УДК 621.396.66

ФОРМАЛИЗОВАННЫЙ ПОДХОД К ОЦЕНКЕ УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

Азаренко Елена; Гончаренко Юлия
Институт геохимии окружающей среды

FORMALIZED APPROACH TO THE ASSESSMENT OF VULNERABILITY OF INFORMATIONAL STRUCTURES OF CRITICALLY IMPORTANT OBJECTS

Azarenko Elena; Goncharenko Yulia
Institute of environmental geochemistry

Аннотация: **Формализован процесс конфиденциального циркулирования информации в информационной инфраструктуре критически важного объекта. Показано, что ее защищенность определяется степенью защищенности самого уязвимого элемента, дальность волновых излучений которого изменяется под воздействием внутренних и внешних факторов.**
Ключевые слова: **информационная инфраструктура, критически важный объект, контур управления, защита информации, множество, одиночный элемент, динамический процесс.**
Summary **Process of confidential circulation of information in informational infrastructure of critically important object is formalized. Presented that protection of information is determined by degree of protection in the most vulnerable element, distance of wave radiation of which are changes under the influence of internal and external factors.**
*Keywords:***information infrastructure, a critical facility, a control loop, information security, set a single element, a dynamic process.**

Введение

Критически важным объектом, по мнению отечественных и зарубежных специалистов [1] – [5], называют такой объект, нарушение или прекращение функционирования которого приводит к потере управления, влечет разрушение инфраструктуры, вследствие чего могут возникнуть необратимые негативные изменения в экономике страны либо административно-территориальной единицы, приводящие к существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях на длительный срок.

Функционирование критически важного объекта и управление им, как впрочем, и любым другим объектом, осуществляется с использованием информационных инфраструктур [6] – [12], в которых основным действующим звеном является информационно-управляющая или информационно-телекоммуникационная система.

Информационная инфраструктура, с точки зрения террористической угрозы, которая сейчас составляет часть ежедневной реальности, представляет собой источник несанкционированного сбора информации о критически важном объекте, являющимся целью воздействия злоумышленников.

Постановка цели и задач научного исследования

Цель данной работы – определить подходы к оценке уязвимости информационной инфраструктуры критически важного объекта на основе формализации процесса его функционирования.

Для достижения поставленной цели необходимо решить следующие задачи: рассмотреть контур управления критически

важным объектом и его составные части; формализовать информационные потоки в контуре управления; определить некоторые подходы к оценке его уязвимости; рассмотреть процесс изменения степени защищенности одиночного узла контура управления.

Структура контура управления критически важным объектом

Контур управления критически важным объектом представляет собой замкнутую цепь звеньев комплекса управления, связывающая в единое целое объект управления и субъект управления (лицо, принимающее решение – ЛПР).

Чтобы успешно осуществлять процесс управления, необходимо иметь достоверную информацию о состоянии объекта управления и о возможных тенденциях развития ситуаций, возникающих в результате его функционирования [9] – [12], которую можно получить с использованием двух систем: системы мониторинга и системы поддержки принятия решений.

В основе организации системы мониторинга лежит использование системы первичных сенсоров: различных датчиков, измерительных устройств, преобразователей информации и т. п., как показано на рис. 1, позволяющих собрать информацию о состоянии объекта управления.

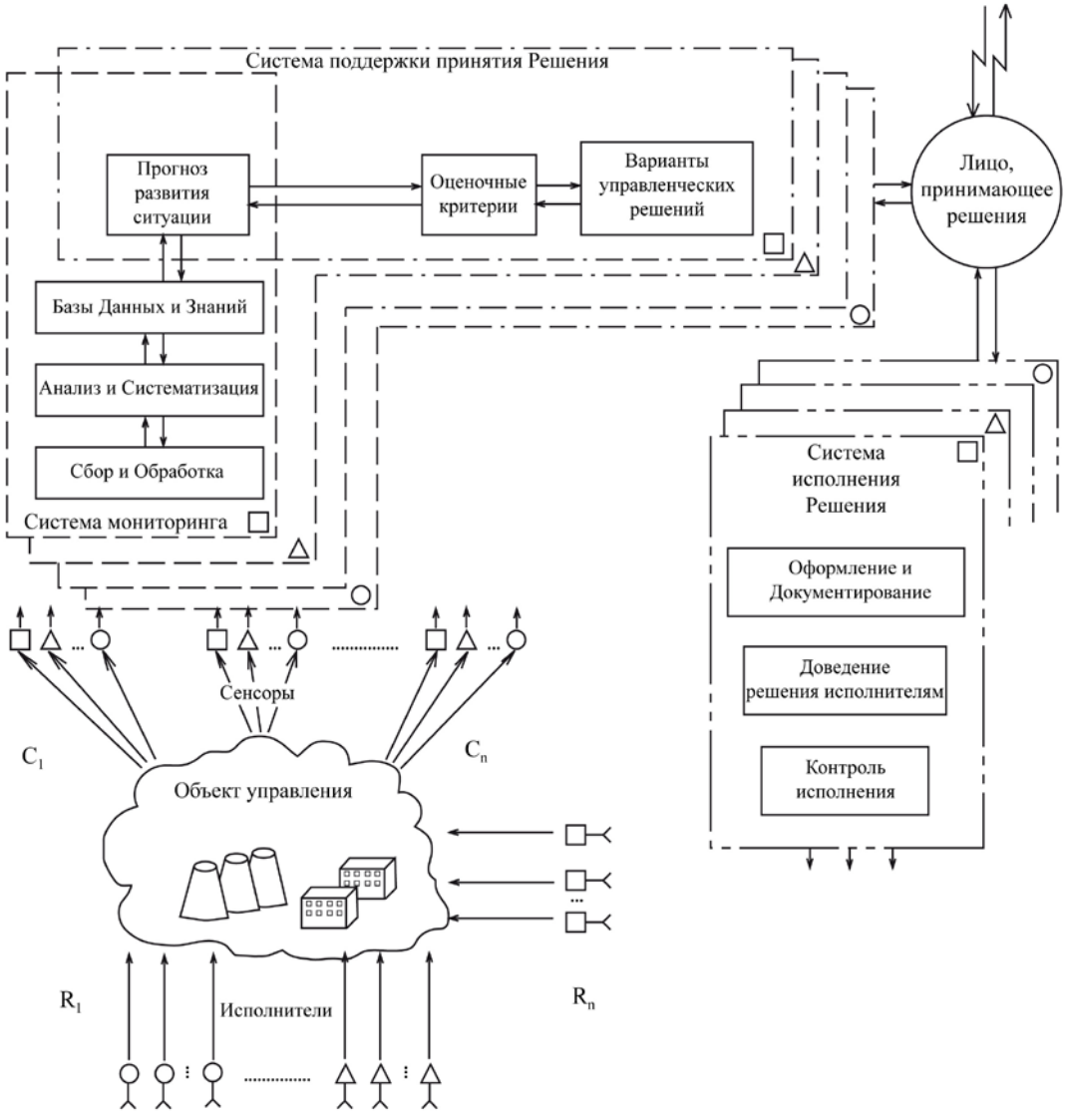

Рис. 1. Структурная схема контура управления критически важным объектом

ISSN 2074-9481
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (31), 2016р.

Система поддержки принятия решений дает возможность прогнозировать развитие ситуации на объекте, в соответствии с определенным набором одиночных критериев оценивать ее и на основе сделанных выводов готовить варианты управленческих решений.

Структура и организация рассмотренных систем могут быть самыми разнообразными в зависимости от типа и назначения объекта управления. Однако и система мониторинга, и система поддержки принятия решений могут содержать одинаковые элементы. К ним можно отнести блоки моделирования, базы данных и знаний и т. д., каждый из которых имеет свои прямые и обратные связи.

ЛПР делает выбор одного из предложенных вариантов управленческого решения, его удовлетворяющее, или вносит коррективы в систему оценочных критериев вследствие изменения текущей ситуации для выработки новых вариантов.

Принятое ЛПР решение направляется в систему исполнения решения, где проводится его оформление, документирование, доведение исполнителям, а также контроль качества его выполнения.

Исполнители воздействуют на объект управления, что приводит к изменению его состояния и фиксируется соответствующими сенсорами системы мониторинга. Круг управления замыкается.

Для эффективной работы контура управления критически важным объектом требуется организация информационной инфраструктуры как совокупности аппаратных и программных средств, средств связи и телекоммуникаций в соответствии с современными информационными технологиями [4] – [9]. Это оргтехника, компьютеры и серверы, их программное обеспечение, данные и средства их хранения, сети для передачи данных, активное и пассивное сетевое оборудование, телефонные и радиотелефонные сети и станции, которые необходимы для обеспечения бесперебойной работы контура управления.

Чем сложнее объект, тем он более функционален, тем большее количество контуров управления входит в его систему управления. Как правило, один контур управления обеспечивает решение определенного круга задач объекта управления. Например, для предприятий ядерно-топливного цикла – это обеспечение ядерным топливом, его утилизация или продление ресурса, физическая защита, ядерная и радиационная безопасность, управление персоналом и др.

Для обеспечения эффективной работы критически важного объекта его система управления как совокупность контуров управления должна иметь хорошо развитую и надежную информационную инфраструктуру.

С точки зрения потенциальной опасности террористической угрозы информационная инфраструктура критически важного объекта является основным источником несанкционированного сбора информации об объекте и, следовательно, представляет собой наиболее уязвимое место объекта, так как дает возможность дистанционно вызвать сбои в системе управления объектом и тем самым парализовать его работу.

Таким образом, основным источником несанкционированного сбора информации с целью воздействия злоумышленников на объект является информационная инфраструктура критически важного объекта.

Формализованный подход к оценке уязвимости информационных инфраструктур критически важного объекта

Пусть систему мониторинга объекта управления обслуживает n точек (сенсоров): $C_1;\ldots;C_n$. В это множество входят аналоговые и цифровые датчики (приборы) устройства ручного введения и т. п.

Если степень защищенности одиночного сенсора определяется величиной P_{C_i}, то

множество $\{P_{C_1};\ldots;P_{C_n}\}$ характеризует степень защищенности всех сенсорных узлов передачи данных $\{C_1;\ldots;C_n\}$ от них в соответствующую систему мониторинга M_i, количество которых определяется числом $к$ – количеством контуров управления объекта, при этом $k << n$.

Каждая система мониторинга в соответствии со своими функциями, обеспечивает сбор, обработку, систематизацию и анализ информации, пополнение баз данных и знаний и имеет степень защищенности P_M. То есть каждому элементу множества систем мониторинга $\{M_1;\ldots;M_k\}$ соответствует элемент множества $\{P_{M_1};\ldots;P_{M_k}\}$, характеризующий степень ее защищенности.

Если передача данных от системы мониторинга M_i в систему поддержки принятия решения S_i осуществляется по линиям связи, защищенность которых определяется величиной P_{MS_i}, то множество $\{P_{MS_1};\ldots;P_{MS_k}\}$ определяет степень защищенности соответствующих средств коммуникации.

Каждая из систем поддержки принятия решений $\{S_1;\ldots;S_k\}$ обеспечивает моделирование и прогнозирование развития ситуации на объекте управления путем сопоставления ее с оценочными критериями, при этом вырабатываются варианты управленческих решений со степенью защищенности $\{P_{S_1};\ldots;P_{S_k}\}$.

Передача данных от системы поддержки принятия решения S_i ЛПР осуществляется по средствам коммуникации, степень защищенности которых определяет множество $\{P_{SL_1};\ldots;P_{SL_k}\}$.

Информация, поступающая ЛПР, циркулирует среди его ближайшего окружения – заместителей, советников, референтов, технических работников его кабинета и служб, общее количество которых равно q. У каждого из них есть свои средства служебной и личной коммуникации. Каждый в той или иной мере обучен правилам конфиденциальности. Тогда степень защищенности от утечки информации множества сотрудников ближайшего окружения $\{OB_1;\ldots;OB_q\}$ определяется множеством $\{P_{OB_1};\ldots;P_{OB_q}\}$.

Из внутреннего круга ЛПР информация об объекте перетекает во внешний круг. Пусть число руководителей низшего звена равно l. Во внешнем круге ЛПР $\{OD_1;\ldots;OD_l\}$ степень защищенности руководящего сотрудника равна соответствующему элементу множества $\{P_{OD_1};\ldots;P_{OD_l}\}$.

Принятые ЛПР решения передаются в системы исполнения решений по линиям связи и телекоммуникаций. Степень их защищенности определяется множеством $\{P_{TJ_1};\ldots;P_{TJ_k}\}$.

Каждая из систем исполнения решений оформляет и документирует их и обладает степенью защиты P_{J_i}, тогда множество $\{P_{J_1};\ldots;P_{J_k}\}$ характеризует степень защищенности всей совокупности систем исполнения.

Результаты действий всех систем исполнения в совокупности передаются исполнителям, каждый из которых реализует принятые решения. Тогда множеству исполнителей $\{R_1;\ldots;R_m\}$ будет соответствовать множество, характеризующее степень их защищенности $\{P_{R_1};\ldots;P_{R_m}\}$, где $m >> k$.

Исходя из сказанного выше, степень защищенности контуров управления, обеспечивающих функционирование объекта, будет определяться надмножеством Z, состоящим из всех перечисленные выше множеств, характеризующих степень защищенности

ISSN 2074-9481
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (31), 2016р.

того или иного элемента контура управления критически важным объектом:

$$Z = \left\{ \begin{array}{l} \left\{P_{C_1};\ldots;P_{C_n}\right\},\left\{P_{M_1};\ldots;P_{M_k}\right\}, \\ \left\{P_{MS_1};\ldots;P_{MS_k}\right\},\left\{P_{S_1};\ldots;P_{S_k}\right\}, \\ \left\{P_{SL_1};\ldots;P_{SL_k}\right\},\left\{P_{OB_1};\ldots;P_{OB_q}\right\}, \\ \left\{P_{OD_1};\ldots;P_{OD_l}\right\},\left\{P_{TJ_1};\ldots;P_{TJ_k}\right\}, \\ \left\{P_{J_1};\ldots;P_{J_k}\right\},\left\{P_{R_1};\ldots;P_{R_m}\right\} \end{array} \right\} \quad (1)$$

Для каждого P_{ij} из множества (1) в области его значений всегда найдутся его наибольшее и наименьшее значения, при этом минимальное значение степени защищенности элемента будет определять степень защищенности совокупности всех контуров управления.

Таким образом, защищенность критически важного объекта может определяться степенью защищенности самого уязвимого элемента (элемента с минимальной защищенностью) информационной инфраструктуры, которая описывается множествами величин защищенности контуров управления, обеспечивающих функционирование объекта.

Изменение степени защищенности одиночного узла контура управления

Пусть имеется элемент n, входящий в состав контура управления, который выполняет определенное назначение F_n, вследствие чего информационный поток I_0 преобразуется в I_n (например, аналогово-цифровой преобразователь).

Во время работы элемента по выполнению функции F_n, в нем возникают внутренние силы (процессы) F_b, которые приводят к появлению внешних излучений ψ_n в виде электрических, магнитных, механических (упругих), электромагнитных (в том числе оптических), тепловых и других волн, рис. 2.

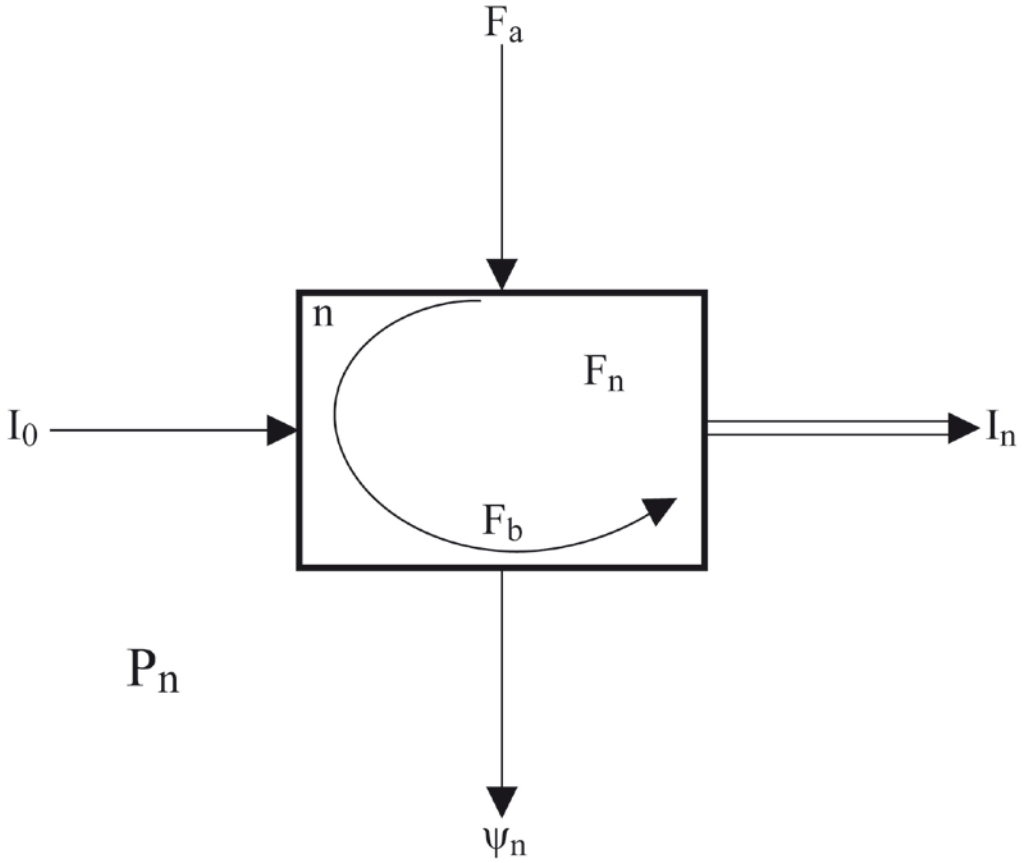

Рис. 2. Схема одиночного элемента контура управления

На процесс внешнего излучения ψ_n и последующего распространения излученных волн также влияют внешние силы (факторы) F_a (например, состояние среды: температура и влажность атмосферы, состояние амортизаторов и заземления, тепло-, виброизоляции и др.).

Считается, что элемент n обладает степенью защищенности, определяемой величиной P_n, если при выполнении работы F_n по преобразованию информации вида I_0 в вид I_n при фиксированных внутренних F_b и внешних F_a воздействиях величина внешних излучений не превышает определенного порога H_n [9, 10]. Применительно к волновым процессорам порог H_n может определяться как энергетическими параметрами – мощностью излучения W_n, так и геометрическими – дальностью регистрации этого излучения.

Следует отметить, что при одной и той же мощности излучения вследствие изменения факторов внешней среды дальность регистрации излучения может быть различной. Это можно проиллюстрировать следующими примерами.

Для световых волн это явление тумана, когда видимость уменьшается до нескольких метров.

Для оптических волн – сверхдальнее распространение оптических волн, когда в море из-за линии горизонта появляются сначала мачты, затем надстройка и только после этого сам корпус корабля. Для электромагнитных (радио) волн это явление непрохождения, когда ультракороткие волны рефрагируют вверх, вследствие чего отсутствует радиосвязь между корреспондентами, находящимися на прямой видимости друг от друга, или явление сверхдальнего распространения радиоволн, когда корабли, стоящие в Одессе, слышат радиопереговоры судов, подходящих к Босфору.

Другими словами, в зависимости от факторов внешней окружающей среды дальность регистрации излучений будет изменяться. Это может также происходить и под воздействием других внешних факторов. Например, обрыв заземления на элементе n приведет к увеличению мощности и, соответственно, дальности регистрации электромагнитных излучений. Получается, что дальность распространения внешних излучений как функция времени будет постоянно изменяться в зависимости от изменения внешних воздействий.

В некоторых случаях ее флуктуации, как показано на рис. 3, в моменты t_1 и t_2 могут значительно превышать D_n, определяющую порог H_n. В таких случаях дальность распространения излучений может выходить за пределы контролируемой зоны критически важного объекта и создавать условия для несанкционированного съема данных с носителей информации, входящих в информационные инфраструктуры.

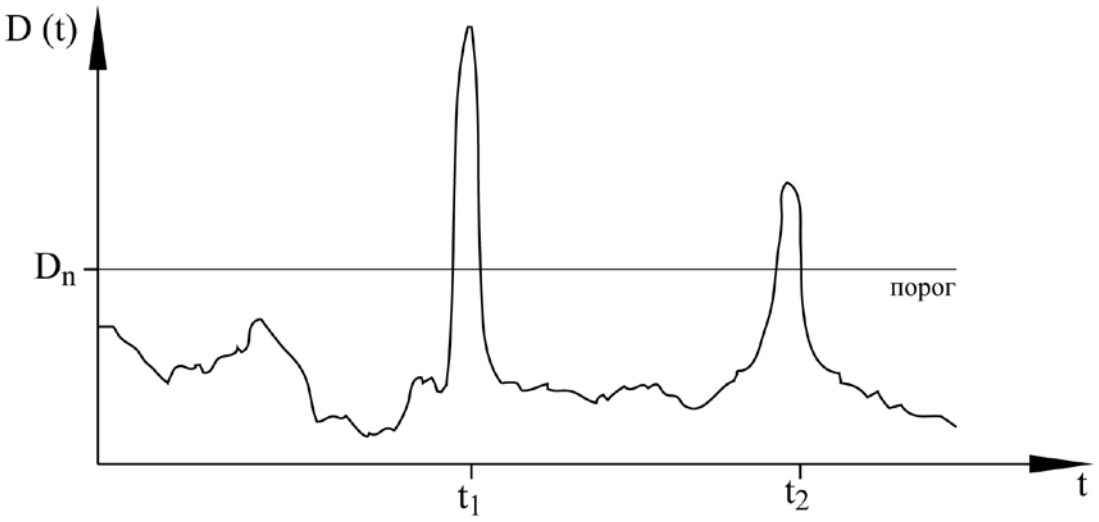

Рис. 3. Диаграмма флуктуаций дальности излучений

ISSN 2074-9481
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (31), 2016р.

Таким образом, внешние волновые излучения каждого одиночного узла контура управления, возникающие во время преобразования информационного потока под действием внешних и внутренних факторов, представляют собой динамический процесс, изменяющийся во времени, при этом дальность распространения волн флуктуирует, и в некоторые моменты может не только превышать пороговые значения, но и выходить за пределы контролируемой зоны критически важного объекта.

Выводы

1. Основным источником несанкционированного сбора информации с целью воздействия злоумышленников на объект является информационная инфраструктура критически важного объекта.

2. Защищенность критически важного объекта может определяться степенью защищенности самого уязвимого элемента (элемента с минимальной защищенностью) информационной инфраструктуры, которая описывается множествами величин защищенности контуров управления, обеспечивающих функционирование объекта.

3. Внешние волновые излучения каждого одиночного узла контура управления, возникающие во время преобразования информационного потока под действием внешних и внутренних факторов, представляют собой динамический процесс, изменяющийся во времени, при этом дальность распространения волн флуктуирует, и в некоторые моменты может не только превышать пороговые значения, но и выходить за пределы контролируемой зоны критически важного объекта.

Перечень ссылок

[1] В. Е. Петрищев, *Антитеррористическая защита критически важных объектов.* 27.08.2014. Доступ: http://www.arms-expo.ru/new_politics_and_sosiety.

[2] *Методика отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации, 2012.* Доступ: http://www.mchs.gov.ru/upload/site1/document_file/rOH6g8ruf.pdf.

[3] *The Cybersecurity Executive Order. Exploiting Emerging Cyber Technologies and Practices for Collaborative Success* [Электронный ресурс] / M. McConnell, S. Labarre, D. Sulek, M. McGowan. Доступ: http://www.boozallen.com/media/file/BA13-051CybersecurityEOVP.pdf.

[4] *System of Systems Engineerings* / Keating, C, Rogers, R., Unal. R., Dryer, D., Sousa-Poza, A., Safford. R. Peterson, W., Rabadi, G. // Engineering Management Journal, Vol. 15, No. 3, – 2003.

[5] *In the Dark. Crucial Industries Confront Cyberattacks.* McAfee second annual critical infrastructure protection report [Электронный ресурс]. Доступ: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf.

[6] *Ключевые системы информационной инфраструктуры* [Электронный ресурс]. – Режим доступа: http://ispdn.narod.ru/ksii.pdf

[7] *Критически важные объекты информатизации.* [Электронный ресурс]. – Режим доступа: http://oac.gov.by/tzi/kvoi.html.

[8] Г. П. Леоненко, *Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины* / Г. П. Леоненко, А. Ю. Юдин // Information Technology and Security. – № 1(3). – 2013. – p. 44 – 48.

[9] Ю. Ю. Гончаренко, *Защита информации – как один из ключевых аспектов предотвращения чрезвычайных ситуаций* / Ю. Ю. Гончаренко, Е. Е. Сычков, В. В. Рыбко // Збірник наукових праць СНУЯЕтаП. – Севастополь: СНУЯЕтаП, 2012. – Вип. 1 (41). – С. 207 – 211.

[10] Ю. Ю. Гончаренко, *Проблема управления экологической безопасностью прибрежных вод и пути ее решения* / Ю.Ю. Гончаренко, Е. В. Азаренко, М. М. Дивизинюк // Збірник наукових праць «Системи обробки інформації». – Харків: Харківський університет Повітряних Сил імені Івана Кожедуба, 2012. – Вип. 2 (100). – С. 271 – 275.

[11] Ю. Ю. Гончаренко, *Компьютерный эколого-экономический мониторинг как информационно-техническое средство управления экологической безопасностью* / Е. В. Азаренко, Ю. Ю. Гончаренко, М. М. Дивизинюк // Наук.- техніч. журнал «Сучасний захист інформації». – Київ: ДУІКТ, 2012. – Спецвипуск. – С. 53 – 56.

[12] Ю. Ю. Гончаренко, *Структура контура управления информационной безопасностью предприятия* / Ю. Ю. Гончаренко // Научно-практический журнал «Экономика и управление». – №5. – Симферополь: НАПКС, 2012. – С. 97 – 101.

References

[1] V. E. Petryshchev, *Antyterrorystycheskaia zashchyta krytychesky vazhnыkh obъektov.* 27.08.2014. Dostup: http://www.arms-expo.ru/new_politics_and_sosiety.

[2] *Metodyka otnesenyia obъektov hosudarstvennoi y nehosudarstvennoi sobstvennosty k krytychesky vazhnыm obъektam dlia natsyonalnoi bezopasnosty Rossyiskoi Federatsyy*, 2012.

Dostup: http://www.mchs.gov.ru/upload/site1/document_file/rOH6g8ruf.pdf.

[3] *The Cybersecurity Executive Order. Exploiting Emerging Cyber Technologies and Practices for Collaborative Success* [Ɔlektronnыi resurs] / M. McConnell, S. Labarre, D. Sulek, M. McGowan. Dostup: http://www.boozallen.com/media/file/BA13-051CybersecurityEOVP.pdf.

[4] *System of Systems Engineerings* / Keating, S, Rogers, R., Unal. R., Dryer, D., Sousa-Poza, A., Safford. R. Peterson, W., Rabadi, G. // Engineering Management Journal, Vol. 15, No. 3, – 2003.

[5] *In the Dark. Crucial Industries Confront Cyberattacks.* McAfee second annual critical infrastructure protection report [Ɔlektronnыi resurs]. Dostup: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf.

[6] *Kliuchevыe systemы ynformatsyonnoi ynfrastrukturы* [Ɔlektronnыi resurs]. – Rezhym dostupa: http://ispdn.narod.ru/ksii.pdf

[7] *Krytychesky vazhnыe obъekty ynformatyzatsyy.* [Ɔlektronnыi resurs]. – Rezhym dostupa: http://oac.gov.by/tzi/kvoi.html.

[8] H. P. Leonenko, *Problemы obespechenyia ynformatsyonnoi bezopasnosty system krytychesky vazhnoi ynformatsyonnoi ynfrastrukturы Ukraynы* / H .P. Leonenko, A. Yu. Yudyn // Information Technology and Security. – # 1(3). – 2013. – r. 44 – 48.

[9] Yu. Yu. Honcharenko**,** *Zashchyta ynformatsyy – kak odyn yz kliuchevыkh aspektov predotvrashchenyia chrezvыchaynыkh sytuatsyi* / Yu.Yu. Honcharenko, E.E. Sыchkov, V.V. Rыbko // Zbirnyk naukovykh prats SNUIaEtaP. – Sevastopol: SNUIaEtaP, 2012. – Vyp. 1 (41). – S. 207 – 211.

[10] Yu. Yu. Honcharenko,. *Problema upravlenyia ekolohycheskoi bezopasnostiu prybrezhnыkh vod y puty ee reshenyia* / Yu. Yu. Honcharenko, E. V. Azarenko, M. M. Dyvyzyniuk // Zbirnyk naukovykh prats «Systemy obrobky informatsii». – Kharkiv: Kharkivskyi universytet Povitrianykh Syl imeni Ivana Kozheduba, 2012. – Vyp. 2 (100). – S. 271 – 275.

[11] Yu. Yu. Honcharenko, *Kompiuternыi ekoloho-ekonomycheskyi monytorynh kak ynformatsyonno-tekhnycheskoe sredstvo upravlenyia ekolohycheskoi bezopasnostiu* / E. V. Azarenko, Yu. Yu. Honcharenko, M. M. Dyvyzyniuk // Nauk.- tekhnich. zhurnal «Suchasnyi zakhyst informatsii». – Kyiv: DUIKT, 2012. – Spetsvypusk. – S. 53 – 56.

[12] Yu. Yu. Honcharenko, *Struktura kontura upravlenyia ynformatsyonnoi bezopasnostiu predpryiatyia* / Yu. Yu. Honcharenko // Nauchno-praktycheskyi zhurnal «Ekonomyka y upravlenye». – #5. – Symferopol: NAPKS, 2012. – S. 97 – 101.

Реферат

Азаренко Олена, Гончаренко Юлія

Формалізований підхід до оцінки вразливості інформаційних інфраструктур критично важливих об'єктів

Критично важливим об'єктом вважається такий об'єкт, порушення або припинення функціонування якого призводить до незворотних негативних змін в економіці країни чи адміністративно-територіальної одиниці. Функціонування цього об'єкта здійснюється з використанням інформаційних інфраструктур або інформаційно-телекомунікаційних систем. Чим складніше об'єкт, тим він більш функціональний, тим більша кількість контурів управління входить в його систему управління. Як правило, один контур управління забезпечує вирішення певного кола завдань об'єкта управління. Для забезпечення ефективної роботи критично важливого об'єкта його система управління як сукупність контурів управління повинна мати добре розвинену і надійну інформаційну інфраструктуру. З точки зору потенційної небезпеки терористичної загрози інформаційна інфраструктура критично важливого об'єкта є основним джерелом несанкціонованого збору інформації про об'єкт і дає можливість дистанційно викликати збої в системі управління об'єктом і тим самим паралізувати його роботу. Формалізуючи цей процес, показано, що захищеність критично важливого об'єкта може визначатися ступенем захищеності самого уразливого елементу (елементу з мінімальною захищеністю) інформаційної інфраструктури, яка описується множинами величин захищеності контурів управління, що забезпечують функціонування об'єкта. Крім цього, зовнішні хвильові випромінювання кожного одиночного вузла контуру управління, що виникають під час перетворення інформаційного потоку, є динамічний процес, що змінюється в часі, при цьому дальність поширення хвиль піддається флуктуаціям, і в деякі моменти може не тільки перевищувати граничні значення, а й виходити за межі контрольованої зони критично важливого об'єкта.

Азаренко Елена, Гончаренко Юлия

Формализованный подход к оценке уязвимости информационных инфраструктур критически важных объектов

Критически важным объектом считается такой объект, нарушение или прекращение

функционирования которого приводит к необратимым негативным изменениям в экономике страны либо административно-территориальной единицы. Функционирование этого объекта осуществляется с использованием информационных инфраструктур или информационно-телекоммуникационных систем. Чем сложнее объект, тем он более функционален, тем большее количество контуров управления входит в его систему управления. Как правило, один контур управления обеспечивает решение определенного круга задач объекта управления. Для обеспечения эффективной работы критически важного объекта его система управления как совокупность контуров управления должна иметь хорошо развитую и надежную информационную инфраструктуру. С точки зрения потенциальной опасности террористической угрозы информационная инфраструктура критически важного объекта является основным источником несанкционированного сбора информации об объекте и дает возможность дистанционно вызвать сбои в системе управления объектом и тем самым парализовать его работу. Формализуя этот процесс, показано, что защищенность критически важного объекта может определяться степенью защищенности самого уязвимого элемента (элемента с минимальной защищенностью) информационной инфраструктуры, которая описывается множествами величин защищенности контуров управления, обеспечивающих функционирование объекта. Кроме этого, внешние волновые излучения каждого одиночного узла контура управления, возникающие во время преобразования информационного потока, представляют собой динамический процесс, изменяющийся во времени, при этом дальность распространения волн флуктуирует, и в некоторые моменты может не только превышать пороговые значения, но и выходить за пределы контролируемой зоны критически важного объекта.

Azarenko Elena, Goncharenko Yulia

Formalized approach to the assessment of vulnerability of informational structures of critically important objects

Critically important object – is object, breach or work termination of which cause irreversible negative changes in economy of country or administrative territorial unit. Functioning of this object is carrying out with using of informational infrastructures or informational and telecommunications systems. The more complicated object has more functions and more control loops, that includes in its control system. As a rule, one management contour provide solution of certain range of tasks of management object. For providing of effective works of critically important object, his management system, as a complex of management contours, should have developed and reliable information infrastructure. From the point of view of potential danger of terrorist threat, informational structure of critically important object is main source for unauthorized collection of information about object, and take possibility for remote formation of failures in system of management of object, which in result paralyze its work. During formalizing of this process, it is showed, that protection of critically important object can be determined by degree of protection of most vulnerable object (element with minimal protection) of informational infrastructure, which describes by sets of protection values of control loops, which provides functioning of object. Except this, external wave radiation of each single nodes of management loop, which formats during informational flow transformation, is represents dynamic process which changes in time, and in some time range wave propagation is fluctuate, and in some moments it can not only exceed thresholds, but also beyond over the borders of controlled zone of critically important object.

Відомості про авторів

Азаренко Олена Василівна

Освіта: Вища повна, 1987 рік, математик викладач.

Місце роботи: Національний педагогічний університет імені Драгоманова, професор, д.ф-м.н.

Область знань: інформаційні технології.

Наукові інтереси: цивільний захист, захист критичної інфраструктури, фізичний захист.

Email: *dekan_eva@list.ru*

Гончаренко Юлія Юріївна

Освіта: повна вища, 2008 рік, магістр комп'ютерних систем еколого-економічного моніторингу.

Місце роботи: Державна установа "Інститут геохімії навколишнього середовища Національної Академії Наук України", доцент, д.т.н.

Область знань: захист інформації.

Наукові інтереси: цивільний захист, захист критичної інфраструктури, фізичний захист.

Email: *iuliay1985@mail.ru*