ПРЕДМЕТНО-СМЫСЛОВЫЕ ОГРАНИЧЕНИЯ ПРИ МОДЕЛИРОВАНИИ КОМПЬЮТЕРНОГО ПРОТИВОБОРСТВА

Яковлев А.В.[1], Пеливан М.А.[2]

Ключевые слова: *критическая информационная инфраструктура, предметная область, сфера энергетики, социальная значимость, экономическая значимость, автоматизированная система управления, информационная безопасность, категория значимости, критерий значимости объекта.*

Аннотация

Цель работы: повышение достоверности моделей компьютерного противоборства на значимых объектах критической информационной инфраструктуры за счет применения результатов онтологического анализа предметной области и формирования границ применимости моделей с учетом нормативных правовых актов Российской Федерации.

Методы исследования: системный анализ, формально-логический анализ, формально-юридический метод.

Результаты: уточнены понятия субъекта и объекта критической информационной инфраструктуры; проанализированы понятийный аппарат и требования российского законодательства в сфере обеспечения информационной безопасности на значимых объектах критической информационной инфраструктуры и на их основе сформированы предметно-смысловые ограничения для построения адекватных моделей компьютерного противоборства; установлены ограничения по субъектам критической информационной инфраструктуры на основе следующих параметров: сфера деятельности, обеспечиваемые технологические процессы, а по объектам критической информационной инфраструктуры — на основе следующих параметров: виды объектов, обеспечиваемые критические процессы, осуществляемая работа с критическими процессами, вид значимости, показатели критериев значимости, категория значимости.

DOI: 10.24682/1994-1404-2024-3-86-95

Введение

Современные мировые геополитические события обусловливают постоянное увеличение, как количества, так и сложности компьютерных атак на информационную инфраструктуру Российской Федерации. Особое внимание с атакующей стороны уделяется *критической информационной инфраструктуре* (КИИ) как совокупности наиболее критичных объектов, нарушение работы которых может привести к существенным нарушениям в политической (PZ_{PLT}), экономической (PZ_{EKN}) и социальной (PZ_{SOC}) сферах государства, экологическим (PZ_{EKL}) авариям, снижению обороноспособности государства и возможности поддержания правопорядка (PZ_{OBR})[3]. Еще в феврале 2022 г. национальный координационный центр по компьютерным инцидентам выдвинул *гипотезу* о целенаправленном увеличении интенсивности компьютерных атак и обратил внимание на необходимость усиления бдительности при мониторинге вредоносной активности[4]. В соответствии с отчетом компании «Ростелеком-Солар» об атаках на российские компании, в третьем квартале 2023 г. выявлено 396 тыс. инцидентов информационной безопасности, что на 85% больше, чем в третьем квартале 2022 г.[5]

[3] Кибербезопасность в 2023—2024 гг.: тренды и прогнозы. Часть третья. URL: https://www.ptsecurity.com/u-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-tretya; Кибербезопасность в 2023—2024 гг.: тренды и прогнозы. Часть четвертая. URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-chetvertaya

[4] Угроза кибератак на российские информационные ресурсы. URL: https://safe-surf.ru/upload/ALRT/ALRT-20220224.1.pdf

[5] Атаки на российские компании в III квартале 2023 года. URL: https://rt-solar.ru/upload/iblock/715/7eiytusnagpc9c9153n40h77alipvuw/Otchet-III-kvartal.pdf

[1] ***Яковлев Алексей Вячеславович,*** *кандидат технических наук, доцент, доцент кафедры информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*

E-mail: yava73@bk.ru

[2] ***Пеливан Михаил Анатольевич,*** *аспирант кафедры информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*

E-mail: witcher89158779996@yandex.ru

На сегодня известно большое количество научных работ по исследованию информационной безопасности КИИ. Данные работы исследуют различные стороны обеспечения информационной безопасности КИИ, к которым относятся исследования особенностей обеспечения безопасности КИИ с Интернетом вещей [4], исследования управления рисками на объектах КИИ [2, 6, 7], особенности проведения аудита информационной безопасности объектов КИИ [8, 9, 20] и др. Вместе с тем отмечается значительное преобладание работ, связанных с разработкой и исследованием моделей объектов КИИ [12, 14, 24], в том числе моделей угроз [5, 17, 18] и нарушителей [19, 21], характерных для объектов КИИ, а также систем обеспечения информационной безопасности на данных объектах [3, 10, 11, 13].

В связи с этим повышается актуальность и практическая значимость исследований, направленных на обеспечение информационной безопасности КИИ, включая синтезирование моделей КИИ и разработку на их основе новых подходов и методов построения *систем защиты информации* [15], учитывающих особенности функционирования объектов КИИ, а также формирование обоснованных предметно-смысловых ограничений при моделировании компьютерного противоборства на значимых объектах КИИ.

Постановка задачи на формирование обоснованных предметно-смысловых ограничений

В работе под *компьютерным противоборством* понимается составная часть отношений и форма борьбы сторон (нарушителя информационной безопасности и системы защиты информации), каждая из которых стремится нанести противнику поражение (ущерб) посредством деструктивных информационных воздействий на его информационную инфраструктуру (в том числе на критически важные объекты информационной инфраструктуры), парируя или снижая негативный эффект от деструктивного воздействия противника.

Моделирование является одним из самых распространенных, эффективных и безопасных методов, позволяющих проводить исследования любых объектов и процессов во всех областях жизни и деятельности человека, в том числе и процессов, связанных с обеспечением информационной безопасности. Однако проведение *качественных* исследований и создание *достоверных* моделей для широкого спектра объектов и процессов не представляется возможным, так как исследуемые (моделируемые) объекты имеют сложную специфичную структуру и содержат большое количество параметров, элементов и связей между ними, число которых может *геометрически* расти при увеличении масштаба объектов исследования (моделирования) и повлечь за собой появление значительного количества ошибок, как при проведении самого моделирования, так и при последующей интерпретации полученных результатов [24].

В свою очередь, объекты КИИ функционируют в разных сферах и предметных областях, имеют различные структурные и функциональные особенности [1, 23] из-за чего построение *обобщённой модели* объектов КИИ приведет к большому количеству приближений и снижению достоверности разработанной модели или же, наоборот, к разработке чересчур сложной модели с большой вероятностью допущения ошибок, высокой сложностью ее структуры и интерпретации результатов. Стоит заметить, что процесс компьютерного противоборства в любых информационных системах, в том числе и на объектах КИИ — это сложный и многопараметрический процесс, для изучения которого требуется создание моделей с высокой степенью достоверности. Для уменьшения ошибок и сложности модели, а также для облегчения интерпретации результатов, сопровождающих построение сложных моделей исследуемых процессов, обеспечивающих высокую степень достоверности, требуется уменьшить *разнородность* моделируемых объектов и процессов.

Введение ограничений на исследуемые объекты и процессы позволяет задать четкие границы применимости методов и результатов исследования, а также обеспечивает повторяемость результатов. Среди всех видов ограничений к основополагающим относятся *предметно-смысловые* ограничения, которые обусловливают тему и направление исследования.

Следовательно, для построения адекватной модели компьютерного противоборства на значимых объектах критической информационной инфраструктуры требуется формирование обоснованных предметно-смысловых ограничений, конкретизирующих направление и объект исследования.

Формирование ограничений по субъектам КИИ

Так как проводимое исследование, связанно с обеспечением информационной безопасности КИИ, то установку ограничений целесообразно начать с владельцев КИИ, т. е. субъектов КИИ. Схема определения ограничений по субъектам КИИ представлена на *рис*. 1.

В соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации»[6] (далее — 187-ФЗ) под субъектами КИИ *понимаются* государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения (S_{ZD}), науки (S_N), транспорта (S_{TP}), связи (S_{SV}), энергетики (S_{EN}), государственной регистрации прав на недвижимое имущество

[6] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс».

Рис. 1. Схема определения ограничений по субъектам КИИ

и сделок с ним (S_{GR}), банковской сфере и иных сферах финансового рынка (S_{BS}), топливно-энергетического комплекса (S_{TEK}), в области атомной энергии (S_{AE}), оборонной (S_{OP}), ракетно-космической (S_{RKP}), горнодобывающей (S_{GP}), металлургической (S_{MP}) и химической промышленности (S_{HP}), российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

В соответствии с определением субъекта КИИ в это понятие входит большое количество организаций, функционирующих в 14-ти крупных сферах деятельности (см. *рис.* 1). Именно сокращение рассматриваемых сфер деятельности позволит значительно сократить объект исследования и повысить достоверность создаваемых в дальнейшем моделей. Из всех сфер деятельности, определенных в 187-ФЗ, выбрана сфера *энергетики*, являющаяся основой для функционирования и развития большинства других сфер и областей деятельности, а также имеющая ключевое значение в жизни и развитии человека[7].

Сфера энергетики разделяется на три технологических процесса (этапа) [22]: генерация (TP_G); транспортировка (TP_T); сбыт (TP_S).

Для дальнейшего исследования выбраны объекты, осуществляющие выполнение технологических этапов транспортировки и сбыта электроэнергии, так как данные объекты наиболее приближены к потребителям и оказывают непосредственное влияние на доступ последних к поставляемой энергии.

Таким образом, дальнейшие исследования направлены на изучение аспектов обеспечения информационной безопасности субъектов КИИ, функционирующих в сфере энергетики и обеспечивающих выполнение технологических этапов транспортировки и сбыта энергии (далее — Субъекты).

Формирование ограничений по объектам КИИ

После определения границ исследования субъектов КИИ необходимо определить границы исследования объектов КИИ, принадлежащих на праве собственности, аренды или на ином законном основании Субъектам.

Объекты КИИ, подлежащие дальнейшему исследованию, должны относиться к категории значимых (Z_Z), в соответствии с 187-ФЗ, так как незначимые (Z_{NZ}) объекты КИИ имеют значительно меньший потенциальный ущерб, а также менее привлекательны для совершения компьютерных атак.

В соответствии с 187-ФЗ под *объектами* КИИ понимаются: информационные системы (ИС, *IS*); информа-

[7] Тупаева А.С. Традиционная энергетика и проблемы развития в современных условиях // Вестник Казанского технолог. ун-та. 2013. Т. 16. № 6. С. 269—271. EDN: PZXGYV.

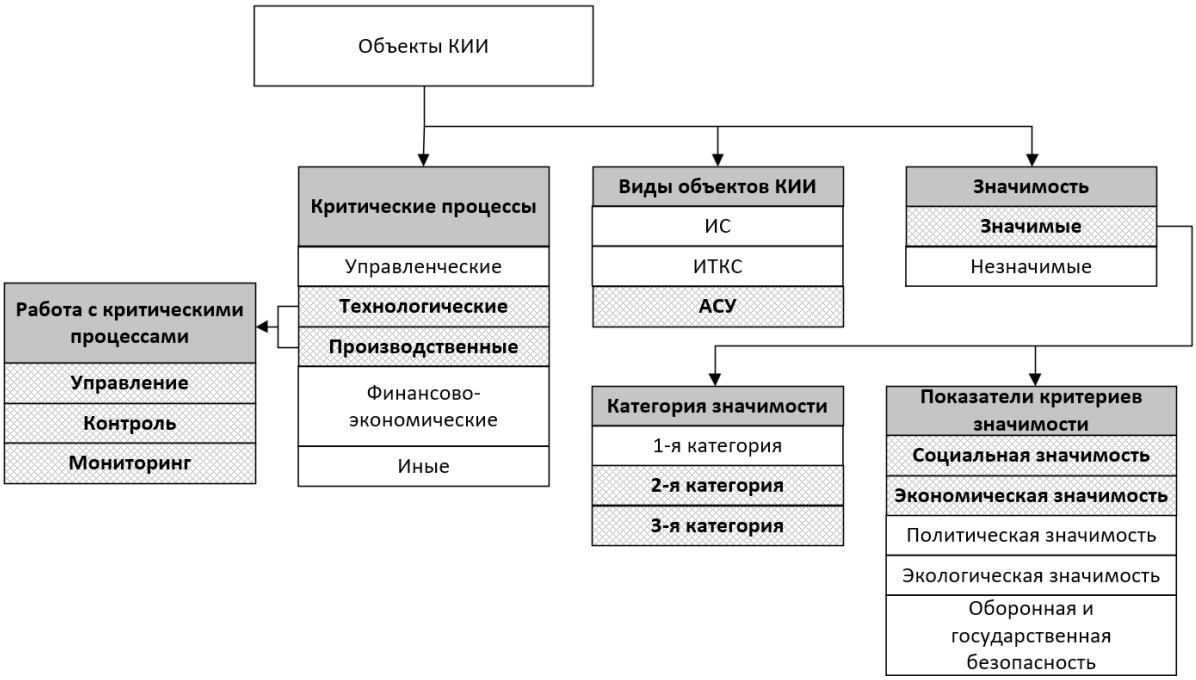

Рис. 2. Схема определения ограничений по объектам КИИ

ционно-телекоммуникационные сети (ИТКС, *ITKS*); автоматизированные системы управления (АСУ, *ASU*).

На основе выбранных Субъектов и анализа Перечня типовых отраслевых объектов КИИ, функционирующих в сфере энергетики[8] определяется перечень объектов КИИ, подлежащих дальнейшему изучению. Анализ Перечня показал, что наибольшее количество объектов, функционирующих в сфере энергетики, относится к автоматизированным системам управления. Кроме того, анализ Перечня позволил выделить из всех критических процессов (управленческие (KP_{UP}), технологические (KP_{TEH}), производственные (KP_{PR}), финансово-экономические (KP_{FE}) и иные (KP_{IN})), процессы, являющиеся актуальными для рассматриваемых объектов, к ним относятся *технологические* и *производственные* процессы, которые обеспечивают управление (P_U), контроль (P_K) и мониторинг (P_M) критических процессов. Схема выбора ограничений по объектам КИИ представлена на *рис.* 2.

На основе анализа функций объектов КИИ энергетики, обеспечиваемых ими критических процессов, а также показателей критериев значимости объектов КИИ, установленных Постановлением Правительства РФ от 8 февраля 2018 г. № 127[9], сделан ***вывод***, что в случае нарушения функционирования объектов КИИ энергетики может быть причинен ущерб жизни и здоровью людей, прекращено или нарушено обеспечение жизнедеятельности населения, кроме того, возможно нанесение ущерба бюджетам Российской Федерации, то есть объекты КИИ энергетики, подлежащие дальнейшему исследованию, обладают социальной и экономической значимостью.

В свою очередь, анализ значений показателей критериев значимости, установленных указанным Постановлением Правительства РФ, для выбранных социальной и экономической «значимостей» позволяет исключить из дальнейшего исследования объекты КИИ, удовлетворяющие первой категории значимости (KZ_1), так как количество объектов, нарушение которых может привести к столь большому ущербу, крайне мало по сравнению с количеством объектов, ущерб которых подпадает под вторую (KZ_2) и третью (KZ_3) категории значимости.

Отсюда дальнейшее исследование направлено на изучение аспектов обеспечения информационной безопасности значимых объектов КИИ, принадлежащих на праве собственности, аренды или на ином законном основании Субъектам, и относящихся к автоматизированным системам управления, обеспечивающим выполнение технологических и производственных процессов по управлению, контролю и мониторингу критических процессов. Кроме того, описанные выше объекты КИИ, должны обладать социальной и экономической значимостью и ущерб от нарушения их функционирования должен соответствовать второй и третьей категориям значимости.

[8] Перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере энергетики. URL: https://minenergo.gov.ru/opendata/7715847529-perechen-obektov-kii-2023

[9] Постановление Правительства РФ от 8 февраля 2018 г. № 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» // СПС «КонсультантПлюс».

Формальное описание введенных ограничений

Концептуальную макромодель компьютерного противоборства на значимых объектах КИИ с учетом изложенного выше можно представить в виде функционала:

$$M_{CP} = f(M_{OB}, M_{UGR}, M_{SZ}), \quad (1)$$

где M_{CP} — модель компьютерного противоборства; M_{OB} — модель значимого объекта КИИ; M_{UGR} — модель угроз для значимого объекта КИИ; M_{SZ} — модель системы защиты значимого объекта КИИ.

Модель значимого объекта КИИ представляется в виде:

$$M_{OB} = f_{OB}(P_S, P_{OB}), \quad (2)$$

где P_S — множество параметров субъекта КИИ; P_{OB} — множество параметров объекта КИИ.

Исходя из описания субъектов КИИ, множество P_S параметров субъекта имеет вид:

$$P_S = \{p_{SF}(p_{TP})\}, \quad (3)$$

где p_{SF} — множество сфер деятельности; p_{TP} — множество технологических процессов.

По результатам проведенного анализа в части определения субъектов КИИ сформированы следующие множества:

– множество сфер деятельности субъектов КИИ, имеющее вид:

$$p_{SF} = \{S_{ZD}, S_N, S_{TP}, S_{SV}, S_{EN}, S_{GR}, S_{BS}, S_{TEK}, S_{AE}, S_{OP}, S_{RKP}, S_{GP}, S_{MP}, S_{HP}\} \quad (4)$$

– множество технологических процессов, выполняемых объектами КИИ:

$$p_{TP} = \{TP_G, TP_T, TP_S\}. \quad (5)$$

Исходя из определенных ограничений по субъектам КИИ, выделены следующие подмножества:

– подмножество актуальных сфер деятельности субъектов КИИ ($p'_{SF} \subset p_{SF}$), подлежащих дальнейшему изучению:

$$p'_{SF} = \{S_{EN}\}; \quad (6)$$

– подмножество актуальных технологических процессов ($p'_{TP} \subset p_{TP}$), подлежащих дальнейшему изучению:

$$p'_{TP} = \{TP_T, TP_S\}. \quad (7)$$

То есть подмножество актуальных параметров субъекта КИИ ($P'_S \subset P_S$), подлежащих дальнейшему изучению, принимает вид:

$$P'_S = \{p'_{SF}(p'_{TP})\}. \quad (8)$$

Исходя из описания объектов КИИ, множество параметров объекта КИИ имеет вид:

$$P_{OB} = \{p_{VOB}, p_{KP}(p_{RKP}), z(p_{PZ}, p_{KZ})\}, \quad (9)$$

где p_{VOB} — множество видов объектов КИИ; p_{KP} — множество критических процессов; p_{RKP} — множество работ с критическими процессами; z — множество «значимостей»; p_{PZ} — множество показателей критериев значимости; p_{KZ} — множество категорий значимости.

По результатам проведенного анализа в части определения объектов КИИ сформированы следующие множества:

– множество видов объектов КИИ

$$p_{VOB} = \{IS, ITKS, ASU\}; \quad (10)$$

– множество критических процессов

$$p_{KP} = \{KP_{UP}, KP_{TEH}, KP_{PR}, KP_{FE}, KP_{IN}\}; \quad (11)$$

– множество работ с критическими процессами

$$p_{RKP} = \{P_U, P_K, P_M\}; \quad (12)$$

– множество «значимостей» объектов КИИ

$$z = \{Z_Z, Z_{NZ}\}; \quad (13)$$

– множество показателей критериев значимости

$$p_{PZ} = \{PZ_{SOC}, PZ_{EKN}, PZ_{PLT}, PZ_{EKL}, PZ_{OBR}\}; \quad (14)$$

множество категорий значимости

$$p_{KZ} = \{KZ_1, KZ_2, KZ_3\}. \quad (15)$$

Исходя из определенных ограничений по объектам КИИ, выделены следующие подмножества, подлежащие дальнейшему изучению:

– подмножество актуальных видов объектов КИИ ($p'_{VOB} \subset p_{VOB}$)

$$p'_{VOB} = \{ASU\}; \quad (16)$$

– подмножество актуальных критических процессов ($p'_{KP} \subset p_{KP}$),

$$p'_{KP} = \{KP_{TEH}, KP_{PR}\}; \quad (17)$$

– подмножество актуальных работ с критическими процессами, совпадающее с множеством работ с критическими процессами

$$p_{RKP} = p'_{RKP} = \{P_U, P_K, P_M\}; \quad (18)$$

– подмножество актуальных значимостей объектов КИИ ($z' \subset z$)

$$z' = \{Z_Z\}; \quad (19)$$

– подмножество актуальных показателей критериев значимости ($p'_{PZ} \subset p_{PZ}$)

$$p'_{PZ} = \{PZ_{SOC}, PZ_{EKN}\}; \quad (20)$$

подмножество актуальных категорий значимости ($p'_{KZ} \subset p_{KZ}$)

$$p'_{KZ} = \{KZ_2, KZ_3\}. \quad (21)$$

Таким образом, подмножество актуальных параметров объекта КИИ ($P'_{OB} \subset P_{OB}$), подлежащих дальнейшему изучению, представляется в виде:

$$P'_{OB} = \{p'_{VOB}, p'_{KP}(p'_{RKP}), z'(p'_{PZ}, p'_{KZ})\}. \quad (22)$$

Исходя из определенных предметно-смысловых ограничений, модель значимого объекта КИИ, подлежащая дальнейшему изучению, имеет вид:

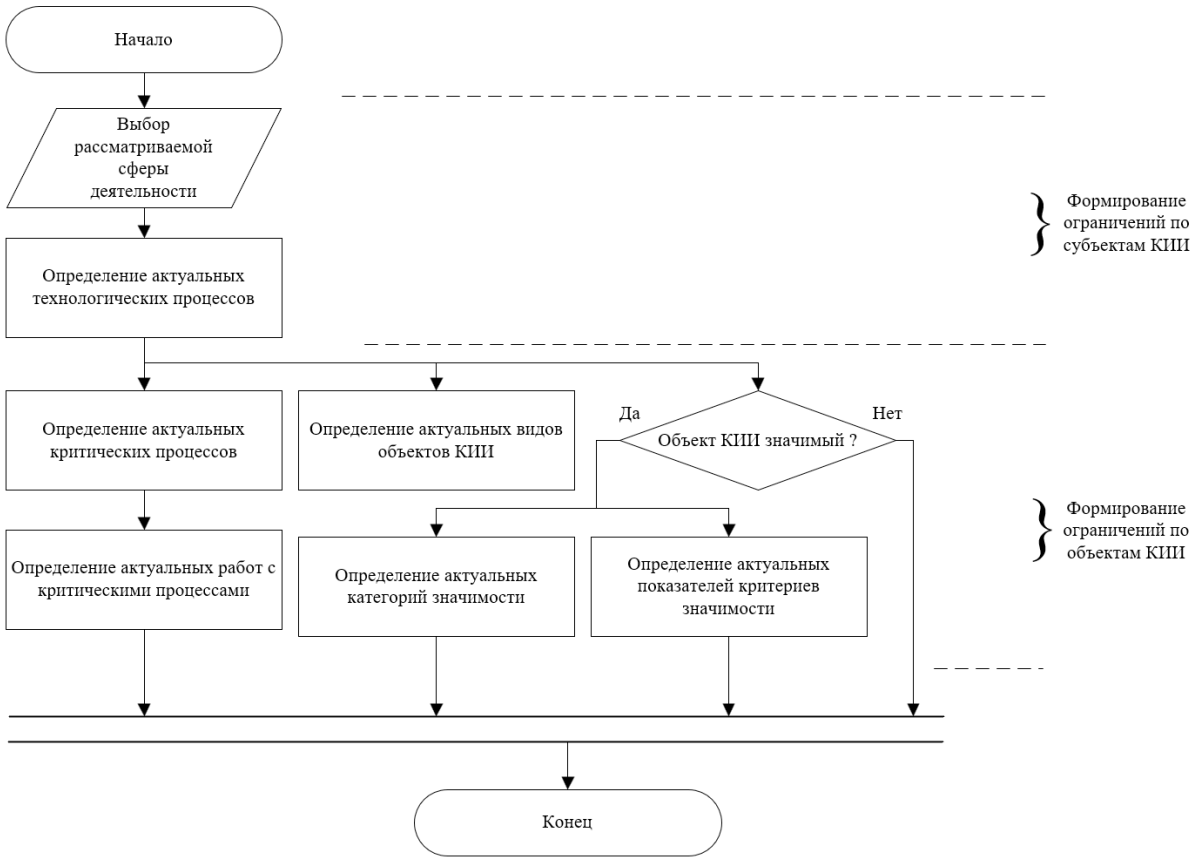

Рис. 3. Алгоритм формирования предметно-смысловых ограничений для значимых объектов КИИ

$$M'_{ОВ} = f_{ОВ}(P'_S, P'_{ОВ}). \quad (23)$$

Описанный процесс формирования предметно-смысловых ограничений (2) — (23) для проведения исследований компьютерного противоборства на значимых объектах КИИ представлен в виде функциональной схемы алгоритма (*рис.* 3).

Представленные в формализованном виде предметно-смысловые ограничения дают наглядное представление о целесообразности их формирования для проведения дальнейшего исследования компьютерного противоборства на значимых объектах критической информационной инфраструктуры и построения соответствующей концептуально-логической модели процесса компьютерного противоборства.

Заключение

Таким образом, одним из первых и основополагающих этапов проведения исследований, обеспечивающих получение точных и достоверных результатов, является введение ограничений. В ходе данной работы были сформулированы предметно-смысловые ограничения для проведения исследований компьютерного противоборства на значимых объектах КИИ и построения соответствующей концептуально-логической модели.

На примере задачи построения концептуальной модели компьютерного противоборства на значимых объектах КИИ, представленной выражением (1), предложен алгоритм формирования ограничений (сужения области исследований), существующих в начальных условиях решения задачи, основанный на детальном учете требований *нормативных правовых актов* [16] Российской Федерации. Представленный выражениями (2) — (23) алгоритм сужения области исследований применим для решения аналогичных задач моделирования процессов и систем объектов КИИ.

В рамках ограничений субъектов КИИ выбрана сфера энергетики, как сфера, оказывающая значительное влияние на другие сферы и обладающая большим количеством объектов. Рассматриваемые технологические процессы ограничены процессами транспортировки и сбыта, как наиболее приближенные к потребителям. В рамках объектов КИИ заданы ограничения по виду объектов — автоматизированные системы управления, по обеспечиваемым критическим процессам — технологические и производственные процессы, по работе с критическими процессами — управление, контроль и мониторинг, по значимости — значимые, по показателям критериев значимости — социальная и экономическая значимости, по категории значимости — 2-я и 3-я категории, определяющие наиболее распространенные объекты КИИ для выбранных Субъектов.

Сформированные предметно-смысловые ограничения позволят повысить достоверность создаваемых в дальнейшем моделей компьютерного противоборства на значимых объектах КИИ за счет сокращения объекта исследования, а также они являются основой для выполнение следующего этапа проведения исследования и построения концептуально-логической модели компьютерного противоборства на значимых объектах КИИ, включая определение актуальных угроз информационной безопасности для рассматриваемых объектов КИИ.

Рецензент: ***Цимбал Владимир Анатольевич,*** *доктор технических наук, профессор, заслуженный деятель науки РФ, профессор кафедры автоматизированных систем управления Филиала Военной академии им. Петра Великого, г. Серпухов, Российская Федерация.*
E-mail: tsimbalva@mail.ru

Литература

1. Абраменко Г.Т., Лансере Н.Н., Фадеев И.И. Анализ особенностей субъектов критической информационной инфраструктуры Российской Федерации, функционирующих в сфере науки // Труды XI Междунар. науч.-техн. конф. «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО 2022) (15—16 февраля 2022 г.). Т. 1 / СПб., Гос. ун-т телекоммуникаций им. проф. М.А. Бонч-Бруевича. СПб. : СПГУТ, 2022. С. 49—54.
2. Бакулин М.А. Управление рисками нарушения информационной безопасности значимых объектов критической информационной инфраструктуры // Системная инженерия и информационные технологии. 2023. Т. 5. № 5 (14). С. 78—87. DOI: 10.54708/2658-5014-SIIT-2023-no5-p78 .
3. Беляков М.И. Модель процесса функционирования системы обеспечения информационной безопасности объекта критической информационной инфраструктуры в задаче оценивания его эффективности // Вопросы оборонной техники. Сер. 16: Технические средства противодействия терроризму. 2020. № 11-12 (149-150). С. 71—75.
4. Бобков Е.О., Балашова Е.А., Панин Д.Н. Обеспечение информационной безопасности критической информационной инфраструктуры с IOT-технологиями // Труды IV Всеросс. науч.-прак. конф. «Экономика и общество: перспективы развития (Сызрань, 14 мая 2020 г.) / Межрег. центр инновац. технологий в образовании. Вып. 4. Киров : МЦИТО, 2020. С. 221—225.
5. Василенко В.В., Климов С.М., Палухин О.А. Модель угроз компьютерных атак на цифровую иерархию объектов критической информационной инфраструктуры // Труды 8-й Междунар. науч.-прак. конф. «Военная безопасность России: взгляд в будущее (16 марта 2023 г.) / РАРАН. В 3-х тт. М. : МГТУ, 2023. С. 194—201.
6. Вульфин А.М. Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных : автореф. дис. … д-ра техн. наук: 2.3.6. Уфа, 2022. 36 с.
7. Гельфанд А.М., Сигачева В.В., Архипов А.В., Сиротина Л.К. Анализ и управление рисками информационной безопасности объекта критической информационной инфраструктуры // Вестник СПб гос. ун-та технологии и дизайна. Сер. 1. Естественные и технические науки. 2023. № 3. С. 21—27. DOI: 10.46418/2079-8199_2023_3_3 .
8. Гильманова Э.А., Ахметшина Р.И. Особенности проведения аудита информационной безопасности объектов критической информационной инфраструктуры в топливно-энергетическом комплексе // Форум молодых ученых. 2022. № 2 (66). С. 29—33. DOI: 10.46566/2500-4050_2022_66_29 .
9. Гильманова Э.А., Ахметшина Р.И. Роль аудита информационной безопасности в жизненном цикле системы обеспечения информационной безопасности объектов критической информационной инфраструктуры // Форум молодых ученых. 2022. № 2 (66). С. 34—37. DOI: 10.46566/2500-4050_2022_66_34 .
10. Забегалин Е.В. Логическая модель деятельности по комплексному техническому диагностированию информационной безопасности организаций и значимых объектов критической информационной инфраструктуры // Системы управления, связи и безопасности. 2019. № 3. С. 145—178. DOI: 10.24411/2410-9916-2019-10308 .
11. Корнеева Е.В., Федин Ф.О. Модель процесса обработки событий информационной безопасности на объекте критической информационной инфраструктуры // Вестник компьютерных и информационных технологий. 2023. Т. 20. № 7 (229). С. 53—60. DOI: 10.14489/vkit.2023.07.pp.053-060 .
12. Кочнев С.В., Лапсарь А.П., Барабошкина А.В. Синтез структуры объектов критической информационной инфраструктуры производственных процессов на основе марковских моделей // Прикаспийский журнал: управление и высокие технологии. 2022. № 1 (57). С. 93—105. DOI: 10.54398/2074-1707_2022_1_93 .
13. Кубарев А.В., Лапсарь А.П., Федорова Я.В. Повышение безопасности эксплуатации значимых объектов критической инфраструктуры с использованием параметрических моделей эволюции // Вопросы кибербезопасности. 2020. № 1 (35). С. 8—17. DOI: 10.21681/2311-3456-2020-01-08-17 .

14. Кубарев А.В., Лапсарь А.П., Асютиков А.А. Синтез модели объекта критической информационной инфраструктуры для безопасного функционирования технической системы в условиях деструктивного информационного воздействия // Вопросы кибербезопасности. 2020. № 6 (40). С. 48—56. DOI: 10.21681/2311-3456-2020-06-48-56 .
15. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
16. Ловцов Д.А., Федичев А.В. Архитектура национального классификатора правовых режимов информации ограниченного доступа // Правовая информатика. 2017. № 2. С. 35—54. DOI: 10.21681/1994-1404-2017-2-35-54 .
17. Новикова Е.Ф., Хализев В.Н. Разработка модели угроз для объектов критической информационной инфраструктуры с учетом методов социальной инженерии // Прикаспийский журнал: управление и высокие технологии. 2019. № 4 (48). С. 127—135. DOI: 10.21672/2074-1707.2019.48.4.127-135 .
18. Овчаров В.А., Харжевская А.В. Формальная модель угроз кибербезопасности объектов критической информационной инфраструктуры // Космонавтика и ракетостроение. 2021. № 3 (120). С. 131—142.
19. Павличева Е.Н., Федин Ф.О., Чискидов А.С., Глыбин Н.Ф. Модель нарушителя информационной безопасности объекта критической информационной инфраструктуры торговой площадки транспортных услуг // Вестник компьютерных и информационных технологий. 2021. Т. 18. № 5 (203). С. 28—34. DOI: 10.14489/vkit.2021.05.pp.028-034 .
20. Смирнов Г.Е., Макаренко С.И. Актуальные вопросы развития теории и практики аудита информационной безопасности объектов критической информационной инфраструктуры // Труды Междунар. науч.-прак. конф. «Проблемы комплексной безопасности Каспийского макрорегиона» (28—29 октября 2021 г.). Астрахань : Астрах. гос. ун-т, 2021. С. 148—157.
21. Суворов А.М. Модель сегментации потенциальных нарушителей информационной безопасности значимых объектов критической информационной инфраструктуры // Труды XI Междунар. науч.-прак. конф. студентов, аспирантов и молодых ученых «Информационные технологии в науке, бизнесе и образовании» (28—29 ноября 2019 г.) / Моск. гос. лигв. ун-т. М. : МГЛУ, 2020. С. 304—307.
22. Уринсон Я.М., Кожуховский И.С., Сорокин И.С. Реформирование российской электроэнергетики: результаты и нерешенные вопросы // Экономический журнал Высшей школы экономики. 2020. Т. 24. № 3. С. 323—339. DOI: 10.17323/1813-8691-2020-24-3-323-339 .
23. Цыпкина А.В., Шабурова А.В. Категорирование объектов критической информационной инфраструктуры в оборонной промышленности // Интерэкспо Гео-Сибирь. 2022. Т. 6. С. 288—293. DOI: 10.33764/2618-981X-2022-6-288-293 .
24. Язов Ю.К., Соловьев С.В. Моделирование значимых объектов критической информационной инфраструктуры в интересах исследования защищенности применяемых в них информационных технологий // Труды 11-й Междунар. науч.-техн. конф. «Безопасные информационные технологии» (6—7 апреля 2021 г.) / МГТУ им. Н.Э. Баумана. М. : МГТУ, 2021. С. 363—369.

SECTION:
INFORMATION AND COMPUTER SECURITY

SUBJECT AND SEMANTIC LIMITATIONS IN MODELLING CYBER CONFRONTATION

Aleksei Iakovlev, *Ph.D. (Technology), Associate Professor at the Department of Information Systems and Information Protection of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: yava73@bk.ru

Mikhail Pelivan, *Ph.D. student at the Department of Information Systems and Information Protection of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: witcher89158779996@yandex.ru

Keywords: *critical information infrastructure, subject area, energy sector, social importance, economic importance, automated control system, information security, class of importance, object importance criterion.*

Abstract

Purpose of the study: increasing the reliability of cyber confrontation models for important objects of critical information infrastructure using the results of ontological analysis of the subject area and determining applicability limits for the models considering laws and legal regulations of the Russian Federation.

Methods used in the study: system analysis, formal logic analysis, the formal legal method.

Study findings: more precise definitions for the concepts of subject and object of critical information structure were given. The conceptual apparatus of and requirements set by Russia's laws and legal regulations in the field of ensuring information security at important objects of critical information infrastructure were analysed, and based on them subject and semantic limitations for building adequate cyber confrontation models are determined. For subjects of critical information infrastructure, limitations are determined based on the following parameters: field of activity and supported technological processes, and for objects of critical information infrastructure, based on the following parameters: types of objects, supported critically important processes, operations performed on critically important processes, type of importance, importance criteria indicators, class of importance.

References

1. Abramenko G.T., Lansere N.N., Fadeev I.I. Analiz osobennostei sub"ektov kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii, funktsioniruiushchikh v sfere nauki. Trudy XI Mezhdunar. nauch.-tekhn. konf. "Aktual'nye problemy infotelekommunikatsii v nauke i obrazovanii" (APINO 2022) (15–16 fevralia 2022 g.). T. 1. SPb., Gos. un-t telekommunikatsii im. prof. M.A. Bonch-Bruevicha. SPb. : SPGUT, 2022. Pp. 49–54.
2. Bakulin M.A. Upravlenie riskami narusheniia informatsionnoi bezopasnosti znachimykh ob"ektov kriticheskoi informatsionnoi infrastruktury. Sistemnaia inzheneriia i informatsionnye tekhnologii. 2023. T. 5. No. 5 (14). Pp. 78–87. DOI: 10.54708/2658-5014-SIIT-2023-no5-p78 .
3. Beliakov M.I. Model' protsessa funktsionirovaniia sistemy obespecheniia informatsionnoi bezopasnosti ob"ekta kriticheskoi informatsionnoi infrastruktury v zadache otsenivaniia ego effektivnosti. Voprosy oboronnoi tekhniki. Ser. 16: Tekhnicheskie sredstva protivodeistviia terrorizmu. 2020. No. 11-12 (149-150). Pp. 71–75.
4. Bobkov E.O., Balashova E.A., Panin D.N. Obespechenie informatsionnoi bezopasnosti kriticheskoi informatsionnoi infrastruktury s IOT-tekhnologiiami. Trudy IV Vseross. nauch.-prak. konf. "Ekonomika i obshchestvo: perspektivy razvitiia (Syzran', 14 maia 2020 g.). Mezhreg. tsentr innovats. tekhnologii v obrazovanii. Vyp. 4. Kirov : MTsITO, 2020. Pp. 221–225.
5. Vasilenko V.V., Klimov S.M., Palukhin O.A. Model' ugroz komp'iuternykh atak na tsifrovuiu ierarkhiiu ob"ektov kriticheskoi informatsionnoi infrastruktury. Trudy 8-i Mezhdunar. nauch.-prak. konf. "Voennaia bezopasnost' Rossii: vzgliad v budushchee (16 marta 2023 g.). RARAN. V 3-kh tt. M. : MGTU, 2023. Pp. 194–201.
6. Vul'fin A.M. Modeli i metody kompleksnoi otsenki riskov bezopasnosti ob"ektov kriticheskoi informatsionnoi infrastruktury na osnove intellektual'nogo analiza dannykh : avtoref. dis. … d-ra tekhn. nauk: 2.3.6. Ufa, 2022. 36 pp.
7. Gel'fand A.M., Sigacheva V.V., Arkhipov A.V., Sirotina L.K. Analiz i upravlenie riskami informatsionnoi bezopasnosti ob"ekta kriticheskoi informatsionnoi infrastruktury. Vestnik SPb gos. un-ta tekhnologii i dizaina. Ser. 1. Estestvennye i tekhnicheskie nauki. 2023. No. 3. Pp. 21–27. DOI: 10.46418/2079-8199_2023_3_3 .
8. Gil'manova E.A., Akhmetshina R.I. Osobennosti provedeniia audita informatsionnoi bezopasnosti ob"ektov kriticheskoi informatsionnoi infrastruktury v toplivno-energeticheskom komplekse. Forum molodykh uchenykh. 2022. No. 2 (66). Pp. 29–33. DOI: 10.46566/2500-4050_2022_66_29 .
9. Gil'manova E.A., Akhmetshina R.I. Rol' audita informatsionnoi bezopasnosti v zhiznennom tsikle sistemy obespecheniia informatsionnoi bezopasnosti ob"ektov kriticheskoi informatsionnoi infrastruktury. Forum molodykh uchenykh. 2022. No. 2 (66). Pp. 34–37. DOI: 10.46566/2500-4050_2022_66_34 .
10. Zabegalin E.V. Logicheskaia model' deiatel'nosti po kompleksnomu tekhnicheskomu diagnostirovaniiu informatsionnoi bezopasnosti organizatsii i znachimykh ob"ektov kriticheskoi informatsionnoi infrastruktury. Sistemy upravleniia, sviazi i bezopasnosti. 2019. No. 3. Pp. 145–178. DOI: 10.24411/2410-9916-2019-10308 .
11. Korneeva E.V., Fedin F.O. Model' protsessa obrabotki sobytii informatsionnoi bezopasnosti na ob"ekte kriticheskoi informatsionnoi infrastruktury. Vestnik komp'iuternykh i informatsionnykh tekhnologii. 2023. T. 20. No. 7 (229). Pp. 53–60. DOI: 10.14489/vkit.2023.07.pp.053-060 .
12. Kochnev S.V., Lapsar' A.P., Baraboshkina A.V. Sintez struktury ob"ektov kriticheskoi informatsionnoi infrastruktury proizvodstvennykh protsessov na osnove markovskikh modelei. Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii. 2022. No. 1 (57). Pp. 93–105. DOI: 10.54398/2074-1707_2022_1_93 .
13. Kubarev A.V., Lapsar' A.P., Fedorova Ia.V. Povyshenie bezopasnosti ekspluatatsii znachimykh ob"ektov kriticheskoi infrastruktury s ispol'zovaniem parametricheskikh modelei evoliutsii. Voprosy kiberbezopasnosti. 2020. No. 1 (35). Pp. 8–17. DOI: 10.21681/2311-3456-2020-01-08-17 .
14. Kubarev A.V., Lapsar' A.P., Asiutikov A.A. Sintez modeli ob"ekta kriticheskoi informatsionnoi infrastruktury dlia bezopasnogo funktsionirovaniia tekhnicheskoi sistemy v usloviiakh destruktivnogo informatsionnogo vozdeistviia. Voprosy kiberbezopasnosti. 2020. No. 6 (40). Pp. 48–56. DOI: 10.21681/2311-3456-2020-06-48-56 .
15. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
16. Lovtsov D.A., Fedichev A.V. Arkhitektura natsional'nogo klassifikatora pravovykh rezhimov informatsii ogranichennogo dostupa. Pravovaia informatika. 2017. No. 2. Pp. 35–54. DOI: 10.21681/1994-1404-2017-2-35-54 .

17. Novikova E.F., Khalizev V.N. Razrabotka modeli ugroz dlia ob"ektov kriticheskoi informatsionnoi infrastruktury s uchetom metodov sotsial'noi inzhenerii. Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii. 2019. No. 4 (48). Pp. 127–135. DOI: 10.21672/2074-1707.2019.48.4.127-135 .
18. Ovcharov V.A., Kharzhevskaia A.V. Formal'naia model' ugroz kiberbezopasnosti ob"ektov kriticheskoi informatsionnoi infrastruktury. Kosmonavtika i raketostroenie. 2021. No. 3 (120). Pp. 131–142.
19. Pavlicheva E.N., Fedin F.O., Chiskidov A.S., Glybin N.F. Model' narushitelia informatsionnoi bezopasnosti ob"ekta kriticheskoi informatsionnoi infrastruktury torgovoi ploshchadki transportnykh uslug. Vestnik komp'iuternykh i informatsionnykh tekhnologii. 2021. T. 18. No. 5 (203). Pp. 28–34. DOI: 10.14489/vkit.2021.05.pp.028-034 .
20. Smirnov G.E., Makarenko S.I. Aktual'nye voprosy razvitiia teorii i praktiki audita informatsionnoi bezopasnosti ob"ektov kriticheskoi informatsionnoi infrastruktury. Trudy Mezhdunar. nauch.-prak. konf. "Problemy kompleksnoi bezopasnosti Kaspiiskogo makroregiona" (28–29 oktiabria 2021 g.). Astrakhan': Astrakh. gos. un-t, 2021. Pp. 148–157.
21. Suvorov A.M. Model' segmentatsii potentsial'nykh narushitelei informatsionnoi bezopasnosti znachimykh ob"ektov kriticheskoi informatsionnoi infrastruktury. Trudy XI Mezhdunar. nauch.-prak. konf. studentov, aspirantov i molodykh uchenykh "Informatsionnye tekhnologii v nauke, biznese i obrazovanii" (28–29 noiabria 2019 g.). Mosk. gos. ligv. un-t. M. : MGLU, 2020. Pp. 304–307.
22. Urinson Ia.M., Kozhukhovskii I.S., Sorokin I.S. Reformirovanie rossiiskoi elektroenergetiki: rezul'taty i nereshennye voprosy. Ekonomicheskii zhurnal Vysshei shkoly ekonomiki. 2020. T. 24. No. 3. Pp. 323–339. DOI: 10.17323/1813-8691-2020-24-3-323-339 .
23. Tsypkina A.V., Shaburova A.V. Kategorirovanie ob"ektov kriticheskoi informatsionnoi infrastruktury v oboronnoi promyshlennosti. Interekspo Geo-Sibir'. 2022. T. 6. Pp. 288–293. DOI: 10.33764/2618-981X-2022-6-288-293 .
24. Iazov Iu.K., Solov'ev S.V. Modelirovanie znachimykh ob"ektov kriticheskoi informatsionnoi infrastruktury v interesakh issledovaniia zashchishchennosti primeniaemykh v nikh informatsionnykh tekhnologii. Trudy 11-i Mezhdunar. nauch.-tekhn. konf. "Bezopasnye informatsionnye tekhnologii" (6–7 aprelia 2021 g.). MGTU im. N.E. Baumana. M. : MGTU, 2021. Pp. 363–369.