ИННОВАЦИИ НА ФИНАНСОВОМ РЫНКЕ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Ашимбаев Т.А. Email: Ashimbayev637@scientifictext.ru

Ашимбаев Толенди Арипбаевич — магистр экономических наук, докторант PhD,
кафедра экономики,
Бишкекская финансово-экономическая академия, г. Бишкек, Кыргызская Республика

Аннотация: целью исследования является определение современных тенденций развития инноваций на финансовых рынках в условиях информатизации и интернетизации. Результаты исследования отражают особенности информационной безопасности финансовых институтов в эпоху инноваций. В статье очень подробно исследуются предпосылки возникновения финансовых инноваций, экономическая сущность и виды инноваций на финансовом рынке, рассматривается финансовый рынок как среда реализации инноваций и производится оценка влияния финансовых инноваций на экономику страны. Другими словами, хозяйствующие субъекты имеют набор инструментов и возможность выбора путей развития, адаптация которых к условиям может принести несомненную пользу отечественной экономике.

Ключевые слова: инновационная деятельность, инновация, информационные технологии, конкуренция, финансовый рынок, экономика.

INNOVATION ON THE FINANCIAL MARKET AND THE INTERNET SECURITY Ashimbayev T.A.

Ashimbayev Tolendi Aripbayevich — Master in Economics, PhD Candidate,
DEPARTMENT OF ECONOMICS,
BISHKEK ECONOMIC AND FINANCIAL ACADEMY, BISHKEK, REPUBLIC OF KYRGYZSTAN

Abstract: the purpose of the study is to identify current trends in the development of innovations in financial markets in the context of information and Internetization. The results of the research reflect the information security features of financial institutions in the era of innovation. In the article, the prerequisites for the emergence of financial innovations, the economic essence and types of innovations in the financial market are studied in great detail, the financial market is considered as an environment for the implementation of innovations and the impact of financial innovations on the economy of the country is assessed. In other words, business entities have a set of tools and the opportunity to choose development paths whose adaptation to the conditions can bring undoubted benefits to the domestic economy.

Keywords: innovation activity, innovation, information technology, competition, financial market, economy.

УДК 2964

Развитие финансового рынка на современном этапе связано с использованием новых информационных технологий, а также с документацией, отчетностью, стратегией и процессами, осуществляемыми с помощью компьютерной техники и интернета. В последнее время можно говорить о возникновении нового явления в жизнедеятельности практически всех стран и людей, такого как «интернетизация», а также, перефразируя известное изречение, можно сказать, что «интернетизация всего мира продолжается». Особенно чувствуется влияние компьютеризации и интернетизации на финансовом рынке, где все инновации в сфере информатизации внедряются и используются в первую очередь, благодаря возможностям и потребностям финансовых институтов.

Комплексная система автоматизации обеспечивает ведение оперативного, финансового и управленческого учета и строится на основе единого информационного пространства, охватывая и координируя всю совокупность бизнес-процессов предприятия. В литературе и проспектах эти системы часто так и называются – корпоративная информационная система (КИС). Предполагается, что корпоративная информационная система объединит подразделения предприятия в единое информационное пространство и обеспечит комплексную автоматизацию управления предприятием.

Информация, имеющаяся в финансовых институтах, является объектом интереса конкурентов и промышленного шпионажа, что вызывает необходимость в защите и сохранности, как носителей, так и самой информации. Эффективность информационных систем и целесообразность затрат на их создание во многом зависят от уровня безопасности, который они обеспечивают от несанкционированного копирования и хищения.

Финансовая отчетность является основой информационного обеспечения деятельности компании, поэтому она представляет интерес для конкурентов или стартапов в этой отрасли, которые могут построить бизнес, ориентируясь на показатели успешной фирмы и мировые бренды.

Требования последних лет по части компьютеризации и автоматизации учета и отчетности затрагивают не только учетные и отчетные данные, но также аудит и анализ этих показателей. Практически повсеместно используются компьютерная техника, приложения и приспособления для ведения учета, составления финансовой отчетности, проведения экономического анализа и аудита. Данные сохраняются в компьютерах и в последнее время именно они становятся объектами хакерских атак и кибер-преступлений [1].

Инновации в среде программного обеспечения могут относиться как к технике и технологии, так и к формам организации производства и управления. Компьютерная технология характеризуется рядом особенностей, которые следует учитывать при оценке условий и процедур контроля. Современный этап характеризуется созданием новой компьютерной информационной технологии на базе децентрализованной обработки бухгалтерских задач.

Расширение технических возможностей делает информацию более доступной для широкого круга пользователей, при этом информационный поток не успевают освоить массы потребителей, которые практически стали игнорировать большую часть поступающей информации как спам, особенно поступающую от продавцов и производителей. Навязчивый сервис и агрессивная реклама пропускается через фильтры, потому что она может содержать вирусы, которые, в свою очередь, нацелены на хищение или уничтожение информации.

Развитие бизнеса, удержание и расширение доли на рынке все в большей степени связываются с использованием новых информационных технологий. Все больший объем информации создается, обращается, обрабатывается и накапливается исключительно в электронном виде. Это относится практически ко всей платежной информации и отчетности предприятий.

Прежде всего, необходимо ясно осознать, что в информационном пространстве уже сформировались основные группы участников, сложились свои специфические законы и обычаи. Кроме этого, желательно по возможности четко определить, что же организация должна оберегать, применяя современные информационные технологии в бизнес-процессах.

Говоря о защищаемых ресурсах, прежде всего, следует отметить персонал, как наиболее ценный и уязвимый ресурс одновременно. В организациях к этому необходимо добавить работоспособность системы, денежные средства, платежную информацию, корпоративные базы данных.

Информационная безопасность напрямую связана с экономической и национальной безопасностью страны, так как приход иностранных компаний в экономику приносит новые инвестиции и технологии, но чревато промышленным и интеллектуальным шпионажем, отслеживанием информации, причем в различных аспектах жизни, начиная с бизнеса и заканчивая религией и политикой.

История современной шпиономании описана в Отчете компании Check Point по информационной безопасности за 2014 год, в котором говорится, что более двадцати пяти лет назад, администратор UNIX, расследуя 75-центовую ошибку в счете, напал на след шпионской сети Восточного Блока, пытавшейся украсть секреты правительства и вооруженных сил США [2, с. 7]. Эта история описана в книге «Яйцо кукушки» и демонстрирует кибер-проникновение на уровне секретных служб тогдашнего СССР и США, которое в настоящее время перешло в повседневную жизнь миллиардов людей, пользующихся услугами банков, интернет-торговли, являющихся держателями пластиковых карт и интернет-банкинга.

К категории наиболее распространенных кибер-преступлений 2000-х годов можно отнести целенаправленные атаки на данные банков или других финансовых институтов и крупных фирм, которые располагают крупными финансовыми средствами. Эти данные могут быть похищены через интернет или путем взлома кодов по счетам и через обслуживающие банки. Компания Check Point, проводившая исследования в этой области, представила динамику развития вредоносных программных обеспечений (ПО), начиная с 1997 по 2014 годы, которые диверсифицируются и модифицируются вместе с развитием информационных технологий (таблица 1).

Таблица 1. Тенденции вредоносного программного обеспечения (ПО) [1, с. 6]

				Вымогающее ПО
				Хактивизм
				APT нового поколения (массовые инструментарии APT)
				Использование инфраструктуры Web (DNS)
				Промышленный шпионаж, спонсированный государством
Вирусы	Черви	Рекламное и Шпионское ПО	DDoS APTs	
1997	2004	2007	2010	2014

В 2014 году компания Check Point проанализировала данные по 9240 организациям со всего мира, в результате которого были получены следующие данные по угрозам информационной безопасности (ИБ), представленные в таблицах 2 и 3:

Таблица 2. География распространения вредоносного программного обеспечения (ПО) [2, с. 6]

Americas	Europe. Middle East and Africa (EMEA)	Asia Pacific and Japan (APAC)
24%	47%	29%

При этом, географически виды вредоносных ПО практически одинаковые, так, например, наиболее распространенными на всех континентах являются:

- Anonymizers: Tor – Ultrasurf – Hotspot Shield;
- P2P File Sharing: BitTorrent Protocol – Soulseek – Box Cloud;
- File Storage and Sharing: Dropbox – Windows Live Office – Hightail (formerly YouSendit);
- Remote Administration: RDP – LogMeln – TeamViewer.

В 2013 году были обнаружены новые модификации вредоносного ПО под названием «HIMAN», которые не были замечены прокси-системами вследствие использования сложной комбинации технологий и представляли собой систему направленных атак на информацию компаний.

Таблица 3. Распространение вредоносного программного обеспечения (ПО) по отраслям [3, с. 7]

Консалтинг	Телекомм уникации	Правительств о	Финансы	Другие отрасли	Промышленност ь
1%	4%	12%	15%	22%	46%

Дальнейшие исследования в этой области продемонстрировали резкое увеличение количества нового вредоносного ПО в 2013 году по сравнению с предыдущими годами (таблица 4), что вызвано глобальным ухудшением экономической ситуации, повлекшей увеличение количества хищений информации или ценностей:

Таблица 4. Динамика количества обнаруженных вредоносных ПО за 2009 - 2013 годы

2009	2010	2011	2012	2013
12,000,000	18,000,000	18,500,000	34,000,000	83,000,000
Источник: AV-Test.org [2]				

В связи с резким увеличением атак вредоносных ПО в 2013 году были изданы стандарты по защите данных отрасли Payment Card Industry Data Security Standards 3.2 (PCI-DSS 3.2), в соответствии с которыми рекомендуется [3]:

- усилить требования практики защиты систем не для конечных пользователей (Point-of-sale POS-терминал);
- повышать информированность пользователей в вопросах возможных атак, таких как фишинг, USB, особенно при работе с конфиденциальной информацией;
- осуществлять систематические проверки контроля и защиты с сегментацией данных держателей карт и другими частями сети;
- особое внимание уделять учетным данным, используемым сервис-провайдерами для удаленного доступа к средам клиентов по PCI-DSS.

В это же время в 2014 году в рамках Европейского союза была введена новая директива по персональным данным Общие правила защиты данных (General Data Protection Regulation, GDPR), в соответствии с которой компании должны привести свои политики в области защиты и обеспечения информационной безопасности и предотвращать утечки информации. Основные направления обеспечения защиты данных предусматривают следующие шаги [4]:

- классификация данных;
- участие пользователей в исправлении;
- защита от потери данных внутри компании;
- защита данных на жестких дисках конечных точек сети;
- защита данных на съемных носителях;
- защита документов;
- управление событиями.

При этом средства защиты вписываются в архитектуру Программной защиты (Software Defined Protection, SDP) с выделением трех уровней [5]:

1. Уровень применения (Enforcement Layer) требует надежности, быстродействия и простоты;
2. Уровень контроля (Control Layer) должен использоваться для контроля доступа к приложениям с высокой степенью риска, таким как анонимайзеры, одноранговые сети, сервисы хранения файлов и приложения для удаленного администрирования;

3. Уровень управления (Management Layer) должен иметь модульность, автоматизацию и прозрачность.

Обеспечение информационной безопасности становится актуальным в последнее время в связи с ухудшением экономической ситуации, что влечет за собой рост хищений и мошеннических схем, которым подвергаются, в первую очередь, материальные и нематериальные ценности, а, значит, финансовые структуры и бухгалтерские службы. В этой связи может усиливаться роль страхования от возможных рисков, которые практикуют страховые компании ведущих стран. Казахстанские страховые организации могут, перенимая опыт экономически развитых стран, внедрять новые продукты в виде страхования от утечки или хищения информации. Транснациональные страховые компании имеют мощный разведывательный аппарат в своем штате, который отслеживает новые тенденции и способствует созданию новых страховых продуктов.

Также применим принцип сепарации от внешнего мира и установку фильтров на сервере для финансовой и бухгалтерской служб, хотя иногда целью хищения могут стать и продукция, технологии, то есть любые инновации, которые можно реализовать на первых порах по завышенной стоимости. Так, многие компании-производители не гнушаются похищать новые модели одежды, обуви, автомобилей, интерьера и так далее.

Таблица 5. Популярные векторы атак (% от числа организаций)

№№	Наименование проникновения или атаки	%%
1.	Исполнение кода	51
2.	Повреждение памяти	47
3.	Переполнение буфера	36
4.	Отказ в обслуживании	23
5.	Раскрытие информации	16
6.	Переполнение целочисленной переменной	12
7.	Обход аутентификации	9
8.	Грубая сила	2
9.	Переполнение стека	2
10.	Эскалация Привилегий	1
11.	Подмена регистрации	0,2
Источник: Check Point software Technologies [5]		

Сам процесс проникновения вредоносных ПО также может осуществляться через внешние сети, когда сервера сканируются по портам и сервисам извне или со стороны скомпрометированного внутреннего клиента и затем становятся целями атак по конкретным версиям работающих на них приложений или операционных систем. Это так называемые удаленные атаки, которые приводят к контролю над системой (таблица 2).

Таким образом, проблема информационной безопасности является первостепенной на уровне правительств, международных и транснациональных организаций, финансовых и промышленных компаний. Обеспечение безопасности в определенной степени зависит от человеческого фактора: забывчивость, невнимательность к деталям, оставление открытых файлов, документов, почты и так далее.

В конце 80-х г. XX в. Институт программной инженерии США (Software Engineering Institute, SEI) выпустил документ «Модель зрелости. Пять уровней зрелости процесса создания программного обеспечения» (Capability Maturity Model, CMM) [6], который оказал огромное влияние на решение вопросов, связанных с качеством информационных систем. Разработанная SEI модель CMM уже много лет с успехом применяется Международной организацией по стандартизации ISO для создания международных стандартов [7]. Используя подход CMM, можно классифицировать этапы развития и существования компании в зависимости от того, как она обрабатывает и использует информацию в процессе своей деятельности, и проанализировать возможность применения тех или иных информационных технологий.

Завершая тему источников угроз, необходимо отметить, что наибольшую опасность несут в себе организованные группы злоумышленников, которые включают внешних и внутренних нарушителей, действующих согласованно. Серьезность возникающих угроз, значительные материальные потери обусловили принятие на уровне государств самых разнообразных мер, направленных на борьбу с киберпреступлениями, стимулирование работ по обеспечению информационной безопасности. В большинстве стран приняты соответствующие законодательные акты, созданы специальные подразделения в правоохранительных органах.

Механизм обеспечения информационной безопасности на уровне организации предполагает повышение общего уровня компьютерной культуры всех пользователей, осознание ими остроты существующих проблем в области информационной безопасности являются важными условиями успешности усилий в борьбе со злоумышленниками.

Безусловно, одними лозунгами и пропагандистскими лекциями достичь необходимого уровня защищенности ресурсов невозможно. Также нельзя полностью полагаться только на эффективность технических средств. В качестве характерного примера можно привести антивирусную защиту. Несмотря на прилагаемые усилия в изучении современных, в том числе эвристических, методов борьбы с вредоносными программами, пока рано говорить о создании действительно эффективных упреждающих антивирусных программ. По-прежнему многое зависит от своевременности обновлений, выбора правильного соотношения между вероятностями ложной тревоги и пропуска вредоносного кода.

Желаемого эффекта можно добиться только за счет оптимального сочетания технических и организационных мер. В данном контексте к техническим мерам отнесем программные и аппаратные средства, а к организационным – комплекс нормативных и организационно-распорядительных документов, регламентирующих действия всех участников создания, обработки, хранения и уничтожения информации.

В настоящее время рынок предлагает большое число различных решений в области антивирусной защиты, контроля доступа и пр. По мере развития информационной системы, существенного увеличения числа пользователей и объемов обрабатываемой информации усложняются и проблемы построения согласованной системы информационной безопасности. Приходится менять привычные представления об объектах защиты. Например, зачастую бывает непросто определить сам периметр защищаемого объекта. Учитывая наличие многочисленных связей между вашей информационной системой и внешними информационными системами, возникает вопрос о разделении зон ответственности.

Помимо киберпреступлений, защита информации необходима для поиска данных за прошедшие периоды, особенно по налоговым отчислениям, работе персонала, переводам денежных средств и другим, которые могут быть востребованы по истечении нескольких лет. Для сохранения и обеспечения безопасности конфиденциальной и отчетной информации ИТ-компании предлагают резервное копирование и архивирование с системой возврата и поиска бэкап (back-up) и бэкэнд (back-end) с возможностью расширения. При этом также немаловажно расширение и надстройку производить для аналогичных систем и серверов с максимальным временным разрывом 2-3 года, а также для различных конфигураций по-разному. Основными задачами управления безопасностью информации являются [8]:

- Консолидация инфраструктуры защиты данных;
- Повышение масштабируемости без миграции данных;
- Использование возможностей распределенной архитектуры для интерфейсных и серверных процессорных узлов;
- Обеспечение катастрофоустойчивости информационных систем и так далее.

Это связано с тем, что не только в нынешних кризисных условиях, но и в периоды экономического подъема, стратегия расширения усилий по обеспечению информационной безопасности не может обеспечиваться экстенсивным подходом.

Достижение более высокого уровня масштабирования возможно следующими путями:

- Применением двойной избыточности (шасси), при котором дублирование происходит на случай отказа одного узла (контроллера) или двух дисков;
- N-кратная отказоустойчивость, например, горизонтальное масштабирование при отказе нескольких узлов или дисков.

Катастрофоустойчивость также является актуальной проблемой, в связи с возможностью природных, техногенных, политических и экономических катастроф. Обеспечение катастрофоустойчивости предлагается ИТ-компаниями в следующими методами:

- Создание удаленной ленты;
- Синхронное зеркалирование;
- Асинхронная репликация на большие расстояния.

До настоящего времени не найден ценовой паритет между затратами на создание системы информационной безопасности и реальными угрозами потери данных. ИТ-специалисты, даже высококвалифицированные, не владеют данными по финансовым потерям или упущенной выгоде при использовании той или иной компьютерной техники и технологиям. Не отработан механизм списания компьютерной техники и программных продуктов, срок использования которых не имеет четких параметров, что немаловажно для определения морального износа и отнесения амортизации на расходы.

Определение уровня опасности и принятие защитных мер в некоторых случаях, например для малого и среднего бизнеса, не оправдан, ни с экономической, ни с организационной точки зрения. Тем более что существует существенная нехватка специалистов в области информационной безопасности. Единственный приемлемый путь выхода из этой ситуации – автоматизация реализуемых

подразделениями информационной безопасности процессов, построение автоматизированной системы управления информационной безопасностью.

Для предотвращения утечки информации и всех имеющихся данных применяются системы защиты, которые разрабатываются ИТ-фирмами в соответствии с изменениями на информационном пространстве. Последние разработки облачных технологий упрощают многие возможности хранения, однако до конца неизвестны последствия заоблачного хранилища.

Список литературы / References

1. Правила размещения электронных информационных ресурсов на Интернет-ресурсах государственных органов. Утверждены постановлением Правительства Республики Казахстан от 13 июля 2007 года № 598.
2. Check Point software technologies LTD. We secure the Internet. Отчет компании Check Point по информационной безопасности за 2014 год / U.S. Headquarters, 2014. 73 с.
3. Payment Card Industry Data Security Standards 3.2 (PCI-DSS 3.2) // [Электронный ресурс]. Режим доступа: https://www.pcisecuritystandards.org/document_library, 2016./ (дата обращения: 31.01.2018).
4. Check Point // [Электронный ресурс]. Режим доступа: <https://www.checkpoint.com/threatcloud-central/downloads/check-point-himan-malware-analysis.pdf/> (дата обращения: 31.01.2018).
5. Securitystandards // [Электронный ресурс]. Режим доступа: https://www.pcisecuritystandards.org/documents/DSS_and_PA_DSS_Change_Highlights.pdf/ (дата обращения: 31.01.2018).
6. Модель зрелости. Пять уровней зрелости процесса создания программного обеспечения. / Пер. с англ. М.: МО, 1995.
7. Королев Д.В. Роль стандарта ISO 9001:2000 в повышении эффективности деятельности современной организации. // Юрист, 2005. № 12.
8. Материалы конференции Fujitsu. Алматы, 2016 // [Электронный ресурс]. Режим доступа: www.fujitsu.com/ (дата обращения: 31.01.2018).