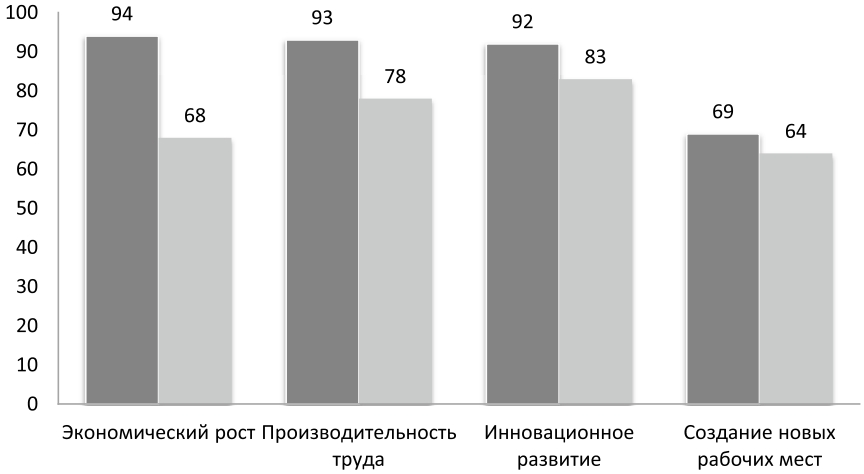


*Рис. 3. Ожидаемое влияние развития технологий ИИ в течение 5 лет (2019-2024),%*

Существуют различные причины выявленных результатов исследования. Около 37% респондентов заявили, что у них нет необходимости в подобных технологиях, 28% сказали, что сфера их деятельности не подразумевается использование ИИ. Примерно 11% признались, что причина отсутствия соответствующих технологий – это недостаток достаточных знаний о них, а 8% заявили, что их смущает достаточно высокая стоимость их внедрения. Еще 6% отказываются от использования потому, что у них маленькая компания, а 4% потому, что в России слабо развиты подобные технологии. Около 4% просто не доверяют современным технологиям и предпочитают человеческий труд.

Так, можно выделить три основные причины отказа бизнеса от использования технологий искусственного интеллекта. Первая – это отсутствие таких наглядных кейсов, которые доказывали бы эффективность данных технологий. Вторая – отсутствие доступных решений и массовых продуктов в данной сфере. Третья причина – нехватка компетенций на рынке.

Таким образом, проведя исследование опыта внедрения искусственного интеллекта на предприятиях, рассмотрев его возможности, стоит утверждать, что у искусственного интеллекта в сфере управления имеются как сложности, так и большие перспективы развития. Современные программные решения создают хорошие возможности для роста и совершенствования компаний. Использование новых технологий для оптимизации процессов управления в компаниях оправдано (рис. 3). Кроме того, что искусственный интеллект облегчает процесс работы, осуществляя задачи на основе заложенных алгоритмов, он способствует более эффективному использованию времени сотрудников, которое может быть направлено на решение глобальных вопросов, с которыми справится только человек.

**Список литературы**

1. Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации»// [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/72738946/

2. Искусственный интеллект (рынок России)// [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_(рынок_России)?source=post_page

3. Петров А.А. Человек, искусственный интеллект и управление // [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/chelovek-iskusstvennyy-intellekt-i-upravlenie

4. Официальный сайт Gridnine Systems.// [Электронный ресурс]. URL: https://gridnine.com/

5. Портал искусственного интеллекта.// [Электронный ресурс]. URL: http://www.aiportal.ru/news/13566.html

## ТЕНДЕНЦИИ РОССИЙСКОГО РЫНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Гулятченко А.Р., Чепурченко А.А.

*Южно-Российский институт управления РАНХиГС, Ростов-на-Дону, e-mail: gulyatchenko@bk.ru*

В данной статье рассматривается российский рынок информационной безопасности в современных условиях, в том числе отмечено влияние пандемии на функционирование рынка ИБ. Выявлены основные тенденции и перспективы развития рынка информационной безопасности. Отмечено влияние информационной безопасности на рынок труда. В статье проводится исследование нормативно-правовой базы, на основе которой функционирует рынок информационной безопасности России.

Информационные технологии играют важную роль в обеспечении реализации стратегических национальных приоритетов РФ – ускоряется экономическое развитие государства и формируется информационное общество. Но за расширением областей применения информационных технологий следует возникновение новых информационных угроз. В связи с нестабильной геополитической ситуацией в мире, возрастанием числа террористических и экс-

тремистских организаций, внедрение информационных технологий без систем обеспечения информационной безопасности, опасно и может нанести ущерб международной безопасности и стратегической стабильности.

В Российской Федерации стратегические цели и направления обеспечения информационной безопасности в различных областях описываются в Доктрине информационной безопасности от 6 декабря 2016 года. Согласно Доктрине в области науки, технологий и образования основными направлениями обеспечения информационной безопасности являются достижение конкурентоспособности российских информационных технологий и развитие научно-технического потенциала в области обеспечения ИБ, создание устойчивых к различным видам воздействия технологий, развитие кадрового потенциала, обеспечение защищенности граждан от информационных угроз и пр.

Сегодня на российском рынке информации безопасности наблюдается недостаток аналитических данных, на основе которых можно было бы сформировать объективное представление о текущем положении на данном рынке и его тенденциях развития. Трудности, обусловленные острым дефицитом аналитических данных и традиционной закрытостью рынка ИБ, в свою очередь порождают противоречивые и в большинстве случаев ошибочные суждения о ситуации. Для отечественных производителей средств защиты такие заблуждения характеризуются потерей времени и денег, снижением потенциала импортозамещения на рынке.

В начале 2019 года интернет сайтом Anti-Malware был опубликован проект открытого исследования рынка информационной безопасности в России [1]. Исследование проводилось посредством обезличенного онлайн-опроса на сайте, и было направлено на определение зрелости рынка, его ёмкости и потенциала. Также Anti-Malware поставил перед собой задачу, которая заключалась в определение проникновения на рынок отдельных продуктовых групп, вероятность инцидентов ИБ и варианты реагирования на них.

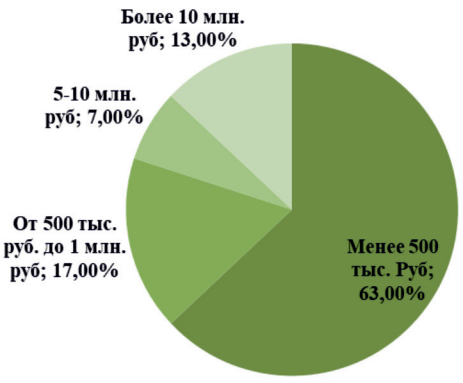


*Рис. 1. Бюджет на информационную безопасность в год*

Результаты исследования (рис. 1) показали, что подавляющее число компаний (63%) выделяют на развитие и внедрение технологий информационной безопасности менее 500 тыс. руб. в год. Бюджет на ИБ у 17% респондентов составляет от 500 тыс. руб. до 1 млн. рублей в год, ещё 7% могут позволить себе вкладывать в ИБ 5-10 млн. руб., и 13% компаний выделяют более 10 млн. руб. из собственного бюджета. Из исследования видно, что большая часть российских компаний выделяет недостаточно денежных средств на обеспечение информационное безопасности. В основном, выделяемые минимальные бюджеты могут обеспечить могут лишь базовые средства защиты (например, антивирусы или межсетевые экраны).

Так же исследование Anti-Malware (рис. 2) выявило недостаток специалистов, способных обеспечивать ИБ в организациях. У 27% опрошенных компаний вообще отсутствуют специалисты в данной сфере, а у подавляющего большинства (54%) опрошенных информационной безопасностью занимаются от 1 до 5 специалистов. Только у 8% компаний на обеспечение ИБ выделено более 20 сотрудников из штата.

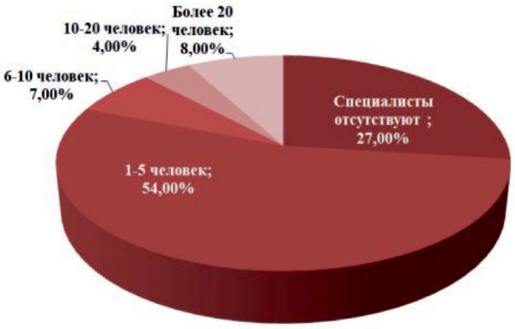


*Рис. 2. Количество специалистов, выделенных на обеспечение ИБ в организациях*

Бесспорно, технологии открывают перед бизнесом новые возможности. Но поскольку абсолютно совершенная техника ещё не создана, всегда существуют риски сбоя, перегрева, поломки, поэтому необходимы специалисты, способные эффективно управлять рисками. К сожалению, только у небольшого количества компаний существует комплексный подход к защите от киберугроз.

Но, не смотря на все недостатки, российский рынок информационной безопасности уверенно растёт и развивается. По оценке TAdviser (рис. 3), объём данного рынка в 2019 году увеличился на 14% и составил 90,6 млрд. руб [2].

В 2020 году уверенный рост на российском рынке систем информационной безопасности продолжается. Среди российских компаний наблюдается тенденция к росту уровня понимания рисков информационной безопасности и последствий, связанных с ней инцидентов.

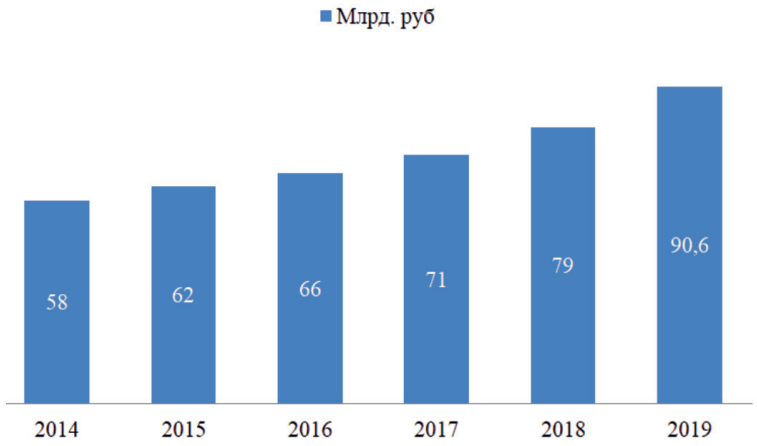


*Рис. 3. Объем рынка Информационной безопасности*

В процессе анализа, было установлено, что в 2020 году самым важным событием на рынке ИБ является массовый переход огромного числа компаний на удалённый режим работы. Организациям, чтобы остаться «на плаву» в период пандемии, пришлось экстренно перестраиваться, менять свой подход к обеспечению информационной безопасности, применять новые технические средства для распознавания `свой-чужой`, в том числе, с использованием разработок в области искусственного интеллекта. В результате существенно возросла нагрузка на ИТ и ИБ-подразделения в организациях и пришло осознание важности высокой киберграмотности сотрудников для предотвращения инцидентов.

Влияние пандемии на рынок информационной безопасности колоссально. 18% российских компаний (и 22% в мире) планируют увеличить штат сотрудников в области кибербезопасности не менее чем на 5% [3]. Рост востребованности специалистов в данной сфере подтверждается российской компанией интернет-рекрутмента HeadHunter. В период с января по октябрь 2020-го года было открыто почти 30 тыс. вакансий для таких специалистов (для сравнения за весь 2018 год было открыто 17 тыс. вакансий). Данная ситуация обусловлена ростом числа цифровых сервисов, систем и объектов, которые нуждаются в защите от киберугроз.

Рынок старается соответствовать постоянно изменяющимся запросам потребителей – появляются новые игроки, генерируются новые решения, совершенствуются существующие средства защиты информации, развивается законодательство в данной области.

В последние годы, благодаря усилиям государства, наметилась тенденция постепенного замещения чисто западных разработок российскими решениями. Обусловлено это не только тем, что основными потребителями средств ИБ являются госсектор и крупный бизнес, но и появлением проектов, представляющих собой качественную отечественную альтернативу зарубежным. Таким образом, проводимая в России политика по импортозамещению предоставляет широкий спектр возможностей по развитию внутреннего рынка информационных технологий в целом и рынка информационной безопасности в частности. Так же современная политика нашего государства способствует выполнению отечественными разработчиками постоянно растущих требований заказчиков, а, следовательно, и повышению качества продукции.

Ужесточение законодательство так же стимулирует развитие отрасли и повышение качества продукции, обеспечивающей информационную безопасность.

Наблюдается рост числа проектов, направленных на приведение ИБ-инфраструктуры сообразно требованиям регуляторов: проектов в области защиты критической информационной инфраструктуры, исполнения требований ГОСТ Р 57580.1−2017 для финансовых организаций, а также ужесточившихся требований ФЗ-152 «О защите персональных данных» в отношении локализации данных граждан РФ на территории страны.

Можно сделать вывод, что активно развивается российское законодательство в сфере регулирования информационной безопасности, на рынке появляются отечественные продукты, которые по качеству не уступают импортным. Теперь проанализируем перспективы развития российского рынка информационной безопасности.

В результате исследования было выявлено, что пандемия существенно не повлияла на пла-

ны «Лаборатории Касперского» – всемирно известной российской компании, занимающейся разработками систем защиты от разнообразных киберугроз. Ежемесячно «Лаборатория Касперского» делает прогнозы на ближайшее будущее на основании ревизии текущих продаж. Как отмечают эксперты, свои ожидания на 2020 год, выведенные ещё до начала пандемии, в компании не меняли. Пока «Лаборатория Касперского» идёт с превышением плана в среднем на 3-5%.

В Infowatch слово «прогноз» стало ругательным. Специалисты считают, что в сложившейся ситуации относительно адекватный прогноз можно сделать лишь в перспективе 3-х месяцев. Что касается конца года, представитель Infowatch полагает, что рынок еще даст возможность их компании отыграть от ожидавшихся продаж в лучшем случае 70%, в худшем – порядка 60% [4].

По мнению экспертов такая ситуация сложилась из-за привязки продаж Infowatch к бюджетам, а бюджеты заложены. Если государство не вмешается и не предпримет действий по возврату этих денег, то у компании появиться возможности отыграть эти цифры.

Согласно заявлению представителей Positive Technologies, по состоянию на конец мая 2020 года компания придерживалась изначально установленной планки – рост на минимум 30% [5].

Подводя итоги, можно сказать, что в свете сложившейся в мире ситуации информационная безопасность становиться более заметной как в бизнес среде, так и на государственном уровне. Ввиду того, что число компаний, которые переходят на схемы ведения бизнеса в онлайн формат, увеличивается, вопрос обеспечения информационной безопасности становится одним из ведущих. На основании всего вышесказанного, можно заключить, что российский рынок информационной безопасности в перспективе ожидает уверенный рост.

**Список литературы**

1. Шабанов И. «Анализ рынка информационной безопасности в России. Часть 1.»// [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Market_Analysis/analysis-information-security-market-russia-part-1 (Дата обращения: 18.11.2020)

2. Информационная безопасность (рынок России)// [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_(рынок_России) (Дата обращения: 18.11.2020)

3. Балашова А. «Эксперты спрогнозировали дефицит специалистов по кибербезопасности»// [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/02/11/2020/5f9c494a9a7947a702aa761f (Дата обращения: 18.11.2020)

4. Официальный сайт InfoWatch. AI-анализ информационных потоков для управления рисками ИБ// [Электронный ресурс]. URL: https://www.infowatch.ru (Дата обращения: 18.11.2020)

5. Официальный сайт Positive Technologies. Сколько стоит информационная безопасность// [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/is-cost-2017/?sphrase_id=79283 (Дата обращения: 18.11.2020)

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВО ВРЕМЯ УДАЛЕННОЙ РАБОТЫ

Дрекслер Д.И.

*Южно-Российский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Ростов-на-Дону, e-mail: drekslerd01@mail.ru*

В данной статье рассматриваются проблемы влияния пандемии COVID-19 на информационную безопасность организаций во время удаленной работы. На основе мнения экспертов рассмотрены распространённые способы атак ИТ-преступников. А также различные способы обеспечения кибербезопасности во время удаленной работы. Предоставлены данные мировых расходом на обеспечение информационной безопасности 2020 года и сделаны выводы на их основе.

Современное общество давно уже является компьютеризированным. Но особенно это стало ощущаться в последнее время. Из-за пандемии COVID-19 большинство сотрудников пришлось перевести на удаленную работу, что в разы увеличило целевые атаки злоумышленников на информационные системы организаций. Поэтому вопрос о защите информации в данной ситуации стал очень важным.

Ранее удаленную работу было проще контролировать ИТ и ИБ службам, сейчас подключение стало массовым и организация безопасности сложнее, так как обеспечить защиту каждому домашнему компьютеру работника достаточно трудно.

Основой исследования данной темы послужили мнения экспертов. Антивирусная компания Eset сообщила о том, что злоумышленники различными способами наживаются на сложившейся ситуации. Они используют тему коронавируса в фишинговых письмах и атаках на результаты и лечение от COVID-19. От имени Всемирной организации здравоохранения и других известных организаций преступники рассылают вредоносные письма, которые в огромном потоке информации сложно отличить от обычных [1].

Примерно 45 % атак происходит самым грубым образом. Так как из-за экономии и неподготовленности многие компании пренебрегли встроенной блокировкой и другими ограничениями на подключение (например, VPN), киберпреступники, собрав учетные данные, путем многократных попыток получают логин и пароль, проходят аутентификацию и взламывают систему простейшим образом.

Так, эксперты по безопасности Лаборатории Касперского отмечают, что количество платформ для проведения онлайн-конференций возросло и поэтому количество вредоносных файлов, которые эксплуатируют названия