УДК 004.056.5

СОВРЕМЕННАЯ МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СРЕДСТВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

П.Б. Гусаков, К.Е. Макаренко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Рассмотрены современные методологические подходы к построению систем защиты информации в контексте обеспечения информационной безопасности в Республике Беларусь. Проанализированы основные принципы проектирования интегрированных программ: непрерывность, комплексность, экономическая целесообразность и адаптивность, которые закреплены в национальном законодательстве. Представлена классификация методов защиты. Проанализированы направления развития в области методологии защиты информации в ходе реализации концепции цифрового суверенитета до 2030 г.

Ключевые слова: методы защиты информации; моделирование угроз; криптография; искусственный интеллект в безопасности; инженерно-техническая защита; квантовое шифрование; управление доступом; информационная безопасность.

MODERN METHODOLOGY FOR BUILDING INFORMATION PROTECTION MEANS AND SYSTEMS

P.B. Gusakov, K.E. Makaranka

Educational Institution "Belarusian State University of Informatics and Radio Electronics", Minsk, Republic of Belarus

Abstract. This article examines modern methodological approaches to building information security systems in the context of information security in the Republic of Belarus. It analyzes the key principles of integrated program design, including continuity, comprehensiveness, economic feasibility, and adaptability, as enshrined in national legislation. A classification of security methods is presented. Development directions in information security methodology are analyzed as part of the implementation of the concept of digital sovereignty by 2030.

Keywords: information protection methods; threat modeling; cryptography; artificial intelligence in security; engineering and technical protection; quantum encryption; access control; information security.

Введение

Актуальность темы данного доклада обусловлена необходимостью совершенствования методологических подходов к построению систем защиты информации в условиях эскалации киберугроз и цифровой трансформации объектов критической инфраструктуры. В Республике Беларусь создана всеобъемлющая правовая база для защиты информации. Ключевыми документами, определяющими государственную политику, выступают Концепция информационной безопасности, утвержденная Постановлением Совета Безопасности № 1 от 18 марта 2019 года, а также Концепция обеспечения суверенитета в сфере цифрового развития до 2030 года, утвержденная Постановлением Совета Министров № 1074 от 31 декабря 2024 года. Данные акты задают вектор развития национальных систем защиты информации в контексте обеспечения информационного суверенитета [1]. В настоящем докладе рассматриваются современные методологические принципы создания СЗИ, классификация методов защиты и перспективные направления развития технологий безопасности с учетом требований национальных регуляторов.

Основная часть

Фундаментальной основой построения системы безопасности является соблюдение принципов, закрепленных в законе Республики Беларусь «Об информации, информатизации и защите информации» № 455-З и подробно изложенных в нормативных документах Оперативно-аналитического центра при Президенте Республики Беларусь.

Принцип непрерывности и надежности защиты подразумевает работу системы безопасности в состоянии постоянной готовности к отражению угроз, временные и пространственные характеристики которых заранее не предопределены. Принцип универсальности обусловлен отсутствием универсальных методов защиты и требует интеграции правовых (регулируемых, в частности, Указом Президента № 422 "О мерах по совершенствованию защиты персональных данных"), организационных, инженерных и программных процедур, обеспечивающих появление системы безопасности. Принцип экономической целесообразности (адекватности) устанавливает взаимосвязь между стоимостью защиты и стоимостью защищаемых информационных активов или возможным ущербом, причиняемым в результате расчетов. Принцип адаптивности (гибкости) особенно важен с методологической точки зрения. Из-за динамичного характера угроз меры безопасности не могут быть статичными. Обнаружение злоумышленником конкретного метода защиты снижает его эффективность, что влечет за собой внедрение механизмов быстрого обновления мер безопасности [2].

Процесс построения системы безопасности регулируется положением о защите технической и криптографической информации (утвержденным Указом Президента Республики Беларусь № 196) и включает в себя следующие этапы:

– детализация предметной области, то есть определение целевых функций системы (контроль доступа, обеспечение конфиденциальности каналов связи, защита от несанкционированного копирования и т.д.);

– построение модели угроз и модели атакующего имеет решающее значение, поскольку позволяет идентифицировать угрозы, связанные с информационной безопасностью. Модель преступника должна учитывать его потенциальные возможности;

– разработка политики безопасности – набора правил и норм, регулирующих обработку информации. Для государственных учреждений, организаций и операторов персональных данных (согласно Закону № 99-З) наличие официальной политики безопасности является обязательным требованием;

– определение структуры и компонентов системы безопасности.

Обобщение и оценка гарантий работоспособности: проверка правильности внедрения механизмов защиты, включая процедуры обязательной сертификации объектов информатики в соответствии с процедурами, установленными ОАЦ.

Современная методология защиты информации предполагает многоуровневый подход, который объединяет различные категории методов.

1. Инженерно-технические методы ЗИ включают в себя создание механических барьеров, организацию зон контролируемого доступа, маскировку каналов утечки информации. Обеспечение физической защиты серверных помещений, аппаратных систем и носителей информации чрезвычайно важно, особенно для критически важных объектов информатизации (КВОИ).

2. Криптографические методы ЗИ. В Республике Беларусь вектор развития смещается в сторону использования национальных стандартов криптографического преобразования и средств, сертифицированных ОАЦ.

3. Программно-аппаратные методы ЗИ. К данной категории методов относятся идентификация, аутентификация и контроль доступа субъектов к информационным ресурсам. Современная методология характеризуется переходом от простых систем паролей к многофакторной аутентификации (MFA), биометрическим технологиям и внедрению концепции нулевого доверия («zero trust»).

Перспективные направления развития методологии обеспечения информационной безопасности:

1. Применение технологий искусственного интеллекта. Искусственный интеллект и системы, основанные на машинном обучении, анализируют закономерности поведения пользователей и сетевой трафик, выявляют аномалии, характерные для атак нулевого дня. Искусственный интеллект был интегрирован в системы SIEM и платформы для автоматизации процессов реагирования на инциденты. Разработка интеллектуальных систем обнаружения вторжений является приоритетным направлением научных исследований [3].

2. Защита облачных сред и распределенных систем

В рамках концепции цифрового суверенитета до 2030 года Беларусь стоит задача по снижению зависимости от зарубежных облачных провайдеров и развитию местной инфраструктуры. Миграция предприятий и организаций в облачную среду создает спрос на методы защиты, которые интегрируются непосредственно в цикл разработки программного обеспечения, что позволяет проверять безопасность кода на этапах его написания и компиляции [3].

Заключение

Таким образом, современная методология построения средств информационной безопасности в Республике Беларусь представляет собой сложную междисциплинарную область, интегрирующую достижения технических наук с императивными требованиями национального законодательства и регулирующих органов. Эффективность средств защиты информации определяется не только использованием передовых технологических решений, но и строгим соблюдением организационных процедур на всех этапах жизненного цикла системы, от моделирования угроз до сертификации ИТ-объекта. Перспективы развития методологии связаны с внедрением адаптивных самообучающихся систем, реализующих концепцию нулевого доверия и обеспечивающих информационный суверенитет государства.

Список использованных источников

1. Голиков В. Ф., Черная И. И., Зельманский О. Б. (2013) Разработка методологии информационной безопасности как основы создания и изучения защищенных информационных систем, 97–98.

2. Конявская С.В. (2013) К вопросу о классификации объектов защиты информации (3), 14–18.

3. Moller P. F. Dietmar, (2025) Cybersecurity for Network and Information Security : Principles, Techniques and Applications.

References

1. Golikov V. F., Chernaya I. I., Zelmansky O. B. (2013) Development of Information Security Methodology as a Basis for Creating and Studying Protected Information Systems, 97–98.

2. Konyavskaya S.V. (2013) Classification of Information Protection Objects (3), 14–18 (in Russian).

3. Moller P. F. Dietmar, (2025) Cybersecurity for Network and Information Security : Principles, Techniques and Applications.

Сведения об авторах

Гусаков П.Б., магистр, начальник цикла, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Макаренко К.Е., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», makarenkokirilka05@gmail.com.

Information about the authors

Gusakov P.B., Mast., head of the cycle, Educational Institution "Belarusian State University of Informatics and Radioelectronics".

Makaranka K.E., student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", makarenkokirilka05@gmail.com.