Молодёжный вестник НФ БГТУ. 2023. Том 03. № 02 (10)
https://rio-nb-bstu.science

ИНФОРМАТИКА

doi: 10.51639/2713-0576_2023_3_2_168
УДК 004.056+ 346.244
ГРНТИ 81.93.29
ВАК 05.13.19

Общая характеристика информационной безопасности Российской Федерации

Лоскутов И. А.

АО «Научно-производственная корпорация «Космические системы информационно-управляющие и электромеханические комплексы имени А Г. Иосифьяна»
107078, Россия, г. Москва, Хоромный тупик, дом 4, стр. 1
Политехнический колледж им. Н. Н. Годовикова
125130, Россия, г. Москва, улица Зои и Александра Космодемьянских, дом 19
Колледж телекоммуникаций МТУСИ
125493, Россия, г. Москва, Авангардная ул., дом 5
Национального исследовательского ядерного университета «МИФИ»
115409, Россия, г. Москва, Каширское ш., дом 31

email: faxvex@ya.ru

Работа носит обзорный характер и посвящена вопросам обеспечения информационной безопасности в Российской Федерации. Для составления полной картины, исследование разбито по частям: законодательный уровень, ее реализация, основы программно-аппаратной защиты, категорирование. В работе были выявлены особенности и проблемы нормативно-правовой части, в частности отмечены восемь недостатков и семь положительных моментов. В исследовании приведены правила реализации законодательных актов и приказов федеральных органов исполнительной власти. В части программно-аппаратной реализации показаны методика оценки воздействия кибератаки, а также рассмотрены значимые защитные системы и подсистемы. Также были отмечены особенности категорирования объектов критической информационной инфраструктуры, выявлен недостаток, связанный с нерешённостью критических процессов. В конечном итоге была приведена общая характеристика обеспечения информационной безопасности в Российской Федерации.

Ключевые слова: КИИ, информационная безопасность, защита информации, законодательная база, киберзащита.

Введение

Киберпреступность стала в XXI веке глобальной проблемой [1], в последнее время проявляется постоянная тенденция на увеличение количества кибератак (КА) [2], от того и информационная безопасность становится важной составляющая любой организации.
В современном обществе существуют два вида борьбы с КА. Первый,- юридический, иначе нормативно-правовой, закладывающий определения, дающий характеристику угрозам, способы обеспечения борьбы с ними на базовом уровне и ответственность атакующей стороны после реализации нападения. Второй, - программно-аппаратный, т. е. реализованный программный продукт (ПП), защищающий подвергающееся нападению

устройство в автоматическом режиме, или в режиме непосредственного взаимодействия с оператором. Для обеспечения должного уровня защиты необходим их симбиоз.
Данная работа обзорная и направлена на структурирование актуальной информации по направлению информационной безопасности (ИБ), которая будет полезна для исследователей и специалистов области, в качестве базиса для дальнейших работ.

Оценка текущего состояния законодательной базы

Как уже было сказано, киберзащищённость - крайне важный параметр современного общества, тем более это касается предприятий, занимающихся реализаций национальных интересов.
Рассмотрим сначала нормативно-правовую базу. Для этого воспользуемся сводными данными, показанными в работах [3, 4, с. 266, 267]. Перечислять в данной работе их не имеет смысла, однако следует дать комментарий об отсутствии в них Федерального закона от 2017 г. № 187-ФЗ, Указа президента от 2021 г. № 400 и других новых юридических актов.
С точки зрения законодательства можно дать следующую характеристику:

- наличие более 30 различных видов законодательных актов, полностью или частично затрагивающих понятие ИБ;
- постоянно проводится работа в области ИБ;
- достаточно широкое толкование понятия компьютерных угроз, их последствий;
- применение в своей логике треугольника «Конфиденциальность-Целостность-Доступность (КЦД)»;
- высокий уровень ответственности нарушителей;
- большой структурный аппарат, работающий в области ИБ;
- проведение политики повсеместной цифровизации.

Однако, нельзя опустить мнение специалистов области на наличие некоторых не решенных на данным момент проблем. В [4] отмечены:

- проблемы регулирования открытой и закрытой информации, особенно на стыках интересов потребителей и государства;
- сбор персональных данных государственными органами нередко затрагивает частную жизнь пользователей;
- плохо организована политика страны в областях поддержки и развития национальных средств массовой информации (СМИ);
- плохая интеграция российского информационного пространства в международное;
- плохая реализация господдержки фирмам, направление деятельности которых связано с реализацией продукции во внешнем информационном пространстве;
- массовая закупка иностранной техники и малая финансовая поддержка внутренних производств. Результатом является высокая вероятность проведения скрытых компьютерных атак, а также зависимость от поставщиков иностранных ПП [5];
- малое финансирование средств противоборства «информационному оружию», направленному против критической информационной инфраструктуры (КИИ) России [4];
- низкий уровень ИБ, особенно в малом и среднем бизнесе, направленном на реализацию продукции не содержащей сведения особой секретности, малое включение национальных информационных ресурсов в указанные отрасли экономики [6].

Также стоит отметить, что применяемый треугольник безопасности КЦД следует законодательно модифицировать в шестиугольник, показанный в работе [7, с. 4380]. Это позволит учесть вариативность подходов к каждому понятию базового треугольника.

В результате первичного анализа, складывается следующая картина – Российская Федерации крайне обеспокоена состоянием информационной безопасности и выделяет значительные ресурсы на развитие связанного с ним правого поля. Уже не раз в СМИ приводилась информация о вхождении государства в список лидеров по направлению. Безусловно с юридической точки зрения не все тонкости были учтены, однако за последние два десятилетия отмечается значительное совершенствование законодательной базы [8]. Кроме того, как показывает работа [9], исследования ученых из России крайне востребованы в области ИБ на мировой арене, что, как следствие, можно также рассматривать за положительную тенденцию заданного государственного курса.
Далее стоит акцентировать внимание на том, как на основании законодательного поля реализуются обеспечение ИБ для объектов КИИ.

Реализация постулатов законодательной базы

Обратимся к ранее озвученному Федеральному закону № 187-ФЗ от 2017 года, Постановлению от 2018 г. № 127 и Приказу ФСТЭК России от 2017 г. № 235.
В соответствии с документами, проводится явное разграничение действия владельцев КИИ и государства. Первые обязаны обеспечивать ИБ, в то время как государство оказывает им всевозможную поддержку. Выглядит это следующим образом: ответственные органы страны информируют о возможных угрозах ИБ, распределяют их по степени опасности и неотложности и помогают в создании программно-аппаратного комплекса информационной защиты. Подразделения специальной направленности КИИ в свою очередь отчитываются о его состоянии, возникших угрозах и проблемах, оказывают посильную помощь государственным органам в поиске атакующей стороны, ликвидации последствий киберинцидентов, дают гарантию о бесперебойном функционировании устройств, связанных с поддержанием ИБ на предприятии. Также нельзя опустить обязанность подключения КИИ к специальной системе ГосСопка (государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак) и передаче информации об киберинцидентах в НКЦКИ (национальный координационный центр по компьютерным инцидентам).
Как вывод, можно отметить достаточную регламентированность действий, что по своей сути может положительно сказаться на ИБ защищаемой компании.
Далее перейдем к особенностям программно-аппаратной реализации информационной защиты.

Программно-аппаратная защита информации

Как уже было ранее сказано, под угрозами понимаются компьютерные атаки, соответственно и изделия для обеспечения безопасности будут по большей части относится к средствам компьютерной техники, реализуемых специальными ПП [10, с.43].
Поскольку ПП есть воссоздание алгоритма в программном коде, следует рассмотреть методику оценки воздействия, оказываемого кибератакой на защищаемую систему, рис. 1 [11, с. 31].
Хорошо спланированная атака проходит следующим образом: перед началом КА, враждебная сторона проводит сбор информации, на основании которого определяются способы реализации нападения. Далее следует активная фаза получения несанкционированного доступа с последующей добычей интересующей информации или дестабилизации системы. А на третьей проводится процедура уничтожения данных о внешнем вторжении. Таким образом, возвращаясь к рис.1, система безопасности должна сработать на первом или начале второго этапах, т.е. на КИИ должны быть заведомо проанализированы пункты 3-6 и реализована соответствующая защита. Кроме того, немаловажно организовать дополнительную охрану потенциальным местам атаки, на

которые направлен 7 пункт. Исходя из реализованных защитных функций, будет возможно проанализировать вероятность успешности атаки и в каком месте может находиться потенциальная охранная брешь.

Рис. 1. Методика оценки воздействия кибератаки

В целом же для обеспечения комплексной защиты необходимо по возможности отработать все варианты, показанные на рис. 2, т.к. они соответствуют базовым нормативным документам, представленным в [12], и уже отмеченным выше законодательным актам.

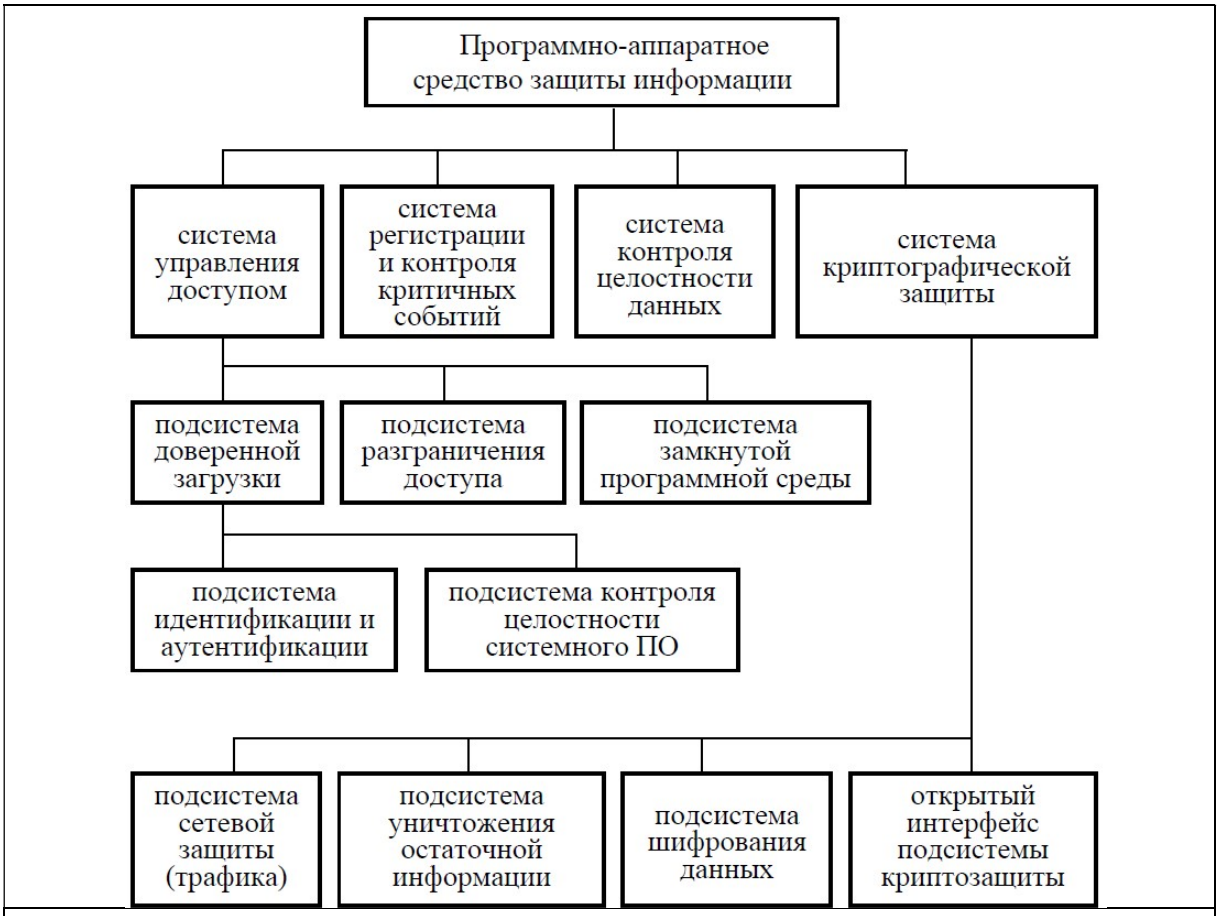

Рис. 2. Защитные системы и их подсистемы

Вывод - указанная стратегия реализует весь функционал системы безопасности, отмеченный в п. 28 Приказа ФСТЭК России от 21 декабря 2017 г. № 235.
Далее акцентируем своё внимание на таком процессе как категорирование.

Категорирование

Упомянутый ранее Федеральной закон от 2017 г. № 187-ФЗ, требует в обязательном порядке провести процедуру категорирования КИИ, за исключением тех случаев, когда такое предприятие не соответствует критериям значимости.
Осуществление процесса категорирования происходит по правилам, показанным в Постановлении от 8 февраля 2018 года № 127.
Процесс присвоения категории неразрывно связан с определением критических процессов. Однако, на данный момент времени нет узаконенного подхода к их выявлению. В соответствии с [13, с. 26, 27] на предприятиях, как правило, используют следующие три метода:

- субъект не выделяет ни один критический процесс;
- на предприятии выделяют все процессы как критические, т. е. происходит явная переоценка значимости;
- критическими отмечаются только основные процессы, связанные с главенствующей специализацией компании.

Безусловно, наиболее верным подходом стоит считать третий, однако даже при таком варианте имеется вероятность не учесть смежный процесс, косвенно относящийся к процессам КИИ и представляющий опасность при КА.
Вывод – нехватка определённости в подходах может привести к плохим последствиям для защищаемого объекта.

Заключение

В результате исследования можно отметить, что на законодательном уровне, в части информационной безопасности, до сих пор имеются некоторые нерешенные проблемы. Несмотря на зарегламентированность действий с помощью приказов федеральных органов исполнительной власти, ошибки допустимы. Хотя нельзя и не отметить, что в целом, картина ИБ России относительно мира весьма положительная, даже можно сказать лидирующая, некоторые аспекты требуют более подробного описания, так будет достигнута куда более защищенность значимых объектов КИИ. Кроме того, в части практической реализации с помощью технических средств уже разработаны подходы, гарантирующие высокий уровень защищенности, что положительно сказывается на ИБ.

Конфликт интересов

Автор статьи заявляет, что у него нет конфликта интересов по материалам данной статьи с третьими лицами на момент подачи статьи в редакцию журнала, и ему ничего не известно о возможных конфликтах интересов в настоящем со стороны третьих лиц.

Список литературы

1. Заернюк В. М. Черникова Л. И. Киберриски – глобальная проблема современности (на примере предприятий горнодобывающей отрасли) // Финансовая жизнь. 2017. № 4. С. 4–8.

2 Актуальные киберугрозы: I квартал 2022 года. – [Электронный ресурс].– URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (29.03.2021)
3 Груздева Л. М. Основы информационной безопасности: учебное пособие в двух частях. Ч. 1. М.: Юридический институт МИИТа. 2017. 101 с.
4 Манохина Н. В. Экономическая безопасность: учебное пособие. - М.: ИНФРА-М, 2019. - 320 с.
5 Арламов Е. А., Панасюк Г. О. Анализ состояния информационной безопасности в современной России // Экономика и менеджмент инновационных технологий. 2016. № 12(63). С. 111–113.
6 Беккалиева Н.К., Редькина Е.А., Кокарева А.А. Анализ информационной защищенности в системе экономической безопасности Российской федерации: проблемы практики // Цифровая наука. 2020. № 11. 11 с.
7 Towards a Triad for Data Privacy / Q. Covert [and other]. // Proceedings of the 53rd Hawaii International Conference on System Sciences. - Hawaii. - 2020. - P.4379-4387
8 Чубукова С. Г. Стратегии развития информационного общества и направления развития законодательства // Правовая информатика. - 2017. - N 2. - С.67–72.
9 Арутюнов В. В., Мещерский А. И. О востребованности результатов исследований российских ученых в области информационной безопасности // Вестник РГГУ. Серия: Информатика. Информационная безопасность. Математика. 2019. № 1. С. 42–50.
10 Вовенда Ю. В. Особенности политики обеспечения информационной безопасности в исполнительных органах государственной власти (на примере Северо-Западного федерального округа): дис. … канд. полит. наук. СПб., 2019. – 362 с.
11 Киберустойчивость информационно-телекоммуникационной сети / М. А. Коцыняк, И. А. Кулешов, А. М. Кудрявцев, О. С. Лаута. - СПб.: ООО "Бостон-спектр", 2015. – 150 с.
12 Духан Е. И., Синадский Н. И., Хорьков Д. А. Программно-аппаратные средства защиты компьютерной информации. Практический курс: учебное пособие. Екатеринбург: УрГУ, 2008. 240 с.
13 Безопасность объектов критической информационной инфраструктуры организации. Общие рекомендации(версия 2.0) М.: 2019, 111 с.

General characteristics of information security of the Russian Federation

Loskutov I. A.

JC “Research and Production Corporation “Space Monitoring Systems, Information & Control and Electromechanical Complexes” named after A.G. Iosifian”
105187, Russia, Moscow, Horomny tupik, 4, p. 1
Polytechnic College named after N. N. Godovikov
125130, Russia, Moscow, Zoya and Alexandra Kosmodemyanskikh, 19
College of Telecommunications MTUCI
125493, Russia, Moscow, Avangardnaya str., 51
National Research Nuclear University "MEPhI
115409, Russia, Moscow, Kashirskoe sh., 31

The work is reviewed and is devoted to ensuring information security in the Russian Federation. To compile a complete picture, the study is divided into parts: the legislative level, its implementation, the basis of software and hardware protection, categorization. In the work, the features and problems of the regulatory part were identified, in particular, eight deficiencies and seven positive points were noted. The study provides the rules for the implementation of legislative acts and orders

Молодёжный вестник НФ БГТУ. 2023. Том 03. № 02 (10)
https://rio-nb-bstu.science

of federal executive bodies. In terms of software and hardware implementation, the methodology for assessing the effects of cyber attacks is shown, as well as significant protective systems and subsystems are considered. Features of the categorization of critical information infrastructure objects were also noted, a deficiency was revealed associated with the unresolved critical processes. Ultimately, a general characteristic of ensuring information security in the Russian Federation was given.

Keywords: CII, information security, information protection, legislative framework, cyber protection.