DOI: 10.18137/RNU.V9187.23.03.P.136 УДК 004.056.52

С.С. Валеев, Н.В. Кондратьева, М.Б. Гузаиров, А.В. Мельников

ЭТАПЫ РЕИНЖИНИРИНГА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ В РАМКАХ ТЕХНОЛОГИИ НУЛЕВОГО ДОВЕРИЯ

Аннотация. Развитие информационных систем предприятия связано с необходимостью поддержки удаленной работы сотрудников. Причины могут носить разный характер. В этих условиях обеспечить защиту периметра предприятия достаточно сложно на основе существующей парадигмы защиты периметра. В настоящее время активно развиваются и внедряются системы защиты на основе архитектуры нулевого доверия. В статье проведен анализ особенностей внедрения этой технологии на предприятии, где применяются традиционные системы защиты информации, основанные на использовании VPN-технологий и межсетевых экранов. Рассматриваются основные шаги, которые позволят в случае необходимости поэтапно выполнить переход на архитектуру нулевого доверия.

Ключевые слова: защита информации, информационная система предприятия, модель нулевого доверия, архитектура нулевого доверия.

S.S. Valeev, N.V. Kondratyeva, M.B. Guzairov, A.V. Melnikov

STAGES OF REENGINEERING THE INFORMATION SYSTEM OF THE ENTERPRISE WITHIN THE FRAMEWORK OF ZERO TRUST TECHNOLOGY

Abstract. The development of enterprise information systems is associated with the need to support remote work of employees. The reasons may be of a different nature. Under these conditions, it is quite difficult to provide enterprise perimeter protection based on the existing perimeter protection paradigm. Currently, protection systems based on zero trust architecture are being actively developed and implemented. The article analyzes the features of the implementation of this technology in an enterprise that uses a traditional information security system based on the use of VPN technologies and firewalls. The main steps are considered that will allow, if necessary, a phased transition to a zero-trust architecture.

Keywords: information security, enterprise information system, zero trust model, zero trust architecture.

Введение

Нулевое доверие (далее – НД) – термин, обозначающий развивающуюся концепцию в области кибербезопасности. При архитектуре с нулевым доверием (далее – АНД) используются принципы концепции нулевого доверия для проектирования защищенной корпоративной информационной системы, а также сопровождения рабочих защищенных процессов на предприятии [1–3].

В рамках концепции НД предполагается, что отсутствует потенциальное доверие при допуске к активам или учетным записям пользователей, основанное исключительно на их физическом или сетевом местоположении или на зафиксированном в системе владении информационными активами. Модели НД используются в настоящее время крупными компаниями Microsoft [4], IBM [5], Oracle [6], АО «Лаборатория Касперского» [7] и др.

По прогнозам компании Gartner, АНД найдет широкое распространение в ближайшие несколько лет (см. Рисунок 1).

Валеев Сагит Сабитович
доктор технических наук, профессор, профессор кафедры управления информационной безопасностью, Уфимский университет науки и технологий, город Уфа. Сфера научных интересов: системы управления организационно-техническими объектами, информационные технологии, защита информации. Автор более 150 опубликованных научных работ.
Электронный адрес: vss2000@mail.ru

Кондратьева Наталья Владимировна
кандидат технических наук, доцент, доцент кафедры информатики, Уфимский университет науки и технологий, город Уфа. Сфера научных интересов: системы управления организационно-техническими объектами, информационные технологии. Автор более 80 опубликованных научных работ.
Электронный адрес: knv24@mail.ru

Гузаиров Мурат Бакеевич
доктор технических наук, профессор, профессор кафедры управления информационной безопасностью, Уфимский университет науки и технологий, город Уфа. Сфера научных интересов: информационные технологии, защита информации, анализ сложных систем. Автор более 400 опубликованных научных работ.
Электронный адрес: Mbguzairov@gmail.com

Мельников Андрей Витальевич
доктор технических наук, профессор, директор, Югорский научно-исследовательский институт информационных технологий, город Ханты-Мансийск. Сфера научных интересов: методы и средства защиты информации, информационные системы, сетевые технологии, методы искусственного интеллекта. Автор более 180 опубликованных научных работ.
Электронный адрес: MelnikovAV@uriit.ru

Рисунок 1. Прогноз развития технологий информационной безопасности [8]

Информационная система типичного предприятия становится всё более сложной, отражая развитие предприятия [9–11]. На одном современном предприятии может использоваться несколько внутренних компьютерных сетей, связанных с удаленными подразделениями со своей локальной информационной инфраструктурой и облачными сервисами [12; 13].

Методы сетевой безопасности на основе концепции периметра безопасности в современных условиях не обеспечивают требуемого уровня информационной безопасности, поскольку для распределенного предприятия нет единого, четко идентифицируемого периметра безопасности. Таким образом, если злоумышленники смогли преодолеть периметр, дальнейшее горизонтальное перемещение в сети для них становится беспрепятственным [14; 15].

Модель нулевого доверия. Особенности

Концепция НД в первую очередь ориентирована на защиту данных и услуг, но может быть расширена на все активы предприятия (устройства, компоненты инфраструктуры, приложения, виртуальные и облачные компоненты) и субъекты (конечных пользователей, приложений и других информационных объектов, которые запрашивают информацию).

В модели безопасности с НД предполагается, что злоумышленник, присутствующий во внешней среде, может присутствовать и в среде, принадлежащей предприятию, и они ничем не отличаются. В связи с этим в рамках этой парадигмы предприятие должно отказаться от безоговорочного доверия к сотрудникам и постоянно анализировать и оценивать информационные риски для своих активов и риски нарушения бизнес-процессов, следовательно, постоянно принимать меры информационной защиты для снижения этих рисков.

При использовании модели НД средства защиты обычно включают в себя системы обеспечения доступа к ресурсам сети (данные и вычислительные ресурсы и приложения/сервисы) только тем субъектам и активам, которые определены как нуждающиеся в доступе, а также обеспечивают выполнение постоянной аутентификации и авторизации личности и анализ состояния безопасности каждого запроса на доступ в систему.

АНД не является единой архитектурой, это набор руководящих принципов для организации рабочих процессов, проектирования системы безопасности, которые можно использовать для повышения уровня безопасности информационной системы предприятия.

На Рисунке 2 представлена концептуальная модель АНД.

На основе этой модели составлен граф G перемещения потоков информации I и потоков данных D. Красным цветом обозначены дуги перемещения запросов к активам информационной системы: данным, приложениям и элементам инфраструктуры. Синим цветом – дуги графа G, обозначающие потоки сбора информации об особенностях запросов к активам системы. На основе этой информации формируется цифровой двойник пользователя или сущности. Эта информация используется для уточнения политики безопасности, которая далее используется в качестве адаптивной эталонной модели доступа. Следует отметить, что при реализации адаптивной системы формирования политики доступа в различных точках информационной системы требуется использование высокопроизводительных вычислителей и формирование аналитики в рамках концепции нарастающих данных.

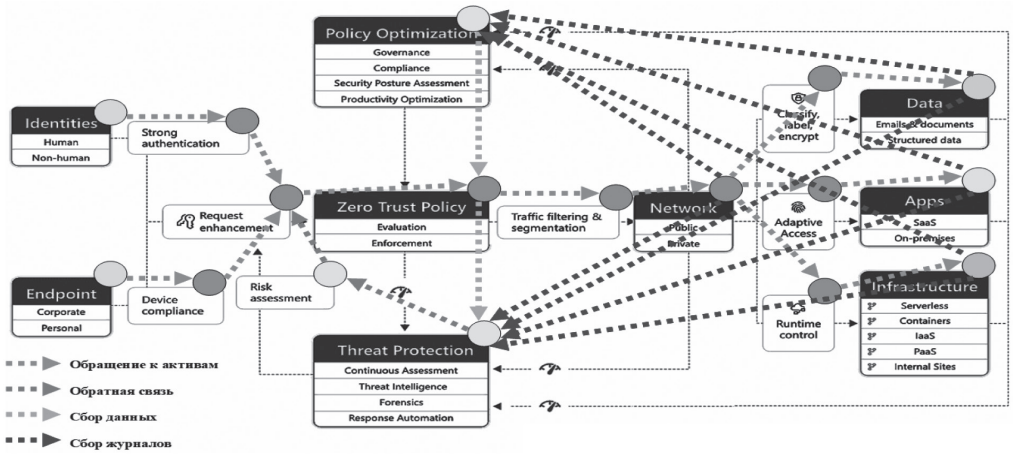

Рисунок 2. Модель нулевого доверия Microsoft и потоки информации и данных

Основные шаги перехода на архитектуру нулевого доверия

Как отмечалось ранее, идея АНД заключается в том, что предлагается отказаться от традиционной модели безопасности, основанной на предоставлении доверия при работе с внутренними сетями и устройствами. Тем самым перейти к более защищенному подходу, основанному на строгой аутентификации и авторизации для каждого доступа к любым ресурсам независимо от того, находится ли пользователь или устройство внутри или вне сети предприятия. То есть предполагается, что ни одна сущность, будь то пользователь, устройство или сетевой ресурс, не может быть доверенным автоматически. Вместо этого каждое подключение и авторизация должны быть проверены и аутентифицированы перед предоставлением доступа к ресурсам. Для перехода к этой архитектуре необходимо выполнить ряд основных шагов.

Шаг 1. Реализовать многофакторную аутентификацию, то есть использовать несколько методов аутентификации (например, пароль и одноразовый код), для того чтобы убедиться в легитимности пользователя.

Шаг 2. Выполнить микросегментацию сети, то есть выполнить разделение сети на отдельные сегменты и создание политик доступа для каждого сегмента, чтобы установить контроль над движением данных внутри сети.

Шаг 3. Осуществить принцип «меньше привилегий», то есть обеспечить предоставление минимально необходимых привилегий для каждого пользователя или устройства, чтобы ограничить возможности злоумышленника в случае компрометации учетной записи или устройства.

Шаг 4. Обеспечить уровень доступа на основе контекста, для этого необходимо выполнить анализ контекста подключения, включая информацию о пользователе, устройстве и местоположении, для принятия решения о предоставлении доступа.

Шаг 5. Обеспечить непрерывный мониторинг, что подразумевает выполнение постоянного мониторинга сети и анализ активности для обнаружения подозрительного поведения и возможной атаки.

Выполнение этих шагов обеспечит реализацию АНД на каждом этапе доступа к ресурсам.

Рассмотрим пример перехода от традиционной схемы защиты периметра к архитектуре НД.

На Рисунке 3 представлена упрощенная схема защищенной информационной системы предприятия на основе защищенного периметра; на Рисунке 4 показана система защиты информации предприятия на основе архитектуры нулевого доверия. На рисунках используются следующие сокращения: СКСД – система контроля сетевого доступа, VPN – защищенный канал связи, МЭ – межсетевой экран, МЭНП – межсетевой экран нового поколения, ТППБ – точка проверки политики безопасности, БД – база данных, ББДО – брокер безопасного доступа в облако, КПП – контроль привилегированных пользователей, ИС – инсталляционный сервер, СКСД – система контроля сетевого доступа, ИСП – информационная система пользователей, ДМЗ – демилитаризованная зона, ОЗИ – отдел защиты информации.

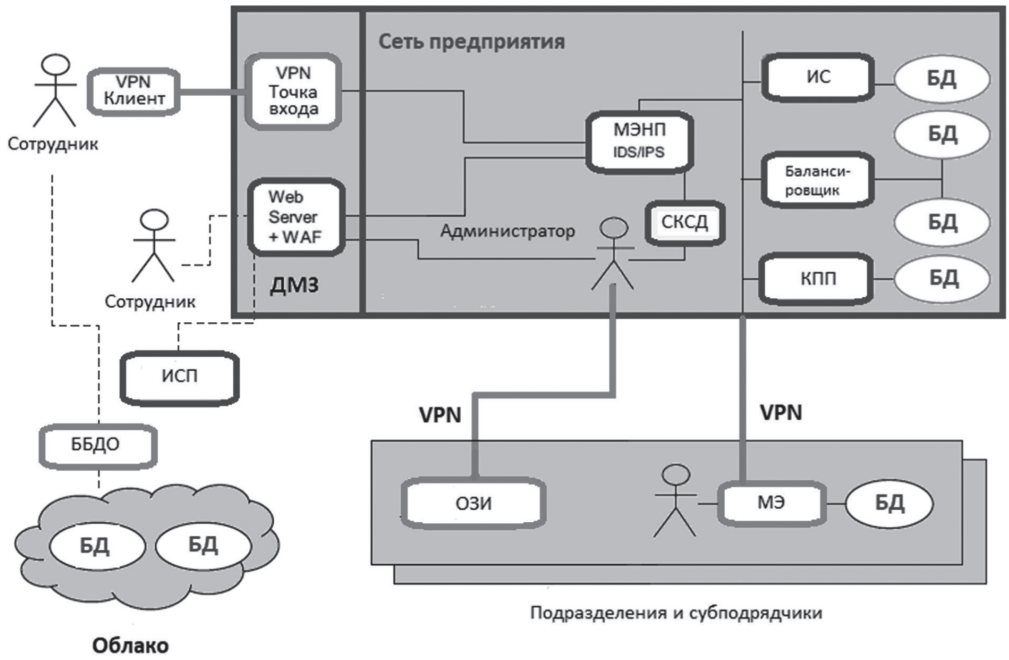

Рисунок 3. Система защиты информации предприятия на основе защищенного периметра

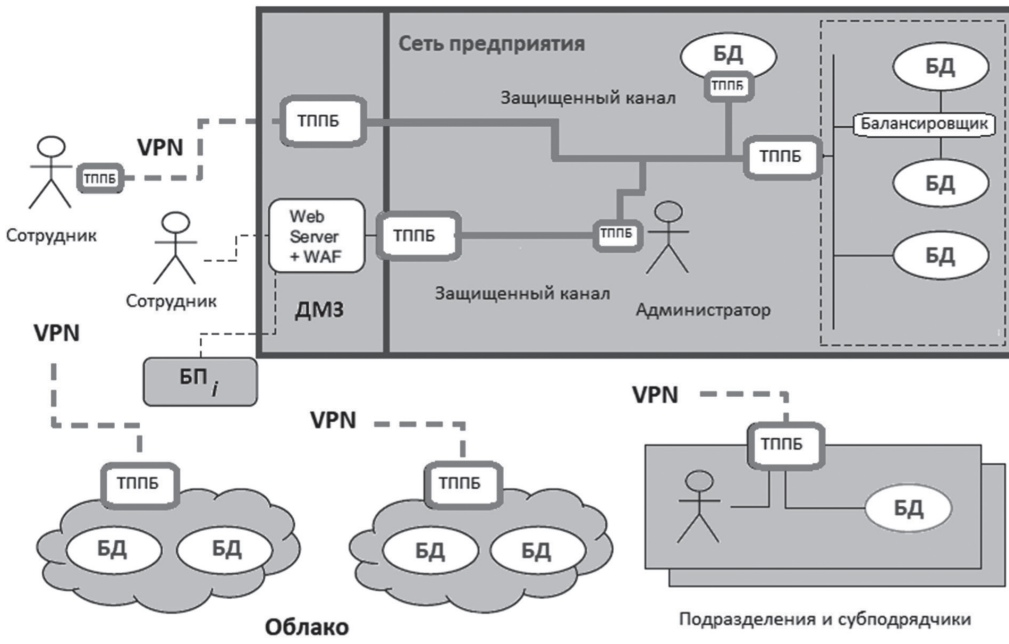

Рисунок 4. Система защиты информации предприятия на основе архитектуры нулевого доверия

В связи с этим можно сделать заключение, что при проектировании системы в рамках АНД следует обратить внимание на разработку политик безопасности для ТППБ. Также возникает задача разработки защищенных каналов связи с VPN.

Выводы и комментарии

Таким образом, можно сделать следующие выводы об особенностях применения АНД.

1. Дополнительная сложность проверки. Каждый запрос или действие должно быть проверено и авторизовано перед выполнением. Это может потребовать дополнительного времени на выполнение проверок и авторизации, что, в свою очередь, может замедлить работу информационной системы предприятия и в результате повлиять на эффективность бизнес-процессов.

2. Дополнительные точки аутентификации. В АНД могут использоваться дополнительные точки аутентификации, такие как множественный фактор аутентификации или проверка идентичности устройства. Эти дополнительные шаги могут потребовать дополнительного времени на их выполнение, что, в свою очередь, может замедлить работу информационной системы предприятия.

3. Увеличенный объем данных. В рамках АНД генерируется больше данных, которые необходимо передавать и обрабатывать для выполнения проверок и авторизации. Это может повлечь за собой замедление работы информационной системы.

4. Распределенная архитектура. АНД имеет распределенную архитектуру, где аутентификация и авторизация осуществляются на распределенных серверах. Передача данных между этими серверами может занять время и снизить производительность системы.

Однако, несмотря на возможную замедленную работу системы, преимущества АНД для обеспечения информационной безопасности могут компенсировать эти недостатки.

Литература

1. *Rose S., Borchert O., Mitchell S., Connelly S.* (2020) Zero Trust Architecture, Special Publication (NIST SP). Gaithersburg: National Institute of Standards and Technology [Электронный ресурс]. https://doi.org/ 10.6028/NIST.SP.800-207 (дата обращения: 21.07.2023).
2. *Singh R., Srivastav G., Kashyap R., Vats S.* (2023) Study on Zero-Trust Architecture, Application Areas & Challenges of 6G Technology in Future. Proceedings of 2023 International Conference on Disruptive Technologies (ICDT), Greater Noida, India, 2023, Pp. 375–380.
3. *Mandal D, Singhal N., Tyagi M.* (2023) Cybersecurity in the Era of Emerging Technology. Emerging Technology and Management Trends. Delhi: Manglam Publications, 2023, Pp. 108–134.
4. Embrace proactive security with Zero Trust [Электронный ресурс]. URL: https://www.microsoft.com/en-us/security/business/zero-trust (дата обращения: 21.07.2023).
5. Zero trust security solutions [Электронный ресурс]. URL: https://www.ibm.com/zero-trust (дата обращения: 21.07.2023).
6. Zero-trust security model [Электронный ресурс]. URL: https://www.oracle.com/security/what-is-zero-trust/ (дата обращения: 21.07.2023).
7. Концепция безопасности Zero Trust: преимущества и принцип работы [Электронный ресурс]. https://www.kaspersky.ru/resource-center/definitions/zero-trust?ysclid=lk9mlepw6a789934230 (дата обращения: 21.07.2023).
8. The Top 8 Security and Risk Trends We're Watching [Электронный ресурс]. URL: https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021 (дата обращения: 21.07.2023).
9. *Valeev S., Kondratyeva N.* (2021) Process Safety and Big Data: монография. Amsterdam: Elsevier, 2021, 315 p.
10. *Аббазов В.Р., Балуев В.А., Мельников А.В., Русанов М.А.* Метод нахождения связанных показателей на основе анализа нормативно-правовых актов методами NLP // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. 2022. Т. 22, № 1. С. 88–96.
11. *Rusanov M.A., Abbazov V.R., Baluev V.A., Burlutsky V.V., Melnikov A.V.* (2022) On the approach to forecasting indicators of socio-economic development of the region based on indirect indicators Modeling. Optimization and Information Technology, 2022, Vol. 10, No. 3, Pp. 2–3.
12. *Фрид А.И., Вульфин А.М., Гузаиров М.Б., Берхольц В.В.* Обеспечение целостности телеметрической информации о состоянии сложного технического объекта // Моделирование, оптимизация и информационные технологии. 2023. Т. 11, № 1 (40). С. 17–18.
13. *Гвоздев В.Е., Гузаиров М.Б., Бежаева О.Я., Курунова Р.Р., Насырова Р.А.* Информационная поддержка проактивного управления функциональной безопасностью компонентов киберфизических систем // Моделирование, оптимизация и информационные технологии. 2020. Т. 8, № 2 (29) [Электронный ресурс]. URL: https://moit.vivt.ru/wp-content/uploads/2020/05/GvozdevSoavtors_2_20_1.pdf (дата обращения: 21.07.2023).
14. *Золотухина М.А., Зыков С.В.* Исследование и определение признаков скрытых атак на предприятии для алгоритмов машинного обучения // Вестник Российского нового университета. Серия: сложные системы: модели, анализ и управление, 2023. Вып. 1. С. 20–28.
15. *Глухих И.Н., Глухих Д.И., Карякин Ю.Е.* Представление и отбор ситуаций на сложном технологическом объекте в условиях неопределенности // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление, 2021. Вып. 2. С. 65–73.

Literature

1. Rose S., Borchert O., Mitchell S., Connelly S. (2020) Zero Trust Architecture, Special Publication (NIST SP). Gaithersburg: National Institute of Standards and Technology, 2020. https://doi.org/10.6028/NIST.SP.800-207 (accessed: 21.07.2023).
2. Singh R., Srivastav G., Kashyap R., Vats S. (2023) Study on Zero-Trust Architecture, Application Areas & Challenges of 6G Technology in Future. Proceedings of 2023 International Conference on Disruptive Technologies (ICDT), Greater Noida, India, 2023, Pp. 375–380.
3. Mandal D, Singhal N., Tyagi M. (2023) Cybersecurity in the Era of Emerging Technology. Emerging Technology and Management Trends. Delhi: Manglam Publications, 2023, Pp. 108–134.
4. Embrace proactive security with Zero Trust. Available at: https://www.microsoft.com/en-us/security/business/zero-trust (accessed: 21.07.2023).
5. Zero trust security solutions. Available at: https://www.ibm.com/zero-trust (accessed 21.07.2023).
6. Zero-trust security model. Available at: https://www.oracle.com/ security/what-is-zero-trust/ (accessed: 21.07.2023).
7. *Koncepciya bezopasnosti Zero Trust: preimushchestva i princip raboty* [Zero Trust security concept: advantages and principle of operation]. Available at: https://www.kaspersky.ru/resource-center/definitions/zero-trust?ysclid=lk9mlepw6a789934230 (accessed: 21.07.2023) (in Russian).
8. The Top 8 Security and Risk Trends We're Watching. Available at: https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021 (accessed: 21.07.2023).
9. Valeev S., Kondratyeva N. (2021) *Process Safety and Big Data*. Amsterdam, Elsevier, 2021, 315 p.
10. Abbazov V.R., Baluev V.A., Melnikov A.V., Rusanov M.A. (2022) Metod nahozhdeniya svyazannyh pokazatelej na osnove analiza normativno-pravovyh aktov metodami NLP [The method of finding related indicators based on the analysis of legal acts by NLP methods]. *Bulletin of the South Ural State University. Series: Computer technologies, control, radio electronics*, 2022, Vol. 22, No. 1, Pp. 88–96 (in Russian).
11. Rusanov M.A., Abbazov V.R., Baluev V.A., Burlutsky V.V., Melnikov A.V. (2022) On the approach to forecasting indicators of socio-economic development of the region based on indirect indicators Modeling. *Optimization and Information Technology*, 2022, Vol. 10, No. 3, Pp. 2–3.
12. Frid A.I., Vulfin A.M., Guzairov M.B., Berkholts V.V. (2023) Obespechenie celostnosti telemetricheskoj informacii o sostoyanii slozhnogo tekhnicheskogo ob"ekta [Ensuring the integrity of telemetric information about the state of a complex technical object]. *Modeling, optimization and information technology*, 2023, Vol. 11, No. 1, Pp. 17–18 (in Russian).
13. Gvozdev V.E., Guzairov M.B., Bezhaeva O.Ya., Kurunova R.R., Nasyrova R.A. (2020) Informacionnaya podderzhka proaktivnogo upravleniya funkcional'noj bezopasnost'yu komponentov kiberfizicheskih sistem [Information support for the proactive management of the functional safety of the components of cyber-physical systems]. *Modeling, optimization and information technology*, Vol. 8, No. 2. Available at: https://moit.vivt.ru/wp-content/uploads/2020/05/GvozdevSoavtors _2_20_1.pdf (accessed: 21.07.2023) (in Russian).
14. Zolotukhina M.A., Zykov S.V. (2023) Issledovanie i opredelenie priznakov skrytyh atak na predpriyatii dlya algoritmov mashinnogo obucheniya [Research and identification of signs of hidden attacks at the enterprise for machine learning algorithms]. *Bulletin of the Russian New University. Series: complex systems: models, analysis and control*, Vol. 1, Pp. 20–28 (in Russian).
15. Glukhikh I.N., Glukhikh D.I., Karyakin Yu.E. (2021) Predstavlenie i otbor situacij na slozhnom tekhnologicheskom ob"ekte v usloviyah neopredelennosti [Representation and selection of situations on a complex technological object under conditions of uncertainty]. *Bulletin of the Russian New University. Series: Complex systems: models, analysis and control*, Vol. 2, Pp. 65–73 (in Russian).