

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ВСЕРОССИЙСКАЯ ГРУППА ТЕОРИИ ИНФОРМАЦИИ IEEE
АКАДЕМИЯ ИНФОРМАТИЗАЦИИ ОБРАЗОВАНИЯ
ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ООО «ОТКРЫТЫЕ РЕШЕНИЯ»
ОБЩЕСТВО «ЗНАНИЕ» РОССИИ
ПРИВОЛЖСКИЙ ДОМ ЗНАНИЙ

*XXI Международная
научно-техническая конференция*

**ПРОБЛЕМЫ ИНФОРМАТИКИ
В ОБРАЗОВАНИИ, УПРАВЛЕНИИ,
ЭКОНОМИКЕ И ТЕХНИКЕ**

Сборник статей

Декабрь 2021 г.

Пенза

УДК 004
ББК 32.81я43+74.263.2+65.050.2я43
П781

П781 **ПРОБЛЕМЫ ИНФОРМАТИКИ В ОБРАЗОВАНИИ,
УПРАВЛЕНИИ, ЭКОНОМИКЕ И ТЕХНИКЕ :**
сборник статей XXI Международной научно-технической
конференции. – Пенза: Приволжский Дом знаний, 2021. – 284 с.

ISBN 978-5-8356-1776-0
ISSN 2311-0406

Под редакцией *В.И. Горбаченко*, доктора технических наук,
профессора;
В.В. Дроздина, кандидата технических наук,
профессора

Информация об опубликованных статьях предоставлена в систему Рос-
сийского индекса научного цитирования (РИНЦ) по договору
№ 573-03/2014К от 18.03.2014.

ISBN 978-5-8356-1776-0
ISSN 2311-0406

© Пензенский государственный
университет, 2021
© АННМО «Приволжский Дом знаний», 2021

*XXI International
scientific and technical conference*

**PROBLEMS OF INFORMATICS
IN EDUCATION, MANAGEMENT,
ECONOMICS AND TECHNICS**

December, 2021

Penza

Сафонов
Павел Павлович
Суркин
Михаил Юрьевич
Усманова
Ирина Викторовна
Филиал ВА МТО,
г. Пенза, Россия

Safonov P.P.
Surkin M.Yu.
Usmanova I.V.
Branch of the VAMTO,
Penza, Russia

УДК 004.056.5

ОЦЕНКА РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Г. В. Бобрышева

SECURITY RISK ASSESSMENT FOR INFORMATION RESOURCES

G. V. Bobrysheva

Аннотация. Обеспечение требуемого уровня безопасности информационных ресурсов, хранимых и обрабатываемых в информационно-вычислительном комплексе компании, напрямую зависит от эффективности управления рисками информационной безопасности и своевременности их оценки. Для оценки рисков информационной безопасности на всех этапах жизненного цикла управления рисками используют качественные и количественные методы.

Ключевые слова: информационная безопасность, информационный ресурс, угрозы, риски, управление рисками, оценка рисков

Abstract. Ensuring the required level of security of information resources stored and processed in the company's information and computing complex directly depends on the effectiveness of information security risk management and the timeliness of their assessment. To assess information security risks at all stages of the risk management life cycle, qualitative and quantitative methods are used.

Keywords: information security, information resource, threats, risks, risk management, risk assessment.

На сегодняшний день обеспечение безопасности информационных ресурсов является первостепенной задачей любой компании не зависимо от формы организационной структуры и направлений деятельности. При этом

актуальность данной задачи непрерывно возрастает, что обусловлено стремительным развитием вычислительной техники, информационных и коммуникационных технологий, а также непрерывно возрастающими требованиями к обеспечению конфиденциальности, целостности и надежности информационных ресурсов компаний, хранимых, обрабатываемых и передаваемых по компьютерным сетям.

Безопасность информационных ресурсов во многом определяется уровнем воздействия существующих рисков информационной безопасности на процессы организации хранения информационных ресурсов, их обработки и передачи. Даже несущественное снижение уровня информационной безопасности является недопустимым для любой компании, поскольку может привести к модификации, утрате, блокировке или переадресации коммерческой информации, вследствие чего может быть упущена экономическая или любая другая выгода.

Вопросами анализа и управления рисками информационной безопасности в компаниях занимаются, как правило, отдельные подразделения, в обязанности которых входит анализ потенциальных угроз информационной безопасности и ущерба от их появления, разработка концепции управления рисками реализации потенциальных угроз и управление информационной безопасностью с использованием современных методов и средств защиты информации.

Под потенциальной угрозой информационной безопасности понимают потенциальную причину возникновения инцидента, который может нанести какой-либо ущерб компании и, прежде всего, финансовый. Основной причиной наличия потенциальных угроз информационной безопасности является высокий уровень уязвимости информационно-вычислительного комплекса компании, который часто объясняется отсутствием сервисов безопасности или наличием недостатков в реализующих их защитных механизмах.

Факторы риска реализации потенциальных угроз информационной безопасности можно классифицировать по различным критериям и признакам, например, по степени влияния, характеру воздействия на риск, степени управляемости, источнику возникновения. Эффективность минимизации рисков информационной безопасности напрямую зависит от качества управления ими.

В настоящее время управление рисками информационной безопасности представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации. Поэтому в компаниях вопросу управления рисками необходимо уделять особое внимание.

Основная задача управления рисками – объективно идентифицировать и оценить наиболее значимые риски информационной безопасности, а также объективно оценить эффективность используемых средств контроля рисков и защиты информационных ресурсов компании.

Для эффективного управления рисками информационной безопасности используются специальные методики, разработанные ведущими организациями в области защиты информации и представленные как международными, так и национальными стандартами, наиболее популярными среди которых являются: AS/NZS 4360:2004, ГОСТ Р ИСО/МЭК 31010-2011, ГОСТ Р ИСО/МЭК 15408-1-2012, ГОСТ Р ИСО/МЭК 27002-2012, ГОСТ Р 51901.1-2002, NIST 800-30:2012, COSO ERM-2004 [1 – 7].

Управление рисками информационной безопасности включает в себя три вида деятельности, которые чередуются циклически (рисунок 1).



Рис. 1. Схема управления рисками

По отношению к выявленным рискам информационной безопасности возможны следующие действия:

- ликвидация риска информационной безопасности, например, за счет устранения причины;

- уменьшение риска информационной безопасности, например, за счет использования дополнительных средств защиты информации;

- принятие риска информационной безопасности и выработка плана действия в соответствующих условиях;

- переадресация риска информационной безопасности, например, путем заключения страхового соглашения.

Для оценки рисков информационной безопасности на всех этапах жизненного цикла управления рисками используют качественные и количественные методы [8].

Качественная оценка рисков информационной безопасности позволяет получить общие сведения об их уровне и подразумевает:

выявление рисков, присущих реализации предполагаемого решения;

определение количественной структуры рисков;

выявление наиболее рискоопасных областей в разработанном алгоритме принимаемого решения.

Основными результатами качественного анализа рисков являются:

выявленные риски и порождающие их причины;

стоимостной эквивалент гипотетических последствий возможной реализации отмеченных рисков;

предложения мероприятий по минимизации ущерба и их стоимостная оценка;

пограничные значения возможных изменений факторов рисков.

Проведение количественной оценки рисков информационной безопасности является продолжением качественного анализа и представляет собой численное определение величины рисков и ущерба от их проявления. При этом ущерб может носить прямой или косвенный характер, или представлять собой упущенную выгоду.

Для количественной оценки рисков информационной безопасности и возможного ущерба от их проявления используются специальные методы:

статистический метод, заключающийся в расчете вероятностей возникновения потерь от их проявления на основе анализа статистических данных результативности операций, проводимых компанией;

анализ целесообразности затрат, ориентированный на идентификацию потенциальных зон риска и заключающийся в расчете перерасхода затрат, которые могут быть вызваны определенными факторами или их комбинацией, основными среди которых являются первоначальная недооценка стоимости и увеличение первоначальной стоимости;

аналитические методы, позволяющие определить вероятность возникновения потерь на основе математических моделей, среди которых наиболее часто употребляемыми на практике являются такие, как анализ чувствительности, метод корректировки нормы дисконта с учетом риска, метод эквивалентов, метод сценариев;

метод экспертных оценок, который основан на обобщении мнений специалистов-экспертов о вероятностях риска и заключается в организованном сборе суждений и предположений экспертов о потенциальных рисках с последующей обработкой полученных ответов и формированием результатов для выработки управленческого решения;

метод аналогий, основанный на предположении, что при анализе рисков компании полезными могут оказаться данные о последствиях воздействия неблагоприятных факторов этих рисков на другие компании.

Однако использование только качественного или количественного метода оценки рисков не позволяет получить полную информацию о существующих рисках информационной безопасности и, соответственно, в полном объеме оценить ущерб от их проявления.

Поэтому на практике компании должны в полной мере осознавать актуальность и важность решения проблем информационной безопасности, иметь четкую концепцию ее решения, а для оценки рисков информационной безопасности применять комбинированную методологию, которая позволяет наиболее качественно выявить потенциальные угрозы информационной безопасности и оценить ущерб от их проявления. Кроме того, процесс оценки рисков информационной безопасности должен иметь непрерывный характер и сопровождаться обновлением или модернизацией используемых механизмов защиты информационных ресурсов.

Данный подход к решению проблем информационной безопасности позволит компаниям оперативно выявлять потенциальные риски, своевременно нейтрализовать их и, соответственно, обеспечить требуемый уровень безопасности информационных ресурсов, хранимых и обрабатываемых в ее информационно-вычислительном комплексе.

Библиографический список

1. AS/NZS 4360:2004. Risk Management Set. Дата введения: 31.08.2004. – URL: https://www.ucop.edu/enterprise-risk-management/_files/as_stdnds4360_2004.pdf (дата обращения: 21.10.2021)
2. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки рисков. Дата введения: 01.12.2012. – URL: <http://docs.cntd.ru/document/gost-r-iso-mek-31010-2011> (дата обращения: 19.10.2021)
3. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Взамен: ГОСТ Р ИСО/МЭК 15408-1-2008. Дата введения: 01.12.2013. – URL: <http://docs.cntd.ru/document/1200101777> (дата обращения: 24.10.2021)
4. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил

менеджмента информационной безопасности. Взамен: ГОСТ Р ИСО/МЭК 17799-2005. Дата введения: 01.01.2014. – URL: <http://docs.cntd.ru/document/1200103619> (дата обращения: 29.10.2021)

5. ГОСТ Р 51901.1-2002. Менеджмент риска. Анализ риска технологических систем (с поправкой) Дата введения: 01.09.2003. – URL: <http://docs.cntd.ru/document/1200030153> (дата обращения: 25.10.2021)

6. NIST 800-30. Guide for Conducting Risk Assessments. Дата введения: 01.09.2012/ – URL: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf> (дата обращения: 28.10.2021)

7. COSOERM. Управление рисками организаций. Интегрированная модель. Дата введения: 01.09. – URL: <https://www.dvbi.ru/risk-management/library/Token/ViewInfo/ItemId/5/Стандарт-управления-рисками-COSO-ERM-eng-rus> (дата обращения: 30.10.2021)

8. Количественная и качественная оценка рисков – URL: <https://studfiles.net/preview/3102588/page/4/> (дата обращения: 23.10.2021).

Бобрышева

Галина Владимировна

Пензенский государственный
университет,
г. Пенза, Россия

Bobrysheva G. V.

Penza State University,
Penza, Russia

УДК 004.3

АВТОМАТИЗАЦИЯ УЧЕТА ЭКСПЛУАТАЦИОННЫХ ДАННЫХ ПО ИЗДЕЛИЮ Р-142Т(ТО)

А.Г. Булатов, М.Ю. Суркин, И.В. Усманова

AUTOMATION OF OPERATIONAL DATA ACCOUNTING ACCORDING TO THE PRODUCT R-142T(TO)

A.G. Bulatov, M.Yu. Surkin, I.V. Usmanova

Аннотация. Обоснована актуальность разработки комплексной автоматизированной информационной системы, предназначенной для применения расчетами современных мобильных образцов вооружения. Рас-