**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ

УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ

(национальный исследовательский университет)»

**Факультет (институт, филиал) №4 Кафедра 406**

**Направление подготовки Радиотехника Группа М4В-302Б**

**Квалификация (степень) \_\_\_\_\_Бакалавриат\_\_**

**РЕФЕРАТ**

На тему: Кретическая информационная инфроструктура и безопасность его объектов

Реферат сдал\_Мартынов Артем Анатольевич\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_)

(фамилия, имя, отчество)

Реферат принял Терехин Алексей Геннадиевич\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_)

(фамилия, имя, отчество)

Москва 2020

**ОГЛАВЛЕНИЕ**

[Введение 3](#_Toc59101842)

[1 Критическая информационная инфраструктура 4](#_Toc59101843)

[2 Безопасность объектов критической информационной инфраструктуры 8](#_Toc59101844)

[Заключение 13](#_Toc59101845)

[Список использованных источников 14](#_Toc59101846)

ВВЕДЕНИЕ

В настоящее время почти все сферы жизни личности, общества и государства стали зависимыми от информационных инфраструктур. Поэтому тема информационной безопасности является актуальной на мировом уровне. Кибератакам чаще всего подвергаются объекты критической информационной инфраструктуры: информационные системы, информационно-телекоммуникационные системы, автоматизированные системы управления государственных органов, государственных учреждений и компаний, которые функционируют во всех областях жизнеобеспечения городов, субъектов и всей страны.

Конкурентным преимуществом на мировом рынке обладают государства, у которых отрасль экономики основывается на технологии анализа больших объемов данных. Эти технологии также активно используют в России, но они основаны на зарубежных разработках. На данный момент отечественные аналоги отсутствуют. Повсеместное внедрение зарубежных информационных технологий и коммуникаций, в том числе на объектах критической информационной инфраструктуры (КИИ), значительно усложняет решение задачи по обеспечению защиты интересов граждан и государства в информационной сфере.

Таким образом, целью данной работы выступает исследование критической информационной инфраструктуры и безопасности ее объектов.

В соответствии с поставленной целью в работе предстоит решить задачи:

- описать понятие критической информационной инфраструктуры;

- охарактеризовать особенности безопасности ее объектов;

- сделать выводы по работе в целом.

1 КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА

В соответствии с законодательством РФ критическая информационная инфраструктура - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов[[1]](#footnote-1).

Критическая информационная инфраструктура – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, а также сети электросвязи, используемые для организации их взаимодействия. Ключевым условием отнесения системы к КИИ является ее использование государственным органом или учреждением, либо российской компанией в следующих сферах:

* здравоохранение;
* наука;
* транспорт;
* связь;
* энергетика;
* банковский (финансовый) сектор;
* топливно-энергетический комплекс;
* атомная энергетика;
* оборонная промышленность;
* ракетно-космическая промышленность;
* горнодобывающая промышленность;
* металлургическая промышленность;
* химическая промышленность.

Также к КИИ будут относиться системы, которые на праве собственности, аренды или на ином законном основании принадлежат российской компании или ИП, и обеспечивают взаимодействие указанных выше систем или сетей.

Вне зависимости от типа системы, к которой принадлежит объект КИИ, основным ресурсом, подверженным изменению из киберсреды, является информация. В задачи систем безопасности объектов КИИ входит предотвращение неправомерного доступа, уничтожения, изменения, блокирования, копирования и распространения защищаемой информации, других неправомерных действий в отношении такой информации, недопущения воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование объекта КИИ. От систем безопасности также требуется восстановление функционирования объектов КИИ. Исходя из этого значимые объекты КИИ являются объектами защиты информации, к которым должны быть предъявлены требования по безопасности информации и реализованы меры по защите информации. Каждому значимому объекту КИИ должен быть присвоен класс безопасности. Одним из критериев значимости объектов КИИ определена социальная значимость, которая выражается, например, в возможном ущербе при нарушении доступа к государственным услугам[[2]](#footnote-2).

Одной из основных проблем государственного регулирования вопросов информационной безопасности до недавнего времени являлся конфликт интересов с одной стороны — бизнеса, с другой — государства и общества. Как правило, при принятии решения о необходимости тех или иных мер защиты владелец информационной системы оценивает свои потери от возможных инцидентов и сравнивает их со стоимостью мер защиты от этих инцидентов. С его точки зрения защита нецелесообразна, если затраты на нее превышают возможные его потери при отсутствии такой защиты. К сожалению, при этом владельцы информационных систем чаще всего принимают в расчет только свои потери, игнорируя сопутствующий ущерб. Если в результате выхода из строя АСУ ТЭЦ город на три дня останется без тепла, это приведет к падению выручки компании менее чем на один процент. Это потери, статистически неотличимые от нуля, и с финансовой точки зрения владелец ТЭЦ мог бы с ними смириться. Для города же три дня, проведенные без тепла и горячей воды, — катастрофа, которую трудно оценить в финансовом выражении[[3]](#footnote-3). Чтобы решить эту проблему, в законе введено понятие «категория значимости».

Категория значимости — это характеристика объекта КИИ, которая позволяет провести водораздел: вот с этими объектами владелец может поступать, как ему заблагорассудится, а вот эти объекты должны защищаться так, как того требует государство.

Определены четырнадцать типов возможных негативных последствий, к которым может привести нарушение или прекращение работы объектов КИИ:

- причинение вреда жизни и здоровью людей;

- нарушение работы систем жизнеобеспечения;

- нарушение транспортного сообщения;

- нарушение связи;

- снижение доходов федерального или местного бюджета и т. п.

В результате для каждого из объектов КИИ вводится четырнадцать показателей категорирования, каждый из которых характеризует размер вреда, который может быть причинен при наступлении соответствующего негативного последствия.

В действительности определение объектов КИИ и категорий их значимости — не такая простая задача. Во-первых, к примеру, даже в пределах отдельного муниципального образования теплоснабжение может обеспечиваться системой из нескольких ТЭЦ и автономных котельных, и определить численность населения, обслуживаемую одним предприятием — задача сама по себе непростая. Во-вторых, объектом КИИ является не предприятие, а каждая информационная система, каждая автоматизированная система управления и каждая информационно-телекоммуникационная сеть предприятия, которые в данном примере используются для теплоснабжения. То есть объектами КИИ будут являться автоматизированные системы управления водогрейными котлами (причем каждый котел может иметь отдельную систему управления), насосами, задвижками и т. п., а в ряде случаев — даже системы учета поставляемой тепловой энергии и взимания платы с потребителей. И категории значимости должны быть определены для каждого такого объекта[[4]](#footnote-4).

Таким образом, категорирование объектов КИИ — довольно сложный процесс, требующий учета многих нюансов деятельности организации.

# **2 БЕЗОПАСНОСТЬ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ**

Принципами обеспечения безопасности критической информационной инфраструктуры являются:

- законность;

- непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры;

- приоритет предотвращения компьютерных атак[[5]](#footnote-5).

Разработка мер защиты информации значимого объекта КИИ должна включать в себя анализ угроз безопасности и разработку модели угроз безопасности КИИ:

1. Анализ угроз включает в себя выявление источников угроз, оценку возможностей нарушителей (т.е. создание модели нарушителя), анализ уязвимостей используемых систем, определение возможных способов реализации угроз и их последствий. Модель нарушителя строится на основе предположений о потенциале атакующих, т.е. о мере усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе (при этом потенциалы нарушителей можно условно разделить на высокий, средний и низкий).

Анализ уязвимостей можно произвести при помощи тестов на проникновение - пентестов (англ. PenTest, сокращение от Penetration Test). При проведении пентестов проверяющие определяют слабые места инфраструктуры компании, выявляют уязвимости в системах защиты, проводят контролируемую эмуляцию настоящей хакерской атаки - в общем, наглядно показывают, что компания - заказчик этого тестирования может быть взломана. Далее заказчик получает рекомендации по устранению выявленных в ходе пентеста недочетов, и через какое-то время пентест повторяется. При проведении анализа уязвимостей и способов реализации угроз рекомендуется использовать Банк Данных Угроз ФСТЭК России - это официальный государственный справочник различных уязвимостей и способов атак, который регулярно пополняется и поддерживается в актуальном состоянии.

 2. Под построением модели угроз безопасности КИИ при защите КИИ подразумевается описание свойств или характеристик угроз безопасности информации, а под угрозой безопасности - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (т.е. базовых свойств информации). Целью моделирования угроз КИИ является нахождение всех условий и факторов, проводящих к нарушению безопасности информации и работы ИТ-систем. Модель угроз может строиться на основе следующего классического подхода: актуальная угроза информационной безопасности возникает при наличии источника угрозы (внешний/внутренний нарушитель или третьи силы), уязвимости актива, способа реализации угрозы, объекта воздействия и самого вредоносного воздействия. Угроза безопасности информации является актуальной, если существует источник угрозы, условия и сценарий для её реализации, а воздействие на активы приведет к негативным последствиям. Процесс моделирования угроз ИБ состоит из следующих этапов:

* определение возможных негативных последствий от реализации угроз по результатам оценки рисков нарушения законодательства, бизнес-процессов и/или нарушения защищенности информации, что может привести к таким негативным последствиям, как нарушение законодательства, экономический или репутационный ущерб;
* определение условий для реализации угроз безопасности информации, т.е. выявление уязвимостей, недекларированных возможностей, доступов к ИТ-системам, которые могут быть использованы злоумышленниками;
* определение источников угроз (техногенных и антропогенных) и оценка возможностей нарушителей (внешних и внутренних);
* определение сценариев реализации угроз с помощью таблицы тактик и техник атакующих;
* оценка уровня опасности угроз безопасности информации путем анализа типа доступа, необходимого для реализации атаки, сложности сценария атаки и уровня важности атакуемых активов[[6]](#footnote-6).

После анализа и моделирования угроз следует переходить к внедрению контрмер. При этом следует иметь в виду, что внедряемые меры защиты не должны оказывать негативного влияния на функционирование самого объекта КИИ – этим подчеркивается, что приоритетом является непрерывность технологических процессов, остановка которых может сама по себе привести к инциденту на КИИ, например, к выходу оборудования из строя или даже аварии.

 В списке организационных и технических мер, предусмотренных в зависимости от категории значимости объекта КИИ и угроз безопасности информации, можно выделить:

* идентификация и аутентификация;
* управление доступом;
* ограничение программной среды;
* защита машинных носителей информации;
* аудит безопасности;
* антивирусная защита;
* предотвращение вторжений (компьютерных атак);
* обеспечение целостности;
* обеспечение доступности;
* защита технических средств и систем;
* защита информационной (автоматизированной) системы и ее компонентов;
* планирование мероприятий по обеспечению безопасности;
* управление конфигурацией;
* управление обновлениями программного обеспечения;
* реагирование на инциденты информационной безопасности;
* обеспечение действий в нештатных ситуациях;
* информирование и обучение персонала[[7]](#footnote-7).

 Кроме этого, при использовании СЗИ для защиты КИИ приоритет отдается штатному защитному функционалу, а при реагировании на компьютерные инциденты в критической информационной инфраструктуре требуется отправлять информацию о них в систему ГосСОПКА. Следует также отметить важность использования СЗИ, которые обеспечиваются гарантийной и/или технической поддержкой, а также на возможные ограничения по использованию программного/аппаратного обеспечения или СЗИ (видимо, имеются ввиду санкционные риски). На значимом объекте КИИ требуется запретить удаленный и локальный бесконтрольный доступ для обновления или управления лицами, не являющимися работниками субъекта КИИ, а также запретить бесконтрольную передачу информации из объекта КИИ производителю или иным лицам. Кроме этого, все программные и аппаратные средства объекта КИИ первой категории значимости должны располагаться на территории РФ (за исключением оговоренных законодательством случаев).

Защита критической информационной инфраструктуры страны требует привлечения огромных материальных сил и финансовых вложений. Полная изоляция объектов критической информационной инфраструктуры от внешнего мира тоже не является решением проблемы, поскольку высокий процент оборудования, используемого на объектах, составляют иностранные разработки. Наиболее оптимальным вариантом полноценного обеспечения защиты объектов критической информационной инфраструктуры считается подключение к ним Центра мониторинга информационной безопасности (Security Operations Center). Он предоставляет полный спектр услуг по мониторингу и администрированию систем защиты информации, выявлению и реагированию на инциденты. Это позволит субъектам критической информационной инфраструктуры более экономно осуществить требования данного федерального закона. Такой подход, возможно, станет одним из важных трендов в области информационной безопасности в России.

# **ЗАКЛЮЧЕНИЕ**

Таким образом, в заключении следует сделать выводы по рассмотренной теме.

Критическая информационная инфраструктура - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

К субъектам критической информационной инфраструктуры относятся государственные органы и учреждения, а так же российские юридические лица и/или индивидуальные предприниматели которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления. У каждого субъекта КИИ есть объекты КИИ - информационные системы, автоматизированные системы управления технологическими процессами, информационно-телекоммуникационные сети - функционирующие 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.

Критическая информационная инфраструктура не является проходной темой в информационной безопасности. Потенциально это крупнейшая тема, как минимум, за последние 10 лет. Всем субъектам КИИ (а их не мало) нужно не только провести массу продолжительных по времени и дорогостоящих мероприятий, но и создавать полноценные системы безопасности. Такие системы должны включать в себя части по управлению, по технической защите и прочее. Системы нужно обслуживать, модернизировать и совершенствовать. Все это требует значительных финансовых и трудовых ресурсов, а также компетенций, которые в рамках рынка еще предстоит наращивать.

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ [Электронный ресурс]. – Доступ из справочно-правовой системы «Консультант Плюс».
2. Абдулоризов А. Н. Критическая информационная инфраструктура как объект обеспечения безопасности // Молодой ученый. — 2020. — № 20 (310). — С. 16-19.
3. Заворина Л.Д., Селифанов В.В. Разработка системы защиты информации значимого объекта критической инфраструктуры Российской Федерации // Сборник научных трудов НГТУ. – 2019. – № 1 (94). – С. 123–131.
4. Лютиков В.С. О безопасности критической информационной инфраструктуры Российской Федерации // Шестая конференция «Информационная безопасность автоматизированных систем управления технологическими процессами критически важных объектов». - 2018.
5. Оюн Ч.О. Объекты критической информационной инфраструктуры // [Интерэкспо Гео-Сибирь](https://cyberleninka.ru/journal/n/interekspo-geo-sibir). – 2018.

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ – ст. 1. [↑](#footnote-ref-1)
2. Абдулоризов А. Н. Критическая информационная инфраструктура как объект обеспечения безопасности // Молодой ученый. — 2020. — № 20 (310). — С. 16. [↑](#footnote-ref-2)
3. Оюн Ч.О. Объекты критической информационной инфраструктуры // [Интерэкспо Гео-Сибирь](https://cyberleninka.ru/journal/n/interekspo-geo-sibir). – 2018. [↑](#footnote-ref-3)
4. Заворина Л.Д., Селифанов В.В. Разработка системы защиты информации значимого объекта критической инфраструктуры Российской Федерации // Сборник научных трудов НГТУ. – 2019. – № 1 (94). – С. 123. [↑](#footnote-ref-4)
5. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ – ст. 4. [↑](#footnote-ref-5)
6. Абдулоризов А. Н. Критическая информационная инфраструктура как объект обеспечения безопасности // Молодой ученый. — 2020. — № 20 (310). — С. 17. [↑](#footnote-ref-6)
7. Лютиков В.С. О безопасности критической информационной инфраструктуры Российской Федерации // Шестая конференция «Информационная безопасность автоматизированных систем управления технологическими процессами критически важных объектов». - 2018. [↑](#footnote-ref-7)