DOI: 10.14451/1.168.20

ПРОБЛЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ТРАНСПОРТНЫХ СИСТЕМ В УСЛОВИЯХ ГЛОБАЛЬНЫХ КИБЕРУГРОЗ

© 2018 **Журавлева Наталья Александровна**
доктор экономических наук, профессор
Петербургский государственный университет путей сообщения Императора Александра I
190031, Санкт-Петербург, Московский проспект, д. 9
E-mail: zhuravleva_na@mail.ru

© 2018 **Никитин Александр Борисович**
доктор технических наук, профессор
Петербургский государственный университет путей сообщения Императора Александра I
190031, Санкт-Петербург, Московский проспект, д. 9
E-mail: nikitin@crtc.spb.ru

Развитие киберпространства в современном мире вызывает стремительный рост киберугроз, влияющих, в большей степени на инфраструктурные отрасли, в частности транспорт. Решение проблем кибербезопасности существенно отстает от цифровизации экономики, генерирующей эти угрозы. В статье приведены результаты исследования влияния цифровых технологий на рост операционной деятельности транспортных организаций и связанных с этим ростом киберугроз. Показаны цели киберпреступности и размеры монетизации ее последствий. Представлен организационный профиль киберрисков и предложены параметры модели кибербезопасности транспортных систем.

Ключевые слова: киберпространство, киберугрозы, киберпреступность, экономическая безопасность, цифровые технологии, транспортные организации, операционная модель.

Введение

Под воздействием цифрового ландшафта существенно меняется область научных исследований глобальных тенденций перехода мировой экономики на новый технологический уклад. Цифровизация, формируя новую экосистему, связывает каждый актив, которым владеет или пользуется организация, в бесконечную цепь взаимосвязанных элементов. Формируются новые организационные и бизнес-модели, в которой рынки, их сегменты, конкуренция и каналы сбыта под воздействием новых технологий не только меняют свою форму существования, но и мировоззрение людей как производителей и потребителей. Этим обусловлено появление новой операционной модели транспортного бизнеса, оптимизирующей способ производства транспортной услуги в режиме реального времени.

Общество уже может оценить выгоды от инвестиций в трансформацию производства, в частности, снижение затрат на техническое обслуживание; рост индекса операционной эффективности, снижение себестоимости производства, прирост длительности бесперебойной работы оборудования и т.д. Очевидно, что процессы монетизации цифровых технологий столь привлекательны для бизнеса, что процесс будет только развиваться. Но при этом уже очевидны существенные, а в ряде случаев, катастрофические потери и угрозы, генерируемые глобальной цифровизацией. Кибербезопасность является серьезной проблемой для организаций во всем мире. Уже сейчас мы находимся в центре того, что можно охарактеризовать как кибер-глобальный кризис, поскольку тренды развития цифровых технологий существенно опережают способы их защиты. Известна оценка глобального влияния киберпреступности на мировую экономику, определяемая в диапазоне между $375 и 575 млрд. При том, что киберинциденты часто не регистрируются, явные масштабы их проявления можно представить по данным четырех крупнейших экономик (США, Китая, Японии и Германии) совокупный ущерб которых составляет более $200 млрд. в год [1].

Следует отметить, что кибербезопасность не идентична информационной безопасности поскольку не вся информация является цифровой и не все цифровые риски — это информационные риски.

Объектом данного исследования является киберпространство, в котором существуют и функционируют транспортные системы. По своей сути транспортно-логистические системы являются инфраструктурой нового технологического уклада. Экономика этих систем генерирует добавленную стоимость за счет сервисов скорости, интермодальности, составления оптимальных маршрутов доставки грузов и пассажиров, обеспечения полной загрузки транспортных средств, контроля прохождения грузов на всех этапах логистической цепочки и т.д., т.е. через интеграцию продуктов и услуг, учитывая доминанту глобального сетевого производства и потребления.

Киберпространство транспортных систем — это сложная среда, не существующая ни в какой физической форме, возникающая в результате взаимодействия людей, ПО, интернет сервисов посредством технологических устройств и сетевых связей. Следует отметить, что это не только информационные и телекоммуникационные технологии, а их непрерывное взаимодействие между собой, определяемое деятельностью людей, которые используют эти технологии. Именно последнее генерирует угрозы разрушения не только бизнес и операционных моделей, но и создает риски жизнедеятельности.

Предметом исследования являются процессы обеспечения экономической безопасности транспортных систем, возникающих в результате киберугроз, генерируемых цифровыми технологиями.

Методология исследования рассматривается как совокупность знаний о структуре, методах и средствах деятельности, применяемых в описании поведения всех субъектов в новом технологическом укладе.

Целью исследования является определение параметров киберугроз, генерируемых ростом операционных моделей транспортных компаний, в процессе цифровизации их деятельности.

Киберпространство транспортных систем

Киберпространство следует рассматривать как, поддерживаемую во всем мире сложную систему распространения физических информационных и коммуникационных технологий (ИКТ), баз данных, виртуально отражающих физические, социальные, духовные, финансовые, политические, эмоциональные, профессиональные, психологические, образовательные или другие типы поведения, а также процессы монетизации результатов ассиметричного анализа этих данных. Множественность типов поведения в киберпространстве генерирует множественность угроз, целью которых является рост киберпреступных денежных потоков. Наиболее распространенными являются: незаконное проникновение в базы данных, информационные системы сбора, хранения и управления технологическими и операционными процессами, кража интеллектуальной собственности, вымогательства, выведения из строя, нанесения убытка стране, конкуренту.

При этом существует еще ряд обстоятельств, усложняющих безопасное функционирование киберпространств, в частности, отсутствие в нем связи между функционирующими субъектами и объектами, и поставщиками цифровых технологий. Устройства и подключенные сети, которые поддерживают киберпространство имеют множественных владельцев с разнонаправленными интересами и поведением.

Следует учитывать, что транспортные системы в киберпространстве приобретают новые свойства с высокой степенью воздействия киберугроз.

Определяющее новое свойство формируют потребители транспортной услуги — грузоотправители и пассажиры. Транспортная компания в процессе их взаимодействия традиционно предоставляет клиенту свои возможности по перевозке, а затем осуществляет саму перевозку. Теперь появилась обратная связь, отражающая экономическую ценность перевозки и это ключевой компонент бизнес-стратегии транспортной организации. Это означает, что на рынке не нужен вагон или грузовой автомобиль как транспортное средство. Товаропроизводителю нужна эффективная перевозка в срок и по конкурентоспособной цене. Он формирует динамическую сеть потребности в перевозке. Образуется двухсторонний поток ценностей и первый параметр эффективности транспорта, обеспечивающий его безопасность: это рост бизнеса за счет предоставления транспортной услуги, соответствующей ценности клиентов. Эти ценности формируются рядом цифровых технологий, таких как, например, Интернет вещей, Big Date, технологии распределенного реестра, блокчейн и пр. Данные рассматриваются как ключевой нематериальный актив, необходимый для создания добавочной стоимости. В случае их

преступного искажения компании теряют операционную устойчивость, а в длительном времени — устойчивость бизнес-стратегии.

Второе изменение определяет конкуренция на рынке транспортных услуг. В новом формате транспортной услуги формируется свойство преимущества смешенной (интермодальной) перевозки в свободной сети партнерских отношений. Цифровые платформы помогают не только обмениваться ценностями, но и обеспечивать саму перевозку, например, беспилотные устройства, в том числе беспилотный транспорт, технологии искусственного интеллекта или программные алгоритмы, поддерживающие принятие решений по перевозке и пр. И, если сеть партнерских отношений становится основным конкурентоспособным активом, то ее разрушение в одном звене, разрушает всю систему перевозки.

Чрезвычайно существенным становятся свойства высоких скоростей, обеспечиваемых высокоскоростными транспортными системами. Потребность в них связана с технологиями, реализующими эффект времени. Именно время, как экономическая категория формирует комплекс эффектов, возникающих в производстве и потреблении высокоскоростной транспортной услуги, а также достигаемом эффекте мультипликации смешанной перевозки. Сегодня идут полевые испытания магнитолевитационных перевозок грузов со скоростью 1200 км\час, то изменит абсолютную сеть ценностей транспортной услуги. Эффективность высоких скоростей обеспечивают технологии роботизации, компоненты робототехники и сенсорика, виртуальный мониторинг, технологии распределенного реестра и т.д. Совершенно очевидно, на сколько могут быть разрушительны последствия киберугроз при таких скоростях.

Эти и другие свойства транспортных систем, возникающие в процессе цифровых изменений, связаны с требуемым ростом эффективности перевозок на национальных и глобальных рынках товаров, услуг и труда. И чем стремительнее будет трансформация транспортного бизнеса, тем значительнее опасность кибератак и последствий киберразрушений.

Описание процессов киберугроз, существенно влияющих на экономическую безопасность транспортных систем

Основные базовые понятия кибербезопасности опираются на международные стандарты ISO (the International Organization for Standardization) и стандарты, разработанные Международной электротехнической комиссией IEC (the International Electrotechnical Commission). Дефиниции терминов «киберугроза», «киберпространство», «кибербезопасность», «кибертерроризм» даны в международном стандарте ISO/IEC27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. Следует отметить, что в соответствии с этим, информационная безопасность и кибербезопасность близкие, но не идентичные понятия. Приведенный стандарт дает четкое понимание связи термина cybersecurity (кибербезопасность) с сетевой безопасностью, прикладной безопасностью, интернет-безопасностью и безопасностью критичных информационных инфраструктур [2]. Сущность кибербезопасности можно свести к условиям, при которых коммуникационные каналы Интернета и других телекоммуникационных сетей, технологическая инфраструктура в период их функционирования защищены от максимально возможного числа угроз и воздействий, имеющих нежелательные последствия. Ряд авторов описывает киберугрозы с позиций их жизненного цикла в экономике [3].

В целях данного исследования, применительно к транспортным системам, мы сужаем понятие киберпространства с точки зрения трех основных составляющих:

• Системы управления движением: файлы (записанные на носителях данные) и динамические потоки (пакеты, команды, запросы, и т.д.), передаваемые по различным сетям, обрабатываемые в автоматизированных системах и представляемые на средствах отображения в графическом или текстовом виде.

• Техническая инфраструктура, ИТ, программное обеспечение, беспилотные устройства, роботы с помощью которых осуществляется реализация основных действий по управлению транспортной системой.

• Информационное взаимодействие всех субъектов перевозки с использованием информации получаемой (передаваемой) и обрабатываемой посредством технической инфраструктуры. Оно охватывает все виды деятельности пользователей или участников киберпространства, которые они осуществляют с использованием информационных ресурсов, потоки и хра-

нилища которых располагаются на технической инфраструктуре.

Опираясь на стандарты ISO/IEC/JTC1, при формировании системы кибербезопасности решается проблема преодоления разрыва между доменами безопасности в киберпространстве. В частности, на их основе разрабатываются технические руководства по отражению инжиниринговых атак, взлома; распространения вредоносного программного обеспечения (Spyware) и другого потенциально нежелательного программного обеспечения.

Основная киберпреступность сосредоточена в технологиях, обеспечивающих максимальную доходность бизнеса, т.е. ее целью является монетизация последствий кибератаки. Этот тезис подтверждают исследования ряда российских авторов, в частности [4, 5, 6].

Сегодня в числе пяти основных глобальных преступлений, с точки зрения их стоимостного влияния на мировой внутренний валовый продукт, киберпреступность занимает четвертое место (0,8%), и эта величина стремительно перемещается в сторону несомненного лидерства. Пока только транснациональная преступность (1,2%), наркотики (0,9%) и подделки/пиратство (0,89 процента), с точки зрения финансовых последствий рангом выше [7]. Несмотря на то, что стоимость киберпреступности не может быть корректно измерена во всем мире, достаточно очевидно влияние киберпреступности на политические решения, разрушение личного пространства граждан, подрыв доверия общества к цифровизации процессов, составляющих общественную инфраструктуру, как глобальную, так и национальную.

Подтверждением тезиса о монетарной цели киберугроз транспортных систем может быть пример оценки монетарных последствий киберпреступности на базе Интернета вещей. Внедрение интернет технологий создает дополнительно, в среднем за год до $4 трлн., или на $320 млрд. увеличивает денежный приток транспортных систем, доля которых в мировом ВВП оценивается на уровне 8% (в среднем, по включаемым в расчет странам). Киберпреступность «выкачивает» до 15% от этой суммы, следовательно, только преступления в сфере Интернет вещей на транспорте снижают эффективность операционных моделей транспортных организаций на $4,8 млрд. в год (рассчитано по: [8, 9]).

Подобное влияние на бизнес транспортных систем можно проследить исходя из применения любой цифровой технологии. Таким образом, рост киберпреступности обусловлен несомненной монетизацией киберпреступлений, прежде всего, из-за высокого уровня потенциальной отдачи от вложений в киберугрозы и низким риском их обнаружения и преследования. Таким образом, кибербезопасность — это не техническая проблема, а проблема защиты операционных и бизнес-моделей организаций или неотъемлемая часть бизнеса.

Основные параметры модели кибербезопасности цифровизации транспортных систем

Человечество ни разу не проверяло объекты критической инфраструктуры, к которой относится транспорт, на предмет реальной атаки организованной компьютерной преступности. По-прежнему нет единых стандартов кибербезопасности в глобальных транспортных сетях. Общество популяризирует компьютерную преступность, которая входит в бизнес и политику. Законодательство стран меняется медленно и без синхронизации с международным законодательством, что не имеет смысла в глобальных сетях.

Сегодня компаниям сложнее чем когда-либо четко обозначить границы цифровой среды, в которой они работают, что делает уязвимой их, прежде всего, операционную деятельность, и создает благодатную почву для кибератак.

Операционная модель любой транспортной организации зависит от *бизнес-моделей* глобальной или национальной транспортных систем. Именно на них отражаются основные последствия киберугроз, поскольку сложная перевозка обеспечивается единым информационным пространством, организованном на технологиях «интернет вещей», Big Date и блокчейн, охватывающих все виды деятельности пользователей или участников киберпространства, которые они осуществляют на соответствующей технической инфраструктуре. В этом случае разрушаются ценности, которые получают пользователи транспортных услуг, отношения с партнерами и капитал, необходимый для получения устойчивых доходов. Это подтверждает и концептуальное описание бизнес-моделей в ряде научных работ, в частности [10].

Угрозы бизнес-модели транспортных компаний можно оценить с вероятностью наступления

следующих событий: вредоносное программное обеспечение 64%; фишинг 64%; кибератаки с целью кражи интеллектуальной собственности 32% или данных; кибератаки с целью кражи финансовой информации 30%; внутренние атаки 25%.

Устойчивость операционной модели обеспечивает *процессная модель организации*, которая в нашем случае должна быть ориентирована на устранение угроз жизни людей. В большей степени она обеспечена технической инфраструктурой (железнодорожной, автомобильной, авиационной, трубопроводной, морской), IT, программным обеспечением, беспилотными устройствами, роботами с помощью которых осуществляется реализация основных действий по управлению транспортной системой. И в данном случае основы кибербезопасности наиболее перспективны на постквантовой криптографии (новом поколение математических алгоритмов), предлагающей новые алгоритмы шифрования, которые сложны для взлома как классическими, так и квантовыми компьютерами. В России на данный момент ведутся научные исследования по разработке постквантовой криптографии и транспортные компании должны быть первыми, кто максимально заинтересован в них.

Основные угрозы операционной модели связаны с двумя видами атак. Первый — сложные атаки, защита от которых должна быть готова к тому, что несанкционированное проникновение может произойти в любой момент, и быть способной как можно раньше его обнаружить. Отправной точкой в организации эффективного выявления киберугроз является создание центра обеспечения информационной безопасности (SOC), который должен стать центральным штабом, координирующим всю работу по этому направлению. Сегодня все чаще можно наблюдать трансформацию функций SOC от пассивной защиты к активной обороне — тщательно спланированной и непрерывной кампании, нацеленной на выявление и нейтрализацию скрытых злоумышленников и борьбу с вероятными угрозами безопасности для сохранения наиболее важных активов организации.

Второй вид — новые атаки, происхождение которых будет неизвестным. Несмотря на всю неопределенность, транспортные организации могут обрисовать для себя контур будущих угроз и выработать такой подход, который позволит принять оперативные меры реагирования в нужный момент. Организации, обладающие надежной системой корпоративного управления, могут разработать системы и процессы, способные эффективно реагировать на неожиданные риски и появляющиеся угрозы, взяв на вооружение принципы «проектируемой безопасности».

Традиционно, операционная модель организации опирается на технологии, бизнес-процессы организации и информацию. Киберпространство добавляет важнейший человеческий ресурс, который участвует во внедрении цифровых технологий и, одновременно, является наиболее проблемным в устойчивости операционной модели.

В результате проведённого исследования можно представить следующие результаты описания профиля киберзащиты и параметров модели кибербезопасности операционной деятельности транспортных организаций.

1. Набор параметров, соответствующих *процессам* перевозки. Они представляют собой организованный набор методов и мероприятий для достижения определенных целей безопасности деятельности на транспорте, набор мероприятий, поддерживающий достижение целей кибербезопасности, увязанных с целями бизнеса. Параметры формируются в соответствии с нормами и нормативами регулирования деятельности, должны учитывать показатели наибольшей уязвимости, соответствовать набору мер оперативной (стимулирующей) поддержки и отвечать требованиям соответствия персонала нужным компетенциям.

2. Параметры, отражающие уровень существующей технологии перевозки и перспективных технологий. Следует отметить, что киберриски появились с начала цифровой эпохи и уже более 30 лет идет увеличение их масштаба и сложности с беспрецедентной скоростью, прежде всего, за счет продвижения новых технологий производства. При этом, киберугрозы ломают барьеры между традиционными технологиями и бизнес-инновациями, следовательно, параметры безопасности должны соответствовать действующей технологической цепочке и перспективам технологических изменений. Набор параметров «технологии» строится на показателях технологического соответствия персонала, архитектуры бизнеса, оперативной (стимулирующей) поддержки защиты.

3. Параметры, отражающие уровень защиты информации как ключевого актива опера-

ционной и бизнес деятельности организации. Информация с одной стороны является основой принятия технологических, организационных, ресурсных, стратегических и других решений, формирующих деятельность бизнеса, а с другой — становится самым уязвимым элементом киберпространства. В операционной модели защиты транспортного бизнеса должны быть учтены, по крайней мере, такие показатели обеспечения безопасности информации, которые изложены в ISO 31000:2009(E) [11] и COBIT 5 Implementation [12].

В общем виде организационный профиль модели отражает последовательность следующих итераций:

a. формализация цели киберзащиты;
b. идентификация «создателей» угроз;
c. оценка уязвимости/сопротивляемости;
d. формирование параметров защиты и управление ими.

Заключение

Использование только технических решений и экспертизы специалистов информационной безопасности в отрыве от выстраивания процессной модели обеспечения кибербезопасности в организации не гарантирует должной защиты от новых атак, в ходе которых злоумышленники используют продвинутые механизмы сокрытия и удержания своего продолжительного присутствия в корпоративной сети.

Применительно к управлению рисками организация должна действовать на опережение, т.е. специальные проверки “background checks”, тесты на проникновение, оценку угроз, активный мониторинг информационной безопасности, а также кибербразведка и оценка уязвимости. Необходимы активные усилия по обмену информацией и координированию действий между заинтересованными сторонами.

Киберустойчивость должна рассматриваться как неотъемлемый компонент получения выгоды, а не только как способ предотвращения рисков. Достижение более высокого уровня устойчивости к рискам — это путь к более высокой долгосрочной экономической эффективности. Необходимо извлекать уроки из ситуационных исследований, посвященных реагированию на катастрофические события.

Библиографический список

1. *Antonucci D.* The Cyber Risk Handbook /Creating and Measuring Effective Cybersecurity Capabilities / by John Wiley & Sons. 2017.
2. ISO/IEC27032:2012 Information technology — Security techniques — Guidelines for cybersecurity.
3. *Сильвестров С.Н., Побываев С.А., Котова Н.Е., Лапенкова Н.В., Смирнов В.В.* Подход к выявлению угроз и оценке состояния экономической безопасности // Экономические науки. 2017. № 11(156). С. 7–10.
4. *Косолапов Ю.В., Костромина Е.А., Сивова А.А.* Киберпреступления в индустрии финансовых услуг// Вопросы экономики и права. 2018. № 4. С.25–30.
5. *Hill, R.* Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT // 7th International Conference on Cyber Conflict — Architectures in Cyberspace (CyCon). Tallinn, Estonia.— MAY26–28, 2015.— p. 119–133. WOS:000380531500010.
6. *Lu, Tianbo, Guo, Xiaobo, Xu, Bing, Zhao, Lingling, Peng, Yong, Yang, Hongyu* Next Big Thing in Big Data: The Security of the ICT Supply Chain // ASE/IEEE International Conference on Social Computing (SocialCom).— Washington, DC,— SEP 08–14, 2013.— P. 1066–1073. DOI: 10.1109; WOS:000330563800167.
7. *Hale Ron*. Foreword the State of Cybersecurity // The Cyber Risk Handbook / Creating and Measuring Effective Cybersecurity Capabilities / by John Wiley & Sons.— 2017.
8. Показатели ВВП стран мира за 2017 год [Электронный ресурс].— Режим доступа: http://www.economynews.ru/mirovaja-jekonomika/359-vvp-stran-mira-2017.html (Дата обращения 20.11.2018).
9. Потери организаций от киберпреступности. — http://www.tadviser.ru/index.php/ (Дата обращения 20.11.2018).
10. *Иову Т. Т.* Концепция бизнес-модели // Экономические науки, 2018, № 7. С.75–80.
11. ISO 31000:2009(E) International Standard: Risk Management — Principles and Guidelines, ISO 1st ed. 2009–11–15.
12. COBIT 5 Implementation: A Business Framework for the Governance and Management of Enterprise IT, ISACA, 2012. GEIT stands for Governance of Enterprise Information Technology.

Поступила в редакцию 07.11.2018