

десорбционной способности (не менее 5 циклов регенерации) материалы утилизируют путем пиролиза с получением тепловой энергии или в качестве смолистых добавок в асфальтобетонные смеси при производстве дорожного покрытия.

Заключение

Была рассмотрена перспективность применения определенных сорбционных материалов на основе промышленных отходов для ликвидации разливов нефтепродуктов с поверхности воды. Установлено, что данные сорбенты обладают механической прочностью, хорошей сорбционной способностью по нефтепродуктам, гидрофобностью, плавучестью, а также возможностью их регенерации и повторного использования.

Экономические науки

ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ РОССИЙСКОГО РЫНКА ИБ

Арутюнян Э.А.

ЮРИЙ РАНХУГС, Ростов-на-Дону,
e-mail: elino4karut@gmail.com

В данной статье проведен анализ российского рынка информационной безопасности. Определены основные тенденции и перспективы, а также исследованы направления влияния в будущем. Определены основные тренды данного рынка, выделяемые российскими ИБ-компаниями. Отмечена востребованность специалистов в сфере ИБ и дальнейший рост. Описаны проблемы, с которыми предстоит столкнуться, и даны прогнозы развития рынка информационной безопасности в России.

На сегодняшний день наблюдается стремительный рост киберпреступлений. Так, например, на недавно прошедшем международном форуме Академии Управления МВД РФ «Стратегическое развитие системы МВД России: состояние, тенденции, перспективы» Group-IB, международная компания, которая специализируется на предотвращении кибератак, представила отчет, в котором был приведен резкий рост числа киберугроз и определены основные тенденции компьютерных преступлений в период пандемии COVID-19. Экспоненциальный рост компьютерных преступлений спровоцировал повышение спроса на Российском рынке информационной безопасности (ИБ) у многих компаний, которые предпочитают увеличить свои расходы на ИБ в 2021 году [1]. Именно поэтому возникают вопросы о том, какие тенденции преобладают на этом рынке и как они повлияют на его развитие в ближайшем будущем.

Данная тема не может не вызывать интерес, так как люди постоянно сталкиваются с мошенничеством. Конечно, это заставляет задуматься о том, как компании борются с киберпреступно-

Список литературы

1. Мизеровский Л.Н., Почивалов К.В. К вопросу о применимости правила фаз к системам аморфно-кристаллический полимер-жидкость // Химия и химическая технология. 2007. Т. 50. Вып. 3. С. 72-78.
2. Бухарова Е.А., Татаринцева Е.А. Применение композиционного сорбента на основе терморасширенного графита в природоохраных технологиях: II Международная молодежная научная конференция. Часть 2. Белгород: Издательство БГТУ, 2014. С. 28-32.
3. Краснов К.С. Физическая химия. М.: Высшая школа, 2001. 512 с.
4. Heuss-Aßbichler S, John M., Huber A.L. A new procedure for recovering heavy metals in industrial wastewater WIT Transactions on Ecology and The Environment. Vol. 202. P. 85-96.
5. Бухарова Е.А., Татаринцева Е.А., Серебряков А.В., Нагар Ю.Н. Получение полимерных композиционных сорбентов на основе терморасширенного и окисленного графита для очистки водных объектов от нефтепродуктов // Водочистка. 2015. С. 20-25.

стью, насколько сейчас развита информационная безопасность и российский рынок в данной сфере. Основой данного исследования послужил опрос среди представителей российских ИБ-компаний, проведенный интернет-порталом TAdviser летом 2020 года.

Начать анализ хотелось бы с того, что объем российского рынка средств информационной безопасности по итогам 2019 года увеличился на 14% и достиг отметки в 90,6 млрд рублей. Также положительную динамику позже мы сможем отметить и опираясь на мнения экспертов в данной области.

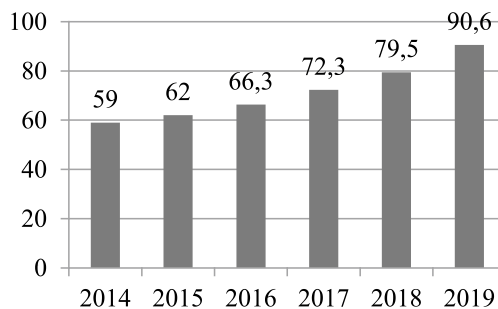


Рис. 1. Объем рынка ИБ в России

Эпидемия коронавируса и вызванный ей режим удаленной работы привел к ускорению цифровой трансформации, которая стала залогом выживания для многих предприятий [2]. Нельзя сказать, что изоляция внесла значительные изменения в общие тренды и направления в сфере ИБ, но существенно сместила акценты на процессную часть большинства направлений. Многие компании взяли курс на то, чтобы сделать кибербезопасность эластичной, так как раньше к информационной безопасности относились как к набору средств для защиты корпоративного периметра, однако теперь, понятие корпоративного периметра размыто.

Итак, TAdviser опросил экспертов следующих ИБ-компаний: «С-Терра СиЭсПи», «CEO Phishman», «Angara», «Аладдин Р.Д.», «Онланта» (входит в группу «Ланит»), «EveryTag», «Калуга Астрал», «СёрчИнформ», «Positive Technologies» и «Инфосистемы Джет».

Вначале стоит отметить, что пандемия затронула все отрасли экономики и рынок информационной безопасности не исключение. Эксперты отметили, что ИБ-компании столкнулись с трудностями при переходе на удаленный режим работы. Многим организациям пришлось перестраиваться на ходу, такие переходы оказались довольно болезненными для бизнеса. Именно поэтому большинство компаний остаются частично на «удаленке» даже после отмены всех ограничений, чтобы снова не пострадать от подобных резких переходов.

Но многие аналитики ищут и положительные стороны, то есть оптимистично оценивают перспективы российского рынка ИБ. Они считают, что такой опыт экстренного закрепления ресурсов в форс-мажорных обстоятельствах 2020 года является катализатором развития спектра решений по информационной безопасности. Проблемы, с которыми пришлось столкнуться компаниям, помогли понять: какие существуют пробелы в этой области, обратить внимание на вопросы готовности к безопасному «цифровому» взаимодействию с клиентами и партнерами. Такой стрессовый период позволяет проверить на прочность представителей данного рынка. Опираясь на вышесказанное, нельзя не согласиться с данными экспертами. Произошёл некий толчок для рынка ИБ – работать, развиваться, уметь справляться с трудностями и продолжать действовать, несмотря на сложившуюся ситуацию.

В приведенном опросе аналитики выделили основные тенденции рынка информационной безопасности. Так директор департамента развития технологий компании «Аладдин Р.Д.» отмечает, что на данный момент многие организации стремятся максимально обеспечить информационную безопасность, и это стремление намного больше, чем было ранее. Как мы уже выделяли, киберпреступность выросла, во многом это связано из-за перехода компаний в онлайн формат, естественно это повлечет за собой некую переоценку ценностей на рынке, и каждая организация будет пытаться принять все меры защиты своего бизнеса. Очевидно, что спрос на системы защиты неминуемо произойдет. Таким образом, рынок ИБ потерпит скорее перераспределение, нежели драматическое падение.

Генеральный директор «EveryTag» полагает, что с ростом угроз в будущем все больше организаций предполагают инвестировать в новые технологии ИБ. Так как ИБ идет в ногу с развитием практически любой технологии, очевидно серьезное увеличение инвестиций в информационную безопасность в целом.

По мнению руководителя Дирекции информационной безопасности компании «Калуга Астрал», с появлением новых угроз, будут и новые средства борьбы с ними. Начнется активное внедрение искусственного интеллекта (ИИ) в решения по защите информации, именно ИИ возьмет на себя часть функций специалистов по информационной безопасности, будет принимать оперативные и ситуационные решения.

Директор по развитию бизнеса «Positive Technologies» [3] отмечает, что возможны изменения ландшафта российского рынка ИБ, за счет потерь некоторых компаний, который не смогут оптимизировать свои затраты и выдержать этот тяжелый год. Компании могут столкнуться с заморозкой проектов вследствие блокировки бюджетов, с удлинившимися сроками поставки оборудования, а также с увеличением числа инцидентов ИБ.

Компания «InfoWatch» [4] подчеркивает то, что основными кибератаками для промышленных предприятий остаются атаки через корпоративный сегмент и доставка вредоносных программ через USB. Часто именно из-за недостаточной квалификации ИБ-кадров, промышленные предприятия не могут разобраться в огромном количестве информации, поступающей с разнообразных средств мониторинга. Тенденция, о которой пойдет речь, это комплексное решение, позволяющее промышленным предприятиям построить эшелонированную защиту, основанную на полноте данных со всех средств защиты. Это позволяет еще на уровне инцидентов оперативно обнаружить атаки на промышленные системы.

Помимо мнений экспертов, важно отметить, что из-за перехода на дистанционный режим работы появилась востребованность специалистов в сфере ИБ, которая привела к дефициту кадров. Снова же это связано с увеличением рисков атак на ресурсы компаний. Проведем сравнительный анализ. Если в 2018 г. было открыто свыше 17 тысяч вакансий, то за 2020 (с января по октябрь) уже почти 30 тысяч. Еще более быстрыми темпами растут резюме ИБ-специалистов: в 2018 г. их было 18 тысяч, в 2019 – 25 тысяч, а за неполный 2020 – уже свыше 55 тысяч. Мы можем предположить, что и в 2021 году будет наблюдаться такой недостаток кадров в сфере ИБ.

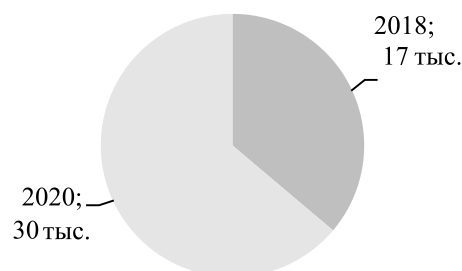


Рис. 2. Открыто вакансий

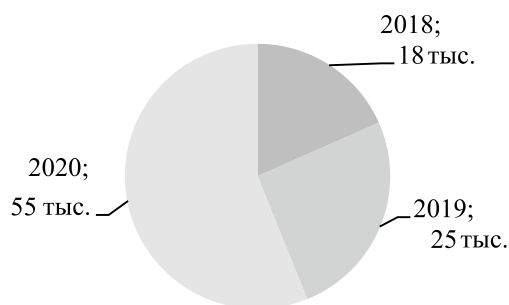


Рис. 3. Рост резюме

По нашему мнению, в будущем на российском рынке ИБ будет сохранена положительная динамика. Во всей сфере ИБ наблюдается рост показателей, поскольку компании инвестируют в решения, обеспечивающие удаленную работу и защиту от кибератак. Сейчас идет активный процесс внедрения современных цифровых технологий в различные сферы жизни, и за счет этого растет киберпреступность, а вместе с ней и спрос на обеспечение безопасности. Но нельзя говорить о полном отсутствии негативных трендов на рынке ИБ. Основная проблема в том, что после снятия ограничений есть вероятность появления определенных изменений в бизнесе ИБ-компаний. Например, переведенные проекты в онлайн не будут восстановлены в офлайн режим, также очевидно, что возникнут проблемы с персоналом.

Таким образом, опираясь на мнения экспертов и анализ, проведенный в процессе исследования, можно сделать вывод, что рынок информационной безопасности переживает пандемию легче других отраслей экономики. Хотя ИБ-компании и столкнулись с определенными сложностями, но большинство смогли адаптироваться к ограничениям, вызванным коронавирусом, и оперативно перешли на удаленный режим работы. Компаниям в сфере ИБ удалось избежать значительного сокращения выручки и бюджета, за счет того, что спрос на предлагаемые ими продукты и товары остался востребованным, и даже вырос. Именно поэтому перспективы и тенденции большинства опрошенных экспертов были положительными. Мы предполагаем, что в будущем рынок ИБ будет продолжать расти, но не исключаем того, что, возможно, в 2021-ом году появятся новые сложности. Но будем надеяться, что и с ними российский рынок информационной безопасности успешно справится и будет продолжать свое активное развитие.

Список литературы

1. ANTI-MALWARE [Электронный ресурс]. – информационно-аналитический центр. – Режим доступа: <https://www.anti-malware.ru/news/2020-11-02-111332/34111> (дата обращения: 16.11.2020).
2. CNEWS [Электронный ресурс]. – электронный журнал. – Режим доступа: https://www.cnews.ru/reviews/security2020/articles/obzor_rynka_ib (дата обращения: 16.11.2020).

3. POZITIVE TECHNOLOGIES [Электронный ресурс]. – официальный сайт. – Режим доступа: <https://www.ptsecurity.com/ru-ru/> (дата обращения: 24.11.2020).

4. INFOWATCH [Электронный ресурс]. – официальный сайт. – Режим доступа: <https://www.infowatch.ru/> (дата обращения: 24.11.2020).

5. Tadviser [Электронный ресурс]. – официальный сайт. – Режим доступа: <https://www.tadviser.ru/> (дата обращения: 13.11.2020).

6. Group IB [Электронный ресурс]. – официальный сайт. – Режим доступа: <https://www.group-ib.ru/> (дата обращения: 14.11.2020).

ОСНОВНЫЕ ИТ-СЕРВИСЫ CRM СИСТЕМ

Брагина В.Ю.

Южно-Российский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Ростов-на-Дону, e-mail: vikspiksi21@mail.ru

В данной статье рассматриваются CRM системы, раскрываются их функции, преимущества и недостатки. Исследуются основные возможности внедрения данных систем в производство. Раскрывается сущность нескольких отечественных CRM систем, а так же сравниваются наиболее популярные из них. Так же приводятся примеры успешных компаний, которые внедрились в свою деятельность данные системы. А согласно, опыту экспертов выделены условия, при соблюдении которых возможно эффективное внедрение CRM.

Современные предприятия начинают применять новые технологии для увеличения конкурентоспособности и прибыли.

Целями внедрения CRM в современном обществе являются: увеличение доли повторных продаж, углубленный мониторинг работы менеджеров, разрешение проблемных вопросов в продажах, существенное снижение показателя потерь клиентов, повышение стоимости «среднего чека» сделки, расширение клиентской базы, внедрение эффективной системы мотивации продавцов, снижение переменных и постоянных расходов, усиление координации бизнеса между подразделениями, уменьшение количества рекламаций. Впервые эта тема была затронута в 1987 году, выйдя на информационный рынок под авторством Пэта Саливана и Майка Мюнейла, разработавших первую CRM-систему [7]. Лидерами по внедрению CRM систем являются финансовая отрасль и торговая (рис. 1).

Выделяют три основных вида CRM систем: операционная, аналитическая, коллаборационная. CRM – системы выполняют следующие функции: учёт клиентов; управление продажами; построение различных статистических отчетов; оценивание эффективности маркетинговых каналов; прогнозирование продаж и планирование изменений [3]. По результатам исследования Института проблем предпринимательства, CRM-системы используют 14% рос-