Торайғыров университетінің хабаршысы
ҒЫЛЫМИ ЖУРНАЛЫ

НАУЧНЫЙ ЖУРНАЛ
Вестник Торайгыров университета

Торайғыров университетінің ХАБАРШЫСЫ

Энергетикалық сериясы

1997 жылдан бастап шығады

ВЕСТНИК Торайгыров университета

Энергетическая серия

Издается с 1997 года

ISSN 2710-3420

№ 4 (2024)

ПАВЛОДАР

НАУЧНЫЙ ЖУРНАЛ
Вестник Торайгыров университета

Энергетическая серия
выходит 4 раза в год

СВИДЕТЕЛЬСТВО
о постановке на переучет периодического печатного издания,
информационного агентства и сетевого издания
№ 14310-Ж
выдано
Министерство информации и общественного развития
Республики Казахстан

Тематическая направленность
публикация материалов в области электроэнергетики,
электротехнологии, автоматизации, автоматизированных и
информационных систем, электромеханики и теплоэнергетики

Подписной индекс – 76136

---

https://doi.org/10.48081/FYZZ1289

МРНТИ 50.43.19

https://doi.org/10.48081/LTKA1105

***У. К. Жалмагамбетова[1], М. Ж. Мусагажинов[2],
О. М. Талипов[3], А. П. Кислов[4]**

[1,3,4]Торайгыров университет, Республика Казахстан, г. Павлодар
[2]Казахский агротехнический университет им. С. Сейфуллина,
Республика Казахстан, г. Астана
[1]ORCID: https://orcid.org/0000-0002-2261-2222
[2]ORCID: https://orcid.org/0000-0002-4521-8172
[3]ORCID: https://orcid.org/0000-0002-8355-1769
[4]ORCID: https://orcid.org/0000-0003-4816-8008
*e-mail: ultuara@mail.ru

ОБЗОР ТЕХНОЛОГИЙ МОНИТОРИНГА И СРЕДСТВ ЗАЩИТЫ В ЭНЕРГЕТИЧЕСКОМ КОМПЛЕКСЕ КАЗАХСТАНА

Для энергетического комплекса информационная безопасность является одним из важных аспектов, изучаемых в рамках обеспечения надежной и безопасной работы. Она включает в себя защиту информационных систем, данных и сетей от различных угроз, таких как кибератаки, несанкционированный доступ и утечки информации.

Традиционная технология эксплуатации и технического обслуживания сети заключается в том, что администратор пассивно ожидает сообщения о неисправности сети, а затем приступает к экстренному восстановлению. Этот метод лишен активного механизма и имеет много недостатков при устранении сбоев сетевой связи. Информационная безопасность – способность системы ее обработки обеспечивать выполнение требований к вероятностным величинам событий, характеризующихся утечкой, хищением, утратой, несанкционированным уничтожением, изменением значения, получением несанкционированной копии, блокировкой информации за заданный промежуток времени.

В этой статье рассмотрены законодательная и нормативно-правовая база в области информационной безопасности в Казахстане. На этой основе анализируются системы и средства защиты информационной безопасности, а также политика безопасности,

проведение организационных и организационно-технических мероприятий для осуществления мониторинга. Достижение высокой степени информационной безопасности возможно только на основе применения соответствующих организационных мер.

Ключевые слова: системы защиты информации, технологии, защита информации, политика безопасности, правовая база, мониторинг.

Введение

В XXI веке информационные технологии стали неотъемлемой частью различных сфер деятельности, включая производство, образование, управление, безопасность, системы связи, научные исследования, финансы, коммерцию и другие. Развитие вычислительной техники и ее широкое применение в этих областях значительно ускорили научно-технический прогресс.

С увеличением объемов данных и необходимостью их обработки в масштабе одной технической системы, роль средств вычислительной техники стала еще более значимой. К примеру ключевую роль в обеспечении безопасности и эффективности энергетических объектов играет мониторинг информационных систем и средств защиты.

Для обзора в области технологий мониторинга информационных энергетических систем и средств защиты информации в Казахстане на сегодняшний день можно перечислить следующие общие тенденции:

– системы мониторинга и управления энергосистемами (SCADA-системы), которые используются для сбора данных о состоянии энергетических объектов, их параметрах и режимах работы. Они позволяют оперативно реагировать на изменения в энергосистеме и предотвращать аварийные ситуации;

– дистанционное управление и контроль, позволяющие осуществлять дистанционное управление и контроль за состоянием энергетических объектов, что обеспечивает более эффективное использование ресурсов и повышает безопасность.

– интеграция с системами защиты, что позволяет оперативно реагировать на угрозы информационной безопасности и предотвращать возможные атаки;

– использование искусственного интеллекта и машинного обучения, для анализа больших объёмов данных и выявления закономерностей в поведении энергосистемы. Они позволяют прогнозировать возможные аварийные ситуации и предотвращать их;

– интеграция с облачными технологиями, позволяющими обеспечить более эффективное использование ресурсов и обеспечить доступ к данным в режиме реального времени;

– применение интернета вещей (IoT), где устройства IoT используются для сбора данных о состоянии энергосистемы и передачи их в систему мониторинга энергетической системы, что позволяет оперативно реагировать на изменения и предотвращать аварийные ситуации;

– использование беспилотных летательных аппаратов (БПЛА для проведения аэрофотосъёмки энергообъектов и выявления возможных нарушений в их работе;

– применение геоинформационных систем для анализа пространственных данных и выявления возможных угроз безопасности энергосистемы.

Использование конкретного направления зависит от назначения информационной энергетической системы. Именно поэтому вопрос защиты информации на сегодняшний день становится наиболее актуальным и актуальным в сфере информатизации.

Учет (или механизм протоколирования) является важным инструментом обеспечения безопасности. Надежная система должна регистрировать на все события, связанные с безопасностью, а запись-ведение протокола дополняется проверкой (аудитом - анализом регистрационной информации).

Надежная вычислительная база (НВБ) - совокупность защитных линий, ответственных за реализацию политики безопасности компьютерной системы. Для оценки надежности компьютерной системы достаточно лишь рассмотреть ее вычислительную базу. Основной задачей НВБ является выполнение задачи монитора отношений, т. е. контроль за выполнением определенных операций с объектами.

Монитор доступа – это возможность контролировать согласованность каждого доступа пользователя к программам или данным со списком возможных действий. По мере усложнения сценариев кибератак стало очевидно, что традиционные сигнатурные методы не всегда в состоянии обеспечить должный уровень защиты. Именно последним обстоятельством и продиктовано стремительное развитие интереса исследователей [1] к интеллектуализации технологий распознавания киберугроз, аномалий и кибератак, в частности в задачах кибербезопасности.

В Республике Казахстан существует законодательная и нормативно-правовая база в области информационной безопасности, основой которой выступает система «Киберщит Казахстана» [2].

При проведении исследования было установлено, что системы и средства информационной безопасности в Республике Казахстан находятся в стадии развитии и нуждаются в совершенствовании, поэтому работы по

обеспечению информационной безопасности объекта делятся на несколько этапов: подготовительный этап, инвентаризация информационных запасов, анализ угроз, реализация защитного плана. По окончании указанных этапов начинается эксплуатационный период [3].

Подготовительный этап необходим для создания организационной основы всех последующих мероприятий, разработки и утверждения документации, а также определения взаимоотношений участников процесса. На подготовительном этапе определяются информационные задачи системы защиты информации.

От этапа анализа угрозы зависит насколько полно и правильно проанализированы условия защиты информационных фондов, зависят результаты следующих мероприятий. Анализ угрозы состоит из: выбора анализируемых объектов и степени детализации их рассмотрения; выбора методологии оценки риска; анализа угроз и их последствий; оценки рисков; анализа защитных мер; осуществления и проверки выбранных мер; оценки остаточного риска [4; 5].

Там, где есть опасность, возникает угроза. Этап анализа угроз является центральным элементом. Отметим, что для предотвращения опасностей необходимы защитные меры, что и определяется на этапе анализа угроз, который состоит, во - первых, в выявлении возможных угроз (их идентификации) и, во-вторых, в прогнозировании - оценке причиняемого будущего вреда.

В результате выполнения данного этапа составляется перечень угроз на объекте и их классификация по степени опасности. Все это позволяет определить требования к системе защиты информации, подобрать наиболее действенные меры и средства защиты, а также определить необходимые затраты на их реализацию.

На этапе составления плана защиты выбираются соответствующие организационные и технические меры, для нейтрализации угроз, выявленных в результате проведенного ранее анализа.

Разработка защитного плана начинается с разработки функциональной схемы системы защиты информации. Для этого определяются задачи, которые выполняет система защиты, и обсуждаются требования к системе с учетом особенностей конкретного объекта. В план включаются следующие документы: политика безопасности; расположение средств защиты информации на объекте; смета затрат, необходимых для включения в работу системы защиты; календарный план осуществления организационных и технических мер защиты информации [6; 7; 8].

Материалы и методы

Информационная безопасность в Республике Казахстан подразумевает защиту информации и всей организации от преднамеренных или случайных действий, ведущих к причинению вреда ее владельцам или пользователям, при этом обеспечение информационной безопасности должно быть направлено в первую очередь на предотвращение рисков, а не на устранение их последствий. Законодательные меры в сфере информационной безопасности направлены на создание в стране законодательной базы, которая рационализирует и регулирует поведение субъектов и объектов информационных отношений, а также определяет ответственность за нарушение установленных норм [9; 10].

Существует следующая законодательная база в этой области: законы Республики Казахстан в области информационной безопасности: «О национальной безопасности», «Об информатизации», «О государственных секретах», «О персональных данных и их защите», «Об электронном документе и электронной цифровой подписи», «О связи», Уголовный кодекс Республики Казахстан, Кодекс Республики Казахстан «Об административных правонарушениях», Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, Концепция кибербезопасности («Киберщит Казахстана») [3].

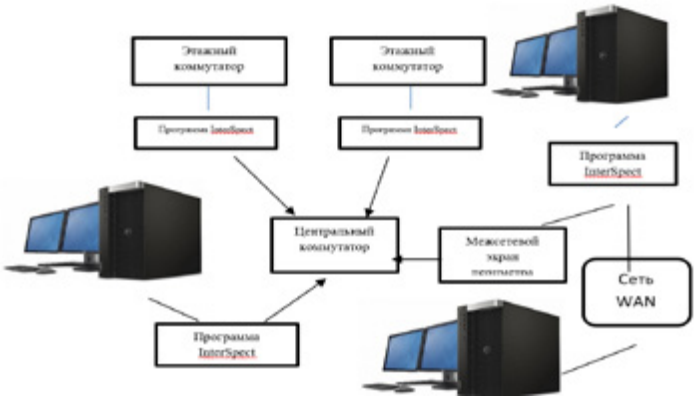

Рисунок 1 – Топология системы информационной безопасности в сети [3].

Риски могут быть вызваны следующими эффектами:
отказы и сбои аппаратуры;
плотины на линиях связи под воздействием внешней среды;
человеческие ошибки как часть системы;
системные и системно-технические ошибки обработчиков;

строительные, алгоритмические и программные ошибки;

аварийные ситуации.

Частота отказов и сбоев аппаратуры увеличивается при выборе и проектировании слабой системы относительно надежности работы аппаратуры. Плотины на линиях связи зависят от правильности выбора мест размещения технических средств по отношению друг к другу и аппаратуре соседних систем [7].

Результаты и обсуждение

Система информационного мониторинга и управления сетью связи на большинстве предприятий являетсяотносительно отсталой, что приводит к неспособности предприятий сформировать интегрированную информационную бизнес-платформу [8]. В настоящее время платформы поддержки эксплуатации сетей связи и управления техническим обслуживанием многих телекоммуникационных предприятий в основном используют режим управления, продвигаемый национальной сетью и провинциальной сетью. Среди них системы мониторинга сети и безопасности, такие как IMS и ISS, в основном используют платформы, развёрнутые национальной сетью и провинциальной сетью.

Однако телекоммуникационным предприятиям не хватает специального интегрированного централизованного решения для мониторинга работы сети связи. Разработка такой платформы позволит предприятиям эффективнее управлять эксплуатацией и техническим обслуживанием своих сетей связи.

Необходимо учесть все требования и особенности телекоммуникационной отрасли при разработке платформы. Она должна быть интегрированной, то есть объединять в себе различные системы мониторинга и управления сетью. Централизованность платформы позволит предприятиям иметь единый инструмент для мониторинга работы своих сетей связи.

Платформа должна быть гибкой и адаптируемой к различным условиям эксплуатации сетей связи. Она должна предоставлять операторам связи всю необходимую информацию для управления эксплуатацией и техническим обслуживанием сети.

Разработка такой платформы — сложная и трудоёмкая задача, Однако результаты разработки могут принести значительные преимущества энергетическим и телекоммуникационным предприятиям, повысив эффективность их работы и улучшив качество предоставляемых услуг [11]. В системе супервизии вся управленческая работа может выполняться только персоналом по эксплуатации и техническому обслуживанию на их соответствующих терминальных узлах, что приводит к отсутствию общего представления об управлении бизнесом. На рисунке 2 показана система мониторинга безопасности.

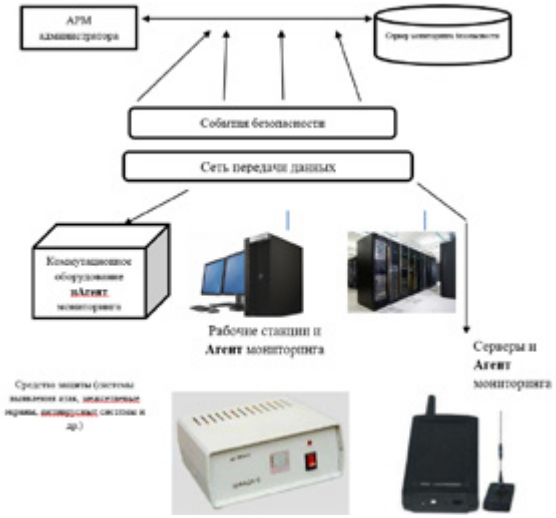

Рисунок 2–Система мониторинга информационной безопасности [4]

Политика безопасности (с точки зрения организации) правильно определяет способ использования средств учета и доступа, а также процедуры предотвращения и осмысления нарушений режима безопасности. Политика безопасности определяет совокупность правовых норм, организационных (правовых) мер, программно-технических средств и комплекса процедурных решений системы защиты информации, направленных на противодействие угрозам [12].

Достижение высокой степени информационной безопасности возможно только на основе применения соответствующих организационных мер. В состав комплекса организационных мероприятий входят работа по созданию, комплектованию и поддержанию деятельности службы информационной безопасности, подготовке системы организационно-распорядительных документов, а также ряд организационных и организационно-технических мероприятий по созданию и сопровождению работы системы защиты [13].

Проведение организационных и организационно-технических мероприятий позволит своевременно находить новые каналы утечки информации, принимать меры по их нейтрализации, полностью совершенствовать защитные системы и оперативно принимать меры против попыток нарушения режима безопасности. Проведение анализа рисков является основным этапом формирования политики безопасности [14].

После решения организационных вопросов наступает очередь программно-технических проблем - что нужно сделать для реализации

выбранной политики безопасности? В настоящее время существует множество видов средств защиты информации, стоимость которых различается по назначению и качеству. Одной из сложных задач является выбор из них того, что соответствует специфике конкретного объекта.

Политика безопасности состоит из следующих элементов: добровольное управление созданием отношений, безопасность повторного использования объектов, безопасность и принудительное управление созданием отношений [15].

Выводы

В связи с широким использованием современных информационных технологий, криптография становится незаменимым инструментом защиты информации. Использование электронных платежей, возможность передачи секретной информации через открытые сети связи, а также решение большого количества других задач информационной безопасности в компьютерных системах и информационных сетях основаны на криптографических методах. Республике Казахстан необходимо обеспечение необходимыми кадрами, которые способны расследовать подобные преступления, так как на данный момент полиция работает с информационными преступлениями не должным образом, раскрытие преступлений в области информационной безопасности имеет очень низкий уровень, в сравнении со странами Запада, где существуют специализированные отделы по борьбе с киберпреступностью.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 **Ахметов, Б.Б.** Совершенствование киберзащиты информационно коммуникационных систем транспорта за счет минимизации обучающих выборок в системах выявления вторжений // Захистінформації. 2018, том 20. № 1. С. 12–17.

2 Об информатизации - ИПС «Әділет» (zan.kz) https://adilet.zan.kz/rus/docs/Z1500000418

3 Состояние защиты информации [Электронный ресурс]. – URL: Ақпараттық қауіпсіздіктің жағдайы қалай – 16.07.2020 | Strategy2050.kz – обзорно-аналитический портал Казахстана.[Date od Accessed 28.06.2022].

4 **Кожамжаров, Е.** Исследование комплексной защиты информации корпоративных сетей / Е. Кожамжаров, Л. М. Исак // Интернаука. – 2017. – № 22(26). – С. 7–10. – EDN ZOFPUZ.

5 **Ахметов, Б. С.** Модели для адаптивной экспертной системы по выявлению киберугроз / Б. С. Ахметов, В. А. Лахно, А. А. Досжанова [и др.] // Проблемы информатики в образовании, управлении, экономике и технике : Сборник статей XVIII МНТК посвященной 75-летию Пензенского

государственного университета., Пенза, 25–26 октября 2018 года. – Пенза : Автономная некоммерческая научно-образовательная организация «Приволжский Дом знаний», 2018. – С. 84–90. – EDN YMJLSH.

6 **Кужаева, М. Р.** Проблемы информационной безопасности в компьютерных сетях / М. Р. Кужаева, А. Л. Золкин // Безопасность информационного пространства: Сборник трудов XIX Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых, Екатеринбург, 08–11 декабря 2020 года. – Екатеринбург: Уральский государственный экономический университет, 2021. – С. 120-123. – EDN AICFNM.

7 **Богачков, И. В., Трухина, А. И., Горлов, Н. И.** Обнаружение сегментов оптического волокна с механическим напряжением в оптических кабелях с использованием рефлектометров Бриллюэна// Материалы СИБКОН–2019 (Томск) с. 1–6.

8 **Маркузе, Д.** Формула потери кривизны для оптических волокон // Журнал Оптического общества Америки 1976. С. 216–220.

9 **Малых, Ю.В., Шубин, В. В.,** Способ расчета эффективности передачи излучения от боковой поверхности изогнутого одномодового оптического волокна к приемному оптическому устройству / Вопросы атомной науки и техники. Математическое моделирование физических Процессы 2016 г. . С. 69–79.

10 **Богачков, И. В., Трухина, А. И., Горлов, Н. И.** Исследование влияния изгиба оптических волокон на рефлектограммы Бриллюэна // Материалы APEIE–2018 (Новосибирск) 1, 2 с. 140–144.

11 **Трухина, А. И., Богачков, И. В., Горлов, Н. И.** Исследования влияния изгибов в оптических волокнах различных видов на системы генерации и обработки сигналов бриллюэновских трасс в области бортовой связи Труды (Москва), 2019 г. стр. 1–5

12 **A. Minardo, R. Bernini, L.** Zeni Bend-Induced Brillouin Frequency Shift Variation in a Single-Mode Fiber IEEE Photonics Technology Letters 25, 2013, 23 С. 2362–2364

13 **Фишер, О., Тома, С., Крепаз, С.** Распределенное волоконно-оптическое зондирование для обнаружения трещин в бетонных конструкциях //Проектирование гражданского строительства. – 2019. – Вып. 1. – нет. 3-4. – С. 97–105.

14 **Ян, М.** и соавт. Влияние переноса деформации на измерения с помощью распределенных волоконно-оптических датчиков // Автоматизация в строительстве. – 2022. – Вып. 139. – С. 104262.

15 **Фэн, Х.** и соавт. Теоретические и экспериментальные исследования по обнаружению трещин с помощью распределенных волоконно-оптических

датчиков BOTDR // Журнал инженерной механики. - 2013. - Вып. 139. - нет. 12. - С. 1797-1807 гг.

REFERENCES

1 **Akhmetov, B.B.** Sovershenstvovaniye kiberzashchity informatsionno-kommunikatsionnykh sistem transporta za schet minimizatsii vyborov obuchayushchikhsya v sochetanii s vtorzheniyami [Improvement of cyber protection of information and communication systems of transport by minimizing training samples in intrusion detection systems] // Zahist informatsiy. 2018, volume 20. No. 1. P. 12–17.

2 Ob informatizatsii [About informatization] – IPS «Adilet1» (zan.kz) https://adilet.zan.kz/rus/docs/Z1500000418

3 Sostoyaniye informatsionnoy bezopasnosti [Information security status] [Electronic resource]. – URL: Akparattyk kauipsizdiktin zhagdayy kalay - 07/16/2020 | Strategy2050.kz m – overview and analytical portal of Kazakhstan. [Date od Accessed 28.06.2022].

4 **Kozhamzharov, E.** Research of complex information protection of corporate networks [Research of complex information protection of corporate networks] / E. Kozhamzharov, L. M. Isak // Internauka. – 2017. – № 22(26). – P. 7–10. – EDN ZOFPUZ.

5 **Akhmetov, B. S.** Modeli adaptivnoy ekspertnoy sistemy obnaruzheniya kiberugroz [Models for an adaptive expert system for detecting cyber threats] / B. S. Akhmetov, V. A. Lakhno, A. A. Doszhanova [et al.] // Problems of informatics in education, management, economics and technology : Collection of articles of the XVIII International Scientific and Technical Conference dedicated to the 75th anniversary of Penza State University., Penza, 25-26 October 2018. – Penza: Autonomous non-profit scientific and educational organization «Volga House of Knowledge», 2018. – P. 84–90. – EDN YMJLSH.

6 **Kuzhaeva, M. R.** Problems of information security in computer networks [Problems of information security in computer networks] / M. R. Kuzhaeva, A. L. Zolkin // Information space security : Proceedings of the XIX All-Russian Scientific and Practical Conference of students, postgraduates and young scientists, Yekaterinburg, December 08–11. 2020. – Yekaterinburg: Ural State University of Economics, 2021. – P. 120–123. – EDN AICFNM.

7 **Bogachkov, I. V., Trukhina, A. I., Gorlov, N.I.** Obnaruzheniye segmentov opticheskogo volokna s mekhanicheskim napryazheniyem v opticheskikh kabelyakh s ispol'zovaniyem reflektometrov Brillyuena [Detection of segments of optical fiber with mechanical stress in optical cables using] Brillouin reflectometers Materials SIBCON–2019 (Tomsk) pp. 1–6

8 **Marcuse, D.** Formula poter' krivizna dlya opticheskikh kabeley [Curvature loss formula for optical fibers] Journal of the Optical Society of America 1976. P. 216–220

9 **Malykh, Yu.V., Shubin, V. V.** Sposob rascheta effektivnosti peredachi signalov ot paneli izognutogo odnoodovogo opticheskogo volokna k priyemnomu opticheskomu ustroystvu [Method for calculating the efficiency of radiation transmission from the side surface of a curved single-mode optical fiber to a receiving optical device] Issues of atomic science and technology. Mathematical modeling of physical Processes, 2016 1 P. 69-79

10 **Bogachkov, I. V., Trukhina, A. I., Gorlov, N. I.** Issledovaniye izgiba opticheskikh volokon na reflektogramme Brillyuena [Investigation of the effect of bending optical fibers on Brillouin reflectograms] // Materials APEIE–2018 (Novosibirsk) 1, 2 P. 140-144

11 **Trukhina, A. I., Bogachkov, I. V., Gorlov, N. I.** Issledovaniya izgotovleniya volokon v opticheskikh voloknakh razlichnykh tipov sistem generatsii i obrabotki signalov brillyuenovskikh trass v oblasti bortovoy svyazi [Studies of the influence of bends in optical fibers of various types on the systems of generation and processing of signals of Brillouin routes in the field of on-board communication] Proceedings (Moscow) 2019 – P. 1–5

12 **A. Minardo, R. Bernini, L.** Zeni Bend-Induced Brillouin Frequency Shift Variation in a Single-Mode Fiber IEEE Photonics Technology Letters 25, 2013, 23 стр. 2362-2364

13 **Fischer, O., Thoma, S., Crepaz, S.** Raspredelennoye volokonno-opticheskoye zondirovaniye dlya obnaruzheniya treshchin v betonnykh konstruktsiyakh [Distributed fiber optic sensing for crack detection in concrete structures] //Civil Engineering Design. – 2019. – T. 1. – № 3–4. – C. 97–105.

14 **Yan, M. et al.** Vliyaniye peredachi deformatsii na izmereniya s ispol'zovaniyem raspredelennykh volokonno-opticheskikh datchikov [Strain transfer effect on measurements with distributed fiber optic sensors] //Automation in Construction. – 2022. – T. 139. – C. 104262.

15 **Feng, X. et al.** Teoreticheskiye i eksperimental'nyye issledovaniya po obnaruzheniyu treshchin s ispol'zovaniyem raspredelennykh volokonno-opticheskikh datchikov BOTDR [Theoretical and experimental investigations into crack detection with BOTDR-distributed fiber optic sensors] //Journal of Engineering Mechanics. – 2013. – T. 139. – № 12. – C. 1797-1807.

Поступило в редакцию 03.12.24
Поступило с исправлениями 03.12.24
Принято в печать 04.12.24

**У. К. Жалмагамбетова[1],М. Ж. Мусагажинов[2],*
О. М. Талипов[3], А. П. Кислов[4]
[1,3,4]Торайғыров университеті, Қазақстан Республикасы, Павлодар қ.
[2]Қазақ агротехникалық университеті. С. Сейфуллин,
Қазақстан Республикасы, Астана қ.
03.12.24 ж. баспаға түсті.
03.12.24 ж. түзетулерімен түсті.
04.12.24 ж. басып шығаруға қабылданды.

ҚАЗАҚСТАННЫҢ ЭНЕРГЕТИКАЛЫҚ КЕШЕНІНДЕГІ МОНИТОРИНГ ТЕХНОЛОГИЯЛАРЫ МЕН ҚОРҒАУ ҚҰРАЛДАРЫНА ШОЛУ

Энергетикалық кешен үшін ақпараттық қауіпсіздік сенімді және қауіпсіз жұмысты қамтамасыз ету аясында зерттелетін маңызды аспектілердің бірі болып табылады. Ол Ақпараттық жүйелерді, деректерді және желілерді кибершабуылдар, рұқсатсыз кіру және ақпараттың ағып кетуі сияқты әртүрлі қауіптерден қорғауды қамтиды.

Желіні пайдалану мен техникалық қызмет көрсетудің дәстүрлі технологиясы-әкімші желінің ақаулығы туралы хабарламаны пассивті түрде күтеді, содан кейін шұғыл қалпына келтіруге кіріседі. Бұл әдіс белсенді механизмнен айырылған және желілік ақауларды жою кезінде көптеген кемшіліктерге ие. Ақпараттық қауіпсіздік-оны өңдеу жүйесінің белгілі бір уақыт аралығында ақпараттың ағып кетуімен, ұрлануымен, жоғалуымен, рұқсатсыз жойылуымен, мәнінің өзгеруімен, рұқсатсыз көшірмесін алуымен, бұғатталуымен сипатталатын оқиғалардың ықтималдық шамаларына қойылатын талаптардың орындалуын қамтамасыз ету қабілеті.

Бұл мақалада Қазақстандағы ақпараттық қауіпсіздік саласындағы заңнамалық және нормативтік-құқықтық база қарастырылған. Осы негізде ақпараттық қауіпсіздікті қорғау жүйелері мен құралдары, сондай-ақ қауіпсіздік саясаты, мониторингті жүзеге асыру үшін ұйымдастырушылық және ұйымдастырушылық-техникалық іс-шараларды жүргізу талданады. Ақпараттық қауіпсіздіктің жоғары дәрежесіне қол жеткізу тиісті ұйымдастырушылық шараларды қолдану негізінде ғана мүмкін болады.

Кілтті сөздер: ақпаратты қорғау жүйелері, технологиялар, ақпаратты қорғау, қауіпсіздік саясаты, құқықтық база, мониторинг.

**U. K. Zhalmagambetova[1], M. J. Musagazhinov[2],*
O. M. Talipov[3], A. P. Kislov[4]
[1,3,4]Toraighyrov University, Republic of Kazakhstan, Pavlodar
[2]Kazakh Agrotechnical University named after S. Seifullin,
Republic of Kazakhstan, Astana
Received 03.12.24
Received in revised form 03.12.24
Accepted for publication 04.12.24

OVERVIEW OF MONITORING TECHNOLOGIES AND PROTECTIVE EQUIPMENT IN THE ENERGY SECTOR OF KAZAKHSTAN

For the energy sector, information security is one of the important aspects studied in the framework of ensuring reliable and safe operation. It includes the protection of information systems, data and networks from various threats such as cyber attacks, unauthorized access and information leaks.

The traditional technology of network operation and maintenance consists in the fact that the administrator passively waits for a message about a network malfunction, and then proceeds to emergency recovery. This method lacks an active mechanism and has many disadvantages in eliminating network communication failures. Information security is the ability of its processing system to ensure compliance with the requirements for the probabilistic values of events characterized by leakage, theft, loss, unauthorized destruction, value change, receipt of an unauthorized copy, blocking of information for a specified period of time.

This article examines the legislative and regulatory framework in the field of information security in Kazakhstan. On this basis, information security protection systems and tools are analyzed, as well as security policy, organizational and organizational and technical measures for monitoring. Achieving a high degree of information security is possible only through the application of appropriate organizational measures.

Keywords: information security systems, technologies, information protection, security policy, legal framework, monitoring.

Теруге 04.12.2024 ж. жіберілді. Басуға 30.12.2024 ж. қол қойылды.
Электронды баспа
29.9 Mb RAM
Шартты баспа табағы 22,2. Таралымы 300 дана. Бағасы келісім бойынша.
Компьютерде беттеген: А. К. Мыржикова
Корректор: А. Р. Омарова, Д. А.Кожас
Тапсырыс №4317

Сдано в набор 04.12.2024 г. Подписано в печать 30.12.2024 г.
Электронное издание
29.9 Mb RAM
Усл. печ. л. 22,2. Тираж 300 экз. Цена договорная.
Компьютерная верстка: А. К. Мыржикова
Корректор: А. Р. Омарова, Д. А. Кожас
Заказ № 4317

«Toraighyrov University» баспасынан басылып шығарылған
Торайғыров университеті
140008, Павлодар қ., Ломов к., 64, 137 каб.

«Toraighyrov University» баспасы
Торайғыров университеті
140008, Павлодар қ., Ломов к., 64, 137 каб.
67-36-69
E-mail: kereku@tou.edu.kz
www.vestnik-energy.tou.edu.kz