Александр С. Мосолов[1], Андрей Е. Краснов[2], Николай А. Урбан[3]
[1]Российский химико-технологический университет им. Д.И. Менделеева, Миусская пл., 9, Москва, 125047, Россия
[2,3]Российский государственный социальный университет, ул. Вильгельма Пика, 4, стр. 1, Москва,129226, Россия
[1]e-mail: asmosolov@yandex.ru, https://orcid.org/0000-0002-3266-9505
[2]e-mail: krasnovmgutu@yandex.ru, https://orcid.org/0000-0002-4075-4427
[3]e-mail: urbannikolai@mail.ru, https://orcid.org/0000-0002-8047-1499

О ПРИМЕНЕНИИ МЕТОДА АНАЛИЗА УЯЗВИМОСТЕЙ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ПРОИЗВОДСТВЕННОГО ОБЪЕКТА ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП С УЧЁТОМ ВЗАИМОСВЯЗИ КОМПОНЕНТОВ

DOI: http://dx.doi.org/10.26583/bit.2022.3.03

Аннотация. Цель статьи – анализ уязвимости систем, обеспечивающих процессы жизнедеятельности объекта топливно-энергетического комплекса. Применение метода смещённого идеала, а также метода сокращённого анализа иерархий позволило найти наиболее уязвимые элементы технологических систем и выявить зависимость работоспособности этих элементов от защищённости информационных потоков в автоматизированных системах управления технологическими процессами. Показана необходимость формирования обоснованных требований к политике информационной безопасности предприятия и акцентирования внимания на обеспечение достаточного уровня защиты от угроз элементам информационной системы предприятия. Исполнение таких угроз может привести к последствиям, наносящих наибольший ущерб по критериям: зона чрезвычайной ситуации, экономический ущерб, количество пострадавших, вероятность отказа системы. Проведён анализ значимости угроз для информационных систем, и анализ устойчивости, как отдельных компонентов, так и их агрегатов. Показан характер взаимосвязанности (отношений) компонентов информационных систем предприятия. В рамках рассмотрения угроз для компонентов информационных систем выявлена иерархическая зависимость защищённости сложных активов информационной системы от защищённости базовых компонентов низшего уровня. Разработана модель угроз на основании утверждённого Федеральной службой по техническому и экспортному контролю перечня угроз в базе данных угроз информационной безопасности для информационных систем. Применение данного подхода позволяет сформировать положения для политики информационной безопасности предприятия и предложить специалистам по обеспечению информационной безопасности разработать меры программно-аппаратной защиты для информационной системы предприятия.

Ключевые слова: угроза, риск, устойчивость, политика информационной безопасности, технологические системы, критическая информационная инфраструктура, топливно-энергетический комплекс.
Для цитирования: МОСОЛОВ, Александр С.; КРАСНОВ, Андрей Е.; УРБАН, Николай А. О ПРИМЕНЕНИИ МЕТОДА АНАЛИЗА УЯЗВИМОСТЕЙ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ПРОИЗВОДСТВЕННОГО ОБЪЕКТА ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП С УЧЁТОМ ВЗАИМОСВЯЗИ КОМПОНЕНТОВ. Безопасность информационных технологий, [S.l.], т. 29, № 3, с. 38–52, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1434. DOI: http://dx.doi.org/10.26583/bit.2022.3.03.

Alexander S. Mosolov[1], Andrey E. Krasnov[2], Nikolay A. Urban[3]
[1]D.I. Mendeleev University of Chemical Technology of Russia, Miusskaya square, 9, Moscow, 125047, Russia
[2,3]Russian State Social University, Wilhelm Pik str., 4, p. 1, Moscow,129226, Russia
[1]e-mail: asmosolov@yandex.ru, https://orcid.org/0000-0002-3266-9505

[2]*e-mail: krasnovmgutu@yandex.ru, https://orcid.org/0000-0002-4075-4427*
[3]*e-mail: urbannikolai@mail.ru, https://orcid.org/0000-0002-8047-1499*

On the application of the vulnerability analysis method of the technological process of the production facility to ensure the information security of the automated process control system, taking into account the interrelation of components

DOI: http://dx.doi.org/10.26583/bit.2022.3.03

Abstract. The purpose of the paper is to analyze the vulnerability of systems that ensure the processes of vital activity of an object of the fuel and energy complex. The application of the shifted ideal method, as well as the method of reduced hierarchy analysis, made it possible to find the most vulnerable elements of technological systems and to identify the dependence of the operability of these elements on the security of information flows in automated process control systems. The need in forming reasonable requirements for the information security policy of the enterprise and focusing on ensuring a sufficient level of protection against threats to the elements of the enterprise information system is demonstrated. The execution of such threats can lead to consequences that cause a huge damage according to the following criteria: the emergency zone, economic damage, the number of victims, the probability of system failure. The analysis of the significance of threats to information systems as well as the analysis of the stability of both individual components and their aggregates are carried out. The nature of the interconnectedness (relationships) of the components of information systems of the enterprise is shown. As part of the consideration of threats to the components of information systems, the hierarchical dependence of the security of complex assets of the information system on the security of the basic components of the lowest level is revealed. A threat model has been developed based on the list of threats approved by the Federal Service for Technical and Export Control in the database of information security threats for information systems. The application of this approach makes it possible to form provisions for the information security policy of the enterprise and to invite information security specialists to develop the software and hardware protection for the enterprise information system.

Keywords: threat, risk, stability, information security policy, technological systems, critical information infrastructure, fuel and energy complex.
For citation: MOSOLOV, Alexander S.; KRASNOV, Andrey E.; URBAN, Nikolay A. On the application of the vulnerability analysis method of the technological process of the production facility to ensure the information security of the automated process control system, taking into account the interrelation of components. IT Security (Russia), [S.l.], v. 29, no. 3, p. 38–52, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1434. DOI: http://dx.doi.org/10.26583/bit.2022.3.03.

Введение

Одной из важных составляющих безопасности объектов топливно-энергетического комплекса (ТЭК) является обеспечение его технологической безопасности. В соответствии с Федеральным законом № 256-ФЗ[1] защитные меры формируются на основании присвоенной объекту категории потенциальной опасности от акта незаконного вмешательства (АНВ) и установленных уровней защищенности его критическим элементам. В 75% из общего количества выполненных проектов по категорированию в качестве АНВ рассматривают угрозу «технического воздействия», включая информационное воздействие на информационную систему предприятия (АСУ ТП) [1], направленное на дестабилизацию функционирования объекта и нарушение технологических процессов [2].

Целью совершения АНВ является причинение ущерба населению, окружающей среде, объекту и, в целом, для государства. При этом категория определяется по

[1]Федеральный закон № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» от 21.07.2011 г.

наибольшему значению показателя одного из критериев категорирования: зона чрезвычайной ситуации, социальный и материальный (экономический) ущерб[1].

Новизна предлагаемого в настоящей статье подхода в том, что предлагается оценивать уязвимость производственно-технологического процесса по совокупности значений показателей множества критериев (включая, но не ограничиваясь критериями категорирования) для определения наиболее привлекательной комбинации отказов [3], к которой будет стремиться привести аварийную ситуацию потенциальный нарушитель. При этом возможно обнаружение уязвимых элементов как, собственно, в технологическом процессе, так и прогнозирование привлекательности наиболее уязвимых технологических блоков в инфраструктуре производственного цикла объекта [4].

Для борьбы с угрозами информационной безопасности применяют различные методики [5–6], самостоятельные программные решения и отдельные комплексы для контроля за параметрами информационной инфраструктуры предприятия [7–8], алгоритмы целевого анализа уязвимости производственно-технологических процессов опасных производственных и критически важных объектов [3].

В [9] рассмотрена система прогнозирования и оценки безопасности опасного производственного объекта с использованием комплексной модели обеспечения безопасности.

В [10] авторы рекомендуют при построении системы защиты от разрушительных программных воздействий (РПВ) использовать декомпозицию задачи выбора рационального варианта системы защиты, что связано с большим количеством ограничений и частных показателей, требующих учёта при проектировании, что, в свою очередь, ссылается на три функциональные категории системы защиты от РПВ – подсистему обнаружения РПВ, подсистему противодействия РПВ и подсистему устранения последствий РПВ.

В [11] отмечены достоинства применения методик и моделей по проектированию систем информационного обеспечения для решения задач технической защиты информации, рассмотрены методы поддержки выбора с расчетом эффективности проектируемой модели посредством факторного анализа. Данный анализ достигается с помощью подхода по применению правила Фишберна, подхода по анализу иерархий Т. Саати, подхода по применению мультипликативной функции Кобба-Дугласа.

В [12] рассмотрены практики по реализации политики безопасности на базе модели угроз информационной безопасности, выстраиваемой по определённой последовательности шагов, как следует из примера использования такой практики на примере предприятий.

1. Определение уязвимости производственно-технологического процесса

Вопросы обеспечения информационной безопасности в АСУ ТП не могут рассматриваться без учета самой природы химических и нефтехимических процессов на опасных производственных объектах (ОПО). Принцип равновероятностной защиты информационного периметра не применим, если существует вероятность потенциальной угрозы АНВ в отношении уязвимых элементов технологической схемы ОПО, для их определения которых применяют метод анализа и оценки риска последствий возможных комбинаций «отказов» по совокупности значений показателей существенно значимых критериев.

Число комбинаций определяется с помощью формулы числа сочетаний из n элементного множества наборами по k элементов:

$$C_n^k = \frac{n!}{(n-k)!*k!}. \quad (1)$$

«Вес» привлекательности комбинации «отказов» в [13] рассчитывают на базе принятых в [1] критериев с использованием методов экспертных оценок: методов полного и сокращенного анализа иерархий, метода многокритериальной комбинации («метода смещённого идеала»).

Для анализа рисков на опасных производственных объектах, к которым относят объекты топливно-энергетического комплекса, применяют модели и алгоритмы прогнозирования эффективности управлением промышленной безопасности и антитеррористической защищенностью таких объектов [14, 15].

Описанный в [13] метод направлен на повышение эффективности процесса категорирования объектов КИИ[2,3]; следует учитывать отсутствие в Указе Президента № 31с[4] таких необходимых операций, как определение критических сегментов в объекте критической информационной инфраструктуры, оценка риска отключения критического элемента, оценка эффективности АСУ ТП предприятия при реагировании на компьютерные атаки.

Разработанную в [13] модель можно использовать для определения критических сегментов в объекте КИИ; уязвимым элементам технологической схемы соответствуют активы и ресурсы объекта АСУ ТП, объединенные в критические сегменты. При этом сегментам или элементам критических информационных инфраструктур присваивают «категории значимости» объектов, а базы критериев значимости КИИ определены в Постановлении Правительства РФ № 127[5].

Степень защиты элемента технологической схемы должна быть не ниже установленных нормативов по обеспечению технологической безопасности[6], аналогичные положения применимы и к АСУ ТП.

Влияние информационных угроз на устойчивость объектов определяется методологией комплексного оценивания уязвимости КИИ и её критических элементов[7].

Информационные потоки данных наиболее уязвимы, и необходимо расширять спектр защитных механизмов, чтобы не допустить, в т.ч. утечки персональных данных[8].

Отнесение элементов объекта КИИ к критичным или некритичным возможно определить в результате анализа фрагмента информационной системы, используя значения показателя вероятности отказа элемента технологического процесса и вероятности его безотказной работы.

Одним из вариантов модели подобного подхода может быть формула (2) из [13]:

$$P = (p_{iотк} * p_{(i+n)отк} * \dots) * (p_{(i+n+k)б/отк} * \dots). \quad (2)$$

[2]Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017.

[3]Постановлением Правительства РФ от 24 декабря 2021 г. N 2431«О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. N 127».

[4]Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». – 3 с.

[5]Постановление Правительства РФ № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» от 8 февраля 2018 г.

[6]Федеральный закон № 116-ФЗ «О промышленной безопасности опасных производственных объектов» от 21.07.1997.

[7]Методика оценки угроз безопасности информации. ФСТЭК России 5 февраля 2021 года. URL: https://docs.cntd.ru/document/607699443 (дата обращения: 22.04.2022).

[8]Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 22.04.2022).

Итоговое значение P будет являться показателем критичности фрагмента системы. Последовательная проверка фрагментов системы позволит определить наиболее уязвимый и привлекательный к АНВ актив системы.

С помощью данного метода может быть решена проблема анализа и оценки бесперебойной работы технического узла.

2. Анализ влияния рисков информационной безопасности на составляющие информационной системы субъекта КИИ

2.1 Уязвимости базовых элементов информационной системы

Для проведения анализа влияния рисков ИБ был применён подход, рассматривающий трёхуровневую иерархическую структуру отношений базовых составляющих информационной системы (ИС) [1].

Иерархическая структура отношений базовых активов ИС представлена иерархическим графом на рис. 1, где агрегат активов представлен в виде A_{12345} и включает взаимодействия между элементами A_1, A_2, A_3 (программное обеспечение BIOS A_1, загрузчики BIOS A_2, главные атрибуты (ключи) загрузчиков A_3), и элементами A_4, A_5 (загрузочные записи операционной системы A_4, системные и пользовательские данные A_5), связанными через их агрегаты – NVRAM-микросхему A_{123} и жёсткий диск A_{45}.

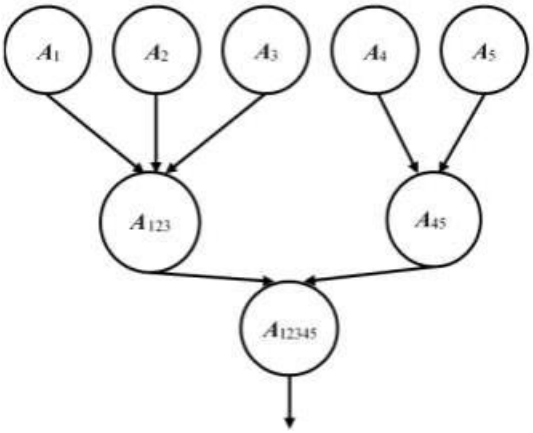

Рис. 1. Граф иерархических уровней связей составляющих ИС
Fig.1. Graph of hierarchical levels of connections of the components of the IC

2.1.1 Угрозы составляющим ИС. Возможность выбора угрозы методом экспертных оценок

Ниже приведены защитные меры от основных угроз (табл.1) согласно базе данных ФСТЭК России[9]:

Kaspersky Industrial CyberSecurity (KICS),

KICS for Nodes, KICS for Networks, Kaspersky Security Center.

KICS for Nodes.

KICS for Networks.

Kaspersky Security Center.

Для определения наиболее вероятных угроз в отношении элементов АСУ ТП среди сотрудников IT-отдела целесообразно провести экспертный опрос на предмет выявления наиболее уязвимого элемента, приоритетного для АНВ.

[9]Банк данных угроз безопасности информации [Информационный ресурс ФСТЭК].URL: https://bdu.fstec.ru/ (дата обращения: 22.04.2022).

Таблица 1. Основные угрозы составляющим ИС

Наименование угрозы
УБИ.004: Угроза аппаратного сброса пароля BIOS (Модификация авторизационной информации).
УБИ.005: Угроза внедрения вредоносного кода в BIOS.
УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS
УБИ.018: Угроза загрузки нештатной операционной системы
УБИ.032: Угроза использования поддельных цифровых подписей BIOS.
УБИ.057: Угроза неконтролируемого копирования данных внутри хранилища больших данных.
УБИ.060: Угроза неконтролируемого уничтожения информации хранилищем больших данных.
УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией.
УБИ.088: Угроза несанкционированного копирования защищаемой информации.
УБИ.091: Угроза несанкционированного удаления защищаемой информации.
УБИ.144: Угроза программного сброса пароля BIOS
УБИ.154: Угроза установки уязвимых версий обновления программного обеспечения BIOS.

В качестве примера приведена табл. 2 с результатами опроса семи специалистов/экспертов, которые в качестве наиболее вероятной стратегии воздействия на АСУ ТП, с целью дестабилизации производственного процесса, выделили угрозы, которые окажут воздействие на базу данных параметров потока энергоносителя.

Таблица 2. Результаты экспертного опроса по выделению угрозы в отношении АСУ ТП

эксперт / угроза	1	2	3	4	5	6	7	Совокупная оценка
УБИ.004	5	1	3	6	4	10	2	4,43
УБИ.005	4	9	5	6	7	8	7	6,57
УБИ.009	4	5	6	7	16	8	7	7,57
УБИ.018	3	10	7	3	5	4	6	5,43
УБИ.032	1	9	8	7	6	10	5	6,57
УБИ.057	18	16	11	10	15	13	14	13,86
УБИ.060	12	9	11	9	4	7	9	8,71
УБИ.067	15	9	12	15	10	10	17	12,57
УБИ.088	14	10	10	11	20	13	15	13,29
УБИ.091	12	8	11	11	3	9	1	7,86
УБИ.144	6	6	10	8	4	7	10	7,29
УБИ.154	6	8	6	7	6	11	7	7,29

Данный выбор был обусловлен предоставленной информацией о наличии уязвимого элемента в производственном процессе, а именно, клапаном на подводящем трубопроводе.

По результатам опроса, в данном конкретном случае, эксперты выделили угрозы УБИ.057, УБИ.067, УБИ.088, поскольку соответствующие средние значения экспертных оценок существенно выше остальных.

На следующем этапе целесообразно для каждой угрозы определить приоритетное значение. Для этой цели рассматриваются возможные критерии, по которым определяются последствия для ИС и в целом объекта в случае реализации той или иной угрозы: УБИ.057, УБИ.067, УБИ.088. Выбор критериев обуславливается размером потенциальных рисков, анализ и оценка которых осуществляется специалистами, эксплуатирующими непосредственно АСУ ТП, производственно-технологические процессы и установки, представителями «Ростехнадзора» и МЧС. Основную угрозу определяем методами «Сокращенного анализа иерархий», «Полного анализа иерархий», «Смещенного идеала» с помощью программного комплекса [16]. Значения показателей критериев имеют разные единицы измерений, поэтому в каждом методе применяют формулы нормирования:

для метода «Полного анализа иерархий» –

$$S_i = \sum_i^j (B_{Sj} \cdot K_{ij}) \tag{3}$$

для метода «Сокращенного анализа иерархий» –

$$K_{ij} = \frac{K_{исх.ij}}{K_{сум.j}} \tag{4}$$

для метода «Смещенного идеала» –

$$d_j^i = \frac{k_j^i - k_j^-}{k_j^+ - k_j^-} \qquad L_i^p = \left[\sum_{j=1}^{m} (V_j d_j^i)^p\right]^{1/p}, \tag{5}$$

где $K_{исх,ij}$ – текущее нормированное значение показателя j-го критерия для i-ой угрозы,

$K_{сум,j}$ – сумма нормированных значений показателей i,

B_{sj} – показатель «важности» i-ой угрозы по отношению к j-му критерию,

S_i – сумма нормированных значений показателей j- того критерия по i-ой угрозе с учетом важности угрозы по отношению к критерию,

k^+ – максимальное нормированное значение по j-му критерию,

k^- – минимальное нормированное значение по j-му критерию.

Экспертные оценки формируются экспертами с учетом структуры АСУ ТП (рис. 2), поскольку уязвимость ресурсов и активов зависит от нижнего, среднего или верхнего уровня АСУ ТП.

Исследуя возможности воздействии на АСУ ТП объекта, в качестве потенциального нарушителя рассматривают начальника установки, который действует совместно с представителем соответствующей службы.

Динамика активности угроз зависит от субъекта, участвующего в технологическом информационном процессе, а время начала реализации угрозы ($t0$) может быть спрогнозировано.

Варианты атак на информационную систему предприятия, угрозы и защита от них представлены в табл. 3.

Рис. 2. Уровни АСУ ТП
Fig. 2. Automated control system levels

Таблица 3. Варианты атак, угроз и защитных мероприятий в АСУ ТП

Атаки	Угрозы	Защита
Внедрение вредоносного программного обеспечения	Получение доступа к системе АСУ ТП третьими лицами Нарушение в работе АСУ ТП	Антивирусная защита Управление доступом Идентификация и аутентификация
Компьютерная атака типа «отказ в обслуживании» (DoS, DDoS)	Полный отказ в обслуживании системы	Предотвращение вторжений Управление обновлениями программного обеспечения
Непреднамеренное отключение системы (без злого умысла)	Порча оборудования, удаление, искажение файлов с важной информацией или программ	Информирование и обучение персонала Обеспечение действий в нештатных ситуациях

Схема реагирования на события информационной безопасности представлена на рис. 3.

2.1.2 Построение модели значимости угроз

Меры реализации и меры уязвимости ***конфиденциальности***, ***целостности*** и ***доступности*** составляющих [17] (или активов A) ИС выстраиваются согласно представленной выше моделей оценки весов угроз (формулы 2–5) и схеме реагирования на события ИБ (рис. 3):

– $\mu_c(T|A_n)$ и $\mu_c(V|A_n)$ – мера (степень) реализации угрозы безопасности (security threat) и мера (степень) уязвимости (vulnerability) ***конфиденциальности*** актива A_n соответственно;

– $\mu_i(T|A_n)$ и $\mu_i(V|A_n)$ – мера (степень) реализации угрозы безопасности и мера (степень) уязвимости ***целостности*** актива A_n соответственно;

– $\mu_a(T|A_n)$ и $\mu_a(V|A_n)$ – мера (степень) реализации угрозы безопасности и мера (степень) уязвимости ***доступности*** актива A_n соответственно.

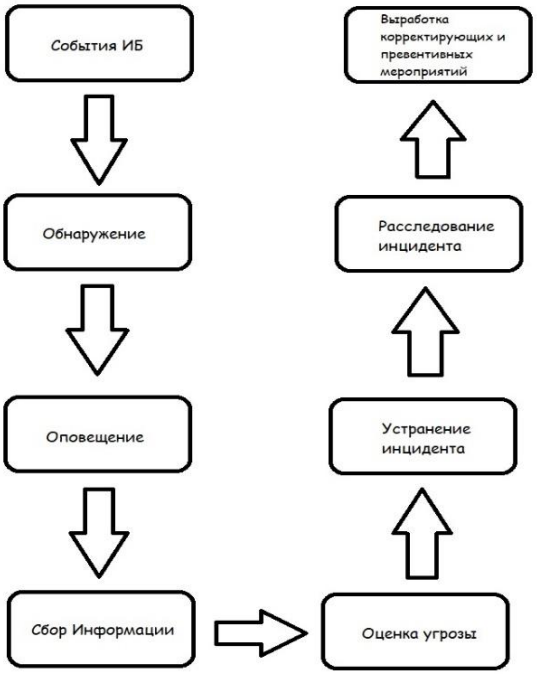

Рис. 3. Схема реагирования на события ИБ
Fig. 3. Response to information security events scheme

Значения всех мер μ задаются в интервале (0÷1). Зададим меры рисков (risk) конфиденциальности, целостности и доступности актива A_n (n = 1, 2, …, N) в виде нечеткого «И»:

$$\mu_c(R|A_n) = k_c(A_n)\ \mu_c(T|A_n)\ \mu_c(V|A_n);$$

$$\mu_i(R|A_n) = k_i(A_n)\ \mu i(T|A_n)\ \mu i(V|A_n);$$

$$\mu_a(R|A_n) = k_a(A_n)\ \mu_a(T|A_n)\ \mu_a(V|A_n); \quad (6)$$

$$k_c(A_n) = K_c(A_n)/[K_c(A_n) + K_i(A_n) + K_a(A_n)];$$

$$k_i(A_n) = K_i(A_n)\ /[K_c(A_n) + K_i(A_n) + K_a(A_n)];$$

$$k_a(A_n) = K_a(A_n)/[K_c(A_n) + K_i(A_n) + K_a(A_n)],$$

где $K_c(A_n)$, $K_i(A_n)$ и $K_a(A_n)$ – ненормированные степени значимости угроз конфиденциальности, целостности и доступности, а угрозы безопасности и уязвимости являются независимыми [1].

Вместо усредненного значения риска Rср(An) для каждого актива An (n = 1, 2, …, N) было рассчитано значение технического риска по выражению

$$Rcia(An) = Rc(An) + Ri(An) + Ra(An) - Rc(An) * Ri(An) - Rc(An) * Ra(An) - Ri(An) * Ra(An) + Rc(An) * Ri(An) * Ra(An). \quad (7)$$

Проведены расчёты по представленным формулам при ненормированных степенях значимости, представленных в 5-балльной системе (табл. 4).

Таблица 4. Значения мер для активов ИС

Номер актива	Актив 1	Актив 2	Актив 3	Актив 4	Актив 5
$K_c(A_n)$	1	3	3	4	5
$K_i(A_n)$	3	3	1	3	4
$K_a(A_n)$	4	2	4	2	1
$\mu_c(T/A_n)$	0,20	0,60	0,60	0,80	1
$\mu_i(T/A_n)$	0,60	0,60	0,20	0,60	0,80
$\mu_a(T/A_n)$	0,80	0,40	0,80	0,40	0,20
$\mu_c(V/A_n)$	0,80	0,40	0,40	0,20	1
$\mu_i(V/A_n)$	0,40	0,40	0,80	0,40	0,20
$\mu_a(V/A_n)$	0,20	0,60	0,20	0,60	0,80
$k_c(A_n)$	0,13	0,38	0,38	0,44	0,50
$k_i(A_n)$	0,38	0,38	0,13	0,33	0,40
$k_a(A_n)$	0,50	0,25	0,5	0,22	0,10
$\mu_c(R/A_n)$	0,02	0,09	0,09	0,07	0,50
$\mu_i(R/A_n)$	0,09	0,09	0,02	0,08	0,06
$\mu_a(R/A_n)$	0,08	0,06	0,08	0,05	0,02

2.2 Устойчивость компонентов информационной системы

2.2.1 Устойчивости элементарных компонентов информационной системы

Устойчивость/надежность элементарных компонентов или активов ИС к потере их конфиденциальности (c), целостности (i) и доступности (a) рассчитывалась при условии зависимости рисков друг от друга [1], причём расчёт значения риска для каждого актива применялся с использованием рекурсии:

$$\mu_{ci}(R|A_n) = \mu_c(R|A_n) + \mu_i(R|A_n) - \mu_c(R|A_n)\,\mu_i(R|A_n); \quad (8)$$
$$\mu_{cia}(R|A_n) = \mu_{ci}(R|A_n) + \mu_a(R|A_n) - \mu_{ci}(R|A_n)\,\mu_a(R|A_n).$$

Тогда из (5) получим выражение для расчета совокупной меры риска для каждого актива A_n:

$$\mu_{cia}(R|A_n) = \mu_c(A_n) + \mu_i(A_n) + \mu_a(A_n) - \mu_c(A_n)\,\mu_i(A_n) - \mu_c(A_n)\,\mu_a(A_n) - \mu_i(A_n)\,\mu_a(A_n) + \mu_c(A_n)\,\mu_i(A_n)\,\mu_a(A_n). \quad (9)$$

Устойчивости отдельных активов рассчитывались, как в [13]:

$$s_{cia}(A_n) = 1 - \mu_{cia}(R|A_n). \quad (10)$$

Согласно (10), получается набор совокупных мер риска активов приведенный в табл. 5.

Таблица 5. Устойчивость компонентов ИС к угрозам ИБ

№A	A_1	A_2	A_3	A_4	A_5
$\mu_{cia}(An)$	0,18	0,22	0,18	0,19	0,54
$s_{cia}(A_n)$	0,82	0,78	0,82	0,81	0,46

2.2.2 Устойчивости агрегатов активов

Рассмотрим степени s устойчивости агрегатов ИС к угрозам на основе иерархических уровней их взаимодействия с помощью графа, представленного на рис. 4.

В работе [1] приведены различные методы оценки степеней устойчивости к угрозам агрегатов, которые применимы ко всем иерархическим уровням графа ИС.

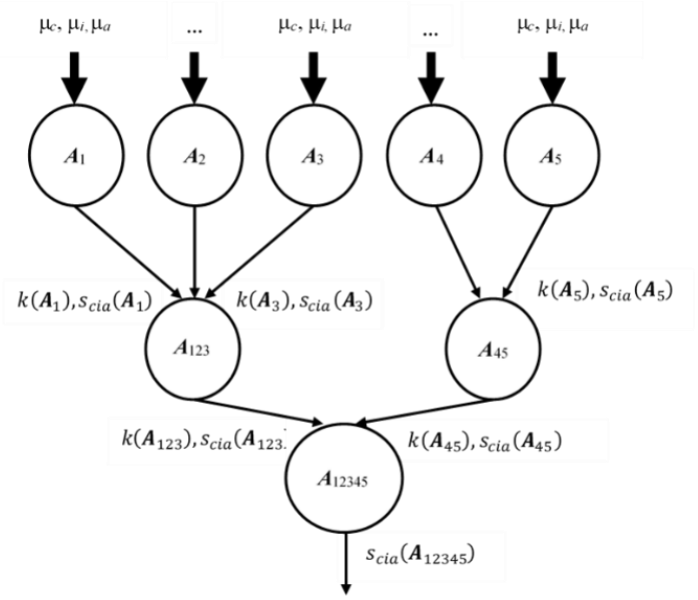

Рис. 4. Граф расчёта устойчивости агрегатов ИС
Fig. 4. Graph for calculating the stability of IC aggregates

Для расчёта по аналогии с (6) будем использовать нормированные коэффициенты $k(A_n) = K(A_n)/\sum K(A_n)$ значимостей активов, где $K(A_n)$ – ненормированные коэффициенты их значимостей, а $n = 1, 2, \ldots, N$.

Рассмотрим устойчивость агрегатов при сильной зависимости компонентов. В связи с тем, что подсистема загрузки персонального компьютера является последовательной, успешность загрузки операционной системы в значительной мере зависит от состояния защищённости и функционирования BIOS материнской платы компьютера, а также состояния защищённости и функционирования жёсткого диска. Тем самым зависимость между данными компонентами будет сильной.

На формальном уровне сильное взаимодействие активов обусловлено их полной взаимозависимостью [1]. Определим степень устойчивости агрегатов при сильном взаимодействии их парных элементов, как:

$$s_{cia}(A_{12}) = \frac{k(A_1)k(A_2)s_{cia}(A_1)s_{cia}(A_2)}{k(A_1)+ k(A_2) - k(A_1)(A_2)}. \quad (11)$$

Тогда для агрегата A_{123} получим:

$$scia(A_{123}) = \frac{k(A_1)k(A_2)s_{cia}(A_1)s_{cia}(A_2)+ k(A_1)k(A_3)s_{cia}(A_1)s_{cia}(A_3)+ k(A_2)k(A_3)s_{cia}(A_2)s_{cia}(A_3)}{1- k(A_1)k(A_2)- k(A_1)k(A_3)-k(A_2)k(A_3)+ 2\,k(A_1)k(A_2)k(A_3)} - \frac{2\,k(A_1)k(A_2)k(A_3)s_{cia}(A_1)s_{cia}(A_2)s_{cia}(A_3)}{1- k(A_1)k(A_2)- k(A_1)k(A_3)-k(A_2)k(A_3)+ 2\,k(A_1)k(A_2)k(A_3)}. \quad (12)$$

Так, при $k(A_1) = k(A_2) = k(A_3)$ и $s_{cia}(A_1) = s_{cia}(A_2) = s_{cia}(A_3) = 1$, получим $s_{cia}(A_{123}) \cong 1$. При $s_{cia}\,(A_1) = 0$, $s_{cia}(A_2) = s_{cia}(A_3) = 1$ получим $s_{cia}\,(A_{123}) \cong 0.02$. Тем самым, выход из строя одного актива приводит к потере устойчивости агрегата.

Похожим образом обстоит ситуация и с агрегатом A_{45}. Степень его устойчивости определяется аналогично (8):

$$s_{cia}(A_{45}) = \frac{k(A_4)k(A_5)s_{cia}(A_4)s_{cia}(A_5)}{k(A_4)+k(A_5)-k(A_4)k(A_5)}. \quad (13)$$

Так, при $k(A_4) = k(A_5)$ и $s_{cia}(A_4) = s_{cia}(A_5) = 1$, получим $s_{cia}(A_{45}) = 1$. При $s_{cia}(A_4) = 0$, $s_{cia}(A_5) = 1$, получим $s_{cia}(A_{45}) = 0$.

В связи с этим, можно утверждать, что выход из строя одного актива приводит к потере устойчивости агрегата, а выход из строя одного из агрегатов также приведёт к потере устойчивости всей системы в целом.

Так, действительно, при нарушении процедуры запуска операционной системы, по различным причинам, конечное состояние информационной системы будет зависеть от успешности разрешения возникших проблем от реализации угроз, направленных на нарушение работоспособности элемента информационной системы. Например, нарушение работоспособности терминала оператора, закреплённого за определённым элементом производственного процесса предприятия, или же сервера производственной сети, могут привести к различным результатам в зависимости от степени тяжести последствий атаки на конкретный элемент.

3. Обсуждение результатов

Из приведенного исследования следует, что наиболее подвержены риску взаимозависимые активы ИС, у которых потеря устойчивости одного из них приводит к потере устойчивости всех подсистем или агрегатов, состоящих их этих активов. Поэтому необходимо дублирование таких подсистем. В действительности, существующие меры по резервному копированию данных, в том числе, создание RAID-массивов, является прямым следствием применения таких мер. В последнее время и потребительские платформы стали оснащать дублируемыми микросхемами BIOS, с помощью которых можно восстановить исходный образ и настройки BIOS.

Персональный компьютер является довольно уязвимым элементом информационной среды, особенно, если у нарушителя есть непосредственный доступ к нему. Самые простые пути воздействия на ИС, при которых будет утрачена работоспособность ИС, включают воздействие на жёсткий диск, но защита программного обеспечения BIOS материнской платы позволяет ограничить доступ к жёсткому диску и его составляющим компонентам, а при отсутствии защиты энергонезависимого сегмента памяти и его главных функционирующих компонентов у злоумышленника будут открыты наиболее простые пути исполнения угроз по направлению к информационной системе в целом.

Поэтому важно всестороннее обеспечение защиты в соответствии со следующими рекомендациями, которые могут стать соответствующими положениями в политике информационной безопасности [18]:

– при работе с конфиденциальными данными шифровать жёсткие диски; это позволяет ограничить конечное время совершения атаки на ИС при допустимом времени реагирования на инциденты;

– для защиты содержимого жёстких дисков отключать дополнительные возможности по загрузке нештатных операционных систем и создать пароль BIOS для предотвращения изменения параметров состояния ПО микросхемы;

– при наличии возможности использовать собственноручно написанные сертификаты безопасности, встраиваемыми в энергонезависимую память BIOS, что

позволяет загружать только разрешённые системы и загрузчики, что позволит, в конечном счёте, оградиться от реализации угроз, направленных на ИС;

– проводить резервное копирование важных данных, а также дублировать элементы информационной системы с наиболее интенсивными потоками обмена информацией с другими элементами, от работоспособности которых зависит работа всей системы в целом.

Заключение

В настоящей статье предлагается оценивать уязвимость производственно-технологического процесса и обнаруживать уязвимые элементы обслуживаемых данные процессы информационных систем посредством анализа совокупности значений показателей критериев в границах требований Законодательства126.

Впервые для определения критических сегментов в объекте КИИ, в т.ч. для определения уязвимости базовых элементов АСУ ТП для обеспечения устойчивости объектов КИИ, в качестве критериев предлагается рассматривать меры уязвимости агрегатов, конфиденциальность, доступность, целостность.

Предложенная система оценки безопасности на опасных производственных объектах, при интеграции усилий специалистов-технологов и IT-специалистов по ее совершенствованию, позволит расширить возможности программного обеспечения, обеспечить устойчивость отдельных элементов АСУ ТП и усилить меры по обеспечению комплексной безопасности ОПО в целом.

СПИСОК ЛИТЕРАТУРЫ:

1. Краснов Андрей Е., Мосолов Александр С., Феоктистова Наталия А. Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности. Безопасность информационных технологий, [S.l.], т. 28, № 1, с. 106–120, 2021. ISSN 2074-7136. DOI: https://doi.org/10.26583/bit.2021.1.09. – EDN JMVYBG.
2. Глава 3. Информационно-экономическая безопасность как специфический элемент системы безопасности постиндустриального общества. 2016, с. 96–170. URL: https://www.elibrary.ru/item.asp?id=28962874 (дата обращения: 22.04.2022 г.) – EDN YJUQWX.
3. Губина Т.А., Мосолов А.С., Акинин Н.И. Алгоритм метода определения приоритетного сценария развития аварийной ситуации на объекте защиты. М.: Кокс и химия, 2019, № 6, с. 41–49. URL: https://www.elibrary.ru/item.asp?id=38220548 (дата обращения: 22.04.2022) – EDN EEOQRG.
4. Ковальский Ф.С., Мосолов А.С., Акинин Н.И. Анализ применения методов смещенного идеала и анализа иерархий при категорировании объекта топливно-энергетического комплекса. РХТУ им. Д.И. Менделеева. 2021, № 3, с. 15–20. URL: https://elibrary.ru/item.asp?id=45165274 (дата обращения: 22.04.2022). DOI: http://dx.doi.org/10.24000/0409-2961-2021-3-15-20 – EDN UFCAWP.
5. Захаров А.А., Римша А.С., Харченко А.М., Зулькарнеев И.Р. Анализ информационной безопасности автоматизированных систем управления техническими процессами газодобывающего предприятия. 2017, № 3(25), с. 24–33. URL: https://www.elibrary.ru/item.asp?id=30770417 (дата обращения: 22.04.2022) – EDN ZXJBRT.
6. Трещев И.А., Вильдяйкин Г.Ф., Ядыменко К.А. О подходе к анализу защищенности корпоративных информационных систем. ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет». 2014, № 3, с. 41. URL: https://www.elibrary.ru/item.asp?id=23580615 (дата обращения: 22.04.2022) – EDN TWAJRH.
7. Чиликиди А.Г. «АСА ИБ». Свидетельство о государственной регистрации программы для ЭВМ RU 2020619745. Дата публикации 24.08.2020, бюл. № 9. URL: https://www1.fips.ru/ofpstorage/Doc/PrEVM/RUNWPR/000/002/020/619/745/2020619745-00001/document.pdf (дата обращения: 22.04.2022).
8. Чиликиди А.Г. «ГРИФОН». Свидетельство о государственной регистрации программы для ЭВМ RU 2021614176. Дата публикации 19.03.2021, бюл. № 3. URL: https://www1.fips.ru/ofpstorage/Doc/PrEVM/RUNWPR/000/002/021/614/176/2021614176-00001/document.pdf (дата обращения: 22.04.2022).

9. Ганченко П.В., Ибадулаев Д.В., Космичев В.П., Лузанов В.Ф., Обломский С.Б., Степанов И.В. Система прогнозирования и оценки безопасности опасного производственного объекта с использованием комплексной модели обеспечения безопасности. URL: https://elibrary.ru/item.asp?id=37814786 (дата обращения: 22.04.2022) – EDN IIPOID.
10. Дроботун Е.Б. Синтез систем защиты автоматизированных систем управления от разрушающих программных воздействий. Военная академия воздушно-космической обороны им. Маршала Советского Союза Г.К. Жукова. 2016, № 3, с. 51–59. URL: https://elibrary.ru/item.asp?id=27537411 (дата обращения: 22.04.2022) – EDN XEPQDX.
11. Соловьев С.В., Язов Ю.К. Информационное обеспечение деятельности по технической защите информации. Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю России, г. Воронеж, Россия. 2021, № 1 (41), с. 69–79. DOI: http://dx.doi.org/10.21681/2311-3456-2021-1-69-79.
12. Региональная информатика и информационная безопасность. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. Том. Выпуск 2. 2016. – 491 с. URL: https://elibrary.ru/item.asp?id=27552889 (дата обращения: 22.04.2022) – EDN XEYLCZ.
13. Губина Т.А., Мосолов А.С., Мосолов А.А. Система оценки безопасности опасного производственного объекта. RU №2709155 C1 от 02.04.2019. Опубликован 16.12.2019. Бюл. №35. МПК G06Q 10/06.
14. Тютин А.В. Организационно-методический аспект совершенствования подсистемы информационной безопасности объектов промышленного комплекса региона: автореф. дис. ... канд. экон. наук: 08.00.05. Иван. гос. ун-т. – Иваново, 2004. – 23 с. URL: https://viewer.rsl.ru/ru/rsl01002665244?page=16&rotate=0&theme=white (дата обращения: 22.04.2022).
15. Метод обработки экспертных оценок для оценки уязвимости производственно-технологического процесса, определяем основную угрозу. Свидетельство о государственной регистрации программы для ЭВМ RU 2021663111. Дата публикации 11.08.2021, бюл. № 9.
16. Кирсанов С.В. Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли. Доклады ТУСУР. 2013, № 2 (28), с. 112–115. URL: https://cyberleninka.ru/article/n/metod-otsenki-ugroz-informatsionnoy-bezopasnosti-asu-tp-gazovoy-otrasli (дата обращения: 22.04.2022).
17. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции. Вопросы кибербезопасности. 2014, № 1(2). URL: https://cyberleninka.ru/article/n/menedzhment-informatsionnoy-bezopasnosti-osnovnye-kontseptsii (дата обращения: 22.04.2022).

REFERENCES:

[1] Krasnov Andrey E., Mosolov Alexander S., Feoktistova Nataliya A. Assessing the resilience of critical information infrastructures to information security threats. IT Security (Russia), [S.l.], vol. 28, no. 1, p. 106–120, 2021. ISSN 2074-7136. DOI: https://doi.org/10.26583/bit.2021.1.09. – EDN JMVYBG (in Russian).
[2] Chapter 3. Information and economic security as a specific element of the security system of post-industrial society. 2016, p. 96–170. URL: https://www.elibrary.ru/item.asp?id=28962874 (accessed: 22.04.2022) – EDN YJUQWX (in Russian).
[3] Gubina T.A., Mosolov A.S., Akinin N.I. Algorithm of the method for determining the priority scenario of the development of an emergency situation at the protection facility. 2019, no. 6, p. 41–49. URL: https://www.elibrary.ru/item.asp?id=38220548 (accessed: 22.04.2022) – EDN EEOQRG (in Russian).
[4] Kovalsky F.S., Mosolov A.S., Akinin N.I. Analysis of the application of methods of displaced ideal and hierarchy analysis in the categorization of the fuel and energy complex object. D.I. Mendeleev Russian Technical University. 2021, no. 3, p. 15–20. URL: https://elibrary.ru/item.asp?id=45165274 (accessed: 22.04.2022). DOI: http://dx.doi.org/10.24000/0409-2961-2021-3-15-20. – EDN UFCAWP (in Russian).
[5] Zakharov A.A., Rimsha A.S., Kharchenko A.M., Zulkarneev I.R. Analysis of information security of automated control systems for technical processes of a gas producing enterprise. 2017, no. 3(25), p. 24–33. URL: https://www.elibrary.ru/item.asp?id=30770417 (accessed: 22.04.2022) – EDN ZXJBRT (in Russian).
[6] Трещев И.А., Вильдяйкин Г.Ф., Ядыменко К.А. О подходе к анализу защищенности корпоративных информационных систем. ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет». 2014, № 3, с. 41. URL: https://www.elibrary.ru/item.asp?id=23580615 (дата обращения: 22.04.2022) – EDN TWAJRH (in Russian).
[7] Chilikidi A.G. ASA IB. Certificate of state registration of a computer program. RU 2020619745. URL: https://www.elibrary.ru/item.asp?id=43965451 (accessed: 22.04.2022) (in Russian).
[8] Chilikidi A.G. GRIFON. Certificate of state registration of a computer program. RU 2021614176. URL: https://www.elibrary.ru/item.asp?id=45820045 (accessed: 22.04.2022) (in Russian).

[9] Ganchenko P.V., Ibadulaev D.V., Kosmichev V.P., Luzanov V.F., Oblomsky S.B., Stepanov I.V. The system of forecasting and assessing the safety of a hazardous production facility using an integrated safety model. URL: https://elibrary.ru/item.asp?id=37814786 (accessed: 22.04.2022) – EDN IIPOID (in Russian).

[10] Drobotun E.B. Synthesis of protection systems for automated control systems from destructive software influences. Military Academy of Aerospace Defense named after Marshal of the Soviet Union G.K. Zhukov. 2016, no. 3, p. 51–59. URL: https://elibrary.ru/item.asp?id=27537411 (accessed: 22.04.2022) – EDN XEPQDX (in Russian).

[11] Solovyov S.V., Yazov Y. K. Information support of activities on technical protection of information. State Research Testing Institute of Problems of Technical Protection of Information of the Federal Service for Technical and Export Control of Russia, Voronezh, Russia. 2021, no. 1 (41), p. 69–79. DOI: http://dx.doi.org/10.21681/2311-3456-2021-1-69-79 (in Russian).

[12] Regional informatics and information security. St. Petersburg Society of Informatics, Computer Technology, communication and Control Systems. Tom. Issue 2. 2016. – 491 p. URL: https://elibrary.ru/item.asp?id=27552889 (accessed: 22.04.2022) – EDN XEYLCZ (in Russian).

[13] Gubina T.A., Mosolov A.S., Mosolov A.A. Sistema otsenki besopastnosti opasnogo proisvodstvennogo ob''ekta [Safety assessment system for a hazardous production facility]. Patent RU 2709155 C1, 02.04.2019 (in Russian).

[14] Tyutin A.V. Organizational and methodological aspect of improving the subsystem of information security of objects of the industrial complex of the region: abstract. dis. ... Candidate of Economic Sciences: 08.00.05. Ivan. state. un-t. – Ivanovo, 2004. – 23 p. URL: https://viewer.rsl.ru/ru/rsl01002665244?page=16&rotate=0&theme=white (accessed: 22.04.2022) (in Russian).

[15] Method for processing expert assessments for assessing the vulnerability of the production and technological process, vulnerability assessment. Certificate of state registration of the computer program RU 2021663111, dated August 11, 2021 (in Russian).

[16] Kirsanov S.V. Method of assessing threats to information security of automated control systems of the gas industry. TUSUR reports. 2013, no. 2 (28), p. 112–115. URL: https://cyberleninka.ru/article/n/metod-otsenki-ugroz-informatsionnoy-bezopasnosti-asu-tp-gazovoy-otrasli (accessed: 22.04.2022) (in Russian).

[17] Dorofeev A.V., Markov A.S. Information security management: basic concepts. Issues of cybersecurity. 2014, no. 1(2). URL: https://cyberleninka.ru/article/n/menedzhment-informatsionnoy-bezopasnosti-osnovnye-kontseptsii (accessed: 22.04.2022) (in Russian).

Поступила в редакцию – 26 апреля 2022 г. Окончательный вариант – 28 августа 2022 г.
Received – April 26, 2022. The final version – August 28, 2022.