Published in the Russian Federation
Sochi Journal of Economy
Has been issued since 2007.
ISSN: 2541-8114
2017, 11(2): 116-123

www.vestnik.sutr.ru

UDC 338.14 + 004.056

Security Risks of Infocommunication Systems in Commercial Enterprises

Vladlena S. Oladko [a, *]

[a] Financial University under the Government of the Russian Federation, Russian Federation

Abstract

Analysis of financial stability is part of company's financial analysis and economic security. Financial stability determines the long-term solvency and competitiveness of the enterprise. The article considers the problem of the negative impact of threats of a different nature on financial stability and the activities of a commercial enterprise. Information and infocommunication resources as objects of risk of a commercial enterprise are considered. The structure of the infocommunication system of the enterprise is analyzed, the main types of risks are identified. Identification of sources of risk was carried out and a chain of implementation of the security threat of a commercial enterprise was built. An approach is proposed to manage security risks and counter threats to the infocommunication system of a commercial enterprise.

Keywords: information security attack, threat, risk, enterprise, business process, financial stability, damage, economic security.

1. Введение

Стабильность положения коммерческого предприятия определяется его финансовой устойчивостью и возможностью обеспечивать непрерывность бизнес-процессов. Являясь характеристиками экономической безопасности и финансового состояния предприятия финансовая устойчивость [1] и непрерывность бизнеса характеризуется источниками финансирования деятельности, составом и структурой инфокоммуникационных систем предприятия, а также рисками, которые могут повлиять на стабильное состояние данных факторов. Находясь в «положительном» стабильном состоянии безопасности коммерческое предприятие является платежеспособным, конкурентоспособным и может реализовывать новые проекты без потери финансовой устойчивости.

Как показано в [2], внешняя среда в Российской Федерации характеризуется высокой изменчивостью и неопределённостью, что в свою очередь создает благоприятную почву для возникновения угроз и дестабилизирующих факторов различной природы и характера. Поэтому деятельность коммерческого предприятия сопровождается большим числом разнообразных рисков, которые влияют на результаты этой деятельности. Для предотвращения рисков или снижения тяжести их последствий, а также поддержания конкурентоспособности предприятия [3] необходимо проводить их своевременную идентификацию и внедрять комплекс мер по управлению рисками, причем управление рисками должно затрагивать не только экономические аспекты функционирования предприятия, но и его информационную и инфокоммуникационную составляющие.

* Корреспондирующий автор
Адреса электронной почты: oladko.vs@yandex.ru (V.S. Oladko)

2. Материалы и методы

Для написания статьи были использованы материалы научной, учебной литературы, законодательство Российской Федерации, статистические данные, собранные из печатных и электронных источников информации.

В качестве основных методов исследования при выполнении работы были использованы: метод описания, системного анализа, сравнения, аналогии и обобщения.

3. Обсуждение

Инфокоммуникационные технологии и системы коммерческого предприятия

Деятельность коммерческого предприятия связана с использованием информации самой разнообразной формы, ценности и типа доступа. Это может быть информация в электронном и бумажном виде, общедоступная информация и коммерческая тайна, персональные данные сотрудников и клиентов, информация для служебного пользования и др. Для хранения, обработки, передачи и применения данной информации в бизнес-процессах коммерческого предприятия используются инфокоммуникационные технологии и системы, которые также являются ресурсами предприятия и объектами риска.

Понятие инфокоммуникационные технологии включает информационные технологии (аппаратные и программные средства), телекоммуникационное оборудование (абонентское, сетевое) и телекоммуникационные услуги (услуги в телефонных сетях общего пользования, услуги в сети Интернет, услуги мобильной телефонной связи и т.п.)

В соответствии с источником [4], инфокоммуникационная сеть представляет собой сеть обмена разного вида сообщениями, интегрирующую в себе систему компьютеров, объединенных каналами передачи данных и информационно вычислительную сеть. Основное назначение - обеспечение эффективного предоставления различных информационно-вычислительных услуг пользователям сети посредством организации удобного и надежного доступа к ресурсам, распределенным в этой сети. Подавляющая часть услуг большинства сетей лежит в сфере информационного обслуживания, передачи данных и автоматизации бизнес-процессов предприятия. В частности, информационные системы, построенные на базе инфокоммуникационных сетей, обеспечивают эффективное выполнение следующих задач:

- хранение данных;
- обработка данных;
- организация доступа пользователей к данным;
- передача данных и результатов обработки данных пользователям.

Таким образом, инфокоммуникационная система (ИКС) - это совокупность телекоммуникационной сети, средств хранения и обработки информации, а также источников и потребителей информации.

В структуре ИКС (см. таблицу 1) можно выделить несколько доменов, на которых функционируют основные подсистемы ИКС.

Таблица 1. Структура и состав доменов инфокоммуникационной системы

Домены	Телекоммуникационная подсистема	Прикладные подсистемы и информационные ресурсы	Источники и потребители информации
Физический домен	Ресурсы сети связи, транспортная сеть, сеть коммутации, структурированная кабельная система	Серверы, накопители данных, носители информации, прикладное программное обеспечение, программно-аппаратные средства информационных служб, системное программное	Пользователи (абоненты и клиенты), технические средства прикладных систем пользователей: терминалы пользователей, сенсоры, сети, датчики

		обеспечение	
Информационный домен	Данные мониторинга сети, состояние трафика, сигналы	Базы данных, структуры данных, базы знаний, Web-ресурсы	Информационные модели источников и потребителей, трафик пользователей, сообщения

Выделенные подсистемы в рамках доменов ИКС являются объектами риска, который может быть информационным, операционным, финансовым, репутационным, стратегическим, рисками ликвидности и несоответствия. Управление рисками подразумевает выделение объектов потенциально подверженных риску, идентификацию источников риска, выявление причин их появления, оценку и сравнение риска, а также принятие мер, направленных на локализацию риска и его снижение.

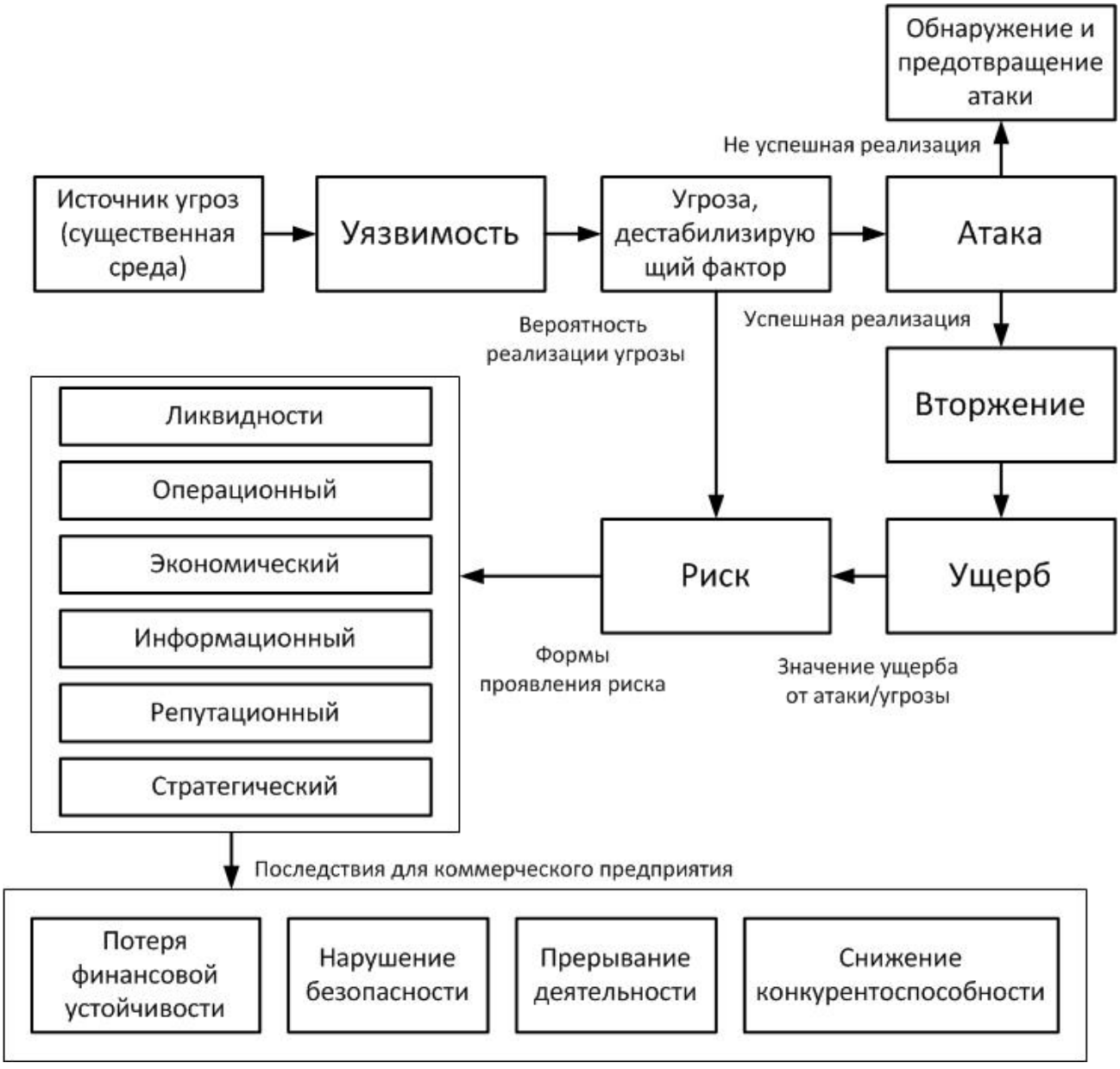

Рис. 1. Типовая цепочка реализации угрозы безопасности в инфокоммуникационной системе коммерческого предприятия

Причины возникновения рисков безопасности инфокоммуникационных систем

В процессе своего функционирования ИКС подвергается воздействию угроз ИБ и дестабилизирующих факторов. В соответствии ГОСТ Р 50922-2006 [4] угроза (безопасности информации) - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Для того что бы угроза могла быть реализована необходимо возникновение некоторого фактора способствующего ее реализации. В общем случае процесс нарушения безопасности в ИКС можно представить в виде следующей цепочки, представленной на рис. 1.

Анализ представленной выше цепочки показывает, что реализация угрозы невозможна без наличия источника потенциальной угрозы и уязвимости в ИКС или окружающей ее инфраструктуры. Уязвимость - это присущие ИКС причины, приводящие к нарушению безопасности информации и обусловленные недостатками процесса функционирования ИКС, свойствами архитектуры, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.

Источниками дестабилизирующих факторов и угроз безопасности вступает существенная среда [5], в которой функционирует ИКС, как правило, источники делятся на 3 типа: обусловленные действиями субъекта (антропогенные источники угроз), обусловленные техническими средствами (техногенные источники угрозы), обусловленные стихийными источниками. Данные источники могут порождать одну или несколько угроз безопасности и оказывать взаимное влияние друг на друга, создавая лавинный эффект и порождая риски стратегического, экономического, информационного и оперативного характера (см. рис. 2).

Рис. 2. Модель угроз безопасности в инфокоммуникационной системе коммерческого предприятия

По уровням организации ИКС угрозы можно разделить следующим образом (см. таблицу 2).

Таблица 2. Классификация угроз безопасности инфокоммуникационной системы предприятия

Уровень ИКС	Угрозы	Последствия
Прикладные подсистемы и информационные ресурсы	– ошибки конфигурирования системы; – отказы программного и аппаратного обеспечения; – разрушение данных; – модификация данных; – несанкционированное использование информационных ресурсов сети; – НСД к программам и данным. – вредоносное ПО	Недоступность информационных сервисов и данных, нарушение целостности и конфиденциальности информации
Телекоммуникационная подсистема	– выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала – разрушение или повреждение аппаратуры сети связи; – электромагнитная подсветка линий связи; – незаконное подключение к линиям связи; – дистанционное преодоление систем защиты; – ошибки в коммутации каналов; – нарушение работы линий связи и сетевого оборудования; – помехи и искажения в каналах связи; – кража сетевого оборудования	Недоступность информации, недоступность сетевых станций и сетевого оборудования, нарушение целостности информации, перехват данных, утечка информации
Источники и потребители информации, обслуживающий персонал, оператор связи	– невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т. п.); – утечка персональных данных пользователей – утечка конфиденциальной информации – невозможность работать с системой в силу отсутствия соответствующей подготовки – отрицание подлинности информации; – навязывание ложной информации. – Фишинг и мошенничество	Нарушение конфиденциальности информации, отказ в обслуживании

В случае своей успешной реализации данные угрозы могут нанести ущерб как пользователям – абонентам ИКС, так и собственникам ИКС и операторам связи. Ущерб может быть различен:

–моральный и материальный ущерб деловой репутации;

–моральный, физический или материальный ущерб, связанный с разглашением персональных данных абонетов;

–материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;

–материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;

–материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;

–моральный и материальный ущерб от дезорганизации деятельности организации собственника ИКС;

Для противодействия данным угрозам используются специализированные средства и механизмы защиты, стратегия использования которых регулируется принятой политикой безопасности ИКС, целью которой является снижение рисков и перекрытие актуальных угроз. В общем виде процесс оценки риска и выбора подсистем безопасности в ИКС можно представить в виде следующей последовательности действий, описанной схемой на рис. 3.

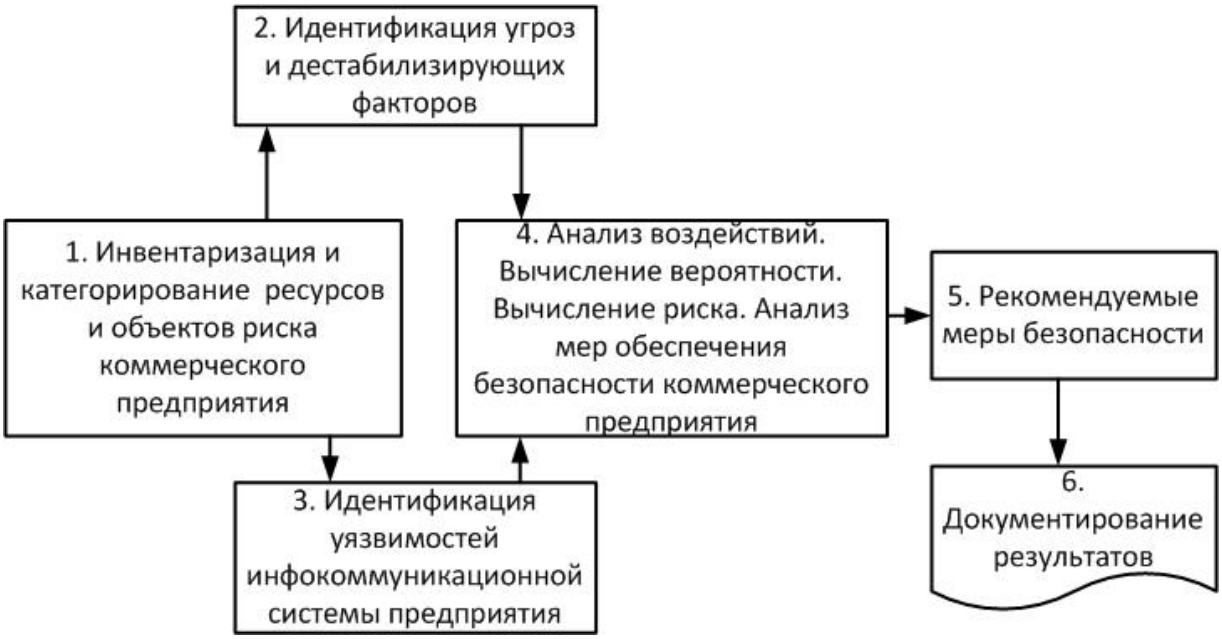

Рис. 3. Модель мер по управлению рисками коммерческого предприятия

В соответствии с ГОСТ Р 53110-2008 [6] в состав системы безопасности ИКС должны входить следующие подсистемы:

- Аутентификации и авторизации.
- Контроля доступа и защиты от НСД.
- Регистрации событий ИБ и аудита.
- Управления.
- Резервирования.

В рамках данных подсистем могут использоваться различные механизмы защиты, реализующие основные функции обеспечения безопасности ИКС коммерческого предприятия от угроз безопасности различной природы и характера. Блокирование и своевременное обнаружение угроз, приводит контролю над рисками, что в свою очередь благоприятно сказывается на финансовой устойчивости и конкурентоспособности коммерческого предприятия.

4. Выводы

Успешное существование современного коммерческого предприятия зависит от множества факторов, среди которых не последние позиции занимает управление рисками безопасности инфокоммуникационной системы. Поэтому для контроля и предотвращения различных видов экономического ущерба, обеспечения финансовой устойчивости и экономической безопасности коммерческого предприятия необходимо своевременно и регулярно идентифицировать риски и принимать адекватные текущей ситуации управляющие решения.

Литература

1. Данилова Н.Л. Сущность и проблемы анализа финансовой устойчивости коммерческого предприятия//Концепт. 2014. №02. С. 1-8. [Электронный ресурс]. URL:

https://cyberleninka.ru/article/v/suschnost-i-problemy-analiza-finansovoy-ustoychivosti-kommercheskogo-predpriyatiya (дата обращения 10.08.2017).

2. Егоренков Г.А. Совершенствование системы управления рисками коммерческого предприятия на основе процессного и системного подходов // Вестник Череповецкого государственного университета .2010. №2. С. 70-74.

3. Nikishova A.V., Oladko V.S. Information protection system as a tool to maintain the competitiveness of enterprises // Sochi journal of Economy. 2017. №1 (11). С.17-28.

4. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения // Электронный фонд правовой и нормативно-технической документации Техэксперт. [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200058320/ (дата обращения 10.08.2017).

5. Аткина В.С. Применение карты рисков для оценки деструктивного воздействия существенной среды на информационную систему // Безопасность информационных технологий. 2013. № 4. С. 21-26.

6. ГОСТ Р 53110-2008 Система обеспечения информационной безопасности сети связи общего пользования. Общие положения // Электронный фонд правовой и нормативно-технической документации Техэксперт. [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200073586 (дата обращения 10.08.2017).

References

1. Danilova N.L. Sushchnost' i problemy analiza finansovoi ustoichivosti kommercheskogo predpriyatiya//Kontsept. 2014. №02. S. 1-8. [Elektronnyi resurs]. URL: https://cyberleninka.ru/article/v/suschnost-i-problemy-analiza-finansovoy-ustoychivosti-kommercheskogo-predpriyatiya (data obrashcheniya 10.08.2017).

2. Egorenkov G.A. Sovershenstvovanie sistemy upravleniya riskami kommercheskogo predpriyatiya na osnove protsessnogo i sistemnogo podkhodov // Vestnik Cherepovetskogo gosudarstvennogo universiteta .2010. №2. S. 70-74.

3. Nikishova A.V., Oladko V.S. Information protection system as a tool to maintain the competitiveness of enterprises // Sochi journal of Economy. 2017. №1 (11). S.17-28.

4. GOST R 50922-2006 Zashchita informatsii. Osnovnye terminy i opredeleniya // Elektronnyi fond pravovoi i normativno-tekhnicheskoi dokumentatsii Tekhekspert. [Elektronnyi resurs]. URL: http://docs.cntd.ru/document/1200058320/ (data obrashcheniya 10.08.2017).

5. Atkina V.S. Primenenie karty riskov dlya otsenki destruktivnogo vozdeistviya sushchestvennoi sredy na informatsionnuyu sistemu // Bezopasnost' informatsionnykh tekhnologii. 2013. № 4. S. 21-26.

6. GOST R 53110-2008 Sistema obespecheniya informatsionnoi bezopasnosti seti svyazi obshchego pol'zovaniya. Obshchie polozheniya // Elektronnyi fond pravovoi i normativno-tekhnicheskoi dokumentatsii Tekhekspert. [Elektronnyi resurs]. URL: http://docs.cntd.ru/document/1200073586 (data obrashcheniya 10.08.2017).

УДК 338.14 + 004.056

Риски нарушения безопасности инфокоммуникационных систем коммерческих предприятий

Владлена Сергеевна Оладько [a, *]

[a] Финансовый университет при Правительстве Российской Федерации, Российская Федерация

Аннотация. Анализ финансовой устойчивости является частью анализа финансового состояния и экономической безопасности предприятия. Финансовая устойчивость определяет долгосрочную платежеспособность и конкурентоспособность предприятия. Статья затрагивает проблему негативного влияния угроз различного характера на

[*] Corresponding author
E-mail addresses: oladko.vs@yandex.ru (В.С. Оладько)

финансовую устойчивость и деятельность коммерческого предприятия. Рассмотрены информационные и инфокоммуникационные ресурсы как объекты риска коммерческого предприятия. Проанализирована структура инфокоммуникационной системы предприятия, выделены основные виды рисков. Проведена идентификация источников риска и построена цепочка реализации угрозы безопасности коммерческого предприятия. Предложен подход к управлению рисками безопасности и противодействию угрозам инфокоммуникационной системы коммерческого предприятия.

Ключевые слова: защита информации, атака, угроза, риск, предприятие, бизнес-процесс, ущерб, финансовая устойчивость, экономическая безопасность.