DOI 10.36622/VSTU.2022.25.4.013
УДК 004.056

НАПРАВЛЕНИЕ СОВЕРШЕНСТВОВАНИЯ НОРМАТИВНО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ НА ОСНОВЕ РИСК-АНАЛИЗА ИХ КИБЕРБЕЗОПАСНОСТИ

А.Г. Остапенко, Д.В. Щербакова, Д.А. Нархов, Ю.В. Макаров, А.С. Кривошеин

Рассматривается проблема развития нормативно-правового обеспечения информационной безопасности предприятия. Подчеркивается, что в нынешних условиях обострения информационного противоборства с Западом ритмичность и скорость модернизации вышеуказанного обеспечения должна неуклонно нарастать. Утверждается, что реальной базой такой модернизации может служить именно риск-мониторинг нарушения кибербезопасности в мире и на предприятии, который станет основой для оперативной выработки актуальных политик, регламентов и инструкций персонала защищаемых организаций. В данном аспекте особое внимание обращается на революционные кибертехнологии, ускоренно внедряемые в ходе цифровой трансформации современного общества. Именно в этом контексте предлагаются варианты целеполагания исследований по совершенствованию нормативно-правовой защиты информации, т.е. определяются его объекты, предметы, цели и задачи. К тому же, предлагается информационная база исследования в виде перечня сайтов, ведущих статистику отказов атакуемых кибер-объектов. Отсюда может быть получена динамика рисков, способствующая нормотворчеству в сфере обеспечения информационной безопасности.

Ключевые слова: безопасность, право, нормативы, атаки, риски, предприятие.

Введение

В условиях обострившегося ныне противоборства в киберпространстве [1-4] весьма актуальным представляется сейчас направление с общим названием «Оценка и регулирование рисков успешности кибератак в целях совершенствования организационно-правового обеспечения информационной безопасности объектов».

Суть подхода заключается в том, что «метод проб и ошибок», зачастую опирающийся на «слепое» копирование западных нормативов [5] в отечественном правовом пространстве, уже не работает эффективно. Особенно очевидным это становится в условиях информационной войны с Коллективным Западом и переводом отечественной социально-экономической системы на мобилизационные рельсы.

При этом, основной задачей информационного права, включая подзаконные акты и нормативы, остается фактически сокращение рисков успешности кибератак, прежде всего на критические объекты. Информационной пищей для принятия законотворческих решений объективно должна быть статистическая база частоты и ущербности этих атак в динамике всемирной и отечественной информационной трансформации общества.

Отсюда и выступает проблема реагирования на инциденты, связанные с реализацией информационных операций и атак. Она обусловлена дедуктивными недостатками в материальном и виртуальном мире, инфраструктуре, общих моделях, универсальном регулировании.

Сущность исследования

Считая, что структура элементов нормы права такова: гипотеза (кто и при каких условиях должен исполнять); диспозиция (права и обязанности, составляющие модель поведения); санкции (последствия при нарушении нормы), по этим элементам можно разложить типы киберколлизий, регистрируемых через риск-анализ (спектр элементов можно развить) [5].

Наложение вышеуказанных элементов на реалии информационного противоборства, резко обострившегося ныне, даст пищу для постановки законотворческих задач и нормативных совершенствований по конкретным видам исследуемых атакуемых

объектов. Кстати говоря, это могут быть не только критические объекты, но и широкомасштабные явления, например, внедрение перспективных технологий, которое сейчас осуществляется через цифровую сферу.

Проектант в данном случае реализует поиск статистики частоты и ущербности (единичной атаки) деструктивных воздействий, её риск-анализ, формирование новых норм по сокращению рисков по всему правовом пространству для заданной темы. Все это должно быть аналитически (численно) обосновано.

Выбрав объект исследования, можно получить статистику отказов атакуемых систем, которая станет основой для последующего риск-анализа, суть которого изложена выше.

Целеполагание исследования

Тематическое многообразие в данном случае таково: «Внутриорганизационное нормативно-правовое регулирование в сфере внедрения технологий … на основе риск-анализа инцидентов нарушения информационной безопасности».

Объект исследования: системы и сети, использующие технологии … и подвергающиеся атакам, нарушающим их информационную безопасность

Предмет исследования: риск-анализ инцидентов нарушения информационной безопасности систем и сетей, использующих технологии …, для выработки рекомендаций для совершенствования их нормативно-правового регулирования по защите информации.

Перспективными видятся следующие варианты рассматриваемых технологий:

1.Искусственного интеллекта;
2.Компьютерных вычислений;
3.Виртуализации реальности;
4.Многомерной печати;
5.Распределенного реестра;
6.Интернета вещей;
7.Облачных вычислений;
8.Роботизации;
9.Создания экосистем;
10.Биометрии;
11.Электронной слежки;
12.Компьютерной разведки;
13.Развития интернет-платформ;
14.Криптовалют.

Цель исследования: повышение защищенности систем и сетей, использующих технологии …, за счет совершенствования средств внутриорганизационного нормативно-правового регулирования на основе риск-анализа инцидентов нарушения информационной безопасности.

Задачи исследования:

1.Исследование существующих механизмов нормативно-правового регулирования систем и сетей, использующих технологии …, на предмет обеспечения их информационной безопасности с акцентом на внутриорганизационный уровень

2.Риск-анализ и прогнозирование динамики зарегистрированных инцидентов нарушения информационной безопасности (ИБ) систем и сетей, использующих технологии …

3.Выработка рекомендаций по совершенствованию нормативно-правового регулирования систем и сетей, использующих технологии …, на уровнях частной политики, регламентов и инструкций обеспечения ИБ предприятия, исходя из прогнозов динамики зарегистрированных инцидентов нарушения ИБ (рис. 1).

Информационный конфликт носит антагонистический характер, когда цели противных сторон (субъектов конфликта) противоречат друг другу. Поэтому для описания информационного конфликта в качестве основного математического аппарата подходит комплекс методов теории игр с нулевой суммой. При рассмотрении информационного противоборства реализации атак и противодействия им один из субъектов в игре проводит информационные операции и атаки, другой защищает свои информационные ресурсы [8].

Рис. 1. Обобщенная блок-схема регулирования рисков (начало)

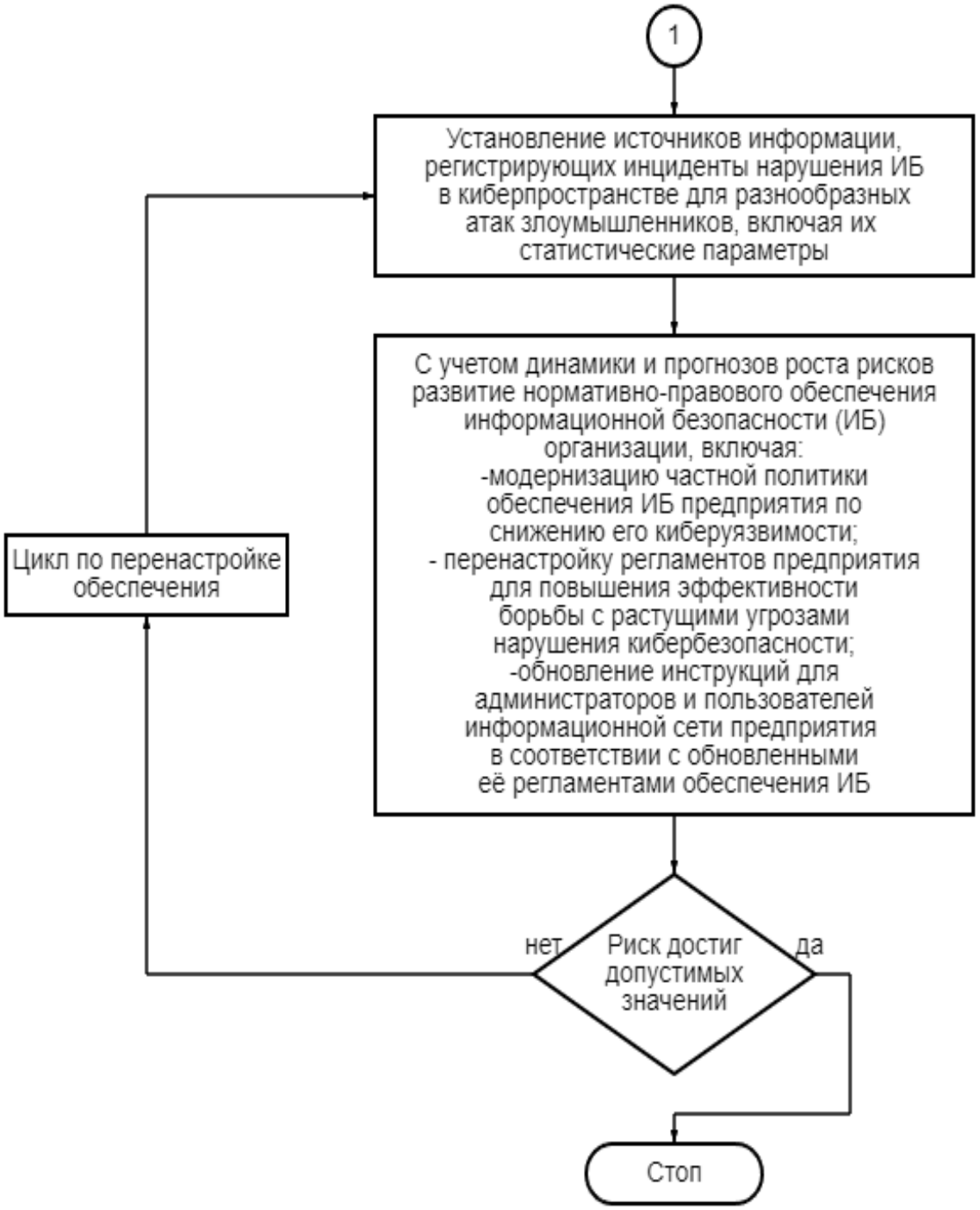

Рис. 1. Обобщенная блок-схема регулирования рисков (окончание)

Заключение

Рассмотренное тематическое многообразие сконцентрировано на уровне IT-предприятия. Это базовое звено обеспечения национальной информационной безопасности, и конкретика в этом срезе может быть получена при углубленном изучении феномена внедрения вышеуказанных революционных технологий цифровой трансформации современного общества.

Каждая из этих технологий несет свою информационную и социально-экономическую специфику не только для организации в целом, но и для каждого её сотрудника, деятельность которых (в

условиях нынешнего обостряющегося киберпротивоборства России и Запада) должна быть регламентирована уже иначе. Причем, модернизация данного нормативно-правового обеспечения должна осуществляться с повышенным темпом, ибо внедрение революционных технологий и расширение множества порождаемых ими угроз сегодня идет семимильными шагами.

В этом случае неусыпный риск-мониторинг нарушений кибербезопасности должен отражать основной для коррекции честных политик, регламентов и инструкций обеспечения ИБ на предприятии информатизации

Список литературы

1. Социальные сети и риск-мониторинг / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2019. – 284 с. (Серия «Теория сетевых войн»; вып. 4).

2. Социальные сети и психологическая безопасность / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2020. – 284 с. (Серия «Теория сетевых войн»; вып. 5).

3. Сетевая эпидемиология / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2021. – 284 с. (Серия «Теория сетевых войн»; вып. 6).

4. Картография защищаемого киберпространства / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2022. – 372 с. (Серия «Теория сетевых войн»; вып. 7).

5. Остапенко Г.А., Машкова Е.А. Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия. Учебное пособие для вузов/ Под редакцией В.Г. Кулакова. – М.: Горячая линия – Телеком, 2008. –208 с.

ФГБОУ ВО «Воронежский государственный технический университет»
Voronezh State Technical University

Поступила в редакцию 14.11.2022

Информация об авторах

Остапенко Александр Григорьевич – д-р техн. наук, заведующий кафедрой, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Щербакова Дарья Владимировна – соискатель, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Нархов Дмитрий Андреевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Макаров Юрий Вадимович – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Кривошеин Александр Сергеевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

THE DIRECTION OF IMPROVING THE REGULATORY SUPPORT OF INFORMATIZATION OBJECTS BASED ON THE RISK ANALYSIS OF THEIR CYBERSECURITY

A.G. Ostapenko, D.V. Shcherbakova, D.A. Narhov, Yu.V. Makarov, A.S. Krivoshein

The problem of the development of regulatory and legal provision of information security of the enterprise is considered. It is emphasized that in the current conditions of aggravation of the information confrontation with the West, the rhythm and speed of modernization of the above-mentioned provision should steadily increase. It is argued that the real basis for such modernization can be precisely the risk monitoring of cybersecurity violations in the world and at the enterprise, which will become the basis for the operational development of relevant policies, regulations and instructions of personnel of protected organizations. In this aspect, special attention is paid to revolutionary cyber technologies that are being rapidly implemented during the digital transformation of modern society. It is in this context that the options for the goal-setting of research on improving the regulatory protection of information are proposed, i.e. its objects, subjects, goals and objectives are determined. In addition, the information base of the study is proposed in the form of a list of sites that conduct statistics of failures of attacked cyber objects. Hence, the dynamics of the figures can be obtained, which contributes to norm-making in the field of information security.

Keywords: security, law, regulations, attacks, risks, enterprise.

Submitted 14.11.2022

Information about the authors

Alexander G. Ostapenko – Dr. Sc. (Technical), Head of the Department, Voronezh State Technical University, e-mail: mnac@comch.ru
Darya V. Shcherbakova – applicant of the Voronezh state technical University, e-mail: mnac@comch.ru
Dmitry A. Narhov – student of the Voronezh state technical University, e-mail: mnac@comch.ru
Yury V. Makarov – student of the Voronezh state technical University, e-mail: mnac@comch.ru
Alexander S. Krivoshein – student of the Voronezh state technical University, e-mail: mnac@comch.ru