

УДК 004.9

DOI 10.52167/1609-1817-2023-126-3-324-334

А.Е.Қызырқанов<sup>1</sup>, М.Бакыт<sup>2</sup>, Ш.Мусиралиева<sup>3</sup>, Г.К.Балбаев<sup>4</sup>, Г.Тулешева<sup>5</sup>

<sup>1</sup>Astana IT университет, Астана, Қазақстан

<sup>2</sup>Евразийский национальный университет им. Л.Н. Гумилева, Астана, Қазақстан

<sup>3</sup>Қазақский национальный университет им. аль-Фараби, Алматы, Қазақстан

<sup>4</sup>Академия логистики и транспорта, Алматы, Қазақстан

<sup>5</sup>Satpayev University, Алматы, Қазақстан

E-mail: bakyt.makhabbat@gmail.com

## ПРОБЛЕМЫ ВЫДЕЛЕНИЯ И РАНЖИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ СОТОВЫХ СЕТЕЙ СВЯЗИ В РЕСПУБЛИКЕ КАЗАХСТАН

**Аннотация.** В данной статье рассматриваются общие вопросы ранжирования угроз, а также методы оценивания эффективности построения системы защиты критических информационных инфраструктур (КИИ) сотовых сетей связи в Республике Казахстан. Одной из основных проблем государственного регулирования информационной безопасности в области ранжирования КИИ сотовых сетей связи является конфликт интересов бизнеса, государства и общества. Ранжирование критических объектов сотовой связи является важной частью обеспечения информационной безопасности. В работе раскрыты проблемы и пути решения задач по защите критически важных объектов правительства и предприятий, которые могут снизить риск атак и защитить от возможных сбоев.

**Ключевые слова.** Информационная безопасность, критическая информационная инфраструктура, граф ранжирования, критерии оценивания безопасности информационных систем, защита критически важных объектов.

### Введение.

Критическая информационная инфраструктура (КИИ) – это система, служба или сеть, которые необходимы для функционирования общественных или экономических отношений. КИИ может быть физическим или виртуальным и может принадлежать государственному или частному сектору. Таким образом критическая информационная инфраструктура – это набор систем и активов, необходимых для функционирования нации или общества. КИИ может быть физическим, например, электростанции или водоочистные сооружения, или цифровым, например, телекоммуникационными сетями или финансовыми системами.

В области критической информационной инфраструктуры в мире не существует единого определения что такое КИИ, каждое государство определяет её по-своему [1].

В данной работе, критическая информационная инфраструктура – это совокупность автоматизированных систем управления (далее - АСУ), а также информационно-коммуникационных сетей (далее - ИКС), предназначенных для обеспечения их взаимодействия, решения задач управления и обеспечения обороны, безопасности, правопорядка, прерывание (или прекращение) функционирования которых может иметь серьёзные последствия. Рассматривая понятие инфраструктуры, предназначенной для нормального функционирования, важно, чтобы инфраструктура работала бесперебойно, то есть выполняла все поставленные задачи, сохраняя настроенные характеристики (параметры) своего функционирования. Существенным условием безопасности такой инфраструктуры является ее устойчивость к компьютерным атакам (КА).

На рисунке 1 показана структура взаимодействия КИИ и системы управления, где объектами КИИ являются устройства управления и их установки, а коммуникационная сеть служит для обмена информацией и сообщениями между объектами КИИ и устройствами управления, и их установками. Дестабилизирующие воздействия – это воздействия, направленные на нарушение стабильного функционирования КИИ.

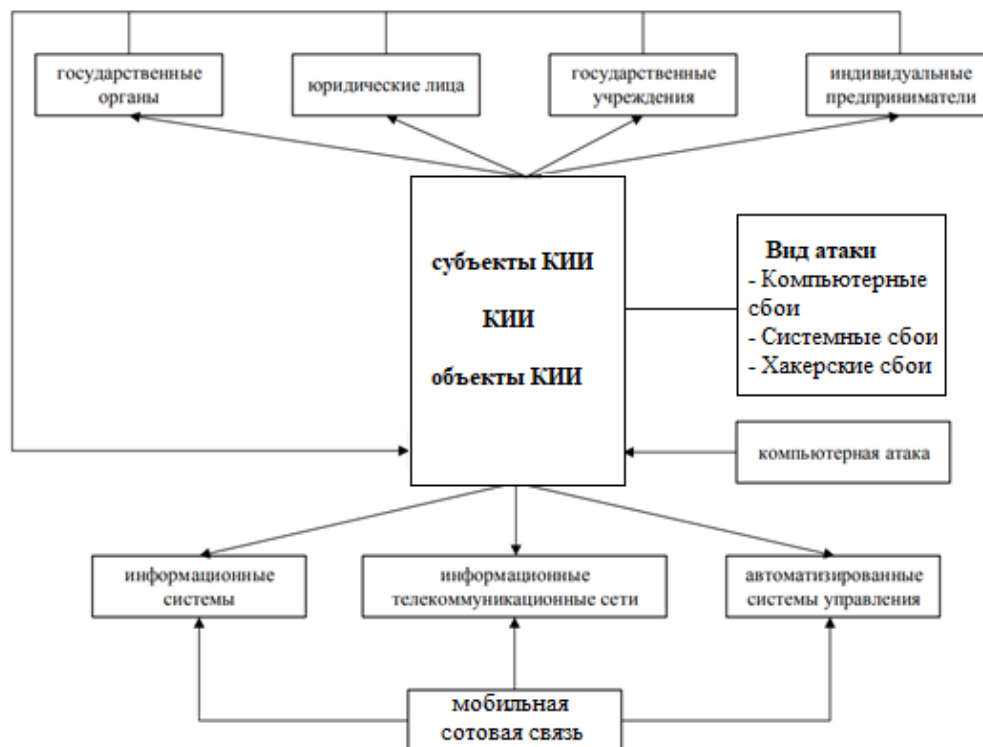


Рисунок 1 - Структура взаимодействия КИИ с объектами

Сотовые сети являются важной частью КИИ, поскольку они предоставляют основные услуги связи предприятиям, правительствам и частным лицам, что наглядно видно из рисунка 1. В данном случае, субъектом КИИ является какая-либо организация, а именно государственный орган, государственное учреждение, юридическое лицо или индивидуальный предприниматель, у которой присутствует объект критической информационной инфраструктуры. При этом объектом КИИ является то, что может быть подвержено атаке, и, как правило, это информационные системы и сети, а также автоматизированные системы управления.

Существует несколько типов классификации атак. Один из них – это классификация по принципу воздействия. Это пассивные сетевые атаки, направленные на получение конфиденциальной информации с удаленного компьютера. К таким типам атак, например, относится перехват входящих или исходящих писем, ежедневно пересылаемых по электронной почте. Что касается активных сетевых атак, то их основной задачей является модификация данных или искажение сообщений, а не доступ к тем или иным данным конфиденциального характера. Одно из наиболее значимых различий между этими типами атак заключается в том, что пассивное вмешательство практически невозможно обнаружить, в то время как активные атаки, как правило, заметны и имеют явные последствия.

В связи с этим важно выявить и защитить критически важные объекты сотовых сетей. Существует ряд факторов, которые можно использовать для выбора и ранжирования критических объектов сотовых сетей.

## Материалы и методы.

### *Выбор объектов критической информационной инфраструктуры.*

Первым шагом при выборе объектов критической информационной инфраструктуры для сотовых сетей является определение актуальной тематики. Эти темы можно определить, рассмотрев следующие факторы:

- 1) Важность объекта для функционирования сотовой сети.
- 2) Уязвимость объекта к атаке или разрушению.
- 3) Воздействие атаки или сбоя в сотовой сети.

После определения соответствующих тем их можно расположить в порядке важности. Это ранжирование можно использовать для определения приоритетов защиты объектов КИИ.

### *Выбор критериев.*

Существует ряд критериев, которые можно использовать для ранжирования объектов КИИ. К этим критериям относятся:

- 1) Влияние сбоя: насколько сбой в работе объекта повлияет на способность сети функционировать?
- 2) Вероятность нарушения: насколько вероятно, что объект будет нарушен?
- 3) Стоимость восстановления: сколько будет стоить восстановление объекта после сбоя?
- 4) Стоимость охраны объект?

Относительная важность этих критериев и факторов будет варьироваться в зависимости от конкретной сети. Например, сеть, используемая для аварийно-спасательных служб, может придавать большее значение последствиям нарушения работы, чем стоимости восстановления. Влияние этих факторов будет варьироваться в зависимости от конкретных обстоятельств. Однако, учитывая все эти факторы, можно разработать систему ранжирования, подходящую для конкретной сотовой сети.

Тематический выбор и ранжирование объектов критической информационной инфраструктуры для сетей сотовой связи является важной задачей. Тщательно учитывая соответствующие факторы, можно выявить и защитить наиболее важные объекты КИИ.

Это поможет обеспечить непрерывную работу сотовых сетей и предоставляемых ими услуг. В дополнение к упомянутым выше факторам существует ряд других факторов, которые можно учитывать при выборе и ранжировании объектов КИИ. К этим факторам относятся также:

- 1) Наличие резервных инфраструктур, альтернатив заменителей объекта.
- 2) Время, необходимое для восстановления работоспособности объекта после атаки или нарушения работы.
- 3) Воздействие атаки или сбоя на экономику.
- 4) Воздействие атаки или сбоя на национальную безопасность.

Учитывая все эти факторы, необходимо разработать комплексную систему ранжирования, которая поможет обеспечить защиту объектов КИИ на государственном уровне. После определения критических объектов сотовой сети важно принять меры по их защите как организационно-правовые, так и технические. В технической части эти меры могут включать:

- 1) Физическая безопасность: защита объектов от физического повреждения или кражи.
- 2) Кибербезопасность: защита объектов от кибератак.
- 3) Аварийное восстановление: планирование восстановления объектов после сбоя.

Вот некоторые дополнительные сведения о каждом из факторов, которые можно использовать для выбора и ранжирования критических объектов сотовых сетей:

*Воздействие сбоя:* Воздействие сбоя на объект можно измерить с точки зрения следующего:

- 1) Количество людей, которые будут затронуты сбоем.
- 2) Время, в течение которого будет продолжаться сбой.

*Вероятность нарушения:* Вероятность нарушения объекта может быть измерена с точки зрения следующего:

- 1) История сбоев на объекте.
- 2) Текущее состояние безопасности объекта.
- 3) Среда угроз.

*Стоимость восстановления:* стоимость восстановления после сбоя объекта может быть измерена с точки зрения следующего:

- 1) Стоимость восстановления объекта до исходного состояния.
- 2) Стоимость потерянной производительности.
- 3) Стоимость репутационного ущерба.

Принимая меры по защите критически важных объектов сотовых сетей, необходимо обеспечить их доступность и надёжность. За основу метода оценки соблюдения мер использовано методика построение из теории графов на основе весовых коэффициентов, которые, в свою очередь, отражают степень значимости той или иной характеристики по отношению к другим. Наибольшее влияние на конечный результат оказывает именно весовой коэффициент. Весовой коэффициент возможно определить множеством способов, но в случае КИИ целесообразно обратиться к методу графов. В простейшем случае используем ненаправленные графы. Построенный граф будет наиболее наглядно и последовательно отражает взаимосвязь объектов, позволяя сегментировать уровни и создавать ранжирование КИИ объектов.

### Результаты и обсуждения.

*Построение графа ранжирования мер защиты ИКТ систем.*

Изложенные ранее критерии можно систематизировать в следующую 4-х уровневую модель и представить в виде графа. Модель содержит в себе 17 групп мер, которые регулируют как техническую часть, так и организационную. Построим граф, касающийся проведения мониторинга уровней безопасности КИИ для серверов сотовых станций или DATA-центров (рис. 2).

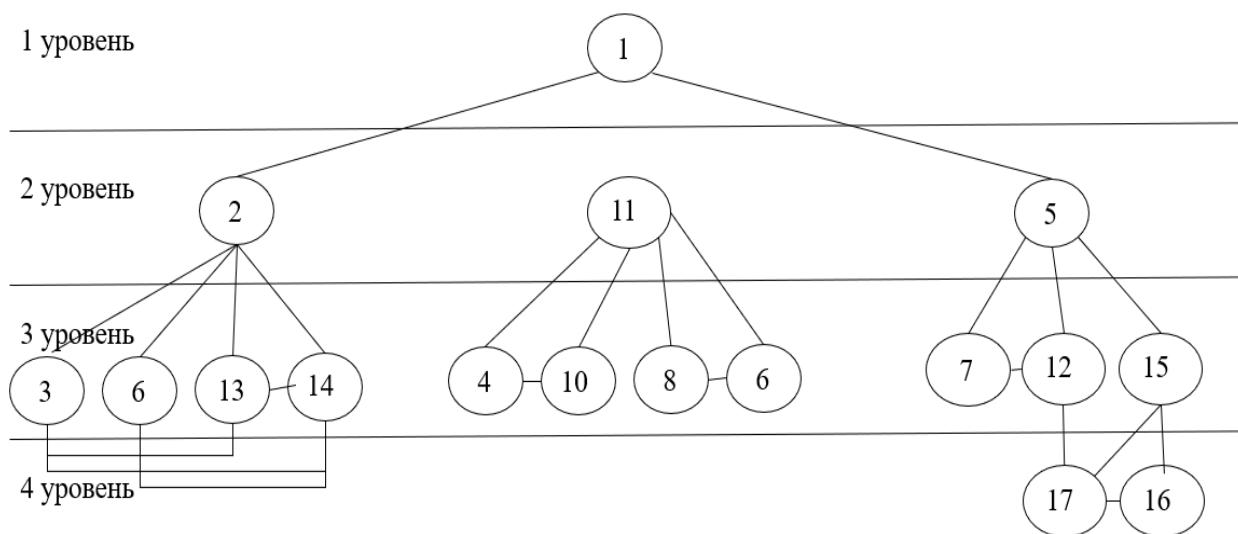


Рисунок 2 - Граф ранжирования мер обеспечения безопасности КИИ

Вершины графа обозначают:

- 1) Идентификация и аутентификация.
- 2) Управление доступом.
- 3) Ограничение программной среды.
- 4) Защита машинных носителей информации.
- 5) Аудит безопасности.
- 6) Антивирусная защита.
- 7) Предотвращение вторжений (компьютерных атак).
- 8) Обеспечение целостности.
- 9) Обеспечение доступности.
- 10) Защита технических средств и систем.
- 11) Защита информационной (автоматизированной) системы и ее компонентов.
- 12) Реагирование на компьютерные инциденты.
- 13) Управление конфигурацией.
- 14) Управление обновлениями программного обеспечения.
- 15) Планирование мероприятий по обеспечению безопасности.
- 16) Обеспечение действий в нештатных ситуациях.
- 17) Информирование и обучение персонала.

Граф построен на основе анализа и систематизации рейтинга SANS CIS Controls 8 в проведении проверок значимых объектов КИИ [2]. Эта диаграмма анализирует и организует оценку SANS CIS Controls 8 во время инспекций критически важных объектов СП. Меры принимаются в соответствии с их весом в системе защиты и процедуре проверки. На рисунке 2 наглядно показаны различные взаимосвязи между группами мер, которые необходимы при построении эффективной системы защиты. Три ветви графа эквивалентны друг другу и представляют собой три параллельные проверки. Граф имеет три уровня.

*Первый уровень графа* имеет одну вершину – группу контрмер, которая связана с идентификацией и аутентификацией. Эта группа показателей имеет наибольший вес и, следовательно, занимает более высокое место по сравнению с другими группами. Если бы не была организована идентификация и аутентификация, любой пользователь или злоумышленник имел бы беспрепятственный доступ к КИИ, что сделало бы дальнейшую защиту совершенно бессмысленной и неэффективной.

*Второй уровень графа* состоит из трёх узлов: контроль доступа, аудит безопасности и защита информационной безопасности и её компонентов. Поскольку этот уровень тесно связан с последующими уровнями, можно сказать, что он обобщает все последующие группы мер, относящиеся к той или иной вершине.

Узел 2, узел контроля доступа, содержит техническую часть организации, то есть набор контрмер, непосредственно связанных с операционной системой и программным обеспечением.

Узел 5, или вершина аудита безопасности, содержит в основном организационные меры, связанные с обнаружением и адекватным реагированием на угрозы, а также с обучением персонала.

Узел 11, вершина защиты информации и ее компонентов, объединяет техническую и организационную части. Этот пик объединяет группу мер, связанных с безопасностью оборудования, доступом к оборудованию и собственно информационной безопасностью.

*Третий уровень графа* содержит следующие группы показателей:

- Узел 2.1 – Управление учетными записями пользователей
- Узел 2.2 – Управление паролями
- Узел 2.3 – Многофакторная аутентификация
- Узел 2.4 – Списки контроля доступа

- Узел 2.5 – доступ с наименьшими привилегиями
- Узел 2.6 – Управление сеансом
- Узел 2.7 – Управление удаленным доступом
- Узел 5.1 – Управление угрозами и уязвимостями
- Узел 5.2 – Реагирование на инцидент
- Узел 5.3 – Осведомленность о безопасности и обучение
- Узел 5.4 – Тестирование безопасности
- Узел 5.5 – Управление безопасностью
- Узел 11.1 – Архитектура и дизайн безопасности
- Узел 11.2 - Охранные операции
- Узел 11.3 - Обеспечение безопасности
- Узел 11.4 – Обучение и подготовка по вопросам безопасности
- Узел 11.5 – Осведомленность о безопасности
- Узел 11.6 – Соответствие требованиям безопасности

В графе меры распределены по уровням согласно их весу в системе защиты, а также последовательности проверки и станут основой для паспортизации объекта. Граф наглядно демонстрирует всевозможные связи групп мер между собой, которые в свою очередь необходимы при построении эффективной системе защиты

#### *Ранжирование КИИ.*

Следующий шаг это, собственно, само ранжирование и определение категории объекта критически важной инфраструктуры. Для проведения данной процедуры необходима дополнительная информация, касательно расположения и назначения объекта КИИ, о его архитектуре, составе и используемых информационных технологиях. А также необходима информация о составленной карте информационных потоков, и информация по используемым современным (криптографическим) средствам защиты информации. Также важны сведения по подключению объекта критической информационной инфраструктуры к сетям электросвязи и операторам связи, который его обслуживает [3]. Наконец, понадобится очень важная информация по обнаруженным уязвимостям, эксплуатирующим элементы объекта лицам, а также информация о мерах по обеспечению физической и промышленной безопасности.

Одной из основных проблем государственного регулирования информационной безопасности в области ранжирования КИИ является конфликт интересов бизнеса и государства и общества. При принятии решения о реализации тех или иных мер безопасности владелец информационной системы оценивает потенциальные потери от инцидентов и сопоставляет их со стоимостью мер. С точки зрения владельца, меры безопасности не стоят того, если стоимость превышает потенциальные потери. К сожалению, владельцы информационных систем часто считают только свои потери, игнорируя возможный ущерб для других [4]. Например, если сбой в системе автоматизации на ТЭЦ оставит город без тепла на трое суток, предприятие потеряет менее 1% выручки. Это статистически незначительная потеря, и владелец ТЭЦ может с этим смириться. Однако трое суток без тепла и горячей воды – это катастрофа для города, а затраты трудно поддаются количественной оценке в финансовом выражении, как показали недавние подобные трагедии в г. Экибастузе.

Для решения этой проблемы в законодательных актах введено понятие «категория значимости» или ранжирование. То есть категория значимости — это характеристика объекта критической информационной инфраструктуры (КИИ), позволяющая чётко разграничить объекты, которые собственник может защищать по своему усмотрению, и объекты, которые должны быть защищены в соответствии с государственными требованиями. Возможные негативные последствия сбоя или выхода из строя КИИ включают:

- 1) Вред жизни и здоровью.
- 2) Нарушение систем жизнеобеспечения.
- 3) Нарушение транспорта.
- 4) Нарушение связи.
- 5) Сокращение доходов республиканского или местного бюджета.

Так, например, в России законодательно для каждого объекта КИИ в приложении к правилам категоризации (постановление Правительства РФ от 8 февраля 2018 г. № 127, новая редакция утверждена 13 апреля 2019 г.) регламентировано четырнадцать показателей категоризации. Каждый показатель характеризует размер вреда, который может быть причинён при возникновении соответствующего неблагоприятного воздействия [5]. Категория значимости объекта КИИ определяется суммой баллов по всем четырнадцати показателям.

*Ранжирование критической информационной инфраструктуры сотовых сетей.* исходя из изложенного ранее рекомендуется осуществлять по ряду факторов, в том числе:

- 1) Значение объекта для общества и экономики.
- 2) Уязвимость объекта к атаке или разрушению.
- 3) Воздействие, которое нападение или разрушение может оказать на общество и экономику.

Ранжирование используется для определения приоритетности ресурсов для защиты критически важных сотовых объектов. Ниже приведены некоторые из критически важных сотовых объектов, которые необходимо ранжировать:

- сети мобильной связи;
- спутники связи;
- центры обработки данных;
- критическая инфраструктура, такая как электростанции и водоочистные сооружения;
- государственные и военные объекты.

Ранжирование критических сотовых объектов представляет собой сложный и постоянно развивающийся процесс. Важно отметить, что рейтинг не является окончательным списком всех критических сотовых объектов в Казахстане. Это просто способ расставить приоритеты ресурсов для защиты наиболее важных и уязвимых объектов. Вот некоторые из проблем, связанных с ранжированием критических сотовых объектов:

- сложно оценить важность объекта для общества и экономики;
- трудно оценить уязвимость объекта для атаки или разрушения;
- трудно предсказать воздействие, которое нападение или разрушение окажет на общество и экономику.

Несмотря на эти проблемы, важно ранжировать критические сотовые объекты, чтобы расставить приоритеты в ресурсах для их защиты. Поступая таким образом, мы можем помочь обеспечить защиту этих важных объектов от атак или нарушений [6]. Ранжирование критических сотовых объектов по социально-значимым факторам должно включать оценку из влияния на общество. В том числе:

1) Важность объекта для критической инфраструктуры. Сюда входят объекты, необходимые для функционирования больниц, электростанций и других критически важных систем.

2) Уязвимость объекта для атаки. Сюда входят объекты, расположенные в отдалённых районах или недостаточно защищённые.

3) Воздействие атаки на объект. Сюда входят объекты, которые в случае нападения на них могут привести к широкомасштабным нарушениям или повреждению.

Ранжирование используется для определения приоритета защиты критических сотовых объектов. Объекты с более высоким рейтингом получают больше ресурсов и внимания, чтобы защитить их от атаки. Ниже приведены некоторые КИИ, которые оцениваются физические структуры сотовой связи:

1) Вышки сотовой связи. Вышки сотовой связи необходимы для функционирования сотовых сетей. Они уязвимы для атак и могут вызвать массовые сбои, если их отключить.

2) Подводные кабели. По подводным кабелям проходит большая часть международного интернет-трафика. Они уязвимы для атак и могут вызвать серьезные сбои в доступе в Интернет.

3) Центры обработки данных. В центрах обработки данных размещаются компьютерные системы, которые хранят и обрабатывают данные. Они уязвимы для атак и могут вызвать серьезные сбои в работе критически важных служб.

4) Правительственные сети. Правительственные сети необходимы для функционирования государственных учреждений. Они уязвимы для атак и могут вызвать серьезные сбои в работе государственных служб.

5) Сети критической инфраструктуры. Критические сети инфраструктуры включают электрические сети, системы водоснабжения и транспортные сети. Они необходимы для функционирования общества и уязвимы для нападения.

Ранжирование критических объектов сотовой связи является важной частью обеспечения безопасности сотовых сетей в Казахстане. Уделяя приоритетное внимание защите критически важных объектов, правительства и предприятия могут помочь снизить риск атак и защитить население от сбоев.

### **Заключение.**

Категорирование или ранжирование объектов критической информационной инфраструктуры – это некая форма оценки рисков информационной безопасности для объектов ИТ-инфраструктуры, которые используются в важных отраслях экономики и государственного управления. Своеобразие этого процесса вызвано тем, что эти объекты могут принадлежать коммерческим компаниям и частным лицам, но при этом, конечно, они создают риски для государства и населению.

Важно отметить, что это лишь некоторые из факторов, которые можно использовать для выбора и ранжирования критических объектов сотовых сетей. Конкретные факторы, которые являются наиболее важными, будут различаться в зависимости от конкретной сети.

Итак, каждому объекту критической информационной инфраструктуры присваивается категория важности в результате ранжирования, которое осуществляется исходя из социальной значимости. Оценку, при этом, необходимо осуществлять на основе анализа возможного ущерба, который может быть причинён жизни или здоровью людей, в случае прекращения или нарушения функционирования объектов КИИ, такие как сетей связи, обеспечения жизнедеятельности населения, транспортного обеспечения, а также максимальном времени отсутствия доступа к государственным услугам для населения. Далее, оценка осуществляется исходя из возможного оказания ущерба интересам государства в вопросах внутренней и внешней политики, экономической значимости. Также оценка определяется на основе анализа возможного причинения прямого и косвенного ущерба субъектам КИИ и (или) бюджетам государства; экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду; значимости объекта КИИ для обеспечения обороны страны, безопасности государства и правопорядка.

В действительности определение объектов критической информационной инфраструктуры и категорий их значимости – непростая задача. Это связано с тем, что объектом КИИ является не предприятие в целом, а каждая информационная система, автоматизированная система управления и информационно-телекоммуникационная сеть внутри предприятия.

Государство может даже стимулировать организации к отнесению их информационных систем к объектам КИИ, предоставляя им налоговые льготы. Например, организация, которая проводит научные исследования и использует в своих исследованиях ИТ-инфраструктуру, также формально является субъектом КИИ.

Наиболее сложная ситуация с организациями ИТ-отрасли, особенно с операторами связи, центров обработки данных и облачных инфраструктур. Ключом к отнесению организации к субъекту КИИ является не её деятельность в одном из «критических» направлений, а владение хотя бы одним объектом ИТ-инфраструктуры, который используется в одном из этих направлений.

Исследование показывает, что чаще всего единственным способом ответить на вопрос, является ли организация субъектом КИИ, является ранжирование её информационных систем.

**Благодарность.** Данная работа выполнена при финансовой поддержке Комитета науки министерства науки и высшего образования Республики Казахстан (ПЦФ, BR18574045).

## ЛИТЕРАТУРА

[1] [https://websites.fraunhofer.de/CIPedia/index.php/Critical\\_Information\\_Infrastructure](https://websites.fraunhofer.de/CIPedia/index.php/Critical_Information_Infrastructure) #Kyrgyzstan.

[2] Zashchita kriticheski vazhnykh ob'yektov infrastruktury ot terroristicheskikh atak [Protecting Critical Infrastructure from Terrorist Attacks]. Sbornik peredovogo opyta. IDKTK i KTU OON [A Compendium of Best Practices. IDKTK and KTU UN]. 2018. 152 p. (In Rus).

[3] A. Sunyaev Critical Information Infrastructures. In: Internet Computing. Springer, Cham. 2020.

[4] R. Setola, E. Luijff, M. Theocharidou Critical Infrastructures, Protection and Resilience. In: Setola R., Rosato V., Kyriakides E., Rome E. (eds) Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control. Springer, Cham. 2016. №90.

[5] Краснов, А. Е. Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности//А. Е. Краснов, А. С. Мосолов, Н. А. Феоктистова//Безопасность информационных технологий. – 2021. – Т. 28. – № 1. – С. 106-120.

[6] Забегалин, Е. В. Логическая модель деятельности по комплексному техническому диагностированию информационной безопасности организаций и значимых объектов критической информационной инфраструктуры//Е. В. Забегалин//Системы управления, связи и безопасности. – 2019. – № 3. – С. 145-178.

## REFERENCES\*

[1] [https://websites.fraunhofer.de/CIPedia/index.php/Critical\\_Information\\_Infrastructure](https://websites.fraunhofer.de/CIPedia/index.php/Critical_Information_Infrastructure) #Kyrgyzstan

[2] Zashchita kriticheski vazhnykh ob'yektov infrastruktury ot terroristicheskikh atak [Protecting Critical Infrastructure from Terrorist Attacks]. Sbornik peredovogo opyta. IDKTK i KTU OON [A Compendium of Best Practices. IDKTK and KTU UN]. 2018. 152 p. (In Rus).

[3] A. Sunyaev Critical Information Infrastructures. In: Internet Computing. Springer, Cham. 2020.

[4] R. Setola, E. Luijff, M. Theocharidou Critical Infrastructures, Protection and Resilience. In: Setola R., Rosato V., Kyriakides E., Rome E. (eds) Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control. Springer, Cham. 2016. №90.

[5] Krasnov, A. E., Mosolov A. S., Feoktistova N. A. Assessing the sustainability of critical information infrastructures to information security threats. - 2021. - Т. 28. - No. 1. - P. 106-120.

[6] Zabegalin, E. V. Logical model of activity for complex technical diagnostics of information security of organizations and significant objects of critical information infrastructure // E. V. Zabegalin // Control systems, communications and security. - 2019. - No. 3. - P. 145-178.

**Абзал Қызырқанов**, сеньор-лектор, Astana IT University, Астана, Қазақстан, Abzzall@gmail.com

**Махаббат Бақыт**, докторант, Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, bakyt.makhabbat@gmail.com

**Шынар Мусиралиева**, PhD, профессор, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан, mussiraliyeva@gmail.com

**Гани Балбаев**, PhD, қауымдастырылған профессор, Логистика және көлік академиясы, Алматы, Қазақстан, g.balbayev@alt.edu.kz

**Гульнара Тулешева**, PhD, доцент, Satbayev University, Алматы, Қазақстан, tulesheva.gulnara@mail.ru

## ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДАҒЫ ҰЯЛЫ БАЙЛАНЫС ЖЕЛІЛЕРІНІҢ МАҢЫЗДЫ АҚПАРАТТЫҚ ИНФРАҚҰРЫЛЫМЫ ОБЪЕКТІЛЕРІН БӨЛУ ЖӘНЕ САРАЛАУ МӘСЕЛЕЛЕРІ

**Аңдтапа.** Бұл мақалада қауіптерді саралаудың жалпы мәселелері, сондай-ақ Қазақстан Республикасындағы ұялы байланыс желілерінің маңызды ақпараттық инфрақұрылымдарын (МАИ) қорғау жүйесін құрудың тиімділігін бағалау әдістері қарастырылады. Ұялы байланыс желілерінің МАИ рейтингі саласындағы ақпараттық қауіпсіздікті мемлекеттік реттеудің негізгі проблемаларының бірі бизнестің, мемлекет пен қоғамның мүдделерінің қайшылығы болып табылады. Критикалық ұялы байланыс объектілерінің рейтингі ақпараттық қауіпсіздіктің маңызды бөлігі болып табылады. Жұмыста шабуыл қаупін азайтатын және ықтимал сәтсіздіктерден қорғайтын үкімет пен кәсіпорындардың маңызды объектілерін қорғау проблемалары мен проблемаларын шешу жолдары көрсетілген.

**Түйінді сөздер.** Ақпараттық қауіпсіздік, маңызды ақпараттық инфрақұрылым, рейтинг графигі, ақпараттық жүйелердің қауіпсіздігін бағалау критерийлері.

**Abzal Kizyrkanov**, senior lecturer, Astana IT University, Astana, Kazakhstan, Abzzall@gmail.com

**Mahabbat Bakyt**, doctoral student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, bakyt.makhabbat@gmail.com

**Shynar Musiraliyeva**, PhD, professor, al-Farabi Kazakh National University, Almaty, Kazakhstan, mussiraliyeva@gmail.com

**Gani Balbaev**, PhD, associate professor, Academy of logistics and transport, Almaty, Kazakhstan, g.balbayev@alt.edu.kz

**Gulnara Tulesheva**, PhD, docent, Satbayev University, Almaty, Kazakhstan, tulesheva.gulnara@mail.ru

**PROBLEMS OF SELECTION AND RANKING OF OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE OF CELLULAR COMMUNICATION NETWORKS IN THE REPUBLIC OF KAZAKHSTAN**

**Annotation.** This article discusses the general issues of ranking threats, as well as methods for evaluating the effectiveness of building a system for protecting critical information infrastructures (CII) of cellular communication networks in the Republic of Kazakhstan. One of the main problems of state regulation of information security in the field of CII ranking of cellular communication networks is the conflict of interests of business, the state and society. The ranking of critical cellular communication objects is an important part of information security. The paper reveals the problems and ways to solve the problems of protecting critical objects of the government and enterprises, which can reduce the risk of attacks and protect against possible failures.

**Keywords.** Information security, critical information infrastructure, ranking graph, criteria for evaluating the security of information systems.

\*\*\*\*\*