АКТУАЛЬНОСТЬ КИБЕРБЕЗОПАСНОСТИ В ГОСУДАРСТВЕННЫХ ОРГАНАХ, ПРИНЦИПЫ ЗАЩИТЫ

Комилов Мехриддин Маликович, Курсант 2 курса Бухарского Государственного Педагогического Института факультета Допризывной военной подготовки

Аннотация: В современном мире государственные органы всё в большей степени зависят от информационных систем и цифровых технологий, что делает их особенно уязвимыми к кибератакам. Нарушения безопасности данных, сбои в работе критической инфраструктуры и утрата доверия со стороны граждан — вот лишь некоторые из последствий слабой киберзащиты. Цель данной работы — проанализировать значимость кибербезопасности для государственных органов, выявить ключевые угрозы и разработать принципы эффективной защиты. В работе рассматриваются актуальные вызовы (такие как устаревшие системы, кадровый дефицит, сложности нормативно-правового регулирования), а также предлагаются такие принципы защиты, как многоуровневая защита, управление доступом, политика реагирования на инциденты и обеспечение устойчивости систем. Работа опирается на современные исследования и нормативные рамки в области кибербезопасности.

DAVLAT ORGANLARIDA KIBERXAVFSIZLIKNING DOLZARBLIGI, HIMOYA TAMOYILLARI

Komilov Mehriddin Malikovich, Buxoro Davlat Pedagogika Instituti Harbiy ta’lim fakulteti 2 bosqich kursanti

Annotatsiya: Zamonaviy dunyoda davlat organlari tobora ko‘proq axborot tizimlari va raqamli texnologiyalarga tayanadi, bu esa ularni kiberhujumlarga nisbatan ayniqsa zaif qiladi. Ma’lumotlarning xavfsizligi buzilishi, muhim infratuzilma faoliyatining izdan chiqishi va fuqarolar ishonchini yo‘qotish — zaif kiberhimoyaning ayrim oqibatlaridir. Ushbu ishning maqsadi — davlat organlari uchun kiberxavfsizlikning ahamiyatini tahlil qilish, asosiy tahdidlarni aniqlash va samarali himoya tamoyillarini ishlab chiqishdir. Tadqiqotda dolzarb muammolar (masalan, eskirgan tizimlar, kadrlar tanqisligi, normativ-huquqiy tartibga solishdagi qiyinchiliklar) ko‘rib chiqiladi, shuningdek, ko‘p darajali himoya, kirishni boshqarish, hodisalarga javob siyosati va tizimlarning barqarorligini ta’minlash kabi tamoyillar taklif etiladi. Ish kiberxavfsizlik sohasidagi zamonaviy tadqiqotlar va normativ asoslarga tayangan.

Kalit so‘zlar: Kiberxavfsizlik, davlat organlari, axborotni himoya qilish, raqamli infratuzilma, xavflarni boshqarish, normativ-huquqiy tartibga solish, ko‘p darajali himoya, hodisalarga javob berish.

RELEVANCE OF CYBERSECURITY IN GOVERNMENT AGENCIES, PRINCIPLES OF PROTECTION

Komilov Mehriddin Malikovich, 2nd-year Cadet of Bukhara State Pedagogical Institute, Faculty of Pre-Conscription Military Training

Abstract: In the modern world, government agencies increasingly depend on information systems and digital technologies, which makes them especially vulnerable to cyberattacks. Data breaches, failures in critical infrastructure, and the loss of public trust are just some of the consequences of weak cybersecurity. The purpose of this paper is to analyze the significance of cybersecurity for government agencies, identify key threats, and develop principles for effective protection. The study examines current challenges (such as outdated systems, staff shortages, and difficulties in regulatory frameworks), as well as proposes principles of protection such as multi-layered security, access management, incident response policies, and ensuring system resilience. The work is based on modern research and regulatory frameworks in the field of cybersecurity.

Keywords: Cybersecurity, government agencies, information protection, digital infrastructure, risk management, regulatory framework, multi-layered security, incident

response.

Введение: С развитием цифровых технологий государства всё активнее переводят службы и процессы в онлайн-формат: электронное управление, базы персональных данных, удалённый доступ сотрудников, Интернет вещей и пр. Это приводит к тому, что государственные органы становятся привлекательными мишенями для киберпреступников, иностранных разведывательных служб, хакеров, действия которых могут нанести серьёзный ущерб не только материальный, но и подорвать доверие граждан, нарушить функционирование критической инфраструктуры и национальную безопасность.

Цель исследования — выяснить, почему кибербезопасность является критически важной для государственных органов, какие угрозы существуют, и какие принципы защиты позволяют минимизировать риски.

Актуальность темы

1. Рост числа кибератак на публичный сектор

Государственные учреждения хранят большие объёмы чувствительной информации — персональных данных граждан, финансовую информацию, данные безопасности. Нарушения защиты данных приводят к утечкам, утрате репутации, финансам и могут стать инструментом давления или шантажа.

2. Критическая инфраструктура и её уязвимость

Инфраструктура, которой управляют государственные органы (энергетика, водоснабжение, транспорт, здравоохранение и др.), часто включает устаревшие системы (legacy systems), что делает их уязвимыми. Атаки на такие системы могут иметь масштабные негативные последствия.

3. Нормативно-правовое давление, требования прозрачности и ответственности

Законодательство многих стран требует от госучреждений соответствия стандартам защиты данных, обязательного уведомления о нарушениях, соблюдения прав граждан на личную жизнь. Несоблюдение приводит к юридическим последствиям.

4. Рост зависимости от цифровых сервисов

При сбоях в цифровых системах нарушается предоставление услуг населению, что прямо влияет на функционирование государства и доверие к власти. Необходимость непрерывности операций поднимает тему устойчивости и способности к восстановлению после инцидентов.

5. Кадровый дефицит и технологическое отставание

Государственные органы часто испытывают недостаток квалифицированных специалистов по кибербезопасности, а также используют устаревшее программное и аппаратное обеспечение, что снижает эффективность защиты.

Основные угрозы

Атаки программ-вымогателей (ransomware) — шифрование систем и требование выкупа.

Фишинг и социальная инженерия — методы, направленные на получение доступа через обман персонала.

Утечки персональных данных и шпионаж — государственные учреждения обладают информацией, которая может быть целью как внутреннего, так и внешнего неправомерного доступа.

Уязвимости устаревших систем — плохо обновляемое ПО, незащищённые интерфейсы, отсутствие поддержки производителей.

Внутренние угрозы — злоупотребления правами доступа, ошибки персонала.

Атаки на цепочки поставок (supply chain attacks) — когда компонент, поставляемый сторонним подрядчиком, содержит уязвимость или вредоносный код.

Принципы защиты

Для минимизации рисков и обеспечения устойчивости государственных органов к

киберугрозам можно рекомендовать следующие принципы защиты.

1. Управление рисками (Risk Management)
Выявление и классификация активов (информационных, системных).
Оценка угроз и уязвимостей.
Определение допустимого уровня риска и меры по его снижению.
2. Надёжная политика доступа и контроль прав пользователей
Принципы минимальных привилегий (least privilege).
Многофакторная аутентификация (MFA).
Отслеживание и аудит привилегированных действий.
3. Многоуровневая защита (Defense in Depth)
Защита на уровне сетей, приложений, конечных устройств.
Сегментация сети.
Защита периметра и внутренних зон.
4. Secure by Design и Secure by Default
Проектирование систем с учётом безопасности с самого начала.
Настройки по умолчанию должны быть безопасными.
5. Обеспечение надёжных поставщиков и управление цепочками поставок
Оценка безопасности поставщиков.
Контроль качества компонентов.
Сертификация, требования безопасности контракта.
6. Мониторинг, обнаружение и реагирование на инциденты
Внедрение систем обнаружения вторжений (IDS/IPS).
Логирование и анализ событий безопасности.
Наличие чётких процедур реагирования на инциденты (incident response plan).
7. Обучение персонала и развитие культуры безопасности
Регулярные тренинги по кибергигиене, по методам фишинга и социального инжиниринга.
Повышение осведомлённости о важности соблюдения политик безопасности.
8. Планирование непрерывности бизнеса и восстановление после инцидентов
Разработка процедур резервного копирования и восстановления данных.
Планы по обеспечению работы критических служб при нарушении основных систем.
9. Соответствие стандартам и нормативам, аудит
Использование признанных стандартов (например, NIST CSF, ISO/IEC 27001 и др.).
Проведение регулярных внешних и внутренних аудитов.
Оценка соответствия законодательству о защите персональных данных.
10. Прозрачность и отчётность
Политика обязательного уведомления о нарушениях.
Отчёты перед общественностью и руководство государственными органами о статусе кибербезопасности.

Практические рекомендации

Государственные органы должны внедрять целостные фреймворки безопасности, адаптированные к масштабу и специфике: например, государственные агенства могут применять NIST CSF или аналогичные национальные стандарты.

Обновление устаревших систем, переход на современные безопасные ОС и ПО.

Инвестиции в человеческий капитал: подготовка, найм специалистов, развитие навыков.

Межведомственное и частно-государственное сотрудничество: обмен информацией об угрозах, совместные учения, общие протоколы реагирования.

Законодательные инициативы: установление минимальных стандартов, ответственность, санкции за недопустимые нарушения, регулирование поставщиков.

Заключение

Актуальность кибербезопасности в государственных органах невозможно переоценить. Без надлежащих мер государственные учреждения рискуют не только материальным ущербом, но и угрожена их легитимность, национальная безопасность и доверие граждан. Реализация перечисленных принципов защиты позволяет смягчить риски, повысить устойчивость инфраструктуры и обеспечить надёжную работу сервисов населения. Государства, которые своевременно реагируют на вызовы киберугроз, адаптируют нормативно-правовую базу и внедряют осознанную стратегию безопасности, получают значительное преимущество в защите своих систем и данных.

Ссылки / литература

1. Data Security For Governments: Current Challenges And The Way Forward — Forbes Technology Council.

2. 6 Cybersecurity Challenges for Governments — WatchGuard.

3. Cybersecurity in government agencies: challenges and opportunities — Rocket.Chat Blog.

4. Cybersecurity principles — Cyber.gov.au framework.

5. Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight — U.S. GAO Report.

6. Top 10 cybersecurity risks in the public sector (2024) — SharkStriker guide.

7. Cybersecurity of Public Sector Institutions — Prawo i Więź (учебно-научная статья).

8. BSA International Cybersecurity Policy Framework — BSA Cybersecurity.

9. OmniDefend: Cybersecurity in Government: Best Practices for Protecting Public Infrastructure.