Экономика и защита информации

УДК 004.056
JEL: O3

ВАРЛАМОВА Светлана Борисовна
Финансовый университет при Правительстве Российской Федерации, Ленинградский просп., 49, Москва, 125993 (ГСП-3), Россия
https://orcid.org:0000-0001-6578166X
Варламова Светлана Борисовна, кандидат экономических наук, доцент Департамента финансовых рынков и банков, доцент, Москва.
E-mail: SBVarlamova@fa.ru

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ИННОВАЦИОННЫХ ПРЕДПРИЯТИЙ МСП [1]

Аннотация

Предмет/тема. Проблемы обеспечения кибербезопасности бизнеса в условиях ускоренного развития и расширения использования информационных технологий и усиления конкуренции наиболее остро стоят перед предприятиями МСП, как наиболее уязвимыми хозяйственными структура с точки зрения их априори слабых финансовых и технических возможностей защиты от киберугроз.

Вместе с тем, существует ряд направлений защиты информации, не требующих значительных капиталовложений и высококлассных специалистов в области IT-технологий, например, по части обеспечения конфиденциальности информации. С этой целью на предприятии малого и среднего предпринимательства (МСП) необходимо ввести строго контролируемый порядок в области приема, передачи, хранения информации, изучить информационные потоки, определить круг лиц, имеющих доступ к конфиденциальной информации. Важно также и введение системных инструментальных мер защиты бизнес – информации по мере финансового умощнения предприятия.

Цели/задачи. Анализ существующих рисков для инновационных предприятий МСП показывает, что на современном этапе развития российской экономики на первое место вышли риски реализации киберугроз. Целью исследования является систематизация международного и отечественного опыта инновационных предприятий малого бизнеса по обеспечению конфиденциальности бизнес-информации и защиты от несанкционированного доступа каналы информационных потоков. В задачи исследования входит анализ источников внутренних и внешних угроз безопасности информационных ресурсов предприятия как объекта защиты.

Методология. Проведение настоящего исследования осуществлялось с помощью общенаучных методов исследования, методов аналогии, сравнения и научного обобщения, представления полученных результатов

[1] Данная статья выполнена в рамках научного проекта международной межправительственной организации в составе 22 государств-членов «Международный центр научной и технической информации» № 201942 «Разработка механизмов информационного и научно-технологического обеспечения инновационного предпринимательства в условиях цифровой экономики.

в виде перечня выявленных направлений и резервов развития объектов исследования.

Вывод: Обеспечение кибербезопасности российских инновационных предприятий МСП на этапе стартапов не требует значительных финансовых вложений и может быть ограничено наведением порядка в работе с бизнес-информационными потоками, однако по мере финансового умощнения инновационного предприятия МСП необходимо выявление возможных источников потери информационной конфиденциальности и внедрения методов аппаратного контроля ее прохождения, блокировки попадания вирусной инфекции в локальные сети предприятия и др. В этих целях целесообразно пользование услугами специализированных аутсорсеров.

***Ключевые слова*:** *МСП, инновационная деятельность, инновационное предприятие, ИТ-технологии, бизнес-информация, киберугрозы, кибербезопасность, ИТ-аутсорсинг, ИБ-аутсорсинг.*

Economy and protection of information

Svetlana B. Varlamova, Ph.D., Associate Professor, Department of Financial Markets and Banks, Financial University under the Government of the Russian Federation, Moscow, Russian Federation
E-mail: SBVarlamova@fa.ru

CYBERSECURITY PROBLEMS OF SME INNOVATIVE ENTERPRISES

Abstract

Subject / Topic The problems of ensuring business cybersecurity in the context of accelerated development and expansion of the use of information technologies and increased competition are most acute for SMEs, as the most vulnerable economic entities in terms of their a priori weak financial and technical capabilities to protect from cyber threats. At the same time, there is a number of areas of information protection that do not require significant investment and high-quality specialists in the field of IT technologies, for example, in terms of ensuring confidentiality of information. To this end, small and medium-sized enterprises (SMEs) need to introduce a strictly controlled procedure for receiving, transmitting and storing of information, study information flows, and determine the number of persons who have access to confidential information. It is also important to introduce system-wide tool measures to protect business information as the company becomes financially more powerful.

Goals/Objectives The analysis of existing risks for innovative SME enterprises shows that at the current stage of development of the Russian economy, the risks of cyber threats have come to the forefront. The purpose of the research is to systematize the international and domestic experience of innovative small businesses in ensuring the confidentiality of business information and protecting from unauthorized access to information flows. The purpose of the research is to analyze the sources of internal and external threats to the information security of the enterprise's information resources as an object of protection.

Methodology This research was carried out using general scientific research methods, methods of analogy, comparison and scientific generalization, presenting the results in the form of a list of identified directions and reserves for the development of research objects.

Conclusion and Relevance The cybersecurity of the Russian innovative SMEs in the start-up does not require significant financial investments and may be limited only by working out the order in the work of the business information flow. However, with financial growth of innovative enterprises, SMEs need to identify possible sources of loss of information privacy and implement the methods of hardware control, blocking, hitting viral infection in the local network of the enterprise, etc. For these purposes, it is advisable to use the services of specialized outsourcers.
Keywords: *SME, innovative activity, innovative enterprise, IT technologies, business information, cyber threats, cybersecurity, IT-outsourcing, IS-outsourcing*.

Введение. В научной литературе и в хозяйственной практике понятие «предпринимательская деятельность» трактуется примерно одинаково, но имеет некоторые нюансировки, связанные по большей части с конкретными её видами. С точки зрения изучения проблем развития и повышения эффективности малого и среднего предпринимательства наиболее точную формулировку этого понятия содержит Гражданский Кодекс РФ, в котором указано: «Предпринимательская деятельность — это самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг лицами, зарегистрированными в этом качестве в установленном законом порядке» (ст.2 ГК РФ).

Современное состояние рынка товаров и услуг характеризуется высоким уровнем конкуренции между товаропроизводителями. Крупное товарное производство имеет безусловные конкурентные преимущества перед малым и средним бизнесом в части хотя бы снижения доли постоянных расходов на единицу продукции в ее себестоимости, а значит и конечной для потребителя рыночной цены, за счёт масштабов производства. В связи с этим, малому и среднему предпринимательству (МСП) для выживания крайне важно найти эффективное решение: либо существенно снизить себестоимость собственной продукции, либо найти рыночную нишу, не занятую крупными товаропроизводителями учитывая ряд причин, например, в случае производства уникальной, ориентированной на конкретного потребителя продукции или услуги, и/или требующей применения ручного труда при производстве и т.п.

Реализация первого пути – существенное снижение себестоимости продукции, сопоставимой по качественным характеристикам с продукцией крупных товаропроизводителей, для малого и среднего предпринимательства – задача крайне сложная, практическим не выполнимая. Тем не менее, в определённой мере она может решаться за счет роста производительности труда. При этом простая интенсификация труда без использования более совершенных в сравнении с применяемыми

на конкретном производстве технологиями не обеспечивает необходимых в конкурентной борьбе успехов.

Реализация второго пути – поиск тех рыночных ниш, которые не заняты крупными товаропроизводителями, большинству предпринимателей МСП представляет более продуктивным. Эти ниши формируются в связи с новыми возможностями, создаваемыми стремительно развивающимися процессами разработки и использования новейших технологий собственно для производства, а также для повышения его эффективности с применением новейших достижений производственного и финансового менеджмента.

Таким образом, проблема выживания и развития МСП в современных условиях конкуренции подталкивают их к инновационной деятельности.

Основная часть. Научное исследование требует четкости в применении терминологии, поэтому сошлемся на формулировку понятия «инновационная деятельность», содержащуюся в федеральном законе «О науке и государственной научно-технической политике» от 23.08.1996 № 127-ФЗ (последняя редакция): «Инновационная деятельность - деятельность (включая научную, технологическую, организационную, финансовую и коммерческую деятельность), направленная на реализацию инновационных проектов, а также на создание инновационной инфраструктуры и обеспечение ее деятельности». Другими словами, инновационная деятельность — это практическое использование инновационно-научного и интеллектуального потенциала в массовом производстве с целью получения нового продукта, который удовлетворяет потребительский спрос в конкурентоспособных товарах и услугах. [1]

Анализ научной литературы и нормативные акты показывают, что наряду с термином «инновационная деятельность предприятия» используется термин «инновационное предприятие», причем нет указаний на наличие каких-либо существенных различий между ними. Так, в особенности в научной литературе, часто встречаются определения, подобные следующим: «Инновационное предприятие – организация, деятельность которой связана с формированием, воплощением в реальность инноваций» [2] или «Инновационным предприятием является коммерческая организация, которая осуществляет практическую реализацию технологий, содержащих конфиденциальные сведения технического, экономического, административного, финансового или иного характера, и получает наибольшую долю доходов от создания и последующей реализации инновационной продукции или вследствие применения инновационных технико-технологических процессов».[3]

В приведенных выше и большинстве других определений понятия «инновационное предприятие» к таковым относятся и предприятия создающие новые технологии, и предприятия, внедряющие уже созданные кем-то новые технологии в собственный производственный цикл. Поэтому

считаем допустимым применение термина «инновационное предприятие» в отношении тех субъектов малого и среднего бизнеса, в деятельности которого инновации играют ведущую роль (по некоторым оценкам не менее 70%). В число таких предприятий, по нашему мнению, могут быть включены и предприятия, разрабатывающие новые технологии, например, предприятия финтеха, и предприятия, использующие их для производства материальных благ и услуг.

В современном мире, в условиях информационной революции основным полем создания и внедрения новаций практически в любой сфере науки и материального производства является развитие и использования ИТ-технологий. В сфере науки современные ИТ-технологий обеспечивают непрерывность процессов обработки, хранения и передачи информации, ее эффективное использование, способствуют существенному ускорению темпов научно-технического прогресса, открывают новые возможности и перспективы для решения ранее не решаемых задач.

В сфере производства и распределения материальных благ информационные технологии позволяют менеджменту анализировать запасы сырья, комплектующих, готовой продукции в режиме *non stop*, проводить маркетинговые исследования для прогноза спроса на различные виды продукции, находить новых партнеров и многое другое. Поэтому в современных условиях существующие предприятия МСП активно приобщаются к использованию IT-технологий, а новые изначально ориентируются на них.

Выполнению важнейшей национальной задачи – развитие и повышение эффективности МСП в России – должно способствовать изучение и распространение опыта успешного функционирования малых и средних предприятий, в первую очередь, зарубежного, накопленного за несколько десятилетий работы на рынке. Результаты изучения этого опыта могут оказаться полезными как для конкретных предпринимателей, так и для государственных органов регулирования и надзора этого сегмента национальной российской экономики, так как дают представление о проблемах МСП и путях их решения как в период до начала информационной революции, так и в период ее ускоренного развития.

Естественно, что в настоящее время наибольший интерес для российских исследователей и практиков представляет анализ количественных и качественных показателей инновационных предприятий, функционирующих в различных странах мира.

Важнейшим из количественных показателей можно считать долю малых инновационных предприятий в зарубежных экономиках. Так, в общем количестве промышленных предприятий малый инновационный бизнес составляет в Ирландии 75%, в Германии 62%, в Норвегии 49%, во Франции 38%. В Индии и Китае инновационно-активными являют не менее 60% всех малых предприятий. [4]

Там же отмечается, что «…именно малый бизнес дает около 50% всех нововведений и большинство новейших технологий, роль которых в европейских странах весьма значительна... В сфере малого бизнеса осуществляется значительная часть всех инноваций в США, например, малый бизнес производит в 13 раз больше патентов и осваивает вдвое больше нововведений, чем крупные корпорации». [5]

По способу формирования существует несколько основных моделей предприятий МСП.[6] Для российских условий наиболее характерна первая модель создания и функционирования предприятий МСП, однако при многих крупных корпораций достаточно активно идет процесс возникновения старт-апов, развивающихся по второй модели.

Первая модель формирования малых компаний является наиболее простой и, как следствие, наиболее распространенной моделью формирования субъектов малого бизнеса в сфере инноваций выступает *кооперация мелких инновационных групп и коллективов*, состоящих, как правило, из наиболее активных и креативных научных работников (исследователи, изобретатели, рационализаторы и т.д.), основной задачей которой выступает проведение в жизнь и реализация проектов, связанных с выпуском на рынок инновационных продуктов (услуг) в целях получения коммерческой прибыли. Особенностью данной модели выступает взаимообусловленность сотрудничества, вследствие того, что каждая из групп, обладая лишь частью знания (теория, технология, адаптация и т.п.), не в состоянии дать конечный продукт, и для успеха реализации проекта необходим весь спектр усилий кооперированных коллективов.

Вопрос аккумуляции необходимого для успеха проекта стартового капитала решается, главным образом, за счет взноса личных средств участников-соучредителей проекта, выделения в распоряжение проекта части капитала юридических лиц, сотрудники которых участвуют в проекте, а также за счет привлечения денежных средств внешних инвесторов – от небольших компаний до транснациональных корпораций, коммерческих банков, инвестиционных банков, венчурных компаний и прочих заинтересованных участников финансового рынка.

Указанные выше агломерации субъектов малого бизнеса в области инноваций объединяют, как правило, новообразованные коллективы (компании), обладающие гибкостью в сфере принятия решений, способностью действовать в условиях экономической неопределенности и принимать на себя высокие риски. Разумеется, не все проекты заканчиваются успехом, но в случае успеха, вознаграждение, связанное с выходом на рынок инновационного продукта (услуги), оказывается высоким сообразно риску, а проект в целом – высокоприбыльным.

Необходимо выделить пять ступеней развития малых компаний и их агломераций, действующих в области выпуска инновационных продуктов (услуг):

- «сид (sid)» – организационный период;
- «старт-ап (start-up)» – период запуска;
- «гроу (grow)» – период роста;
- «экспанжн (expansion period)» – период расширения;
- «эксит (exit)» – период свертывания бизнеса и выхода из него.

Как показывает практика, наиболее активны и продуктивны малые инновационные компании показывают на этапах роста и расширения, то есть те компании, которые действуют на рынке не более 5 лет – именно на их долю приходятся основные успехи в создании новых товаров (услуг), выпущенных с применением инновационных технологий и ноу-хау.

Это позволяет назвать 3 и 4 этапы развития «периодом вознаграждений». При этом динамично развивающийся бизнес не только позволяет учредителям компенсировать понесенные затраты и получить существенную прибыль, но также выполняет и социальную роль, выражающуюся, главным образом, в создании новых рабочих мест, что особенно важно в регионах, удаленных от столиц и крупных городов и от их финансовых возможностей.

Динамично развивающиеся малые инновационные компании, получившие в специальной литературе наименование *«газелей»*, на сегодняшний день создают от 75 до 80% новых рабочих мест в Европе, в то время как их число среди зарегистрированных хозяйствующих субъектов не превышает 5 %.

Второй моделью формирования малых компаний, действующих в сфере развития инноваций, выступает *формирование организационных структур внутри крупного предприятия (корпорации) с образованием самостоятельного юридического лица.* Данная модель имеет как преимущества, так и недостатки. Преимуществом является обеспеченность капиталом, помещениями, станками, оборудованием, инструментом, оргтехникой и т.п., а также разделением рисков с «материнской» компанией. К недостаткам следует отнести меньшую гибкость в принятии стратегических решений, так как их необходимо согласовывать с руководством «материнской» компании, а кроме того, необходимость делиться с последней полученной прибылью, причем доля прибыли, причитающейся «материнской» компании, может быть весьма высокой. Также немаловажно то, что все инновационные разработки, сделанные малым предприятием такого типа, оказываются, как правило, достоянием все той же «материнской» организации. В то же время, такая форма позволяет опередить самостоятельные малые компании в конкурентной борьбе и заполучить свою долю рынка.

Третьей моделью формирования малых компаний выступает *создание организационных структур внутри крупного предприятия (корпорации) без образования самостоятельного юридического лица.* Фактически, такие коллективы, носящие, как правило наименование ПБ (проектных бригад) и

ВТК (временных творческих коллективов), являются структурными подразделениями большой компании, сотрудники которых получают лишь зарплату (как правило, большую, чем сотрудники других подразделений компании). Такие коллективы еще больше зависят от прихоти руководства «материнской» фирмы, однако одновременно они выступают потенциальными самостоятельными хозяйствующими субъектами. В России данная организационная модель выступает зачастую как своего рода «золотой парашют» для руководства «материнской» корпорации: риски и затраты, связанные с разработкой инновационного продукта/услуги приходятся на долю «материнской» компании, а в случае успеха ПБ или ВТК преобразуется в самостоятельное юридическое лицо, унося с собой все права на разработанный продукт. При этом бывший «куратор» проекта, как правило, становится владельцем и руководителем новой малой компании.

Развитие малого и среднего бизнеса в условиях современной России проходит в довольно жесткой конкурентной среде. Предприятия МСП вынуждены изыскивать пути повышения конкурентных преимуществ, принимать меры, направленные на их реализацию для повышения своей конкурентоспособности, использовать новые рыночные методы и инструменты, чтобы обеспечить необходимую доходность деятельности, удержать и расширить свою рыночную нишу в условиях постоянно меняющейся конъюнктуры рынка. Такие методы и инструменты создают современные информационные технологии, которые объективно становятся одним из главных факторов развития и повышения конкурентоспособности предприятий МСП.[7]

Применение современных информационных технологий создает для предприятия МСП возможности:

– быстро и четко доводить до сведения потребителей информацию о своей продукции и ее преимуществах, размещенной в соответствующих каталогах в электронной форме;

– осуществлять заказы на покупку нужных предприятию товаров и услуг без посредников и магазинных «накруток»;

– привлекать к сотрудничеству высококвалифицированных специалистов в качестве фрилансеров;

– переводить часть сотрудников на дистанционный режим работы и экономить на затратах на аренду офисного помещения и др.

Однако использование информационных технологий наряду с несомненными достоинствами несет в себе новые риски – киберугрозы[15]. В их числе могут быть угрозы: кражи денежных средств; кражи конфиденциальной информации; вбросы в систему коммуникации с клиентурой фейковых сообщений о финансовом состоянии предприятия, его продукции, его планах, способных существенно подорвать доверие клиентов и контрагентов к предприятию, понизить его рыночную

репутацию, наконец, нарушить порядок и сроки протекания автоматизированных производственных процессов и др.

Ученые-аналитики и предприниматели-практики отмечают рост репутационных и бизнес-рисков в сфере предпринимательства, связанных с расширением использования IT-технологий в деятельности инновационных предприятий. Эти опасения отразились на результатах глобального опроса российских инвесторов, аналитиков и руководителей предприятий, проведенного компанией «PricewaterhouseCoopers» в 2019 году.

Установлено, что почти половина опрошенных (41%) полагают, что наибольшую опасность для бизнеса и репутации компании в 2018 году составили кибератаки. Такой результат можно увязать с активным ростом подверженности киберугрозам предприятий МСП. Так, если в 2017 году жертвами кибератак стали 11% таких предприятий, то в 2018 году их число удвоилось и дошло до 22%.

Опрос выявил также наиболее опасные с точки зрения кибератак направления бизнеса: телекоммуникации (+70% за год), развлечения и медиа (+26%), промышленное производство (+28%), фармацевтика и здравоохранение (+13%) и финансовые услуги (+2%). Поэтому в целях сохранения высокой рыночной репутации, а также снижения финансовых потерь необходимо особое внимание к вопросам кибербезопасности. По данным Опроса такого мнения придерживаются 64% респондентов.

Исследование показало, что интересы киберпреступников в области МСП, кроме кражи денежных средств, распространяются на такую информацию, как списки клиентов (регулярных покупателей продукции предприятия), их реквизиты, включая почтовые адреса и контактные телефоны, имена владельцев и менеджеров, финансовые и производственные интересы, включая банковские расчетные и карточные счета, способы контактов и конкретные контракты с фирмой-поставщиком и др.

Интересы киберпреступников могут локализоваться в области получения информации о ценовой политике и в целом рыночной стратегии предприятия - жертвы кибератаки, а также его производственные процессы, применяемые технологии, состав и техническое состояние основных производственных фондов, номенклатура и характеристики выпускаемой продукции вплоть до ее дизайна, а также планы расширения и модернизации производства, источники инвестиционного финансирования, уровень квалификации и настроение персонала и многое другое.

В рамках «V Российского форума малого и среднего предпринимательства» (май 2019 года, Москва) проведено обсуждение результатов исследования Общероссийской общественной организации малого и среднего предпринимательства «ОПОРА РОССИИ», в ходе которого было констатировано, что большая часть предпринимателей

малого и среднего бизнеса нуждаются в рекомендациях по выявлению киберугроз и методам противостояния им.

Своеобразным резюме Форума и его результатом стали рекомендации, сформулированные в «Лаборатории Касперского» и опубликованные как «Советы по кибербезопасности для малого бизнеса: понимание основ»: «Киберпреступников интересуют ваши деньги, ваши данные и ваше IT-оборудование. Если хакер получит доступ к вашей корпоративной сети, то для нанесения ущерба компании он может использовать все, что он в ней найдет…». [8, 16] Однако, как показала практика, большинство предпринимателей МСП, в особенности тех из них, чей бизнес находится на этапах «сид», «старт-ап» или «гроу» с этими рекомендациями не знакомы.

Вместе с тем, рекомендаций «Лаборатории Касперского» опираются на широко известные в мировой практике рекомендации по защите малого и среднего предпринимательства от киберугроз, собранные в «Полное руководство по кибербезопасности для малого и среднего бизнеса — 2020» (обновлено 8.01.2020). [9,17] Автором Руководства является Ариэль Хохстадт - поборник онлайн-конфиденциальности и соучредитель vpnMentor, а в прошлом - Gmail менеджер по маркетингу по всему миру. Состав рекомендаций по защите малого и среднего предпринимательства от киберугроз для наглядности представлен в виде схемы направлений защиты данных и бизнеса. (Рисунок 1).

Первая группа мер – исключение возможности утечки или кражи важной для предприятия конфиденциальной информации и данных.

К наиболее уязвимым местам предприятия с точки зрения кибербезопасности относится жизненно важная для него информация и данные, разглашение которых может дать конкурентам возможность срочно скорректировать свою стратегию на рынке и «переманить клиентуру» (покупателей, потребителей), принять соответствующие меры для снижения или уничтожение конкурентных преимуществ этого предприятия. К числу такой информации может быть отнесен широкий круг сведений о предприятии, начиная от интеллектуальной собственности до информации и о клиентах и контрагентах предприятия, их наименования, номера банковских счетов, адреса, контактные телефоны, факсы и другие реквизиты. Жизненно важными часто оказываются данные: о финансовом состоянии предприятия, в частности: данные инвентарных ведомостей, сведения об объемах производства, о планах развития и др.

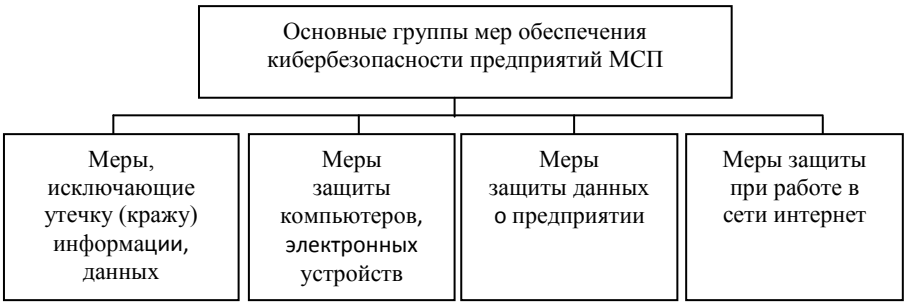

Рисунок 1 – Основные меры защиты предприятий МСП от киберугроз (Составлено автором в соответствие с рекомендациями, опубликованными в «Полное руководство по кибербезопасности для малого и среднего бизнеса — 2020»

Источник: https://ru.vpnmentor.com/blog. [9].

Поэтому в числе самых первых мер обеспечения кибербезопасности должна стать инвентаризация – тех мест в технологии предприятия и действий сотрудников, где может произойти утечка или кража конфиденциальной информации и данных, например, при удаленных контактах с клиентами и контрагентами.

В целях исключения или, по крайней мере, существенного снижения риска утечки или кражи конфиденциальной информации необходимо определить, описать и зафиксировать в качестве внутрифирменного документа все действия, которые должны выполняться руководством и всеми сотрудниками предприятия при соборе, сохранении и уничтожении устаревшее и более ненужной информации и данных.

Вторая группа мер – защита компьютеров, серверов и прочих электронных, других устройств, задействованных в создании, сборе, хранении и уничтожении конфиденциальной информации и данных.

Киберугрозы для предприятия МСП возникают в связи с тем, что компьютеры и другие электронные устройства имеют непосредственный доступ к интернету, посредством которого осуществляется распространение вредоносных вирусов и патогенных программ.

Для исключения или снижения киберрисков необходимо:

– установить на компьютеры предприятия новые или самые последние версии того программного обеспечения, с которым работает предприятие и делать это регулярно. Это мероприятие существенно снижает риск кибератак в связи с тем, что хакерам нужно некоторое время, чтобы исследовать новую версию с целью выявления так называемых «багов», то есть таких мест в программе, куда можно встроить вредоносный вирус или подпрограмму, с помощью которых осуществить кражу денег, информации или важных данных о предприятии;

– защитить компьютеры (компьютерную сеть) от вредоносных вирусов и программ путем подключение их к интернету через VPN-сервис, который обеспечивает автономность работы компьютера (компьютерной сети) предприятия. Эта мера способствует исключению внедрения патогенных вирусов и программ в компьютер или локальную сеть предприятия. Кроме того, надежный VPN-провайдер всегда предупреждает пользователей, когда они пытаются перейти на другой сайт по подозрительным ссылкам;

– установить файрвол «firewall» – технологический барьер, для предотвращения несанкционированного или нежелательного сообщения между компьютерными сетями или хостам, например, при подключении к ДБО. Файрвол отфильтровывает и пропускает через защищенную часть сети только авторизованный трафик и не позволяет злоумышленникам вычленить опознавательные данные каждого компьютера для внедрения в него вредоносных вирусов и программ.

Третья группа мер – защита данных предприятия МСП. Определившись в рамках первой группы мер по обеспечению кибербезопасности предприятия МСП с основными объектами защиты – конфиденциальная информация о предприятии, о его рыночной стратегии, о его клиентах и контрагентах и данные о финансовом состоянии, объемах производства и др., необходимы меры, исключающие утечку или потерю данных. В их числе:

– внедрить процедуры резервного копирования важных данных, которое может быть полным (данные копируются и сохраняются полностью) или частичным (копируются и сохраняются только наиболее важные данные или те данные, которые потребуются для расчетов, планирования и т.п. в некотором будущем). Скопированные данные в электронной форме хранятся на изолированных от внешнего мира и внутренней компьютерной сети устройствах или носителях, например, на флэшках. Доступ к этим устройства должно иметь крайне ограниченное число ответственных лиц из числа руководства предприятия;

– зашифровать важную информацию, размещаемую и сохраняемую в облаке (хранилища типа Dropbox) и оберегать ключи шифрования от случайной загрузки в облако. Предприятию на этапах «сид», «старт-ап» или «гроу» целесообразно работать с бесплатным сервисом BitTorrent Sync. Сервис предоставляет доступ к файлам по модели P2P, которые используют самое продвинутое шифрование (AES-256) и поддерживают двухфакторную аутентификацию;

– защитить пароли. С этой целью рекомендуется следующие простые, не требующие дополнительных пояснений меры (шаги, как они названы в Руководстве):

1. Для разных сервисов следует использовать разные пароли.

2. Необходима периодическая смена паролей.

3. Избегать установку простых паролей (такие пароли просто запомнить сотрудникам фирмы, но также просто и «расшифровать» киберпреступникам). Поэтому необходимы сложные пароли, например, микс из цифр и букв в разных регистрах (не менее 7 знаков).

4. Следует исключить автоматизированное заполнение логинов и паролей для входа в систему.

5. Следует использовать двухэтапную верификацию.

6. Составить перечень всех используемых на предприятии паролей (менеджер паролей — программу, где в зашифрованном виде хранятся все пользовательские пароли).

7. Исключить отправку по электронной почте или в СМС любого пароля, используемого на предприятии. Установить порядок обновления паролей и доведения их новых версий для конкретных пользователей внутри предприятия:

– установить порядок выдачи и аннулирования разрешений на доступ к информации. Учетные записи администратора должны быть только у уполномоченного администрировать системы и устанавливать новое ПО сотрудников предприятия. При увольнении или перемещении внутри предприятия сотрудника, имевшего доступ к работе с компьютерной сетью или электронными устройствами, вход в которые требовал введения пароля, пароли к ним должны быть незамедлительно изменены;

– обеспечить защиту беспроводных сетей. Необходимость защиты возникает при приеме и передаче информации и данных с использованием сети Wi-Fi. В этом случае необходимо обязательно удостовериться, что активированы все функции безопасности, которыми оснащены устройства, поддерживающие подключения по Wi-Fi. Кроме того, необходимо ограничить доступ к сети Wi-Fi только для определенных компьютеров, задав точки доступа;

Четвертая группа мер – защита информации при работе в интернете. Возникновение киберугроз при работе в сети интернет при незашифрованном подключении или случайном входе на опасные сайты, а также небрежное отношение сотрудников, работающих дистанционно к сохранению конфиденциальной информации, данных и принадлежащих им ноутбуков и смартфонов от доступа к ним посторонних, утери или кражи. Эта группа мер пресечения киберугроз включает:

– установить защиту от не санкционированного входа путём подключения компьютеров (компьютерной сети) предприятия к интернет сети через VPN-сервис, который обеспечивает автономность работы компьютера (компьютерной сети) предприятия;

– обеспечить защиту важных данных, созданных сотрудниками, работающими дистанционно.

Опасность возникает, когда такие сотрудники работают с устройствами (домашний компьютер, ноутбук, гаджет), не подключенными к локальной компьютерной сети предприятия и пользуются публичными точками Wi-Fi. Такая опасность реализуется также при потере сотрудником своего ноутбука или гаджета, а также при их краже. Для предотвращения угроз необходимо установить такое подключение или установить VPN-приложение, которое будет шифровать все данные, передаваемые через эти устройства. Следует также озадачить сотрудников, работающих дистанционно, необходимостью строгого соблюдения сохранности

созданной ими конфиденциальной информации или данных, а также принадлежащих им электронных устройств от попадания их в третьи руки.

Большая часть из перечисленных мер не требуют значительных усилий и затрат, однако ряд процессов, обеспечивающих деятельность предприятия МСП в условиях конкурентной среды, связанных с использованием современных информационных технологий, например, облачных или более «продвинутой» технологии блокчейна порождают угрозы, устранение которых требует специальных знаний и навыков, что под силу только высококвалифицированным специалистам, именуемым в просторечии «айтишнитками». [10]

У предприятия малого предпринимательства априори, а у среднего, как правило, нет средств на приобретение дорогостоящего оборудования и поддержку технических средств, на содержание квалифицированных специалистов, обучение персонала и т.п. Поэтому практически треть его представителей доверяют решение вопросов информационной безопасности сотрудникам, не имеющим опыта в этой области.[11] На это обстоятельство указывают и данные, полученные в результате исследования, проведенное в конце 2019 года «Лаборатории Касперского», и потому российский малый бизнес по-прежнему уязвим к киберугрозам.

Вместе с тем, вполне очевидно, что с развитием ИТ- технологий и расширением использования их в бизнесе объем атак на компании всех масштабов будет только расти. В этих условиях наиболее эффективным способом удовлетворения потребности предприятий МСП в обеспечении информационной безопасности является передача этих функций специализированному аутсорсеру. Как показывает зарубежная практика, аутсорсинг информационной безопасности (ИБ-аутсорсинг) — наименее затратный способ поддержания приемлемого уровня информационной защиты.

В российских условиях по причине практически полного отказа крупных ИТ-аутсорсеров сообщества финтеха сотрудничать с предприятиями МСП проблему помощи этим предприятиям в части обеспечения информационной безопасности берут на себя коммерческие банки, в первую очередь те из них, который обслуживают малый и средний бизнес. Так, ИБ-аутсорсинг для предприятий МСП предлагает на рынок дочернее предприятие крупнейшего ритейлового банка страны ПАО «Сбербанк» - компания BI. ZONE. Компания со второго полугодия 2019 года запустила новое направление бизнеса – управляемые сервисы кибербезопасности (Managed Security Services, MSS).[12] Компания на базе собственного Центра мониторинга и реагирования на инциденты кибербезопасности (Security Operation Center, SOC) предоставляет предприятиям МСП облачные решения и сервисы для защиты ИТ-инфраструктуры на базе компании BI.ZONE. Все сервисы развернуты во внутренней инфраструктуре BI.ZONE и территориально размещены таким

образом, чтобы обеспечить пользователям высокую доступность и надежность MSS. В их основу легли собственные технологические разработки компании и экспертные модели для определения различных инцидентов кибербезопасности. Предлагаемые компанией BI.ZONE MSS-сервисы предоставляют облачные решения для защиты электронной почты, противодействия DDoS-атакам и атакам на веб-приложения, а также услуги по администрированию средств защиты, мониторингу и реагированию на инциденты.

Подобные структурные подразделения созданы в ряде других ведущих российских банков с высокой долей предприятий МСП в клиентской базе. Среди них ПАО ВТБ, АО «Тинькофф Банк», АО «Газпромбанк» и др.

Заключение. Развитие информационных технологий, расширение их использования в бизнес-процессах способствует росту киберугроз для бизнеса, что актуализирует проблему обеспечения его кибербезопасности. Особенно остро эта проблема встает перед МСП так, как реализация практически любой из них приводит к гибели предприятия.

Вместе с тем, в соответствие с Законом № 209-ФЗ в России на государственном уровне именно МСП придается мощный импульс развития [13].

Паспорт национального проекта «Малое и среднее предпринимательство и поддержка индивидуальной предпринимательской инициативы»[14] включает 5 Федеральных проектов, содержащих условия, реализация которых позволит выполнить государственное задание: увеличить число занятых в сфере МСП на 30% с 19,2 до 25 млн. человек, доли МСП в структуре ВВП в 1,4 раза с 22,3 до 32,5%, доли экспорта субъектами МСП с 8,6 до 10%. Каждый из этих проектов учитывает зарубежные и отечественные теоретические наработки и опыт создания и функционирования предприятий МСП, в том числе основы обеспечения кибербезопасности в конкурентной среде.

Недостаток специальных знаний, недостаток или отсутствие финансирования на организацию собственной системы защиты от киберугроз на предприятиях МСП обусловливает потребность в сотрудничестве аутсорсерами, специализирующихся на ИБ-аутсорсинге, а также тех, которые предлагают его на рынок в числе других продуктов и услуг ИТ-аутсорсинга. Поэтому создание и функционирование основной массы научно-технологических и проектно-конструкторских старт-апов в области МСП в российских условиях с большой долей вероятности целесообразно в рамках *второй модели,* а производственно-хозяйственного назначения — в рамках *третьей модели* формирования малых компаний. Однако, несмотря на финансово-технологическую мощь материнской корпорации, обеспечение кибербезопасности потребует использования ИБ-аутсорсинга, способного учесть индивидуальные для каждого предприятия особенности информационных потоков. В этом залог рост

числа и развитие предприятий ИТ-технологий и ИБ-аутсорсинга, в том числе малых.

Список источников:

1. Марутян (2018) – *Марутян А.А. Инновационная основа деятельности предприятия // Молодой ученый*. — 2018. — №43. — С. 242-243. — URL https://moluch.ru/archive/229/53366/ (дата обращения: 07.03.2020).

2. Корчагин Ю.А. *Инновационное предприятие это* Доступно на сайте: https://center-yf.ru/data/ip/innovacionnoe-predpriyatie-eto.php (Дата обращения 3.0.3.2020)

3. Основные направления политики администрации США в сфере малого и среднего бизнеса Доступно на сайте: https://rustradeusa.org/Attachment.aspx?id=319 (Дата обращения 3.0.3.2020)

4. Королев (2017) – *Королев В.И. Механизмы инновационного развития малого бизнеса в зарубежных странах*. // Российский внешнеэкономический вестник. № 11. 2017 с. 52-60.

5. Махмуд Аль Хамзе, Кузубов (2017) – *Аль-Равашдех Хамзе Махмуд, Кузубов А.А. Мировая практика формирования малого инновационного бизнеса* //Azimuth of Scientific Research: Economics and Administration. 2017. Т. 6. № 3(20).

6. Овсяницкая, Подповетная, Подповетный (2017) – *Овсяницкая Л.Ю., Подповетная Ю.В., Подповетный А.Д. Пути решения проблем обеспечения информационной безопасности малого бизнеса*. // Управление в современных системах №3(14) 2017, с.19-25.

7. Кикоть (2017) – Кикоть И.Р. *Анализ угроз информационной безопасности предприятия, занимающегося научно-исследовательской и производственной деятельностью*.// Молодой исследователь Дона. №1(4). 2017.С.39-45.

8..Советы по кибербезопасности для малого бизнеса: понимание основ. Доступно на сайте: https://www.kaspersky.ru/resource-center/preemptive-safety/small-business-cyber-security (Дата обращения 9.03.2020)

9. Полное руководство по кибербезопасности для малого и среднего бизнеса — 2020 (Обновлено 8.01.2020) Доступно на сайте: https://ru.vpnmentor.com/blog. (Дата обращения 9.03.2020).

10. Кораблев, Бобкин (2018) – *Кораблев А.Ю., Бобкин Р.Е. Информационные технологии как фактор повышения конкурентоспособности предприятий малого и среднего бизнеса* // Азимут научных исследований: экономика и управление Т. 7. № 1(22). 2018. С.44-47

11. Авдеева, Чаплыгина (2017) – *Авдеева Е.А., Чаплыгина У.А. Особенности развития малого и среднего бизнеса в информационной среде* // Научно-методический электронный журнал «Концепт». - 2017. - № S13. - 0,2 п.л. Доступно на сайте: URL: http://e-kon-cept.ru/2017/470166.htm (Дата обращения 9.03.2020).

12. BI.ZONE открывает направление аутсорсинга кибербезопасности. Доступно на сайте: https://www.anti-malware.ru/news/2019-07-10-1447/30119 (Дата обращения 24.02.2020).

13. Федеральный закон «О развитии малого и среднего предпринимательства в Российской Федерации» от 24.07.2007 № 209-ФЗ (в ред. от 27.12.2019)

14. Паспорт национального проекта «Малое и среднее предпринимательство и поддержка индивидуальной предпринимательской инициативы». Доступно на сайте: URL: http://government.ru/info/35563/ (дата обращения: 15.03.2020).

Douglas Maughan, David Balenson, Ulf Lindqvist, Zachary Tudor (2013) – *Douglas Maughan, David Balenson, Ulf Lindqvist, Zachary Tudor. Crossing the 'valley of death': Transitioning cybersecurity research into practice*. Published in: IEEE Security & Privacy (Volume: 11, Issue: 2, March-April 2013). Pages 14-23. United States.

Bhattacharya (2015) – *Bhattacharya D. Evolution of cybersecurity issues in small businesses* / 4th Annual ACM Conference on Research in Information Technology at University Hawaii – 29 September 2015. United States. https://ieeexplore.ieee.org/abstract/document/6493323

Guaman, Calvo-Manzano, Feliu (2018) - *Rea-Guaman M., Calvo-Manzano J.A., Feliu, T.S. A prototype for cybersecurity management in small companies*. Materials of the conference on information systems and technologies, CISTI / Volume 2018-June. CISTI 2018; Spain / / Electronic resource. Access Mode: https:
//www.researchgate.net/publication/326050298_A_prototype_to_manage_cybersecurity_in_small_companies

Reference:

Marutyan (2018) – *Marutyan A.A. The innovative basis of an enterprise* // Young scientist. - 2018. – No. 43. - p. 242-243. – URL https://moluch.ru/archive/229/53366/ (accessed: 03/07/2020).

Korchagin Y.A. *An innovative enterprise*. Electronic resource: https://center-yf.ru/data/ip/innovacionnoe-predpriyatie-eto.php (accessed 3.0.3.2020)

The main directions of the policy of the US administration in the field of small and medium-sized businesses. Electronic resource: https://rustradeusa.org/Attach-ment.aspx?id=319 (Date of acccess 3.0.3.2020)

Korolev V.I. Mechanisms for the innovative development of small businesses in foreign countries. // Russian Foreign Economic Bulletin. No. 11. 2017 p. 52-60

Al-Ravashdeh Khamze Mahmoud, Kuzubov A.A. World practice of formation of a small innovative business // Azimuth of Scientific Research: Economics and Administration. 2017. Vol. 6. No. 3 (20).

Ovsyanitskaya L.Y., Povetovnaya Y.V., Podpovetny A.D. Ways to solve the problems of ensuring information security of small businesses. // Management in modern systems No. 3 (14) 2017, pp. 19-25.

Kikot (2017) – Kikot I.R. Analysis of threats to the information security of an enterprise engaged in research and production activities. // Young researcher of Don. No. 1 (4). 2017. p. 39-45.

Cybersecurity advices for Small Businesses: Understanding the Basics. Electronic resource: https://www.kaspersky.ru/resource-center/preemptive-safety/small-business-cyber-security (Date of access 9.03.2020)

The Complete Guide to Cybersecurity of Small and Medium Businesses - 2020 (Updated 8.01.2020) Electronic resource: https://en.vpnmentor.com/blog. (Date of access 03.03.2020).

Korablev, Bobkin (2018) – Korablev A.Y., Bobkin R.E. Information technology as a factor in increasing the competitiveness of small and medium-

sized enterprises // Azimuth of Scientific Research: Economics and Management. 2018. V. 7. # 1 (22) p. 44-47

Avdeeva, Chaplygina (2017) – Avdeeva E.A., Chaplygina U.A. Features of the development of small and medium-sized businesses in the information environment // Scientific and methodical electronic journal "Concept". - 2017. - No. S13. - 0.2 p.p. Electronic resource: http://e-kon-cept.ru/2017/470166.htm. (Date of access 03.03.2020).

BI.ZONE opens the direction of outsourcing cybersecurity. Electronic resource: https://www.anti-malware.ru/news / 2019-07-10-1447 / 30119 (Date of access 02.24.2020).

The Federal Law “On the Development of Small and Medium Enterprises in the Russian Federation” dated July 24, 2007 No. 209-FZ (as amended on December 27, 2019)

Passport of the national project “Small and medium-sized enterprises and support of individual entrepreneurial initiative” Electronic resource: http://government.ru/info/35563/ (date of access: 03.15.2020).

Douglas Maughan, David Balenson, Ulf Lindqvist, Zachary Tudor (2013) – *Douglas Maughan, David Balenson, Ulf Lindqvist, Zachary Tudor. Crossing the 'valley of death': Transitioning cybersecurity research into practice*. Published in: IEEE Security & Privacy (Volume: 11, Issue: 2, March-April 2013). Pages 14-23. United States.

Bhattacharya (2015) – *Bhattacharya D. Evolution of cybersecurity issues in small businesses* / 4th Annual ACM Conference on Research in Information Technology at University Hawaii – 29 September 2015. United States. https://ieeexplore.ieee.org/abstract/document/6493323

Guaman, Calvo-Manzano, Feliu (2018) - *Rea-Guaman M., Calvo-Manzano J.A., Feliu, T.S. A prototype for cybersecurity management in small companies*. Materials of the conference on information systems and technologies, CISTI / Volume 2018-June. CISTI 2018; Spain p. 680-685 [Electronic resource] Access Mode: https: //www.researchgate.net/publication/326050298_A_prototype_to_manage_cybersecurity_in_small_companies (Date of access 02.24.2020).

Статья поступила 31.03.2020; принята к публикации 10.04.2020г. Автор прочитали и одобрили окончательный вариант рукописи. The article was received on 31.03.2020; accepted for publication on 10.04.2020. The author has read and approved the final version of the manuscript.