УДК 004.056

Киселев Николай Николаевич
аспирант, МГТУ им. Н.Э. Баумана, Москва
Kiselev Nikolay Nikolaevich
Bauman Moscow State Technical University

Научный руководитель:
Смирнов Сергей Николаевич, д.т.н., профессор,
МГТУ им. Н.Э. Баумана, Москва
Smirnov Sergey Nikolaevich
Bauman Moscow State Technical University

ЗАКОНОДАТЕЛЬСТВО И ОРГАНИЗАЦИОННЫЕ МЕРЫ КАК ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РЕГИОНАЛЬНОГО УРОВНЯ УПРАВЛЕНИЯ В МЕДИЦИНСКОМ УЧРЕЖДЕНИИ
LEGISLATION AND ORGANIZATIONAL MEASURES AS THE BASIS OF INFORMATION SECURITY OF THE CRITICAL INFORMATION INFRASTRUCTURE OF THE REGIONAL MANAGEMENT LEVEL

Аннотация: В данной статье проводится обзор и анализ законодательства РФ и специализированных мер, регламентирующих информационную безопасность критически важной информационной инфраструктуры регионального уровня управления. Представлена структура и перечень этапов процесса категорирования объекта критической информационной инфраструктуры (далее по тексту – КИИ), с акцентом на особенности регионального уровня управления.

Abstract: This article analyzes and reviews the legislation of the Russian Federation and specialized measures regulating information security of critical information infrastructure at the regional management level. A detailed study was conducted on what a critical information infrastructure is (hereinafter referred to as CII), how to categorize CII.

Ключевые слова: законодательство РФ в области КИИ, информационная безопасность, критическая информационная инфраструктура, категорирование объекта КИИ, управление.

Keywords: legislation, measure, information security, critical information infrastructure, management.

Введение. В 2017 году был принят Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее по тексту – Закон «О безопасности КИИ»), который вступил в силу в 2018 г [1]. Данный закон касается государственных и частных организаций, которые функционируют в областях, критически значимых для жизни страны – в частности тех, сбой в работе которых скажется на состоянии здоровья, защищенности, а также комфорте граждан Российской Федерации.

Материалы и методы. Используя метод компьютерной обработки, проведен анализ отечественной литературы, а также законодательства России посвященной данной проблеме.

Целью исследования является разработка алгоритмов действий организации КИИ, необходимых для обеспечения защиты информационной инфраструктуры КИИ в соответствии с действующим законодательством. Указанной целью определены постановка и решение следующих задач:

1. Выявление сущностно-содержательных аспектов информационной инфраструктуры КИИ.
2. Определение понятия критической информационной инфраструктуры.
3. Исследование роли и значения Государственной системы выявления, предотвращения также ликвидации результатов компьютерных атак для обеспечения деятельности региональных объектов КИИ.

4. Изучение и анализ уголовно-правовой характеристики наказаний.

К областям деятельности, подпадающим под действие Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» относятся здравоохранение, наука, автотранспорт, связь, электроэнергетика, банки, топливная индустрия, ядерная энергетика, оборонная индустрия, ракетно-космическая индустрия, горнодобывающая индустрия, металлургическая индустрия также химическая индустрия. Кроме того сюда относят компании, которые обеспечивают работу организаций данных областей, например, дают спецоборудование в аренду либо разрабатывают для них программное обеспечение (далее по тексту – ПО).

Нарушения нормального режима деятельности организации из данной области приведет к отрицательным последствиям, которые окажут негативное воздействие на качество жизни для граждан всей страны. По этой причине к IT-инфраструктуре, а также безопасности информационных технологий на этих фирмах предъявляют специальные требования [7].

Федеральный закон определяет области деятельности определяющие объекты КИИ, в которых работают организации. Это организации, осуществляющие свою деятельность в области здравоохранения, энергетики, транспорта, связи, оборонной промышленности.

На рис.1 наглядно представлены объекты и субъекты КИИ.

Рис.1. Объекты и субъекты КИИ [8].

В случае если нормальная деятельность организации из данной области будет нарушена, это отрицательно скажется на уровне жизни граждан, общества и государства. По этой причине к IT-инфраструктуре также безопасности информационных систем на этих фирмах предъявляют специальные требования [7].

К одной из особенностей медицинских учреждений регионального уровня можно отнести дефицит квалифицированных кадров в областных центрах, способных обеспечить необходимые требования безопасности информационных систем, а также полное их отсутствие в некоторых отдаленных муниципальных образованиях. Например, в подведомственном учреждении министерства здравоохранения – медицинском информационно-аналитическом центре такие специалисты есть, но их количество не позволяет в должной мере реализовать спектр задач на территории всего субъекта.

Следует отметить, что поддержку специалистам информационно-аналитическом центра могут оказать специалисты областной больницы, которые обладают некоторым уровнем необходимой квалификации. Но в городских больницах и других медицинских пунктах, в том числе удаленных, специалистов с достаточным уровнем квалификации практически нет.

Внимание к деталям, обусловленное медицинской спецификой, работников больниц подкрепленное исполнительской дисциплиной, обеспечиваемой административным ресурсом руководителя больницы или поликлиники, можно превратить в конкретные действия, необходимые для обеспечения защиты информационной инфраструктуры КИИ в соответствии с действующим законодательством. Для этого необходимо предложить четкую и понятную для непрофильного сотрудника методику, ориентируясь на сотрудника, работающего в медицинской организации продолжительное время и подробно знающего внутреннюю работу медучреждения.

На сотрудника, обладающего необходимыми компетенциями, можно возложить задачу по сбору, анализу и предоставлению необходимых сведений в головные организации. Предлагаемый подход отличается от распространенной в настоящий момент практики возложения задач на непрофильного специалиста. Обычно, при такой формальной процедуре назначенный специалист даже не знает, что необходимо делать и какие критерии успешности его деятельности будут применяться для оценки.

Основные положения закона об информационной безопасности (далее по тексту ИБ) критически важных структур:

– в целях защиты критической инфраструктуры создана Государственная система выявления, предотвращения и ликвидации результатов компьютерных атак (ГосСОПКА);

– предметы критически значимой инфраструктуры должны быть присоеденены к ГосСОПКА. Для этого необходимо определить и приобрести специальное ПО, которое будет использоваться для наблюдения за защищенностью инфраструктуры компании;

– одна из ключевых мер предотвращения результатов компьютерных атак – контроль и сертификация технического оснащения, ПО и, при необходимости, всей инфраструктуры; данный комплекс мероприятий применяется на предприятиях, отнесенных к критически важной инфраструктуре;

– субъекты критической информационной инфраструктуры должны информировать федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (на текущий момент, согласно Указу Президента Российской Федерации от 22.12.2017 № 620, это Федеральная служба безопасности РФ) об инцидентах в собственных информативных системах;

– осуществлять требования муниципальных служащих предъявляемые к организации системы защиты информации и используемым средствам обеспечения защиты информации, так как это предписывает закон. Например, применять только лишь сертифицированное Федеральной службой безопасности и Федеральной службой по техническому и экспортному контролю ПО;

– все без исключения IT-системы критически важных предприятий обязаны быть защищены от незаконного доступа, а также постоянно взаимодействовать с ГосСОПКА. При разработке IT-инфраструктуры критически важные предприятия обязаны руководствоваться приказом № 239 от 25 декабря 2017 г. ФСТЭК. В нем определены основные требования к организации защиты данных на соответствующих предприятиях;

– Правительство РФ при необходимости осуществляет дополнительный, в том числе внеплановый, контроль объектов критически важной инфраструктуры, в частности, при фиксации компьютерных инцидентов типа взлома систем, либо утраты информации.

Результаты и обсуждение. Критическая информационная инфраструктура – это информационные системы справочно-телекоммуникационные сети, автоматизированные системы управления, но кроме того сети электросвязи, применяемые в целях организации их взаимодействия. Основным обстоятельством отнесения системы к КИИ считается ее применение государственным органом либо учреждением, или российской фирмой, ведущей деятельность в сфере 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 [6].

К мерам защиты конфиденциальной информации относятся правовые, организационные, технические, а также способы их реализации. В ряде практических случаев реализация технических мер защиты сводится к выбору в приобретении средства защиты информации того или иного вендора. Учтивая, что рынок данный вопрос в некоторой степени регулирует, то приобретение тех или иных средств будет определено финансовыми возможностями организации и удобством использования средств для конкретных сотрудников или подразделений, которые эти средства применяют. С организационными и правовыми мерами ситуация обстоит сложнее. В ряде организаций могут возникнуть трудности при отнесении своих систем к той или иной категории. Соответственно и выбор необходимых мер средств будет также существенно различаться.

К КИИ будут иметь отношение системы, которые на праве собственности, аренды либо на другом законной основе управляются российской компанией, либо ИП и обеспечивают решение возложенных на них задач, включая интеграцию и гарантированную связь с системами или сетями более высокого уровня.

ГосСОПКА – это общий регионально распределенный спецкомплекс, содержащий силы и ресурсы, назначенные для выявления, предотвращения и ликвидации результатов компьютерных атак также реагирования на компьютерные инциденты (далее по тексту – КИ).

Согласно собственной сути, ГосСОПКА считается регионально распределенной совокупностью центров (сил также средств), в числе которых – Национальный координационный центр по компьютерным инцидентам (далее по тексту – НКЦКИ).

Обобщенная структура ГосСОПКА показана на рис.2.

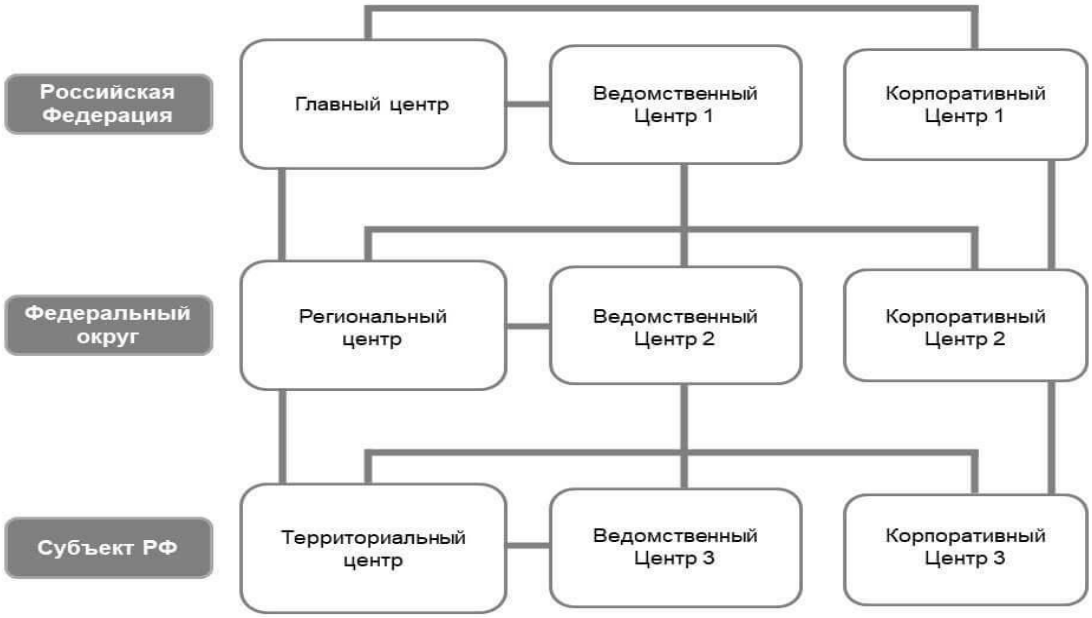

Рис.2. Обобщенная структура ГосСОПКА [9].

НКЦКИ – структура, отвечающая за управление и координацию работы субъектов КИИ, является ключевой составляющий частью ГосСОПКА.

НКЦКИ создана и сформирована в соответствии с приказом ФСБ Российской Федерации №366 от 24 июля 2018 г. «О Национальном координационном центре по компьютерным инцидентам» [5].

В функции НКЦКИ входит:

– координация реакции на события и содействие в мероприятиях согласно реагированию на КИ;

– организация и реализация взаимообмена данными о КИ в структуре ГосСОПКА;

– осуществление методического обеспечения деятельности подчиненных организаций;

– участие в мероприятиях по обнаружению, предотвращению и ликвидации результатов компьютерных атак;

– обеспечение уведомления о компьютерных атаках уполномоченных органов государственной власти и организаций;

– сбор и исследование данных о КИ.

Все работы по обеспечению информационной безопасности критически важной информационной инфраструктуры можно разделить на 2 большие группы:

1. Категорирование КИИ.
2. Проектирование и внедрение СОИБ КИИ.

Группа работ по категорированию включат в себя этапы, показанные на рис.3.

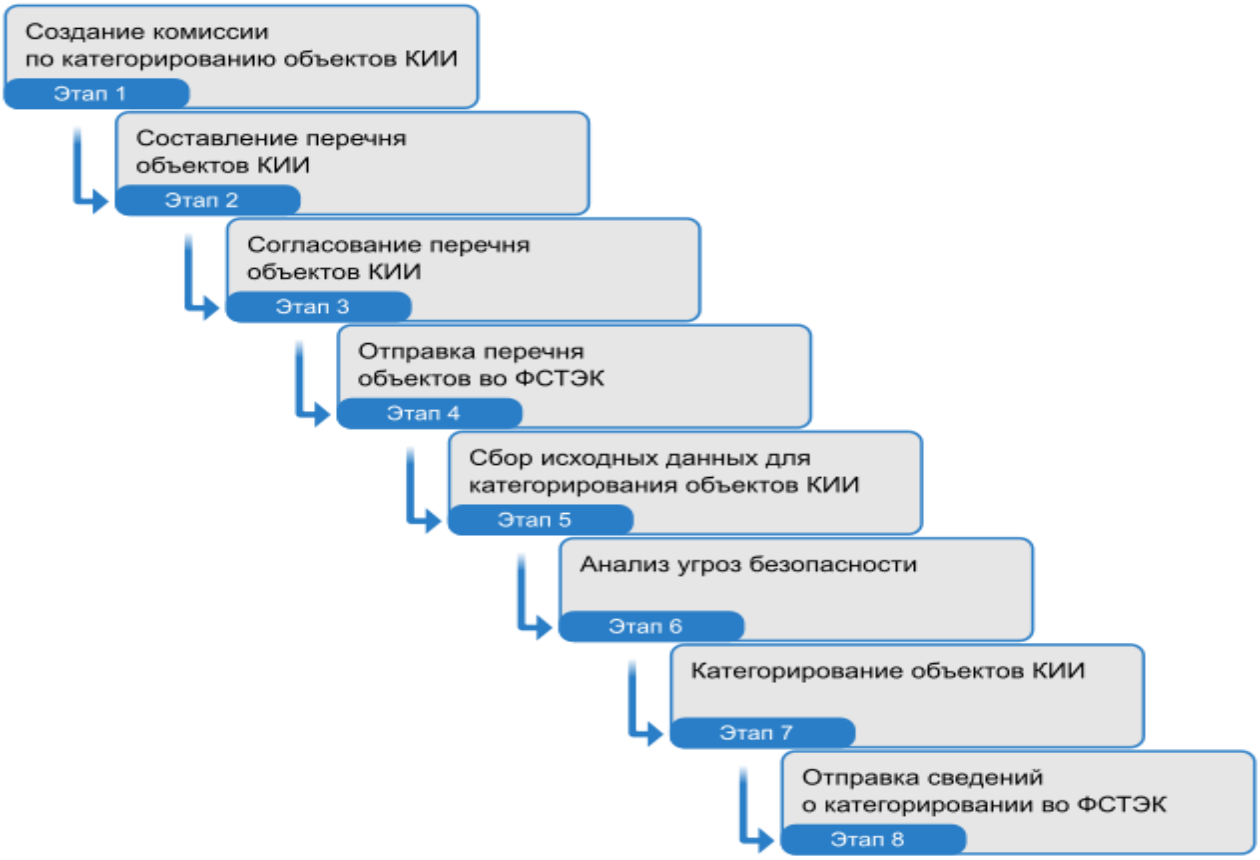

Рис.3. Этапы группы категорирования [10].

Вторая группа «Проектирование и внедрение СОИБ КИИ» включает в себя этапы:

– Этап 10. Проектирование СОИБ КИИ

– Этап 11. Внедрение СОИБ КИИ

– Этап 12. Разработка организационно-распорядительной документации (ОРД) для субъекта и объектов КИИ

Результатом работ должна быть функционирующая система предоставления информационной защищенности критической информационной инфраструктуры.

В Приказе ФСТЭК Российской Федерации №239 указывается, что приоритетным является использование интегрированных средств охраны. Также отмечается, что организации обязаны использовать средства охраны, прошедшие оценку соотношения в формах сертификации, испытаний, либо приемки.

Таким образом, сертифицированные ресурсы охраны обязаны использоваться не во всех случаях. Но, если сертифицированные средства используются, в организации необходимо наличие соответствующих сертификатов. Таблица категорий сертификатов представлена в таб.1.

Таблица 1

Категория сертификата

Категория значимости \ Сертификат	СЗИ	СВТ	НДВ
1 категория	не ниже 4	не ниже 5	не ниже 4
2 категория	не ниже 5	не ниже 5	не ниже 4
3 категория	не ниже 6	не ниже 5	–

[Составлено автором].

Выше проведен анализ перечня субъектов и объектов КИИ и перечня необходимых действий для исполнения требований ФСТЭК.

Анализ был бы не полным без описания ответственности, образующейся в случае невыполнения условий обеспечения требований ИБ на объектах КИИ. Согласно Указа Президента РФ от 25.11.2017 г. №569 [4], утвержденным Указом Президента РФ с 16.08.2004 г. №1085 федеральным органом исполнительной власти (ФОИВ), уполномоченным в сфере обеспечения защищенности КИИ является ФСТЭК. Правительственный надзор в сфере обеспечения защищенности значимых объектов КИИ будет реализовывать ФСТЭК в виде плановых, а также неплановых проверок с дальнейшим оформлением соответствующего предписания в случае обнаружения нарушений.

Плановые проверки проводятся:

– по истечении 3-х лет со дня внесения данных об объекте КИИ в реестр;

– по истечении 3-х лет со дня реализации последней плановой проверки.

Неплановые проверки могут быть проведены в случае:

– истечения срока выполнения субъектом КИИ предписания об устранении обнаруженного нарушения;

– появления КИ, повлекшего отрицательные результаты;

– согласно поручению Президента РФ, либо Правительства РФ, или на основе требования Прокуратуры РФ.

Если ФСТЭК обнаружит несоблюдение предусмотренных законодательством процедур и регламентов, будет выписано предписание с определенным сроком ликвидации, который возможно будет продолжить по уважительным обстоятельствам. Отметим, что возможен вариант проверки Прокуратурой РФ, которая начинается с постановления об управленческом правонарушении, со ссылкой на статью 19.5 ч.1 КоАП РФ о невыполнении в определенный период постановления госнадзорного органа [3].

Отметим еще несколько важных моментов о мерах наказания, которые предусмотрены за невыполнение условий по обеспечению безопасности критической информационной структуры. В соответствии с Федеральным законом от 26.07.2017 № 194-ФЗ «О внесении изменений в УК РФ и УПК РФ» [2] во взаимосвязи с принятием ФЗ «О безопасности критической информационной инфраструктуры РФ» предусмотрена наибольшая мера наказания, за нарушения норм безопасности КИИ, которой является лишение свободы вплоть до 10 лет.

Автоматизация и наличие интернет доступа в медицинских учреждениях стали практически повсеместными. В 2019-2020 годах на территории отдаленных районов субъекта Федерации организован доступ во всемирную паутину, а значит и возможность предоставлять услуги в цифровом формате получили 13 фельдшерско-акушерских пунктов.

Учитывая, что все медорганизации, которые пользуются информсистемами, информационно-телекоммуникационными сетями, автоматизированными системами управления, – являются субъектами критической информационной инфраструктуры, можно утверждать, что в подавляющем большинстве регионов в медицинских организациях имеются объекты КИИ.

Данный факт позволяет рассмотреть медицинскую организацию как типовой объект КИИ с возможностью дальнейшей экстраполяции результатов исследования на конкретное учреждение.

Для наглядности, рассмотрим процесс категорирования объектов КИИ в здравоохранении, а именно процесс оценки необходимости выполнения требований ФЗ № 187 на примере медицинского учреждения «Клиника».

Медицинское учреждение «Клиника» является юридическим лицом и имеет согласно ОКВЭД следующие виды деятельности: Основной вид деятельности: – 86.22 Специальная врачебная практика. Дополнительные виды деятельности: – 85.30 Обучение профессиональное; – 86.21 Общая врачебная практика.

Медицинские организации, как правило, являются юридическими лицами или государственными учреждениями. В рассматриваемом примере организация – юридическое лицо. Для государственного учреждения в сфере здравоохранения дальнейший анализ проводится аналогично.

Первоначально необходимо определить сферу деятельности. Основным видом деятельности организации является ОКВЭД 86.22 «Специальная врачебная практика», и дополнительным ОКВЭД 86.21 «Общая врачебная практика», которые входят в группу 86 «Деятельность в области здравоохранения», соответственно медицинское учреждение функционирует в сфере здравоохранения. Помимо сферы здравоохранения, в некоторых случаях, организация может функционировать в других сферах. В таком случае рассматриваются обе сферы.

На следующем этапе необходимо определить, согласно ФЗ-187, принадлежат ли организации на праве собственности, аренды или на ином законном основании информационные системы, информационно-телекоммуникационные сети и/или автоматизированные системы, функционирующим в сфере здравоохранения, т.е. высокотехнологичное компьютеризированное оборудование (томографы, лаборатории, рентгены и т.п.).

На этом этапе возможны два варианта.

1. Вариант 1. Организации не принадлежат описанные системы. Такое возможно если организация имеет только неавтоматизированное медицинское оборудование (например, стоматологическая установка) и бумажный документооборот. В этом случае, может быть сделан вывод, что Клиника является юридическим лицом, функционирующим в сфере здравоохранения, но автоматизированные системы, функционирующие в этой сфере, отсутствуют, следовательно, организация не является субъектом КИИ хотя и функционирует в сфере здравоохранения, и в выполнении контроля требований ФЗ № 187 нет необходимости.
2. Вариант 2. Организация имеет высокотехнологичное автоматизированное компьютеризированное оборудование (например, рентгенодиагностические аппараты с цифровым терминалом, гамма-камеру, автоматизированные лаборатории и т.п.). В этом случае организации принадлежат на праве собственности, аренды или на ином законном основании автоматизированные системы, функционирующие в сфере здравоохранения, поэтому Клиника является субъектом КИИ, которому необходимо выполнять требования ФЗ № 187.

Здесь необходимо обратить внимание на юридически значимое определение права собственности. Принадлежит – числится на балансе, оборудование физически размещено в организации, информационные системы документально введены в эксплуатацию и т.п. Если имеющееся система используется, но не принадлежит Клинике (система вышестоящей организации, для которой Клиника просто пользователь, например, информационная система «Инфоклиника» (принадлежит МИАЦ), Федеральный Регистр сахарного диабета (принадлежит ФГБУ Эндокринологический Научный Центр) и т.п.), то такую систему рассматривать в контексте КИИ не нужно.

Если же по результатам проведенного анализа организация является субъектом КИИ, то необходимо проводить работы по категорированию.

Приведем описание медицинского учреждения, которое будет накладывать ограничения на предлагаемую модель.

Отличительной особенностью будет являться удаленность от регионального центра. Существенной особенностью будет являться отсутствие компетентных кадров области ИБ или ИТ.

Учитывая отдаленность, невысокую численность населения и персонала, узкий характер взаимодействия между собой (все друг друга знают) появление внешнего человека вызовет повышенный интерес и внимание к его персоне, вследствие этого, а также требований соблюдения режима контролируемой зоны появление внешнего нарушителя в физическом периметре можно в модели нарушителя не учитывать.

Учитывая невысокий интерес в большинстве случаев к малой организации со стороны внешних нарушителей из сетевого пространства, то внешний нарушитель – это либо дилетант, либо автоматизированный робот, либо случайный нарушитель. Соответственно имеет низкую подготовку и осведомленность.

К мотивам внешнего нарушителя следует в таком случае отнести шалость в сети или автоматизированный сбор каких-либо сетевых сведений.

Также, учитывая отсутствие компетенций, подготовленность внутреннего нарушителя можно считать низкой или по крайней мере не выше средней.

Мотивы внутреннего нарушителя могут быть различными. Для целей составления модели угроз существенны два фактора – случайный или намеренный.

Действие случайного фактора можно снизить путем регламентации действий. От намеренного фактора призван защищать закон и ответственность за его неисполнение, а также система мер обеспечения ИБ на КИИ.

Реализация данных рисков может вызвать отказ в работе оборудования и в итоге причинить ущерб здоровью человека.

Таким образом исполнение требований законодательства и обеспечение организационных мер защиты для представленной модели медицинского учреждения будет не только основой обеспечения информационной безопасности, а также будет способствовать защите от приведенных в модели угроз и снижать до приемлемого уровня соответствующие риски.

Перечень действий для организации, субъекта КИИ в здравоохранении, для выполнения требований ФЗ №187 «О безопасности КИИ в РФ»:

1. Создать комиссию по категорированию (Приказ о создании комиссии по категорированию объекта КИИ);
2. Определить и направить в ФСТЭК перечень объектов КИИ, утвержденный Информационным сообщением ФСТЭК от 24 августа 2018 г. № 240/25/3752 (Образец перечня объектов КИИ подлежащих категорированию);
3. Провести анализ актуальных угроз;
4. Провести категорирование в соответствии с Постановлением Правительства №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;
5. Составить акт результатов категорирования;
6. Направить сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий в ФСТЭК.

Форма сведений в ФСТЭК утверждена Приказом N 236 от 22 декабря 2017 г. «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

На основании необходимого перечня действий для выполнения требований законодательства составим методику для непрофильного сотрудника медицинского учреждения:

1. Запросить в головной организации при необходимости образец приказа о создании комиссии по категорированию объекта КИИ, указав в запросе должности и функционал сотрудников учреждения, предлагаемых для включения в состав комиссии с целью подтверждения легитимности их включения в комиссию.

2. Предоставить в головную организацию перечень используемого оборудования и цели его применения в целях определения объектов КИИ. В целях упрощения и ускорения взаимодействия данная процедура возможна как в письменном, так и в устном формате.

3. Совместно с компетентными сотрудниками провести анализ угроз, исходя из предложенной модели нарушителя и реальных условий функционирования организации и эксплуатации оборудования. При анализе необходимо руководствоваться своим опытом и знаниями, а также опираться на опыт коллег, исходя из возможности реализации наихудшего варианта развития предполагаемых событий реализации угрозы. Отдельное внимание при этом следует уделять обеспечению объектов гарантированным электропитанием.

4. Убедиться в корректности проведения категорирования путем сопоставления с правилами и с учетом мнения коллег и экспертов. После чего направить сведения во ФСТЭК.

Приводимая методика создана для возможности оценки непрофильными специалистами состояния объекта КИИ с целью присвоения ему одной из категорий значимости.

В качестве прототипа предлагаемого подхода целесообразно рассматривать информационную систему, контролирующую мероприятия по информационной безопасности на территории одного из субъектов федерального округа.

Спецификой рассматриваемых систем в области медицинского обслуживания населения является сравнительно высокий уровень финансирования в сфере цифровизации в целом и информационной безопасности в частности.

Для эффективной эксплуатации высокотехнологичных систем медицинского обслуживания населения необходимо создание и аттестация по требованиям безопасности информации соответствующих подсистем обеспечения информационной безопасности КИИ. Наличие таких подсистем позволит обеспечивать оперативное информирование операторов информационных систем субъекта об актуальных угрозах безопасности, а также осуществлять контроль реализации рекомендованных регуляторами мер защиты.

Анализ приведенного в статье варианта методики для цифровой информационной системы указывает на необходимость затрат значительных средств для создания и аттестации подсистемы и технических мощностей для ее развертывания. Кроме того, сопровождение системы требует специальных знаний и навыков. Указанные факторы затрудняют ее применение в отдаленных районах субъектов России.

Предложенную в статье методику целесообразно применять в условиях наличия отдаленных медицинских учреждений при отсутствии на местах квалифицированных ИТ-кадров.

В этих условиях экономически эффективнее собирать сведения в традиционных форматах, а часть задач передавать для решения силами, имеющимися на местах, оказывая им методическую поддержку и руководство.

Такой вариант организации работ несколько ухудшит временные характеристики системы, но снизит требования к квалификации специалистов. Предлагаемый подход снизит нагрузку на головные учреждения в части поддержки подведомственных организаций, а сами организации избавит от необходимости содержать выделенного сотрудника для обеспечения требований обеспечения безопасности КИИ.

Расширение предложенной методики путем создания алгоритмов действий по обеспечению информационной безопасности КИИ для конкретного удаленного медучреждения может позволить избежать необходимости выезжать и обследовать объекты на месте со стороны головных организаций и тем самым позволит осуществить экономию бюджетных средств, а также ускорить работу по выполнению требований регуляторов в данном направлении.

Практическая значимость для обеспечения безопасности КИИ в медицинском учреждении на региональном уровне будет состоять в том, что работу по определению объектов КИИ с присвоением ему одной из категорий значимости и направлением этих сведений в головные организации можно будет вести по плану и на регулярной основе, вне зависимости от выделения средств на выездные командировки.

Предлагаемый вариант позволит улучшить состояние работ по обеспечению информационной безопасности объектов КИИ медицинской сферы в субъекте Федерации.

Заключение. Проведенное исследование позволяет сформулировать следующие выводы:

1. Региональные КИИ – это комплекс автоматизированных технологий управления производственными и научно-техническими процессами критически важных объектов РФ, которые обеспечивают решение задач правительственного управления, обеспечения обороноспособности, защищенности и правопорядка граждан, общества и государства.

2. Проект приказа ФСТЭК о подключении 30 объектов КИИ к интернету предполагает постановку новых задач в области обеспечения информационной безопасности объектов КИИ. Он будет действовать только для вновь формируемых объектов и потребует согласования подключения объектов КИИ к сети связи единого пользования путем направления во ФСТЭК копии модели угроз, в том числе схемы организации связи, номеров сертификатов, либо протоколов оценки тестирования объектов КИИ.

3. Аттестация объектов КИИ в сфере здравоохранения является сложной задачей, требующей специальных знаний и/или четких инструкций для предоставления сведений в головную организацию, способную провести анализ на уровне, достаточном для вынесения решения регулятора.

Проблема состоит в том, что с одной стороны, есть типовые решения по типам информационных систем в сфере здравоохранения и требованиям к ним, с другой стороны, имеются информационные системы, обладающие определенной спецификой. На абстрактном уровне оба типа систем обеспечивают схожие, а может быть и одинаковые процессы. При определении принадлежности конкретного регионального медицинского объекта к объектам перечня объектов КИИ необходимо учитывать наличие соответствующих ресурсов. При этом не включение в перечень каково-либо конкретного объекта может повлечь за собой нарушении безопасности критической информационной инфраструктуры Российской Федерации, что недопустимо.

Результат работы авторов заключается в сужении круга возможных нарушителей в региональном медицинском учреждении и составлении упрощенной методики для проведения категорирования, без необходимости детального погружения в специфику, основанной на законодательстве и организационных мерах. Он позволит непрофильному специалисту провести категорирование объекта КИИ с целью присвоения ему одной из категорий значимости. При этом указанному сотруднику не потребуется проходить для этого специальную подготовку, что снизит как временные характеристики скорости оценки или переоценки отдаленных объектов КИИ, так и финансовую нагрузку на медицинские учреждения, связанную с необходимостью обучения сотрудников.

Научная новизна заключается оригинальном походе к разработке методики, модели нарушителя, основанных на практическом опыте работы в органах исполнительной власти, имеющего в своем составе отдаленные медицинские учреждения, в организации подчинения которых к сети широкополосного доступа и приёмке работ автор принимал непосредственное участие.

Список литературы:

1. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ (последняя редакция) // Собрание законодательства 26 июля 2017 года N 187-ФЗ

2. Федеральный закон "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 194-ФЗ (последняя редакция) // Собрание законодательства

3. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 01.07.2021, с изм. от 09.11.2021) (с изм. и доп., вступ. в силу с 01.12.2021) // Собрание законодательства

4. Указ Президента Российской Федерации от 25.11.2017г. №569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085» // Российская газета

5. Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 366 "О Национальном координационном центре по компьютерным инцидентам" // Российская газета (Зарегистрирован 06.09.2018 № 52109)

6. Повышение уровня стратегической безопасности объектов критически важной информационной инфраструктуры / Н. А. Фомин, А. И. Самошина, О. О. Евсютин [и др.] // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2020. – № 7. – С. 161-166. – DOI 10.37882/2223-2966.2020.07.36.

7. Хлопов О.А. Проблемы кибербезопасности и защиты критической инфраструктуры // The Scientific Heritage. 2020. №45-5 (45). URL: https://cyberleninka.ru/article/n/problemy-kiberbezopasnosti-i-zaschity-kriticheskoy-infrastruktury (дата обращения: 20.12.2021).

8. Инжиниринговый Центр «Региональные системы» – https://www.ec-rs.ru/blog/all/bezopasnost-kii-korotko-o-glavnom/ (дата обращения 20.12.2021)

9. ООО "АМ Медиа" – https://www.anti-malware.ru/practice/solutions/gossopka (дата обращения 20.12.2021)

10. ООО «РТМ ТЕХНОЛОГИИ» – https://rtmtech.ru/articles/kriticheskaya-informatsionnaya-infrastruktura-2019/ (дата обращения 20.12.2021)