M. Iskusstvo upravlenija informacionnymi riskami. M. : DMK «Press», 2020. 312 s.

2 Borodushko I. V., Vasil'eva Je. K. Strategicheskoe planirovanie i kontrolling: Teorija i praktika strategicheskogo planirovanija na predprijatii. SPb. : Piter, 2020. 192 s.

3 Zavgorodnij V. I. Informacionnye riski i jekonomicheskaja bezopasnost' predprijatija. M. : Finakademija, 2018. 160 s.

4 Zavgorodnij V. I. Informacionnye riski : sushhnost', koncepcija upravlenija. M. : Jekonomika, 2017. 175 s.

5 Zavgorodnij V. I. Upravlenie informacionnymi riskami predprijatija. M. : INION RAN, 2019. 174 s.

6 Kalashnikov A. O. Modeli i metody organizacionnogo upravlenija informacionnymi riskami korporacij : monografija. M. : Jegves, 2021. 312 s.

7 Kalashnikov A. O. Upravlenie informacionnymi riskami organizacionnyh sistem: bazovaja model' // Sistemy upravlenija i informacionnye tehnologii : nauchno-tehnicheskij zhurnal. 2018. № 1.3(31). S. 366–371.

8 Miloslavskaja N. G., Senatorov M. Ju., Tolstoj A. I. Upravlenie riskami informacionnoj bezopasnosti : ucheb. posobie dlja vuzov. 2-e izd., ispr. M. : Gorjachaja linija-Telekom, 2023. 130 s.

9 Ostapenko O. A. Metodika ocenki parametrov riska s primeneniem nepreryvnyh raspredelenij verojatnosti ushherba // Informacija i bezopasnost'. 2016. T. 9, № 1. S. 55–58.

10 Petrenko S. A. Upravlenie informacionnymi riskami. Jekonomicheski opravdannaja bezopasnost'. M. : Kompanija AjTi ; DMK Press, 2014. 348 s.

11 Petrenko S. A. Osobennosti organizacii zashhity informacii v korporativnyh sistemah Internet/Intranet // Jekspress– jelektronika. 2021. № 12. S.50–83.

12 «Risk-kontrolling informacionnoj i jekonomicheskoj bezopasnosti : monografija / G. I. Zolotareva, S. V. Fil'ko, I. V. Fil'ko, I. V. Fedorenko. — Krasnojarsk : SibGU im. akademika M. F. Reshetnjova, 2018. — 192 s. — ISBN 978-5-86433-759-2

13 ISO/IEC 27031:2011 "Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Rukovodstvo po gotovnosti informacionno-kommunikacionnyh tehnologij k obespecheniju nepreryvnosti biznesa" (Information technology – Security techniques – Guidelines for information and communications technology readiness for business continuity). Biblioteka normativnoj dokumentacii https://files.stroyinf.ru/Index/55/55334.htm

14 ST RK ISO/IEC 27031-2013 "Informacionnye tehnologii. Metody obespechenija bezopasnosti. Rukovodstvo po gotovnosti informacionno-kommunikacionnyh tehnologij dlja obespechenija nepreryvnosti biznesa". IS «Jurist» https://online.zakon.kz/Document/?doc_id=36259376

15 ISO/IEC 15408-1:2009 "Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Kriterii ocenki bezopasnosti IT. Chast' 1. Vvedenie i obshhaja model'" (Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model).

16 ST RK ISO/IEC 15408-1-2017 "Informacionnye tehnologii. Metody i sredstva obespechenija bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tehnologij. Chast' 1. Vvedenie i obshhaja model'".

17 ISO/IEC 15408-2:2008 "Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Kriterii ocenki bezopasnosti IT. Chast' 2. Funkcional'nye trebovanija bezopasnosti" (Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components).

18 ST RK ISO/IEC 15408-2-2017 "Informacionnye tehnologii. Metody i sredstva obespechenija bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tehnologij. Chast' 2. Funkcional'nye trebovanija bezopasnosti".

19 ISO/IEC 15408-3:2008 "Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Kriterii ocenki bezopasnosti IT. Chast' 3. Trebovanija k obespecheniju zashhity" (Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components).

20 ST RK ISO/IEC 15408-3-2017 "Informacionnye tehnologii. Metody i sredstva obespechenija bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tehnologij. Chast' 3. Trebovanija obespecheniju zashhity".

21 Kalashnikov A. O. Modeli i metody organizacionnogoupravlenija informacionnymi riskami korporacij : monografija.M. : Jegves, 2021. 312 s.

22 Christopher, A., Audrey, D. (2002) Managing Information Security Risks: The OCTAVE Approach Addison-Wesley Professional, ISBN: 0-321-11886-3

23 Schmidt, M. Information security risk management terminology and key concepts. Risk Manag 25, 2 (2023). https://doi.org/10.1057/s41283-022-00108-8

24 Owusu Kwateng, K., Amanor, C. and Tetteh, F.K. (2022), "Enterprise risk management and information technology security in the financial sector", Information and Computer Security, Vol. 30 No. 3, pp. 422-451. https://doi.org/10.1108/ICS-11-2020-0185

25 Althonayan and A. Andronache, "Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management Alignment," 2019 International

Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Oxford, UK, 2019, pp. 1-9, doi: 10.1109/CyberSA.2019.8899445

26 Asamoah, D., Nuertey, D., Agyei-Owusu, B. and Acquah, I.N. (2022), "Antecedents and outcomes of supply chain security practices: the role of organizational security culture and supply chain disruption occurrence", International Journal of Quality & Reliability Management, Vol. 39 No. 4, pp. 1059-1082. https://doi.org/10.1108/IJQRM-01-2021-0002

27 Luo, Y. A general framework of digitization risks in international business. J Int Bus Stud 53, 344–361 (2022). https://doi.org/10.1057/s41267-021-00448-9

28 Lund, S., DC, W., & Manyika, J. (2020). Risk, resilience, and rebalancing in global value chains.

29 Nilo Legowo, Yoyo Juhartoyo. Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001. ISSN 1816-6075 (Print), 1818-0523 (Online). Journal of System and Management Sciences. Vol. 12 (2022) No. 3, pp. 181-199. DOI:10.33168/JSMS.2022.0310

30 Analiz i upravlenie riskami v informacionnyh sistemah na baze operacionnyh sistem Microsoft [Jelektronnyj resurs] //Intuit: [sajt]. URL: http://www.intuit.ru/studies/courses/531/387/lecture/8996 (data obrashhenija: 26.12.2023).

ТҮЙІН

Мақалада IBM, Sun Microsystems, Cisco Systems және Microsoft сияқты ірі әлемдік компанияларда олардың дамуын ескере отырып, ұйымдарда қауіпсіздік саясатын қалыптастырудың әртүрлі тәсілдері қарастырылады. IBM тәсілі ISO / IEC 17799 халықаралық стандартын қолдануға негізделген және ақпараттық тәуекелдерді анықтау, қауіпсіздік саясатын әзірлеу, төтенше жағдайлар стратегияларын әзірлеу және қалдық тәуекелдерді бағалау кезеңдерін қамтиды. Sun Microsystems ұйымның қауіпсіздік саясаты жобасын әзірлеуден бастап ақпараттық қауіпсіздік режимін сақтауға дейінгі Стратегиялық тәсілді қалайды. Cisco Systems желідегі тәуекелдерді бағалауға назар аударады және оқиғаларға жауап беру үшін арнайы жұмыс тобын құруды ұсынады. Майкрософт ақпараттық тәуекелдерді басқаруға негізделген және тәуекелдерді бағалауды, қауіпсіздік саясатын әзірлеуді, қорғаныс құралдарын енгізуді және қауіпсіздік аудитін қамтитын өз стратегиясын ұсынады. Бұл тәсілдер ұйымдардың қауіпсіздігін қамтамасыз етуде ақпараттық тәуекелдерді талдау мен басқарудың маңыздылығын көрсетеді.

УДК 338.43
МРНТИ 68.75.01

Рустенова Э.А., кандидат экономических наук, https://orcid.org/0000-0001-5542-4204
НАО «Западно-Казахстанский аграрно-технический университет имени Жангир хана», г. Уральск, ул. Жангир хана 51, 090009, Казахстан, elvira02@mail.ru

Rustenova E.A., candidate of economic sciences, https://orcid.org/0000-0001-5542-4204
NJSC «West Kazakhstan Agrarian and Technical University named after Zhangir khan», Uralsk, st. Zhangir khan 51, 090009, Kazakhstan, elvira02@mail.ru

ПЕРЕХОД К УСТОЙЧИВЫМ МОДЕЛЯМ ПОТРЕБЛЕНИЯ И ПРОИЗВОДСТВА: ОПЫТ И ПЕРСПЕКТИВЫ В КАЗАХСТАНЕ
TRANSITION TO SUSTAINABLE CONSUMPTION AND PRODUCTION PATTERNS: EXPERIENCE AND PROSPECTS IN KAZAKHSTAN

Аннотация

В настоящей статье рассматривается проблема перехода к рациональным моделям потребления и производства в контексте современных экологических вызовов. В работе представлены значительные шаги, предпринятые в Казахстане для решения этой проблемы, а также основные направления дальнейших действий. Особое внимание уделяется развитию