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

этих сервисов, в ближайшее время будут увеличиваться. Сейчас на первом месте по кибератакам – Zoom (42,42%), на втором – WebEx (22,51%) и на третьем – GoToMeeting (12,86%).

Причинами утечки информации во время удаленной работы является: использование незащищенной сети; использование личной техники; незащищенность удаленного канала компании; доступность корпоративных ресурсов; передача рабочих документов в социальных сетях; хранение документов в личных облаках; отсутствие сертификата вшитого в устройство работника или второго фактора аутентификации. И, конечно, самым главным фактором, влияющим на утечки, служит сам человек. Большинство организаций не уделяют должного внимания обучению сотрудников правилам кибербезопасности при удаленной работе. Из-за чего использование теневых ИТ-сервисов и незащищенность перед новыми уловками преступников, появившихся в период коронавируса, увеличилось [2].

Обеспечение безопасности стоит больших усилий и средств. Малый и средний бизнес может обойтись бесплатными платформами, а вот крупный бизнес, госкорпорации, федеральные министерства и ведомства обязаны предоставлять комплексное обеспечение информационной безопасности при удаленном доступе сотрудников в соответствии с требованиями регуляторов в сфере ИБ.

Кибербезопасность – это реализация мер по защите систем, сетей и программных приложений от цифровых атак. Она является условием нормального развития современного общества.

Основными документами, определяющими подход к обеспечению информационной безопасности в РФ, являются:

– Федеральный закон РФ 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Доктрина информационной безопасности Российской Федерации;

– Закон Российской Федерации 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Стратегия развития информационного общества в Российской Федерации 2017-2030 гг.;

– Стратегия развития информационного общества в Российской Федерации 2017-2030 гг.;

– Указ Президента России 2013г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ» [3].

Но наиболее важным документом, обеспечивающим информационную безопасность, является Концепция стратегии кибербезопасности Российской Федерации [4]. Данная концепция базируется на понятии киберпространства, как сферы деятельности в информационном пространстве; а «кибербезопасность» – это совокупность условий, когда составляющие киберпространства находятся под защитой от угроз и воздействий с неприятными последствиями.

Многие компании прибегли к таким системам защиты, как безопасные VPN-соединения и многофакторная аутентификация, системы защиты от утечек (DLP) и контроля привилегированных пользователей (PIM/PAM).

Программная система VPN способна объединить две сети или отдельных пользователей сети через общедоступную открытую сеть, при этом обеспечить полную защиту данных. При подключении к VPN-серверу вся информация зашифровывается и это не позволяет киберпреступникам получить личные данные о пользователе.

В то же время VPN не всегда удобен для пользователей, из-за этого ИТ-службы обеспечивают возможность сотрудникам пользоваться корпоративными сервисами без VPN, но при этом использовать надежную многофакторную аутентификацию, позволяющую работать как с десктопных ОС, так и с личных устройств.

Многофакторная аутентификация сначала удостоверяется в личности пользователя, а только потом дает разрешение на использование каких-либо ресурсов. Самыми популярными способами являются: использование физических токенов (генерация сложных комбинаций), смартфонов (использование для аутентификации, например: Authy, Google Authenticator, ESET Secure Authentication) или биометрических данных (отпечатки пальцев, сетчатка глаза).

Система защиты от утечек информации (DLP) позволяет производить мониторинг и своевременно блокировать входящую и исходящую информацию сотрудников, отправленные файлы на внешние носители и облака с целью обеспечения безопасности.

По последним данным на первом месте по количеству внедрений проектов ИБ с учетом партнеров вендор – Rostelecom-Solar, на втором – Fortinet, на третьем – Positive Technologies, на четвертом – Cisco Systems, на пятом – Eset.

Сейчас наглядно хочу продемонстрировать изменившийся спрос в сфере развития информационной безопасности. По приведенным данным (рисунок) мы видим, что перевод на удаленную работу по-разному повлиял на сегменты информационной безопасности. Сильно повысился спрос на программы защиты конечных точек (антивирусы, EDR/XDR-системы), а также на MFA, VPN, PAM/PUM. При этом уменьшился спрос на системы защиты периметра, межсетевые экраны/NGFW и системы мониторинга безопасности. Значительно увеличилось количество проектов по направлениям многофакторной аутентификации, защиты удаленного доступа и веб-ресурсов.

Мировые расходы на обеспечение информационной безопасности

По данным специалистов, самым востребованным продуктом компании «ИнфоТеКС» за время пандемии стал ViPNet Client, обеспечивающий безопасность при передаче данных. Спрос на него увеличился вдвое по сравнению с предыдущим годом.

Наиболее динамично стала развиваться облачная безопасность. Gartner предсказывают увеличение затрат на реализацию проектов в данном сегменте на треть, так как это очень удобный способ получения требуемого количества ресурсов за короткое время. Среди популярных решений, такие как: anti-DDoS, WAF, защищенная удаленная работа (NGFW, шифрование каналов).

Особенно стоит обратить внимание на разработку трех технологий в области облачного ИБ: SASE, CSPM и CASB. Первая способна преобразовывать SD-WAN и службы сетевой безопасности, включая брандмауэр следующего поколения (NGFW), безопасный веб-шлюз (SWG), сетевой доступ к сети с нулевым доверием (ZTNA) и посреднические службы облачной безопасности (CASB), в единую модель обслуживания. Вторая – сканирует, отслеживает, обеспечивает безопасность и устраняет проблемы конфигурации в учетных записях общедоступного облака в соответствии с передовыми практиками и стандартами соответствия AWS, Azure, Google Cloud и Oracle Cloud. Третья предназначена для обеспечения единой политики безопасности предприятия при доступе к облачным ресурсам защиты данных в облаках, располагаются они между потребителями и поставщиками облачных систем [5].

Таким образом, мы видим, что многие компании беспокоятся о безопасности личных и корпоративных данных. Для защиты выделяются средства, предлагаются новые проекты, а также усовершенствуются уже существующие. ИБ и ИТ службы делают все для обеспечения комфорта и кибербезопасности организаций в режиме удаленной работы.

Список литературы

1. Tadviser [Электронный ресурс]. – официальный сайт. – Режим доступа: https://www.tadviser.ru/ (дата обращения: 20.10.2020 г.).

2. Silverfort [Электронный ресурс]. – официальный сайт. – Режим доступа: https://www.anti-malware.ru/ (дата обращения: 20.10.2020 г.).

3. КонсультантПлюс [Электронный ресурс]. – официальный сайт. – Режим доступа:
http://www.consultant.ru/ (дата обращения: 28.10.2020 г.).

4. Концепция стратегии кибербезопасности РФ [Электронный ресурс] – официальный сайт. – Режим доступа: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 23.10.2020 г.).

5. CNEWS [Электронный ресурс]. – электронный журнал. – Режим доступа: https://www.cnews.ru/analytics (дата обращения: 02.11.2020 г.)

РЕАЛИЗАЦИЯ КОНЦЕПЦИИ ЦИРКУЛЯРНОЙ ЭКОНОМИКИ

Захарова Д.А.

ФГБОУ ВО «Кемеровский государственный университет», Кемерово, e-mail: rector@kemsu.ru

Концепция циркулярной экономики зародилась относительно недавно, и сегодня, когда мировое сообщество движется к достижению Целей устойчивого развития ООН, ее актуальность только возрастает. В данной статье рассматривается практическое применение данной концепции на примере отдельно взятых стран Азиатско-Тихоокеанского и европейского регионов. Особое внимание также уделяется практике и перспективам развития циркулярной экономики в России.

Понятие цикличности имеет глубокие исторические истоки и используется в различных философских школах. Однако, активное