УДК 330.47

ПЕРСПЕКТИВЫ РАЗВИТИЯ ТРЕНДОВ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М.Е. ЛИСТОПАД, доктор экономических наук, доцент, профессор кафедры мировой экономики и менеджмента, Кубанский государственный университет
e-mail: mlistopad@inbox.ru

С.Е. КОРОТЧЕНКО, магистрант программы «Экономическая безопасность и устойчивость», Кубанский государственный университет
e-mail: evilcookies10@gmail.com

Аннотация

В статье рассмотрены перспективы развития трендов в информационной безопасности. Особый акцент делается на описании и прогнозировании будущего развития рынка обеспечения информационной безопасности. Развитие высоких технологий и Интернета – главный тренд на ближайшее будущее, который не только повлияет на привычные нам сферы деятельности, но и скажется на обеспечении безопасности и сохранения информации и личных данных.

Ключевые слова: *тренды, индикаторы, информационная безопасность, прогнозы, цифровые технологии.*

В мире, который все шире и шире развивается благодаря большим данным, социальным сетям, онлайн-транзакциям, информации, управляемой через Интернет, и автоматизированным процессам, осуществляемым с использованием информационных систем, информационной безопасности (далее ИБ) и конфиденциальности данных, мы постоянно сталкиваемся с большими рисками потери данных. С развитием новых инструментов и методов взлома уровень киберпреступности последовательно растет с точки зрения количества нападений и ущерба, нанесенного ее жертвам.

Потребление большого количества каналов связи и Интернета, а также полная автоматизация производственных и бизнес-процессов формируют концепцию нынешнего этапа промышленной революции, которую именуют «Индустрия 4.0». Данные выступают ключевым ресурсом организаций и государства, следовательно, требуется формирование и соблюдение мер по защите от киберугроз. ИБ – это главный тренд ИТ-сферы.

Перспективы развития трендов в обеспечении ИБ можно представить в виде трех систем. Первая система была сформирована на базе серверов (мейнфреймов) и терминалов, на которых функционировали тысячи пользователей и программ. Вторая система характеризовалась наличием персональных компьютеров, Интернета и множества приложений. В основе третьей системы лежит быстро растущее количество постоянно подсоединенных к Интернету смартфонов в союзе с широким применением социальных сетей и развитой облачной базы, используемой для решения совокупных практических задач. Весь контент, приложения и услуги, используемые в третьей системе, сегодня доступны миллиардам пользователей. Большие данные, облачные вычисления, социальные и мобильные технологии обеспечивают взаимное развитие всех сфер общества.

Сегодня каждый пользователь смартфона генерирует большое количество контента, которое безопаснее сохранять по средствам облачных технологий. С геометрическим ростом мобильных устройств связи растет количество активных пользователей социальных сетей. Аккумулируемые в них данные выступают базовым источником для оценки и получения ценных данных с помощью средств обработки больших данных.

Одним из наглядных примеров, для которого необходимы технологии третьей системы, является применение программного обеспечения на устройстве с мобильной связью для

получения доступа к корпоративным данным или информации, имеющимся в социальных сетях, а также обработка этой информации в режиме реального времени и прогнозирование дальнейших действий в зависимости от приобретенных сведений.

Развивая новые способы получения несанкционированного доступа к сетям, программам и данным, злоумышленники стремятся скомпрометировать конфиденциальность, доступность и целостность информации, выстраивая свои цели от отдельных лиц к малым или средним компаниям и даже бизнес-гигантам. Каждый год приносит большее количество атак, угрожающих безопасности чрезвычайно крупных компаний, что влияет на безопасность информации, непрерывность бизнеса и доверие клиентов. Подобная тенденция достигла пика в 2016 г., известном как «год кибератак». Если не будут приниматься средства защиты информации, то тенденция роста продолжится и в будущем. Кибер-атаки становятся повседневной реальностью как для компаний всех размеров, так и для отдельных лиц. В целом отсутствует понимание различных типов атак, характеристик и возможных результатов, которые могут создавать препятствия для защиты информационной безопасности.

Становление рынка ИКТ характеризуется увеличением больших объемов данных. Постоянная интеграция бизнес-процессов в ИТ-сферу включает новые сферы и заставляет компании вне зависимости от размера и отрасли анализировать и аккумулировать большие массивы данных, что заставляет модернизировать инфраструктуру ИБ [1].

Технологическая эволюция также несет в себе прогресс кибер-преступности, поэтому постоянно совершенствуются способы совершения нападений, достижения еще более трудных для проникновения целей. Однако традиционные киберугрозы остаются источником наиболее распространенных атак. Так, можно выделить основные типы угроз ИБ, которые будут развиваться и на которые следует обратить пристальное внимание:

1. Атака «человек в середине» происходит, когда атакующий стоит между двумя концами связи, поэтому каждое сообщение, отправленное из источника А в источник В, достигает атакующего прежде, чем достигнет пункта назначения. Риски, связанные с этим типом атаки, включают несанкционированный доступ к конфиденциальной информации или возможности изменить информацию / сообщение, которое достигает адресата.

2. Атака методом грубой силы включает повторяющиеся попытки приобрести доступ к защищенной информации (пароли, шифрование). Это продолжается до тех пор, пока не будет найден правильный ключ и информация получит статус «открыта».

3. DDoS-атаки (распределенный отказ в обслуживании) – это тип атаки, которая ставит под угрозу доступность данных за счет того, что злоумышленник посылает жертве (например, серверу) множество команд, после чего доступ к информационным ресурсам блокируется.

4. Вредоносное ПО – общий термин, описывающий типы вредоносного программного обеспечения, применяемые злоумышленником для нарушения доступности, конфиденциальности и целостности данных. Наиболее распространенные типы вредоносных программ: вирусы, черви, трояны, шпионские программы, вымогатели, рекламное ПО и копии товаров.

5. Фишинг – метод, направленный на хищение конфиденциальной информации от пользователей посредством маскировки в качестве надежного источника (например, веб-сайта).

6. Социальная инженерия – это общий термин, который описывает методы, используемые для получения несанкционированного доступа к информации посредством взаимодействия человека.

В будущем ожидается, что количество кибератак будет расти, ожидается рост шпионажа и кибербезопасности благодаря улучшенным стратегиям и инструментам хакеров по скрытию их личности / местонахождения и получению данных, ведь злоумышленники постоянно разрабатывают новые способы использования сетей, программ и данных.

Кибер-шпионаж, скорее всего, нацелен на сектор государственного управления, средств массовой информации и правоохранительной деятельности и весьма маловероятен для других секторов бизнеса (розничная торговля, телекоммуникации, онлайн-услуги).

Уже сейчас социальные сети выступают одним из основных механизмов по привлечению новых покупателей, а также продвижению своего товара. В этом году ожидается

еще больший рост активных групп в социальных сетях крупнейших компаний. Из бюджета организации выделяются средства на ведение такого вида деятельности как одного из ключевых элементов маркетинговой стратегии и кампании по привлечению новых клиентов. С помощью этого инструмента происходит сбор большого объема информации (мнение о компании, продуктах, узнаваемость бренда, пожелания, недостатки в продукте), которая является очень результативной при планировании будущих разработок в организации [2].

В нашей стране рынок ИБ-услуг и сферы ИТ за прошлые годы показывает снижение темпов роста, несмотря на большие инвестиционные государственные проекты типа «Электронное правительство» и проведение зимних Олимпийских игр в Сочи, а также попыток сохранить высокие цены на нефть. По-прежнему большинство отечественных компаний, которые специализируются на обеспечении ИБ, не раскрывает подробностей своей сферы деятельности, следовательно, рынок ИТК услуг остается недостаточно прозрачным. На практике получается, что большинство проектов, которые взаимосвязаны с новейшими информационными технологиями, реквизиты компаний заказчиков остаются в тайне по условию договора о соблюдении секретности и остаются недоступными общественности.

В современных реалиях с развитием открытого доступа к личным данным из любой точки мира и любого устройства назревает вопрос о безопасности облачного хранения персональной информации. Так, по данным всемирной исследовательской организации International Data Corporation (IDC), специализирующейся на изучении международного рынка информационных телекоммуникаций и технологий, в ближайшие 2–3 года 83 % компаний планируют вкладывать инвестиции в развитие сектора облачных технологий. Также отмечается увеличения интереса покупателей к средствам контроля и идентификации доступа, который в 2017 г. вырастет на 8,3 %.

С учетом быстрорастущей отрасли высокотехнологических устройств и быстрой смены практических решений в сфере ИБ специалисты IDC выделяют ключевым трендом организации обращать внимание на достоверность информации и работоспособность ИТ-активов.

В итоге от ближайшего будущего следует ожидать постоянства при обеспечении ИБ, которые можно характеризовать как «надежную безопасность». В этом случае роль «бумажной безопасности» до следующего года намного уменьшится. В целом государственный и, конечно, коммерческий сектор изменят приоритеты от всеобщего и легкого исполнения рекомендаций регуляторов в сторону наибольшей эффективности обеспечения ИБ.

Сложные отношения с Западными странами очередной раз подтолкнули к необходимости уменьшить зависимость нашей страны от импортных ИБ-систем, увеличить количество разработок собственного производства с открытым кодом, укрепить ИБ инфраструктуры в критически важных направлениях (военном, государственном, финансовом). При этом многие крупные игроки, которые выступают на мировой арене, продолжают также уделять внимание крупным программам на территории России. Все это обусловлено тем, что в перспективе весь рынок высокотехнологичного производства будет зависеть не только от экономического положения страны, но и от крупных государственных проектов, в которых государство играет роль гаранта. Однако нельзя забывать неэффективность таких проектов, которые нацелены на «слепое» финансирование и полную безответственность в разрезе бюджетирования. В итоге получаем низкий уровень взаимодействия государственных и субъектных властей, что обуславливается стремительным ростом стоимости ИБ-проектов, превышением (дефицитом) бюджета и как следствие несоблюдением сроков исполнения.

Однако все эти негативные тенденции имеют и положительную динамику. Так, например, принятый новый закон об обработке и аккумулировании персональных данных внутри страны позволит снизить утечку данных обо всех организациях и жителях страны. Также это изменение повысит надобность в формировании систем хранения и центров обработки данных. Плюс увеличивается рост программного и аппаратного обеспечения отечественного производителя, которое может не только выступать аналогом зарубежного, но и выйти на мировой рынок, повысив конкурентоспособность страны в высокотехно-

логичном секторе. За этим последует увеличение средств на ИТ-услуги, разработку заказного ПО, ИТ-консалтинг и системную интеграцию [5].

Необходимо отметить, что новые перспективы для развития рынка ИКТ в России появились благодаря сотрудничеству с Китаем и созданию Евразийского экономического союза (ЕАЭС). В итоге наша страна заключила крупнейший в истории газовый контракт, а также ряд соглашений, которые затрагивают аэрокосмическую, транспортную, банковскую, телекоммуникационную и другие отрасли, что стимулирует модернизацию ИБ-инфраструктуры. С 2015 г. ЕАЭС начала свою работу и стала одним из крупнейших рынков на постсоветской территории с общим объемом ВВП в 3,1 трлн дол. В итоге отечественные разработчики ИТ-услуг и продуктов получили большой доступ к широкому рынку и смогли принимать участие в совместных проектах в странах – участницах союза.

ИТ характеризуются средствами ИБ, которые обеспечивают будущие перспективы и тренды развития всей сферы ИКТ. В основном это:

– оцифровка и наращивание цифрового контента во всех сферах человеческой деятельности;

– глубокое развитие интернет-сервисов по средствам облачных технологий и анализа больших данных;

– мгновенные передачи сообщений и потоковые данные;

– системы управления цифровым контентом;

– мобильные технологии и приложения;

– «Большие данные»;

– постоянное совершенствование IT-технологий, их сменяемость и быстрое внедрение (так, например, в середине 1970-х гг. появился первый мобильный телефон, а сейчас в мобильных сетях зарегистрировано столько абонентов, сколько жителей на Земле, – и это в пределах одного поколения).

Информационные технологии, безусловно, определяют сегодня основные вехи эволюции человечества и жизнедеятельности. Вместе с тем рост и развитие новых технологий заставят отказаться от некоторых уже устоявшихся канонов современной общественной жизни или видоизменить их.

В этом году тренд ИБ на импортозамещение на территории нашей страны не изменится. Обострившиеся за прошлые годы межгосударственные отношения и государственные проблемы приведут к продолжающей политике ограничений и санкций стране. Это в свою очередь вызовет дефицит поставок зарубежного высокотехнологичного оборудования, комплектующих и ПО. В итоге формирование российских решений во всех высокотехнологичных областях будет еще более востребованным [6].

Главным заказчиком остается государство, предвидится рост спроса в этом сегменте. Требования, как к средствам защиты информации, так и к системам на их базе будут ужесточаться, что приведет к снижению доли рынка или перепрофилированию тех компаний, которые реализуют преимущественно зарубежную продукцию, в том числе под видом отечественной.

Рынок будет пытаться идти к соединению различных ИБ-продуктов в комплексные решения. Так, если раньше средства защиты, такие как средства шифрования, персональный межсетевой экран, инструменты контроля устройств, защиты от несанкционированного доступа, использовались по отдельности и устанавливались, возможно, от разных производителей, то сейчас заметно явное движение в сторону союза обозначенного функционала.

Также одним из трендов является переход ИБ-разработчиков на модульные продукты. В сложившихся экономических условиях организации очень ценят такой подход. Уже сегодня заказчики имеют потенциал постепенно увеличивать количество компонентов защиты – в зависимости от необходимости и бюджета.

Необходимо помнить и про тенденцию к росту киберпреступлений. В этом случае замечается переориентация целей, и под удар попадают рядовые граждане с мобильными устройствами. Плюс этому увеличиваются многофункциональные хакерские атаки с применением социальной инженерии на организации. Исходя из классического обеспечения ИБ намечается модернизация существующего комплекса мер ИТ и ПО и применение интеллектуальных средств защиты информации [7].

В 2016 г. сфера угроз разрешила киберпреступникам существенно повысить многообразие методов атак и типов атакуемых целей.

Большие изменения в организациях во всем мире увеличат необходимость соблюдения регламента «Акта о защите персональных данных» (General Data Protection Regulation, GDPR). Также можно прогнозировать появление новых методов атак на крупные корпорации, расширение тактик онлайн-вымогательства, которые будут затрагивать все более разнообразные устройства, а также применение методов киберпропаганды для манипуляции общественным мнением.

Если в 2016 г. наблюдался значительный рост числа новых программ-вымогателей, то сейчас он заметно снизился, поэтому хакеры будут искать новые пути использования уже существующих разновидностей таких программ. Похожим образом инновации в сфере Интернета вещей позволяют хакерам находить себе другие цели для атак, а изменения в программном обеспечении подталкивают их искать новые уязвимости.

Рост количества новых семейств программ-вымогателей замедлится и будет достигать порядка 25%, однако их воздействие распространится на устройства Интернета вещей, PoS-терминалы и банкоматы.

В настоящее время уже недостаточно просто внедрять средства защиты информации, необходимо понимать, что реально происходит в системе организаций. Потребность мониторинга состояния информационных систем на регулярной основе приводит руководство компаний к пониманию, что им нужны средства автоматизации получения и обработки данных для аналитики или построения полноценных SOC›ов (Security Operation Center).

Одним из ключевых и самым непредсказуемым ИБ-трендом 2017 г. станет «предвидеть непредвиденное» – формирование нового тренда, который нельзя предугадать или предвидеть. Такой внезапностью ушедшего года стали хакерские атаки на выборы в США.

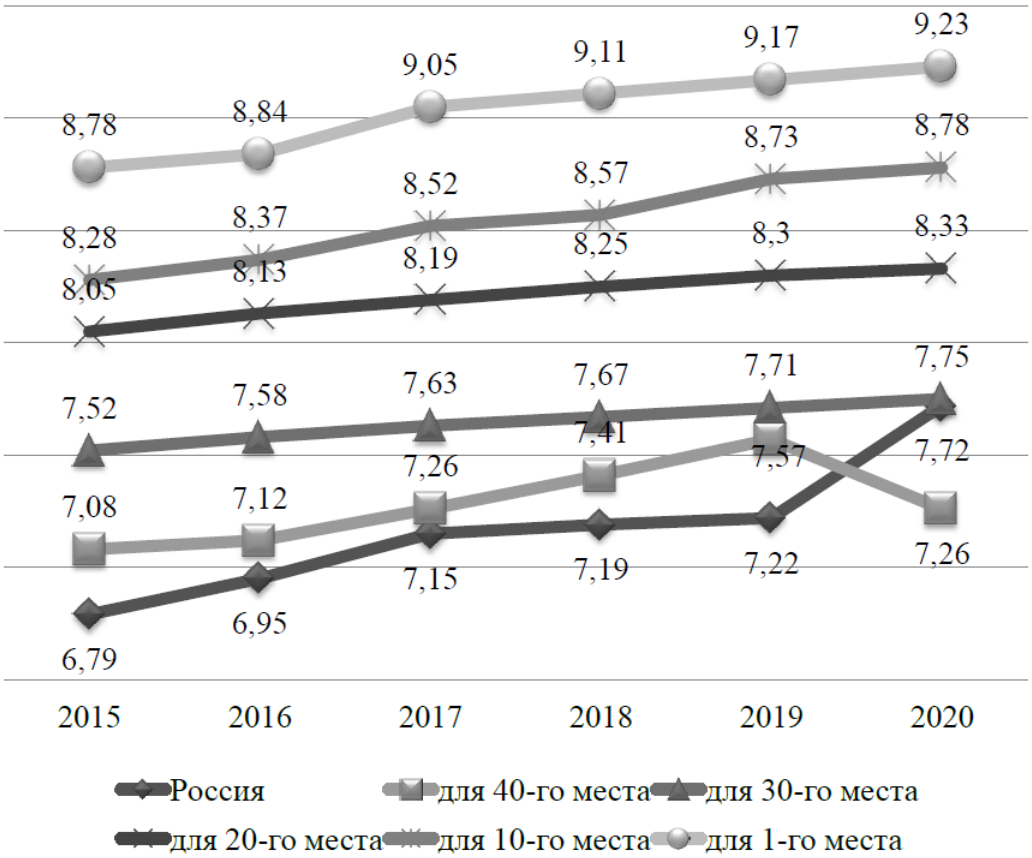
На сегодняшний день есть тренд в сфере ИТ, который можно сравнить с изобретением Интернета – это облачные технологии. Они позволяют открыть новые горизонты для развития бизнеса. К ним можно отнести организацию новых видов услуг, таких как привлечение покупателей через новые каналы взаимодействия, персональное страхование, повышение лояльности за счет индивидуального обращения с каждым клиентом, увеличение производительности труда, рост гибкости и эффективности бизнес-процессов, диверсификация затрат [8].

Спрос на ИТ-услуги обеспечивается растущим многообразием и сложностью используемых корпоративных ИТ-систем, требующих больших затрат на установку, интеграцию, обучение и обслуживание. ИТ-аутсорсинг, т.е. передача сторонним организациям функций по поддержке и обслуживанию ИТ-инфраструктуры, является одним из перспективных направлений на данном рынке.

Также необходимо рассматривать позиции в рейтинге Индекса развития ИКТ как индикатора уровня ИБ в стране. При этом можно спрогнозировать увеличение пропускной способности мирового интернет-канала, значительный рост которой замечается у большинства стран. Наиболее бурное развитие мобильного и стационарного высокоскоростного Интернета в домашних хозяйствах необходимо рассматривать как дополнительный «драйвер роста». Остальные подындексы применения ИКТ остаются на прежнем уровне. Не следует ожидать значительной динамики, но при этом необходимо их фиксировать для сохранности имеющегося рейтинга. Динамика среднесрочного прогноза, основанная на ступенчатой экстраполяции показателя Индекса ИКТ, находящихся с 1-й по 40-ю позицию в рейтинге, с включением России, при неизменной динамике текущих значений по 11 критериям, Индекс до 2020 года, в котором наша страна занимает место не выше 25-го, представлена на рисунке.

Данный прогноз был сформирован таким образом, что в первую очередь анализировалась динамика значения Индекса стран, которые занимали первую строку в рейтинге. Этот показатель является верхним интервалом Индекса, , после этого анализ повторялся для тех стран, которые занимали 2-е место. Выбранные данные являлись верхним интервалом для государств, которые в 2017–2020 гг. займут 3-е место в рейтинге. Эта процедура повторялась для всех позиций до 40-го места (значение России за последние 2 года).

В итоге анализ показал, что уровень Индекса развития ИКТ в России не достигнет и 30-го места. В настоящее время разрыв со страной, занимающей 30-е место (Мальта), находится на уровне 10 % (0,71 пункта) и его преодоление при нынешнем положении



Прогноз показателя Индекса развития ИКТ на 2017–2020 годы (составлен автором по материалам [3])

развития страны без существенного изменения политики состояния ИБ невозможно. Следовательно, давая оптимистические оценки, можно предположить, что в 2017 г. Россия займет 37–39-е место, обойдя Польшу и Португалию, которые находятся на 44-й и 43-й позиции соответственно.

Библиографический список

1. *Белокуров С.В., Сотников Н.В., Лунёв Ю.С.* Моделирование информационных угроз и действий по защите информации в интегрированных системах безопасности // Охрана, безопасность, связь. 2017. № 1–2. С. 137–141.

2. *Брынцев А.Н., Перекрестов М.В.* Минимизация рисков в условиях цифровой экономики // Российский экономический интернет-журнал. 2017. № 1. С. 6.

3. Интернет-издание информационно-аналитического агентства «Центр гуманитарных технологий», 2017 г. URL: http://gtmarket.ru/ratings/ict-development-index/ict-development-index-info.

4. *Лившиц И.И., Неклюдов А.В.* Анализ существующих ИТ активов для обеспечения информационной безопасности // Вопросы защиты информации. 2017. № 1 (116). С. 46–57.

5. *Парфенова В.М.* Развитие национальной инновационной системы как стратегическая цель обеспечения национальной экономической безопасности // Наука и практика. 2017. № 1 (25). С. 101–108.

6. *Сидорина Т.Ю.* Российское общество в контексте тенденций мирового общественного развития // Мир России: социология, этнология. 2017. Т. 26. № 2. С. 128–153.

7. *Сироткин О.С., Волостнов Б.И., Поляков В.В.* Актуальные проблемы инновационно-технологического развития России // Проблемы машиностроения и автоматизации. 2017. № 1. С. 10–21.

8. *Скрыль С.В., Сычев А.М., Мещерякова Т.В.* Оценка эффективности информационных процессов в автоматизированных системах обработки данных в условиях угроз безопасности информации: концепция и возможности // Охрана, безопасность, связь. 2017. № 1–2. С. 236–243.