УДК 338.24

ТЕНДЕНЦИИ РАЗВИТИЯ ТЕХНОЛОГИЙ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ РАСПРОСТРАНЕНИЯ ЦИФРОВЫХ ПЛАТФОРМ

Тихомирова С.А.

магистрант,

Национальный исследовательский ядерный университет «МИФИ», Москва, Россия

Черепанов С.П.

аспирант,

Национальный исследовательский ядерный университет «МИФИ», Москва, Россия

Аннотация

Эпидемиологическая обстановка 2020-го года привела к необходимости развития облачных сервисов во всех индустриях. В условиях нехватки специалистов в области кибербезопасности, такой переход усложнил управление и защиту данных, сделав многие системы привлекательнее для киберпреступников и, тем самым, уязвимее к кибератакам. В статье описываются современные тенденции и угрозы, которые вызваны ускорением процесса цифровизации.

Ключевые слова: цифровая экономика, кибербезопасность, тенденции развития, большие данные, цифровизация.

TRENDS IN THE CYBERSECURITY TECHNOLOGIES DEVELOPMENT IN THE CONDITIONS OF DIGITAL PLATFORMS IMPLEMENTATION GROWTH

Tikhomirova S.A.
graduate student,
National Research Nuclear University «MEPhI»,
Moscow, Russia

Cherepanov S.P.
postgraduate,
National Research Nuclear University «MEPhI»,
Moscow, Russia

Abstract
The epidemiological situation of 2020 has led to the need to cloud services development across all industries. With a shortage of cybersecurity professionals, this change has complicated data management and protection. Thus, cloud services have become more attractive to cybercriminals and to a greater extent vulnerable to cyber-attacks. The article describes current trends and threats caused by the acceleration of the digitalization process.

Keywords: digital economy, cybersecurity, development trends, big data, digitalization.

В настоящее время пандемия COVID-19 и связанные с ней изменения ускорили цифровизацию бизнес-процессов, мобильность устройств и распространение облачных решений в большинстве организаций. Из-за изменений условий труда компаниям стало труднее обеспечивать безопасность.

Удаленная работа также увеличила использование онлайн-платформ для совместной работы, цифровых инструментов для ведения бизнеса, а также видеоконференцсвязи.

Цифровые платформы стирают границы между отраслями, формируют новые неожиданные индустриальные альянсы, а также новые индустрии [1]. Компании, которые выбирают платформенный формат ведения бизнеса, как правила, являются востребованными и быстрорастущими.

В свободное время люди все чаще стали выходить в Интернет. Все эти факторы создали огромную нагрузку на средства контроля и операции в области кибербезопасности.

Кибербезопасность должна быть центральным элементом каждого стратегического решения и важным компонентом каждого ИТ-продукта в компании. Все компании должны иметь системы для мониторинга и разработки плана реагирования на кибер сбои в цепочке поставок.

Проникновение информационных технологий во все аспекты жизни и деятельности людей, повышенная активность в сетях использования онлайн-сервисов создают новые условия, характеристики которых принято называть «цифровая экономика».

Цифровая экономика может быть описана в виде трех уровней, которые в тесном взаимодействии совместно влияют на экономическое развитие, жизнь граждан и общества в целом [3].

1. Рынки и сферы деятельности, в рамках которых осуществляется взаимодействие поставщиков и потребителей товаров, работ и услуг.
2. Платформы и технологии, в рамках которых формируются научные компетенции для развития рынков и сфер деятельности.
3. Среда, в рамках которой создаются условия для развития платформ и технологий охватывает информационную инфраструктуру, образование и кадры, информационную безопасность и т.д.

К цифровым технологиям относятся: нейротехнологии и искусственный интеллект, технологии больших данных, промышленный интернет, системы

распределенного реестра, технологии виртуальной и дополненной реальности, квантовые технологии и многие другие.

Цифровая среда строится на базе информационной инфраструктуры цифровых платформ и экономических систем [4].

Среди основных тенденций, меняющих отрасль, можно выделить следующие:

- Облака – децентрализация хранения данных.
- Мобильность – доступность информационных сервисов.
- Аналитика – появление новых сервисов и бизнес-моделей.
- Социальность – высокая скорость распространения информации.

Все отрасли подвержены киберугрозам из-за растущей цифровизации. С ростом рынка интернета вещей также увеличивается внедрение решений и интернет-услуг в приложениях ИТ-безопасности. Таким образом, внедрение интернета вещей и машинного обучения в сфере безопасности является одной из быстро развивающихся тенденций рынка кибербезопасности. В свою очередь, технология больших данных помогает компаниям изучать и анализировать потенциальные риски.

Распространение облачных вычислений также является одной из ключевых тенденций, которая способствует общему росту рынка кибербезопасности. Многие вычисления основаны на сложных математических моделях прогнозирования, обрабатывающих большие объемы данных.

Кибербезопасность – это процесс защиты и восстановления компьютерных сетей, устройств и программ от любого типа кибератак. Кибератаки представляют собой все большую опасность для сохранения конфиденциальных данных, поскольку злоумышленники используют новые методы, основанные, например на искусственном интеллекте, таким образом обходя традиционные меры безопасности. Все отрасли сталкиваются с угрозой кибератак. Согласно

опросу McKinsey, 75% экспертов во многих отраслях считают киберриски главной проблемой [6].

Среди основных кибератак выделяют следующие: вредоносные домены, вредоносное программное обеспечение и вымогательство.

Риск кибербезопасности – это вероятность раскрытия информации или потерь в результате кибератаки или утечки данных. Риск кибербезопасности растет, что обусловлено использованием облачных сервисов, таких как Amazon Web Services, для хранения конфиденциальных данных и личной информации [5]. Широко распространенная плохая конфигурация облачных сервисов в сочетании со все более изощренными киберпреступниками означает, что риск того, что ваша организация пострадает от успешной кибератаки или утечки данных, растет.

По мере того, как предприятия становятся все более зависимыми от компьютерных систем, наблюдается рост влияния потенциальных утечек данных. Прогнозы аналитиков не успевают за таким быстрым ростом, переориентацией вредоносных программ с персональных компьютеров и ноутбуков на смартфоны и мобильные устройства.

Стоит отметить, что киберпреступники будут стремиться использовать все большее число новых способов атак, т.к. все большее количество работодателей вводят дистанционный режим работ и устанавливают удаленное подключение для своих сотрудников к своим системам.

Существует отдельный вид угроз, который связан с большой нагрузкой на цифровые сервисы и технологии. Таким образом, большинство сервисов столкнулись с определёнными сложностями.

Однако у бизнеса нет выбора, т.к. рынок Интернет-торговли и услуг стремительно расширяется и терять потребителей в этой сфере экономически нецелесообразно.

Потребители все чаще стали выбирать варианты безналичной оплаты товаров и услуг. В результате в некоторых секторах компании инвестируют в мобильные приложения и веб-порталы, тем самым упрощая платежи и переводы (рис. 1). Такие приложения в свою очередь создают новые уязвимости, которые необходимо вовремя устранять. Одной из причин успешности компьютерной атаки является наличие уязвимостей программного обеспечения, используемого в составе автоматизированных систем [2].

Среди самых распространённых уязвимостей выделяют небезопасное хранение данных и недостаточную аутентификацию.

По мере того, как технологии искусственного интеллекта совершенствуются и становятся все более распространёнными, они позволят осуществлять углубленный поведенческий мониторинг и индивидуальное профилирование клиентов по их местоположению, устройствам и методам аутентификации.

До недавних пор, например в секторе финансовых услуг, банки полностью могли контролировать путь клиента, однако с ростом открытого банкинга это изменилось. Теперь потребители пользуются банковскими услугами через сторонние приложения, которые находятся вне контроля банков.

Сеть 5G вскоре будет развернута в больших масштабах, что также означает резкое увеличение доступа и использования подключённых устройств Интернета вещей. Это приведет к увлечению уязвимости сети и данных для взломов и краж.

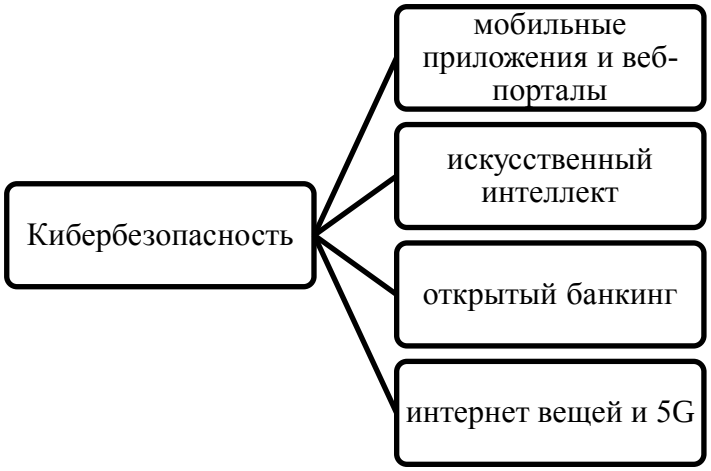

Рис. 1 – Тенденции в области кибербезопасности

В связи с тем, что новые технологии набирают обороты в мире Business to business, развивается вредоносное ПО, сложные облачные системы и инфраструктура 5G являются основным направлением тенденций развития технологий кибербезопасности 2020 года.

Практически все современные компании к 2025 году перейдут на несколько облачных решений, что усложнит управление и защиту. В сочетании с новыми угрозами компании должны находить новые инструменты и подбирать квалифицированный персонал с необходимыми ресурсами для обнаружения атак и устранения проблем по мере их возникновения. Так, одной из главных задач обеспечения кибербезопасности является проблема дефицита кадров и повышение требований к профессиональной подготовке специалистов в этой области.

Кроме того, быстрое преобразование 5G в сетевое будущее требует быстрого развития инфраструктуры и защиты конечных точек. Ускоренное внедрение и международное влияние вызывают множество проблем с безопасностью, но компании будут внедрять технологию 5G до того, как она будет защищена.

Противостояние угрозам в постоянно меняющемся мире современных технологий, адаптация к новым потребностям корпоративного и частного

пользователя – первоочередные задачи специалистов информационной безопасности, решение которых может потребовать принципиально новых подходов к обеспечению кибербезопасности.

Таким образом, всем компаниям необходимо пересмотреть подход к обеспечению кибербезопаснсти. С одной стороны, необходимо удовлетворить все потребности клиентов и предоставить им доступ к финансовым услугам через различные каналы, включая Интернет, мобильные устройства и Интернет вещей. С другой стороны, каждый такой канал создает новые уязвимости, некоторые из которых могут остаться неизвестными до тех пор, пока не произойдет атака.

Библиографический список:

1. Иванов В.В., Путилов А.В. Цифровое будущее: следующий шаг в развитии атомных энергетических технологий // Энергетическая политика. – 2017. - №3. – С. 31-42.
2. Михайлов Д.М., Жуков И.Ю., Шеремет И.А. Защита автоматизированных систем от информационно-технологических воздействий. М.: НИЯУ МИФИ, 2014. – 184 с.
3. Путилов А.В. Развитие технологий и подготовка кадров для цифровой экономики в энергетике // Энергетическая политика. – 2017. - № 5. – С. 58-65.
4. Цифровые платформы управления жизненным циклом комплексных систем: монография / А. В. Путилов, В. В. Харитонов, А. И. Гусева [и др.] / под ред. д-ра экон. наук, проф. В.А. Тупчиенко. – М.: Научный консультант, 2018. – 439 с.
5. Черепанов С.П. Достоинства и недостатки аппаратных решений систем обработки больших данных // Современные наукоемкие технологии. – 2020. - № 8 – С. 86-89.

6. McKinsey: Six ways CEOs can promote cybersecurity in the IoT age. [Электронный ресурс]: – Режим доступа – URL: https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/six-ways-ceos-can-promote-cybersecurity-in-the-iot-age (Дата обращения: 20.09.2020).

Оригинальность 89%