ЗАЩИТА ИНФОРМАЦИИ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

INFORMATION PROTECTION AT CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

УДК 004.056.52

DOI: 10.24411/2658-4964-2021-10354

Зудинов Антон Сергеевич, студент 2 курс, магистр, кафедра КБ-1 «Защита информации», Институт комплексной безопасности и специального приборостроения, РТУ МИРЭА, Россия, г. Москва

Zudinov Anton Sergeevich, student 2 course, Master, Department KB-1 «Information Security", Institute of Integrated Security and Special Instrumentation, RTU MIREA, Russia, Moscow

Аннотация

Статья посвящена защите информации на объектах критической информационной инфраструктуры. В статье рассматриваются такие аспекты как законодательная база, влияющая на защиту объектов КИИ, какие объекты подпадают под ее действие, значимость объектов КИИ, разница между требованиями для объектов являющимися частью КИИ и теми кто не является ее частью. Так же рассматриваться виды данных которые могут обрабатываться или храниться на данных объектах.

Annotation

The article is devoted to the protection of information at critical information infrastructure facilities. The article discusses aspects such as the legal framework affecting the protection of CII objects, which objects fall under its action, the

significance of CII objects, the difference between the requirements for objects that are part of the CII and those who are not part of it. The types of data that can be processed or stored on these objects are also considered.

Ключевые слова: информационная безопасность, законодательная база, контроль доступа, меры защиты информации, КИИ, НДС

Keywords: information security, legal framework, access control, information protection measures, CII, VAT

Введение

Еще год назад, когда речь шла о безопасности критически важных объектов, на ум приходила защита промышленных объектов и 31-й Приказ ФСТЭК России. Ситуация изменилась — на государственном уровне было решено, что если, например, кибератака остановит на неделю работу крупного банка, то ущерб для людей будет значительным. С 1 января 2018 года вступил в силу Федеральный закон №187 от 26.07.2017 г. «О безопасности КИИ РФ», вводящий понятие критической информационной инфраструктуры. Стоит рассмотреть какие объекты подпадают под его действие и какие меры необходимо предпринять для обеспечения безопасности в соответствии с новыми требованиями.

Законодательная база

Рассматривая законодательную базу стоит уточнить что основополагающим документом нашей страны является Конституция РФ, принятая 12 декабря 1993 года (ред. от 04.07.2020) [1]. Конституция — это основной закон государства, обладающей большой юридической силой, утверждающий его экономическую и политическую систему, задающий принципы деятельности и организации органов государственной власти, суда, управления, основные права, свободы и обязанности граждан. Следом за ней идут Федеральные Законы, в частности, ФЗ от 27.07.2006 N 149-ФЗ (ред. от 3.04.2020 г) «Об информации, информационных технологиях и о защите информации».

В области защиты информации центральное место также занимает «Доктрина информационной безопасности» [3], утвержденная Указом Президента РФ от 5 декабря 2016 г. N 646. Доктрина формирует общий взгляд государства на национальную безопасность РФ.

Начиная рассматривать правовую базу регулирующую работу и защиту КИИ стоит начать с Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ в котором описываются процессы и требования позволяющее наладить устойчивое функционирование объектов КИИ.

Первым что стоит уточнить это относиться ли ваш объект к КИИ, а именно функционирует ли он в любой из представленных ниже сфер деятельности: здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.[4]

Следующим пунктом будет присвоение объекту категории значимости сама процедура подробно описана в Постановление Правительства РФ от 08.02.2018 N 127. Факторы, влияющие на присвоение объекту категории значимости представлены в таблице 1.

Таблица 1. Критерии и показатели значимости

Социальная	Ущерб жизни и здоровью граждан Обеспечение жизнедеятельности населения Транспортная инфраструктура Сети связи Гос. Услуги
Политическая	ГИС, сайты гос. Органов Международные отношения
Экономическая	Экономический ущерб Финансовые услуги
Экологическая	Окружающая среда
Обеспечение обороны	Ситуационные центры Гос. оборон заказ

Отдельно стоит отметить разницу между требованиями к офисной ИС и критически важной ИС, сравнение представлено в таблице 2.

Таблица 2. Сравнения требований для разных типов ИС.

Требование	Офисная ИС	Критически важная ИС
Производительность	Высокая	Средняя
Управление рисками	Риски определяет и управляет ими бизнес	Управляются бизнесом и государством (экология, жизнь людей и пр.)
Доступность	Средняя (допустима перезагрузка системы)	Высокая Обязателен резерв
Конфиденциальность	Определяется бизнесом	Высокая (охраняемая законом информация)
Целостность	Определяется бизнесом	Высокая (не допускается разрушение или потеря данных)

Так же стоит отметить что данные законы не рассматривают саму информацию, которую необходимо защищать, данный вопрос рассматривает федеральный закон N 149. В нем говорится что, организация должна обеспечить организационные и технические меры, направленные на обеспечение защиты конфиденциальной информации от НСД, модифицирования, уничтожения, копирования, блокирования, распространения, представления и других неправомерных действий. Информация же в свою очередь так же делаться на виды, они представлены на рисунке 1.



Рисунок 1. Субъекты информации в правовом поле

Как видно из рисунка, конфиденциальная информация включает в состав:

– коммерческую тайну;
– служебную тайну;
– профессиональную тайну;
– персональные данные.

В соответствие с Федеральным законом от 29.07.2004 N 98-ФЗ (ред. от 18.04.2018) «О коммерческой тайне» [5], в котором определены меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

– определение перечня информации, составляющей коммерческую тайну;
– ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля соблюдения такого порядка;
– учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
– регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров.

К НСД к персональным данным при их обработке в информационных системах (ИС), в частности, относятся [6]:

– доступ к персональным данным или действия с персональными данными, нарушающие установленные права и (или) правила разграничения доступа с использованием штатных средств, предоставляемых ИС;
– несанкционированное воздействие на ресурсы ИС, осуществляемое с использованием вредоносных программ (вредоносного кода).

Меры защиты информации на объектах КИИ

Разбирая меры по защите информации стоит выделить что, они принимаются на всех стадиях (этапах) создания информационной системы (определены ГОСТ 34.601-90), а также в ходе эксплуатации и вывода из эксплуатации. Меры защиты информации включают комплекс средств и способов воздействия. Обобщенная схема обеспечения защиты представлена на рисунке 2 (включая программно-аппаратные и инженерно-технические средства).

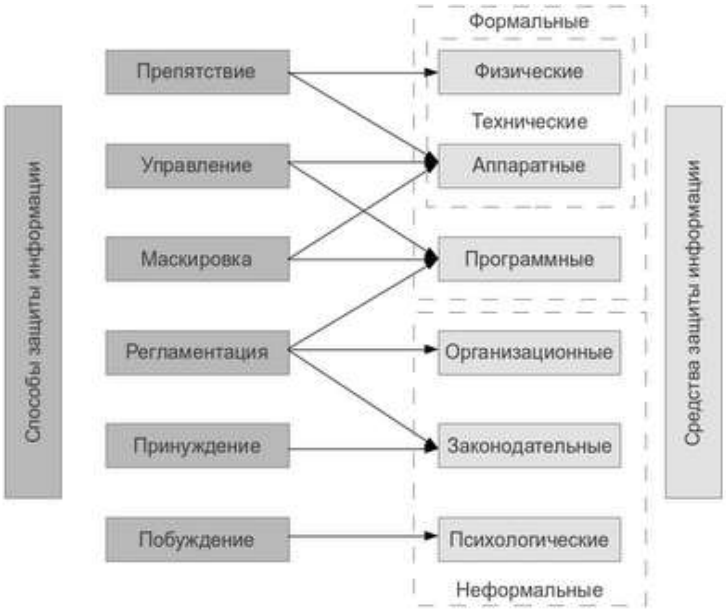

Рисунок 2. Меры защиты информации в организации

К организационно-правовым методам относятся законодательство страны, внутренние регламенты эксплуатации программного обеспечения и устав организации. По функциональному назначению средства инженерно-технической защиты делятся на следующие группы:

Физические средства – средства физической охраны (сооружения, ограждения, сейфы и т.п.). Примером также может служить охрана здания, где размещаются серверы организации. Основная задача аппаратных средств – обеспечение защиты информации от утечки и несанкционированного доступа через технические средства.

Программные средства – программные продукты, препятствующие компрометации информации даже в случае получения злоумышленником доступа к оборудованию, используемого при эксплуатации базы данных. На рисунке 2 представлена классификация средств программно-аппаратной защиты информации классической автоматизированной системы (АС).

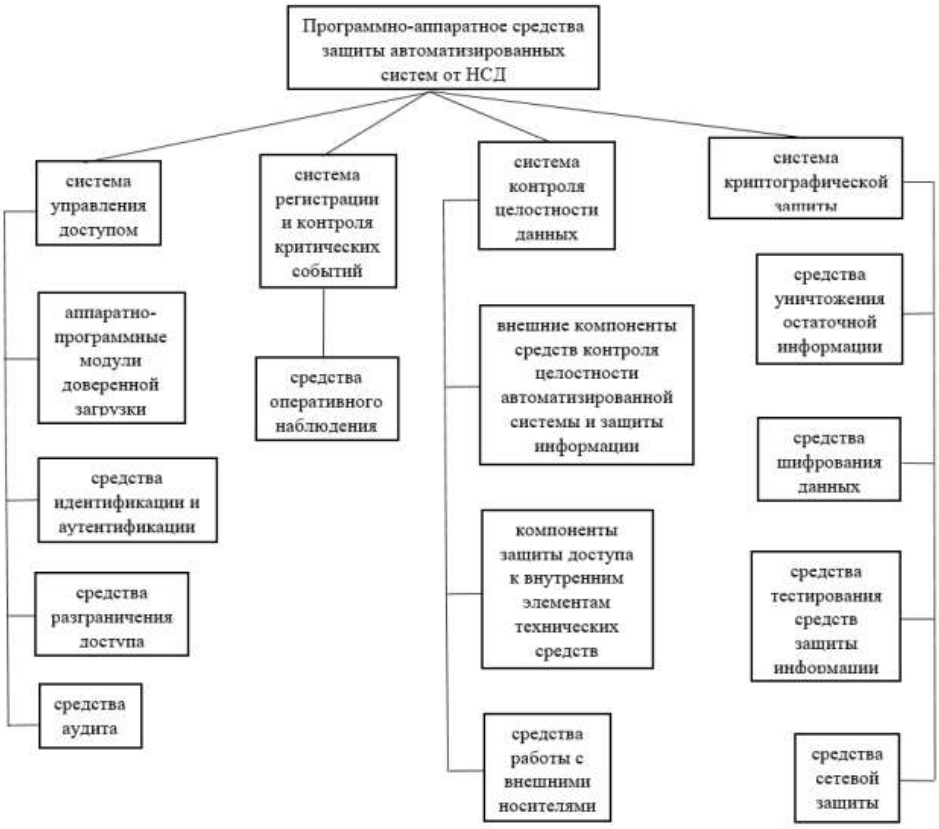

Рисунок 3. Программно-аппаратная защита информации АС

Мандатное управление доступом подразумевает сопоставление меток классификации, отражающих место субъекта в правовой иерархии – главный принцип реализации в данном методе. Посредством меток объектам и субъектам назначаются категории секретности, иерархия уязвимостей и другие классификации. По сути, данные метки служат основой мандатного принципа предоставления доступа. При вводе новой информации в ИС, комплексом средств защиты должно запрашиваться и осуществляться получение от санкционированного субъекта классификации меток данных. При плановом занесении в список пользователей нового санкционированного субъекта должно

происходить сопоставление ему классификационных меток. Внешние метки субъектов и объектов должны строго соответствовать внутренним меткам.

Дискретная модель характеризуется разграничением доступа между поименованными объектами и субъектами. Субъект с определенным уровнем доступа может передать это право другому субъекту. Для каждой пары (субъект - объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, редактировать и т.д.), которые являются санкционированными для данного субъекта (или группы субъектов) к данному ресурсу (объекту).

Заключение

Таким образом, на основе анализа нормативно-правовой документации можно сделать вывод о том, что все аспекты по обеспечению ИБ организации имеются в нормативно-правовых документах и рекомендациях на всех уровнях структуры нормативно-правовой базы.

Отдельно стоит добавить, что все рассмотренные выше меры повышают уровень защищенности на объекте, однако необходимо учитывать, что будет использоваться комплекс мер и основная задача специалиста наладить правильное их совместное функционирование. Так же необходимо уточнить что требования по обеспечению безопасности должны соблюдаться на всех стадиях его жизненного цикла: создания, эксплуатации и вывода из эксплуатации значимого объекта.

Литература

1. Конституция РФ: [принята всенар. Голосованием 12 декабря 1993 г.] : офиц. текст : по сост. на 21 июля 2014 г. – М. : Инфра-М;
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ;
3. Доктрина ИБ РФ [Электронный ресурс] URL: http://www.rg.ru/oficial/doc/min_and_vedom/mim_ bezop/doctr.shtm (дата обращения: 10.05.2021);

4. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ
5. Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ;
6. Артемов А.В. Информационная безопасность: III курс лекций / А.В. Артемов. – Орел: МАБИВ, 2018. – 125 с.
7. Федеральный Закон «О безопасности КИИ РФ» от 26.07.2017;
8. Гордиенко В. В., Лисицин А. Л. Технические и организационные методы борьбы с внутренними угрозами утечки информации организаций и предприятий // Auditorium. 2019. № 4 (24). [Электронный ресурс] URL: https://cyberleninka.ru/article/n/tehnicheskie-i-organizatsionnye-metody-borby-s-vnutrennimi-ugrozami-utechki-informatsii-organizatsiy-i-predpriyatiy (дата обращения: 10.05.2021)
9. Статистика инцидентов по отраслям компаний [Электронный ресурс] URL: https://www.ptsecurity.com/ (дата обращения 10.05.2021).
10. Шабуров А.С., Никитин А.С. Модель обнаружения компьютерных атак на объекты критической информационной инфраструктуры. – Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления, 2019;
11. Андреев Ю. С., Дергачев А. М., Жаров Ф. А., Садырин Д. С. Информационная безопасность автоматизированных систем управления технологическими процессами. Текст научной статьи по специальности «Компьютерные и информационные науки», университет ИТМО, 2019

Literature

1. The Constitution of the Russian Federation: [adopted by the General Assembly. By voting on December 12, 1993]: officer. text: according to comp. on July 21, 2014 - M.: Infra-M;
2. Federal Law "On Information, Information Technologies and Protection" of 27.07.2006 N 149-FZ;

3. Doctrine of the IS RF [Electronic resource] URL: http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop / doctr.shtm (date of access: 05/10/2021);
4. Federal Law "On the Security of Critical Information Infrastructure of the Russian Federation" dated 26.07.2017 N 187-FZ.
5. Federal Law "On Commercial Secrets" dated July 29, 2004 N 98-FZ;
6. Artemov A.V. Information security: III course of lectures / A.V. Artyomov. - Oryol: MABIV, 2018 .-- 125 p.
7. Federal Law "On the safety of the CII RF" dated July 26, 2017;
8. Gordienko VV, Lisitsin AL Technical and organizational methods of dealing with internal threats of information leakage of organizations and enterprises // Auditorium. 2019. No. 4 (24). [Electronic resource] URL: https://cyberleninka.ru/article/n/tehnicheskie-i-organizatsionnye-metody-borby-s-vnutrennimi-ugrozami-utechki-informatsii-organizatsiy-i-predpriyatiy (date accessed: 10.05.2021)
9. Statistics of incidents by industry of companies [Electronic resource] URL: https://www.ptsecurity.com/ (date of treatment 05/10/2021).
10. Shaburov A.S., Nikitin A.S. Model of computer attacks on objects of critical information infrastructure. - Bulletin of the Perm National Research Polytechnic University. Electrical engineering, information technology, control systems, 2019;
11. Andreev Yu. S., Dergachev AM, Zharov FA, Sadyrin DS Information security of automated control systems for technological processes. Text of a scientific article in the specialty "Computer and Information Sciences", ITMO University, 2019.