DOI:10.26104/IVK.2019.45

ИЗВЕСТИЯ ВУЗОВ КЫРГЫЗСТАНА, № 12, 2019

Тамакчи А.С.

САНАРИПТИК ЭКОНОМИКАНЫН ТҮПТӨЛҮҮ ШАРТЫНДА ЭКОНОМИКАЛЫК КООПСУЗДУКТУ КАМСЫЗ КЫЛУУ КАРАЖАТТАРЫН ӨНҮКТҮРҮҮ

Тамакчи А.С.

РАЗВИТИЕ ИНСТРУМЕНТОВ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ СТАНОВЛЕНИЕ ЦИФРОВОЙ ЭКОНОМИКИ

A.S. Tamakchi

DEVELOPMENT OF SOFTWARE TOOLS ECONOMIC SECURITY IN THE CONTEXT OF THE FORMATION OF THE DIGITAL ECONOMY

УДК: 338

Бүгүн жаңы санариптик технологиялар, инновациялык бизнес-моделдер коомдун жашоосунун бардык чөйрөсүнө кирди. Аны менен ал элдин жашоо шартынын экономикалык маңызын жана сапаттык түзүмүн өзгөрттү. Санариптик экономиканын калыптанышы чоң маалыматтардын системасы менен объективдүү байланышкан. Бүгүнкү күндө маалыматтардын сапаты микро жана макродеңгээлде да ар кандай бизнес-процесстин эффективдүүлүгүнүн маселесин чечет. Чынында санариптик экономика болжолдонгон экономиканын модели болуп саналат, маселе катары жыргалчылыктын өндүрүшүн индивидуалдаштыруу коюлган.

Негизги сөздөр: *санариптик экономика, чакырыктар, коркунучтар, өнүктүрүү стратегиясы, тобокелдиктер, акылдуу өсүш, персонификациялоо, чоң маалыматтар, проекративдик өнүктүрүү, долбоор-менеджмент.*

Становление цифровой экономики объективно связано с системой больших данных. Сегодня, как никогда раньше, количество и качество информации решает вопрос эффективности любого бизнес-процесса, как на микро-, так и на макроуровне. Фактически цифровая экономика – это модель прогностической экономики, где в качестве краеугольного камня поставлена индивидуализация производства благ. Сам способ генерации экономической добавленной стоимости зависит от умения менеджмента бизнеса слышать своих клиентов, проективно развивая диалог в формате взаимовыгодного сотрудничества путем инкорпорации бизнеса в жизнь своих стейкхолдеров.

Ключевые слова*: цифровая экономика, вызовы, угрозы, стратегия развития, риски, умный рост, персонификация, большие данные, проективное развитие, проектный менеджмент.*

The emergence of the digital economy is objectively connected with the big data system. Today, more than ever before, the quantity and quality of information solves the question of the effectiveness of any business process, both at the micro and macro levels. In fact, the digital economy is a model of a predictive economy, where the individualization of the production of goods is set as the cornerstone. The very way of generating economic value added depends on the ability of business management to hear their customers, proactively developing dialogue in the format of mutually beneficial cooperation by incorporating business into the life of their stakeholders

Key words: *digital economy, challenges, threats, development strategy, risks, smart growth, personification, big data, proactive development, project management.*

Введение. Современный этап развития технической мысли человечества кардинально отличается от ранее существующих бизнес-моделей: именно в цифровой экономике основным постулатом является информационные технологии как особый комплекс нематериальных активов, определяющий траекторию развития как отдельного бизнеса, так и национальной экономики в целом.

Результаты исследований. За два десятилетия XXI века информация и технологии приобрели математически выраженную экспоненциальную форму роста, что обусловило колоссальный рост агентских отношений между гражданами и коммерческими, некоммерческими и государственными институциональными структурами. Если ранее такое взаимодействие носило преимущественно линейный характер по принципу «запрос - рассмотрение - решение», то сегодня модель коллаборации становится принципиально иной: «запрос - совместное рассмотрение –

DOI:10.26104/IVK.2019.45

оценка орбитального влияния на сопряженных стейкхолдеров - тестирование жизнеспособности решения - решение - обновление версии решения по истечению времени». При этом современный стейкхолдер ожидает не просто типового решения, а индивидуального подхода с предоставлением ему пакетного решения проблемы, что соответственно требует создания качественного массива данных с установлением режима регулярного обновления и актуализации.

Именно вопрос коммерциализации личных данных граждан, расширение категории «коммерческая тайна» для бизнеса, рост количества агентских конфликтов и рост киберпреступлений обусловливает необходимость разработки современных инструментов обеспечения экономической безопасности [1;2; 4].

Анализ научной литературы и тематических публикаций по вопросам кибербезопасности позволил нам сформировать актуальную типологию угроз для экономической безопасности национальной экономики РФ с учетом развития общества (табл.1).

Таблица 1

Типология актуальных киберугроз для национальной экономики и их характеристика

Вид киберугроз	Характеристика
1. Хакеры, спонсируемые государством	Основной целью является атака на системообразующие банки и третьи стороны, отвечающие за проведение транзакций. *Объекты атаки*: VIP-клиенты, топ-менеджмент банка, рисковые операции, использование банка для доступа к другим банкам. *Примеры хакерских команд*: Equation Group, Lazarus
2. Диверсии и проведение тайных военных операций с использованием кибероружия	Атаки на государственные структуры, банки и базы данных с целью их уничтожения, повреждения, выведения из нормального режима работы. *Объекты атаки*: рисковые и мошеннические операции от имени банка, инфлуенс-торги на бирже, разрушение банковской инфраструктуры, монетизация ограбленных ранее объектов, вымогательство. *Примеры хакерских команд*: Cobalt, Black Energy, Idustroyer, HAVEX
3. Нарушение систем связи (Internet) на государственном уровне	Основной целью является нарушение стабильности интернет-коммуникаций, блокировка отдельных зон связи, ре-маршрутизация данных. *Объекты атаки*: крупные телеком-компании, инфраструктура, шлюзы и порты национального уровня. *Примеры хакерских команд*: APT10, WINNITI, Regin
4. Социальная инженерия	Основной целью является получение приватной информации о пользователе путем взлома его аккаунта, создания сайтов-двойников *Объекты атаки*: интернет-банкинг, аккаунты в социальных сетях, смартфоны *Примеры хакерских команд*: APT10, Equation Group, Lazarus
5. Рынок криптоиндустрии	Основной целью является использование технологии блокчейн для проведения операций и атак, хранения накопленных материалов, хищение ценностей у пользователей. *Объекты атаки*: крипто биржи, индивидуальные кошельки *Примеры хакерских команд*: THRIP, REXAN, Muddy Water
6. Торговля инструментами хакеров с открытым кодом	Основной целью является масштабирование инструментов хакерских атак путем свободного обращения в интернете инструментов хак-атак в форме конструкторов.

Примечание – Источник: [1, с. 100; 2, с. 478; 4, с. 160-162].

Исходя из представленных актуальных киберугроз рассмотрим методику оценку интегральной устойчивости бизнес-структуры или института к киберугрозам:

$$R_F = (x_1 \times d_1 + x_2 \times d_2 + x_3 \times d_3 + x_4 \times d_4) \times z, \quad (1)$$

где $d_1 \ldots d_4$ – коэффициенты весомости факторов, определяемые экспертным путем таким образом, чтобы в идеальном случае R = 100, т. е. при $x_1 = x_2 = x_3 = x_4 =$ 100 и $d_1 + d_2 + d_3 + d_4 = 1$, z = 1;

x_1 – фактор «Опыт защиты от киберугроз», характеризующий накопленный опыт бизнеса в защите от киберугроз;

x_2 – фактор «Технологическое обеспечение информационной безопасности» характеризует уровень применяемых средств технической защиты информации;

x_3 – фактор «Организационное обеспечение

DOI:10.26104/IVK.2019.45

информационной безопасности» характеризует наличие в организации квалифицированных специалистов и руководителей в области информационной безопасности, система корпоративных правил и инструкций противодействия информационным киберугрозам;

x_4 – фактор «SR-менеджмент» характеризует политику компании в части коммуникаций со специализированными институтами информационной безопасности и криптозащиты в части разработки совместных решений и;

z – коэффициент «Достоверность» характеризует полноту и достоверность сведений, представленных организацией в части отчетов по вопросам кибератак и кибербезопасности [5, с. 29-30; 7, с. 14-16].

В свою очередь, факторы $x_1 – x_4$ определяют через субфакторы, которые могут быть рассчитаны, используя информацию, предоставляемую оцениваемой организацией, а данные для расчета фактора z выдает третье лицо. Порядок расчета факторов представлен в таблице 2.

Таблица 2

Методика оценки интегральной устойчивости бизнес-структуры или института к киберугрозам [5;7].

Фактор	Порядок расчета
1. Опыт защиты от киберугроз	$$x_1 = d_{11} \times x_{11} + d_{12} \times x_{21}, \quad (2)$$ где x_{11} – субфактор «Наличие собственных систем безопасности и информационного аудита», определяющих наличие разработок систем безопасности, выполненных непосредственно специалистами компании; x_{12} – субфактор «Эффективность защиты от киберугроз», представленный в виде коэффициент успешно отраженных угроз и угроз, принесших потери бизнесу; $d_{11, 12}$ – коэффициенты весомости.
2. Технологическое обеспечение информационной безопасности	$$x_2 = d_{21} \times x_{21} + d_{22} \times x_{22}, \quad (3)$$ где x_{21} – субфактор «Материально-техническая база» учитывает уровень технического обеспечения для осуществления информационного аудита, защиту коммерчески ценной и тайной информации; x_{22} – субфактор «Финансовая защита» характеризует систему защиты финансовых потоков и денежных счетов компании $d_{21, 22}$ – коэффициенты весомости.
3. Организацион-ное обеспечение информационной безопасности	$$x_3 = d_{31} \times x_{31} + d_{32} \times x_{32} + d_{33} \times x_{33}, \quad (4)$$ где x_{31} – субфактор «Служба безопасности» характеризует уровень организации и оснащенности службы безопасности в части отражения киберугроз; x_{32} – субфактор «Наличие профессиональных компетенций» характеризует уровень квалификации специалистов в области кибербезопасности; x_{33} – субфактор «Профессиональная коллаборация» учитывает активность сотрудничества компании с профессиональными компаниями в области кибербезопасности
4. SR-менеджмент	$$x_4 = d_{41} \times x_{41} + d_{42} \times x_{42} + d_{43} \times x_{43} + d_{44} \times x_{41} + d_{45} \times x_{45} + d_{46} \times x_{46}, \quad (5)$$ где x_{41} – субфактор «Информационная открытость» – характеризует уровень сложности проведения атак на бизнес путем проведения QA-тестов; x_{42} – субфактор «Устранение нарушений» характеризует реакцию бизнеса на успешно проведенные атаки; x_{43} – субфактор «Политика защиты корпоративных данных» – наличие в организации систем защиты корпоративных данных и их технический уровень x_{44} – субфактор «Уровень доверия / лояльности» характеризует уровень доверия ключевых стейкхолдеров к системе безопасности компании; x_{45} – субфактор «Сертифицированная система менеджмента» характеризует наличие сертификатов на систему менеджмента, выданных в соответствии с действующим законодательством; x_{46} – субфактор «проекты НИОКР» учитывает наличие расходов на реализацию проектов НИОКР и коммерциализацию их результатов

DOI:10.26104/IVK.2019.45

Рассмотрев непосредственно модель оценки интегральной устойчивости бизнес-структуры или института к киберугрозам, перейдем к инструментальному обеспечению кибербезопасности в типичной бизнес-структуре (табл. 3).

Таблица 3

Характеристика инструментов кибербезопасности в типичной бизнес-структуре

Инструмент	Характеристика
1. Сканеры для сетевых ресурсов, тесты на возможность проникновения, взлом	*Характеристика группы инструментов*. Ориентированы на поиск точек уязвимости в архитектуре информационной модели бизнеса, поиск потенциальных входов в систему, т.н. черные дыры в кодировке. *Зона применения*. Экспресс-тест системы на уязвимости, либо проверка на устойчивость к экстремальным нагрузкам. Данная группа направлена на предотвращение атак, либо проверку жизнеспособности программных продуктов перед их запуском в производство. *Примеры продуктов и их характеристика:* – OpenVAS – комплекс сервисов и инструментов для проверки уязвимостей и управления уязвимостями при разных сценариях атак; – Kali Linux для цифровой криминалистики и проведения тестирования на проникновение, включает в себя программы: nmap (сканер портов), Wireshark (анализатор пакетов), John the Ripper (взломщик паролей) и Aircrack-ng (программный пакет для тестирования WI-FI сетей).
2. Сетевой мониторинг, сбор данных из открытых источников	*Характеристика группы инструментов*. Ориентированы на фоновый анализ потоков информации и оценку их угроз путем поиска по ключевым дистрибутивам, расширениям, форматам. *Зона применения*. Регулярный тест системы в фоновом режиме на предмет поступления опасных файлов или приложений под видом текущих данных. *Примеры продуктов и их характеристика:* – httpry – специализированный пакетный снифер для анализа и протоколирования HTTP-трафика. Его цель – сбор, обработка и регистрация трафика для его последующего анализа; – passivedns – инструмент пассивного сбора записей DNS для обработки различного рода инцидентов и мониторингу сетевой безопасности (NSM) и общей цифровой криминалистике.
3. Системы противодействия вторжениям и защиты	*Характеристика группы инструментов*. Ориентированы на защиту информационного поля от вредоносных файлов путем запрета на их принятие по заданным заранее ключевым параметрам. Как правило к таким инструментам прилагается база данных с функцией автоматического импорта инцидентов для актуализации состава параметров потенциально опасных файлов. *Зона применения*. Защита системы на входе /выходе от возможной утечки данных при попадании в саму систему опасных файлов или фрагментов вредоносного кода. *Примеры продуктов и их характеристика:* – Stealth – комплекс средств для проверки целостности файла с опцией запуска контроллера с другого компьютера и проверкой определенных псевдослучайных интервалов, что позволяет замаскировать тест-действия системы под обычную самопроверку операционной системы
4. Инструменты разведки в сети Internet	*Характеристика группы инструментов*. Ориентированы на защиту информационной системы при ее работе непосредственно в сети Internet. Основной принцип работы – помещение потенциально вредоносных файлов в искусственно создаваемое облако и анализ их поведения с целью последующей блокировки уже на входе *Зона применения*. Защита системы при работе в сети Internet. Имеется риск разрушения облака и попадания вируса / угрозы непосредственно в информационное поле *Примеры продуктов и их характеристика:* – Cuckoo Sandbox – программное обеспечение для автоматизации анализа подозрительных файлов которое отслеживают поведение вредоносных процессов во время работы в изолированной среде и запоминает их поведение с помощью алгоритмов реакции.
5. Инструменты захвата сетевых пакетов	*Характеристика группы инструментов*. Ориентированы на захват вредоносных приложений, файлов, их локализацию и анализ содержимого. Фактически, это программы-охотники за вирусными и иными риск-файлами, которые умышленно позволяют заразить себя. *Зона применения*. Аналитическая работа криминалистов в области информационной

DOI:10.26104/IVK.2019.45

	безопасности, служба безопасности, профессиональные лаборатории. *Примеры продуктов и их характеристика:* – Xplico – инструмент для извлечения из интернет-трафика данных приложений (адрес электр. почты (протоколы POP, IMAP и SMTP), все содержимое HTTP, каждый VoIP-вызов (SIP), FTP, TFTP и т. д. – Dshell – сеть для криминалистического анализа с функцией разработки плагинов для разбиения и захватов сетевых вредоносных пакетов.

Примечание – Источник: [4-10].

Дополнительно рассмотрим инструмент продуцирования инструментов защиты – онтологического инжиниринга, целью которого является конструирование специальных решений для обеспечения информационной безопасности экономических бизнес-процессов и связанных с ними данных. Типичная архитектура бизнес-модели онтологического инжиниринга представлена на рисунке 1 и включает в себя:

1. Интерфейсы – команда специалистов, отвечающая за диалог с программной средой, выборку параметров и критериев анализа информационных потоков, определение действий с опасными файлами.

2. Сервисы – непосредственно блок машинного анализа потоковых данных на предмет наличия угрозы для информационной системы бизнеса.

3. Бизнес-логика – экспертная система, построенная на принципах искусственного интеллекта, отвечающая за анализ файлов-потенциальных нарушителей на предмет реальности угрозы, ее последствий для бизнеса.

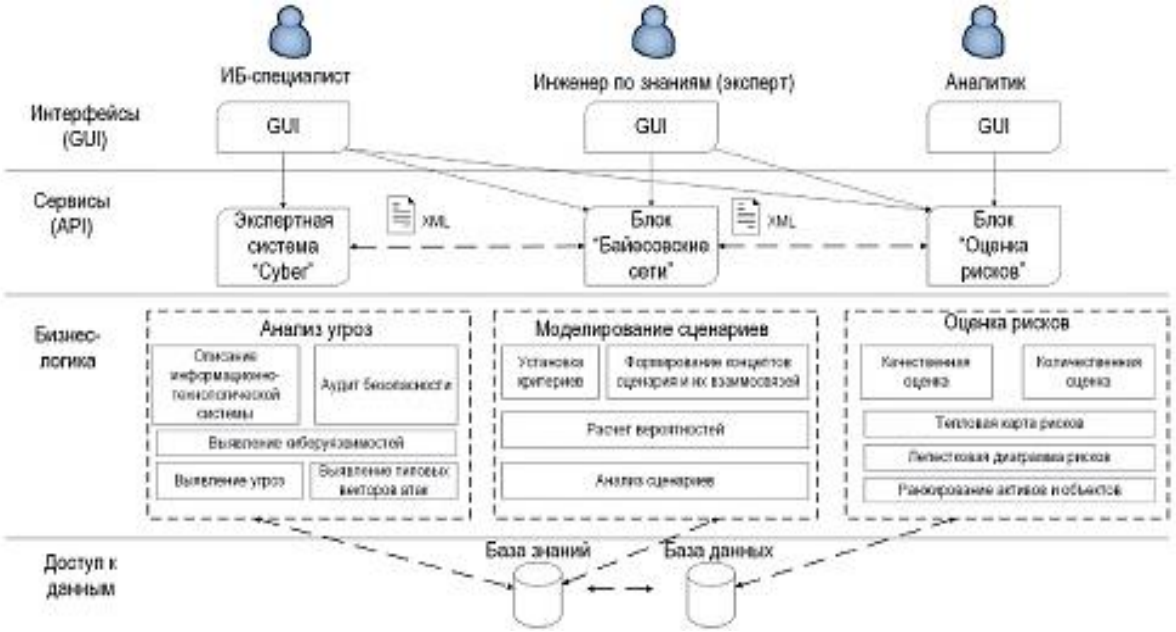

Рис. 1. Общий вид архитектуры бизнес-модели онтологического инжиниринга.

Примечание – Источник: [6, с. 70].

4. Доступ к данным – облачные cloud-серверы, хранящие опыт анализа и реакций искусственного интеллекта на различные типы угроз и атак. Такая система не только способна анализировать риск-файлы, но и сама генерировать сценарии развития событий, обучая систему отвечать на поставленные задачи по траектории минимальных потерь.

Заключение. Современная бизнес-модель устройства социально-экономической системы предполагает тотальную цифровизацию бизнес-процессов, что обусловливает актуальность вопроса обеспечения безопасности экономических и финансовых процедур в мировом пространстве. Так, в отличие от большинства развитых стран, в России до сих пор не принята

DOI:10.26104/IVK.2019.45

доктрина кибербезопасности, и, как следствие, отсутствуют соответствующие стандарты, как, например, в США: «Guidelines for Smart Grid Cyber Security» (Руководство по обеспечению кибернетической безопасности Smart Grid).

Литература:

1. Андрюшин С.А. Финансовые рынки, технологические инновации и финансовая стабильность: риски и проблемы регулирования / С.А. Андрюшин // Актуальные проблемы экономики и права. - 2019. - Т13. - №3. - С. 92-103.
2. Барыкин С. А. Риски и перспективы государственного регулирования рынка финансовых технологий в Азии в рамках сценарного анализа / С.А. Барыкин // ARS ADMINISTRANDI (Искусство управления). - 2019. - Т.11. - №3. - С. 473-487.
3. Борисова Е.С. Инновации как инструмент обеспечения информационной безопасности и повышения эффективности деятельности банковской системы / Е.С. Борисова // Актуальные проблемы экономики и права. - 2019. - Т13. - №3. - С. 125-134.
4. Ревенков П.В. Кибербезопасность в условиях Интернета вещей и электронного банкинга / П.В. Ревенков // Национальные интересы: приоритеты и безопасность. – 2016. - №11. - С. 158-169.
5. Ревенков П.В. Расширение профиля операционного риска в банках при возрастании DDoS-угроз / Вопросы кибербезопасности. - 2017. - С. 24-32.
6. Хлопов О.А. Проблемы кибербезопасности и защиты критической инфраструктуры / О.А. Хлопов // The Scientific Heritage. - 2020. - №45. - С. 64-73.
7. Цветков В.А. Пять проблем экономической безопасности и экономического роста в современной России // Вестник Финансового университета. 2016. Том: 20. - №2 (92). - С. 6-15.
8. Цветков В.А., Дудин М.Н., Лясников Н.В., Заидов К.Х. Проблемы и перспективы развития электронных платежных систем в России // Экономика и управление. 2018. - №2. - С.13-21.
9. Эксиндаров М.А. Направления развития финтеха в России: экспертное мнение финансового университета / М.А. Эксиндаров // Мир новой экономики. - 2018. - №12. - С. 6-23.
10. Юрьева А.А. Развитие информационного общества как условие формирования инновационной экономики // Проблемы рыночной экономики. - 2016. - №3. - С.14-20.