УДК 004.056.52

Азимкова К.А.
Магистр,1 курс, финансовый факультет
РЭУ им. Г. В. Плеханова
Г. Москва, РФ

ВАЖНОСТЬ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Аннотация

Для продуктивной работы государства и создания стабильных условий в экономике и обществе существует ряд важных условий, таких, как: безопасная и надежная работа сетей передачи данных, мобильных гаджетов и компьютерных систем. Большое количество факторов влияют на правильную и безопасную работу основных информационных инфраструктур общего пользования. К таким факторам относятся: нарушения работы программного и аппаратного обеспечения, кибератаки, неполадки, которые вызваны физическим воздействием, а также человеческие ошибки.

На сегодняшний день отчетливо видна зависимость общества от стабильной работы информационных систем. Особенно это прослеживалось во время карантина, когда большинство предприятий перешло на удаленную работу.

Значительное повышение происшествий, которые возникли в кибер сфере, вызвало потребность в системном анализе источников появления таких угроз. Одним из важных понятий для этого среди специалистов является кибербезопасность.

Ключевые слова:

Сети, кибербезопасность, защита информации, угрозы, технологии, кибератаки, гаджеты.

THE IMPORTANCE OF ENSURING CYBER SECURITY

Abstract

To ensure stable work in the economy and society, there are a number of important conditions, such as: safe and reliable operation of data transmission networks, mobile gadgets and computer systems. A large number of factors influence the correct and safe operation of the main information of public infrastructures. These factors include: software and hardware malfunctions, cyberattacks, problems caused by physical tampering, and human errors.

Today clearly shows the dependence of the company on the stable operation of information systems. This is especially traced during the quarantine period, when most businesses are transferred to the remote work.

The significant increase in incidents that have arisen in the cyber sphere has caused the need for a systematic analysis of the sources of such threats. One of the important concepts for this among experts is cybersecurity.

Keywords:

Networks, cybersecurity, information protection, threats, technologies, cyber-attacks, gadgets.

Актуальность выбранной темы определена потребностью в разработке и введении условий, позволяющих обезопасить данные в киберпространстве.

Такие условия очень важны для достижения определенного уровня безопасности информации в такой среде.

На сегодняшний день практически у каждого человека есть мобильное устройство для осуществления связи или взаимодействия через социальные сети, а также другие различные средства. С одной стороны гаджеты позволяют легко общаться друг с другом, находить новые знакомства, но с другой стороны их повсеместность создает для государственных и негосударственных субъектов ряд неотъемлемых уязвимостей и возможные векторы атак. Применение таких уязвимостей обычно приводит

к глобальным проблемам для национальной безопасности путем намеренных действий таких, как шпионаж, неэффективное командование и управление объектами, кража интеллектуальной собственности и информации личного характера, нарушение предоставления услуг и работы очень важной инфраструктуры или нанесение ущербов экономике и промышленности.

С постоянным развитием технологий принципы и методы, а также характер кибератак постоянно меняются и совершенствуются. Исходя из сказанного, применяется традиционный подход. Данный подход базируется на акценте, направленном на защиту более важных ресурсов от угроз, которые уже известны. Этот подход не является эффективным, пока все ресурсы направлены на защиту самых важных аспектов, упускаются менее важные компоненты при этом. Мне кажется, что данных подход может понести еще большие риски в целом для безопасности из-за этого недочета. Следовательно, чтобы осуществлять контроль и повышать уровень безопасности, необходим постоянный мониторинг, анализ, а также регулярное обновление системы кибербезопасности.

Проанализировав данные Forbes, можно сделать вывод, что в 2016 году глобальный рынок кибербезопасности достиг $ 75 млрд. В 2017, 2018 и в 2019 годах он продолжает неуклонно расти. К 2020 году достигает более $170 млрд. Такой молниеносный и резкий рост можно объяснить наличием огромного числа технологических инноваций и тенденций, а также регулярно изменяющимися требованиями к безопасности. Из чего следует, что с каждым годом тема кибербезопасности становится все более актуальной и необходимой в современном мире.

Каким образом повысить уровень защищенности данных в информационной инфраструктуре?

2020 год принес немало изменений в обыденную жизнь, что вызвало большой рост киберрисков.COVID-19 заставил организации пустить в дело удаленную рабочую силу. Это означает, что работа осуществлялась посредством облачных платформ. В конечном итоге, значительно увеличилось количество кибератак и утечек данных компаний в облачные пространства.

Внедрение 5G повысило пропускную способность интернет – устройств во много раз, но они стали более уязвимыми для кибератак.

По прогнозам специалистов ожидается, что с 31 млрд. в 2020 году до 35 млрд. - 2021 году и 75 млрд. в 2025 году вырастет количество подключенных к Интернету устройств. Можно предположить, что из-за роста количества интернет-устройств увеличатся и попытки незаконного проникновения в эти устройства.

Большой проблемой так и остается отсутствие умения по борьбе с кибербезопасностью как на уровне пользователя, так и на уровне администраторов системы.

Исходя из всего сказанного, необходимо подчеркнуть основные направления по борьбе с кибератаками компаний на 2021 год:

1. Применение альтернативного подхода к анализу, предуведомление рисков безопасности, которые связаны с удаленной работой.

2. Повышение расходов на безопасность в киберпространстве, обучение персонала (на всех уровнях).

3. Создание и введение автоматических систем мониторинга и поведенческого анализа изменения данных, доступа в систему.

4. Создание, введение и изучение новых информационных технологий, которые гарантируют ограничение доступа и защиту целостности информационных баз данных.

Несмотря на все эти меры предосторожности, необходимо осознавать, что невозможно предотвратить абсолютно все угрозы, это неосуществимо даже при неограниченных ресурсах. Но компаниям придется приспосабливать свою деятельность к постоянно меняющимся характерам киберугроз.

В общей сложности, направления 2017-2020 гг. позитивны, необходимо отметить улучшения в том, как организации стараются решить проблемы, путем применения комплексного подхода к уменьшению кибер-рисков и защите ценных данных.

Многие владельцы бизнеса, пострадавшие от таких атак, имеют желание вернуть свои финансовые

потери и деловую репутацию, а также владельцы, которые просто хотят в будущем предотвратить такие атаки, обращаются к страховым механизмам для этого. Из этого следует, что рынок страхования по таким риска активно растет и развивается.

Анализируя статистические данные, можно заметить рост рынка страхования с каждым годом: в 2015 году он составил примерно 1,5 млрд. долларов США, к 2018 году его объем вырос до 4,85 млрд. долларов США, а к 2020 году – до 7,8 млрд. долларов. По прогнозным оценкам специалистов, можно сделать вывод, что, если сохранится данная тенденция роста, прогнозная стоимость страхования киберрисков к 2025 году будет составлять 20,4 млрд. долларов США.

Одно из самых главных звеньев в дальнейшем обеспечении безопасности в киберпространстве является уровень сотрудничества причастных участников: научно-исследовательские институты, государство, заказчики и потребители, разработчики и производители инфокоммуникационных решений.

Еще одним решением может быть организация ряда системных НИОКР среди компетентных предприятий, которые объединены похожими целями и ответственны за предоставление на рынок востребованных продуктов общемирового уровня. Благодаря такой модели государство может формировать безопасную инфраструктуру кибербезопасности на федеральном уровне, при этом обеспечивая развитие экономики с помощью повышения числа рабочих мест и объема производства.

Список использованной литературы:

1. Гарнаева М.А., Функ К. Kaspersky security bulletin 2017// Вопросы кибербезопасности. 2016. №3. С.65-68;
2. Материалы, опубликованные на вебсайте Statista;
3. Материалы, опубликованные на сайте Allianz Global Corporate & Specialty (AGCS);
4. Материалы сайта RISKIQ;
5. CNews|безопасность - [электронный ресурс] Сергей Попсулин - http:// safe.cnews.ru/news/top/index. shtml?201 3/08/02/53761 4&utm
6. https://www.forbes.ru/

УДК 620.9:621.22

Алтунин К.В.
канд. техн. наук, доцент КНИТУ-КАИ
г. Казань, РФ

РАЗРАБОТКА МАГНИТНО-ГИДРАВЛИЧЕСКОГО ДВИГАТЕЛЯ ПОВЫШЕННОЙ ЭФФЕКТИВНОСТИ

Аннотация

Статья посвящена разработке нового экологически чистого магнитно-гидравлического двигателя повышенной эффективности и экономичности. Рассмотрена проблема загрязнения окружающей среды. Представлены материалы описания заявки на изобретение.

Ключевые слова:

двигатель, эффективность, жидкость, поплавок, капсула, магнит

Введение

В настоящее время в мире можно выделить как минимум пять основных экологических проблем, включая загрязнение воздуха, вырубку леса, загрязнение воды, разрушение озонового слоя, утрату биоразнообразия [1]. Экологическая ситуация в мире ухудшается с каждым днем, и каждый из нас участвует