УДК 004.056
DOI 10.24411/2409-3203-2019-12038

ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РЕАЛИЗАЦИИ ПРОГРАММЫ «ЦИФРОВАЯ ЭКОНОМИКА РОССИЙСКОЙ ФЕДЕРАЦИИ»

Чибисова Изабелла Станиславовна
старший преподаватель кафедры экономика и управления АПК
ФГБОУ ВО Красноярский ГАУ Ачинский филиал
Россия, г. Ачинск

Аннотация: Как Российская Федерация движется в сторону цифровизации во всех сферах деятельности сказано не мало. Имеются многочисленные отчеты в которых приведены сухие цифры статистики. В данной же статье рассмотрен вопрос развития информационных технологий для цифровой экономики Российской Федерации. Показан один из основных аспектов трудностей и проблем, с которыми сталкиваются научные организации в условиях современной реальности – безопасность информации. Процесс цифровых трансформаций в мире приводит не только к внедрению новых технологий, но и к росту количества направлений для киберпреступности. При использовании информационных технологий, цифровых сервисов каждая организация сталкивается с проблемой противостояния деструктивному сочетанию тенденций на быстрое развитие кибернетических угроз и появление новых их разновидностей.

Ключевые слова: цифровая экономика, информационные технологии, безопасность данных, облачные сервисы, информационная безопасность.

THE PROBLEM OF INFORMATION SECURITY IN THE IMPLEMENTATION OF THE PROGRAM "DIGITAL ECONOMY OF THE RUSSIAN FEDERATION"

Chibisova Isabella S.
Senior Lecturer in Economics and Management
Krasnoyarsk State Agrarian University Achinsk branch
Russia, Achinsk

Abstract:: As the Russian Federation moves towards digitalization, not a little has been said in all areas of activity. There are numerous reports in which dry statistics are given. This article also discusses the development of information technology for the digital economy of the Russian Federation. One of the main aspects of the difficulties and problems faced by scientific organizations in modern reality is shown - information security. The process of digital transformations in the world leads not only to the introduction of new technologies, but also to an increase in the number of areas for cybercrime. When using information technologies and digital services, each organization faces the problem of confronting the destructive combination of trends in the rapid development of cyber threats and the emergence of new varieties of them.

Keywords: digital economy, information technology, data security, cloud services, information security.

Прошло уже более двух лет, как Президент Российской Федерации утвердил программу «Цифровая экономика Российской Федерации» Распоряжением Правительства РФ № 1632-р от 28.07.2017 г. Многие научные деятели оценивают текущее состояние,

описывают перспективное будущее и затрагивают реальные проблемы, с которыми сталкивается наша действительность при реализации вышеуказанной программы.

Среди прочих тезисов и направлений можно выделить один из приоритетов – это «переход к передовым цифровым, интеллектуальным производственным технологиям, роботизированным системам, новым материалам и способам конструирования, создание систем обработки больших объемов данных, машинного обучения и искусственного интеллекта» [1]

В настоящее время научное сообщество России обладает всеми необходимыми ресурсами для создания основы, платформы, где в дальнейшем будет развиваться цифровая экономика. И уже в 2017 году ФИЦ ИУ РАН представила общественности ресурсы для исследований в различных областях. Также создан действующий макет системы управления научными сервисами. Как можно заметить, самая большая проблема при ближайшем рассмотрении, это не проблема финансирования научных исследований или разработок в данной области, а проблема безопасности и информационной защищенности разрабатываемых систем и комплексов автоматизации производства. В условиях быстрого темпа наращивания вычислительный мощностей этому вопросу уделяется недостаточно внимания. Одно дело разработать платформы и автоматизированные системы, другое – вникнуть во все возможные угрозы и учесть их при проектировании и/или разработки автоматизированных комплексов.

Трудность обеспечения безопасности разрабатываемых или внедряемых информационных технологий состоит из нескольких крупных групп.

К первой группе, самой распространённой, относятся угрозы, исходящие изнутри предприятия и/или компании, которая внедрила и применяет новые информационные технологии… Происходит это, чаще всего, даже не из злого умысла, а из-за цифровой, информационной неграмотности сотрудников организации. Работники часто пренебрегают элементарными правилами поведения в глобальных и локальных сетях, и не придают значения безопасности на своем рабочем месте. Даже, если специалисты по информационной безопасности грамотно настроили рабочее место сотрудников, те в свое время могут предоставлять доступ к персональному компьютеру третьим лицам, не пользоваться блокировкой и так далее.

В условиях сегодняшней реальности в России при увольнении сотрудники могут унести с собой значительную часть оперативной информации, с которой они работали. Также не редки случаи порчи информационных данных. Облачные технологии для современного пользователя – это лишь удобство, но редко кто из них задумывается о безопасности документов, которые размещаются на таких сервисах.

Следующая группа угроз – это устройства IoT (устройства интернет-вещей). В настоящее время каждое, разрабатываемое устройство так или иначе связано с глобальной сетью. Роботизированные системы управляются через свои каналы связи, однако об их защите тоже мало кто задумывается. По статистике в странах с развитой цифровой экономикой кибернетические преступления не редки. Так по данным исследования компании Fortinet, количество атак, приходящееся на одну организацию, увеличилось на 82%. За 2018 год. [4]

Немаловажной остается группа вредоносного программного обеспечения. Тенденция применения нелицензионного программного обеспечения, взломанных приложений в Российской Федерации пока остается на прежнем уровне. Вредоносное программное обеспечение все чаще направлено на поражение именно промышленных систем и систем управления производственными процессами.

Поскольку мир информационных технологий не стоит на месте, то и разнообразие атак на информационные системы развивается с большой скоростью. Так можно привести в пример стенографические атаки, которые в последнее время увеличили свою активность.

Сегодня уже недостаточно проинструктировать работников компании и установить хорошее антивирусное программное обеспечение. Сегодня необходимы полноценные

автоматизированные системы, которые также, как и вредоносное программное обеспечение, могло бы обучаться. Для Российской Федерации, которая только встала на путь цифровизации, необходимо не просто масштабно внедрять информационные технологии, но и решать задачи по защите внедряемых информационных систем и комплексов сразу предугадывая возможные угрозы и риски. Тем более, что большинство Интернет-порталов и платформ работают в браузерах, разработанных заграничными компаниями.

Список литературы:

1. Стратегия научно-технологического развития Российской Федерации (утверждена Указом Президента РФ №642 от 01.12.2016 г.). URL: http://www.youngscience.gov.ru/media/files/file/dVwMOeQ2OsjrSsodEazQjnkmICrTHSfh.pdf (дата обращения 02.11.2019)
2. Программа «Цифровая экономика Российской Федерации» (утв. Распоряжением Правительства РФ от 28.07.2017 №1632-р) http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения 12.11.2019)
3. Аналитика развития, безопасности и сотрудничества: Большая Евразия – 2030. Сборник материалов 4-й Международной конференции 29.11.2017г., Общественная палата РФ. – М.: Когито-Центр, 2017. – 253 с.
4. Статистика кибернетических атак по данным компании Fortinet за 2018 год URL: https://www.crn.ru/news/detail.php?ID=124734 (дата обращения 02.10.2019)