SCIENTIFIC CONFERENCE OPEN PROCEEDINGS
Global Academic Knowledge Repository

СОВРЕМЕННЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГОСУДАРСТВЕННЫХ ОРГАНОВ

Курбонова Фируза Зариповна

Доктор философии по техническим наукам, доцент, Академия Министерства внутренних дел Республики Узбекистан, Ташкент

https://doi.org/ 10.5281/zenodo.20960526

Аннотация: В статье рассматриваются современные подходы к обеспечению кибербезопасности в информационных системах государственных органов. В условиях активной цифровизации государственных услуг, развития электронного правительства и увеличения объёма обрабатываемых данных вопросы защиты информационных ресурсов становятся особенно актуальными.

Анализируются основные угрозы для государственных информационных систем, включая несанкционированный доступ, вредоносное программное обеспечение, DDoS-атаки, социальную инженерию и утечки данных. Особое внимание уделяется современным технологиям защиты: искусственному интеллекту, системам обнаружения и предотвращения вторжений, криптографической защите, многофакторной аутентификации и концепции Zero Trust.

Рассматриваются перспективы повышения устойчивости государственных информационных систем и совершенствования механизмов защиты критической информационной инфраструктуры.

Ключевые слова: кибербезопасность, государственные информационные системы, электронное правительство, защита данных, искусственный интеллект, информационная безопасность, цифровая инфраструктура.

Введение

В современном цифровом обществе информационные технологии играют важную роль в деятельности государственных органов. Развитие электронного правительства, цифровых сервисов и автоматизация административных процессов позволяют повысить эффективность государственного управления.

Государственные информационные системы используются для хранения и обработки большого количества важных данных:

- персональных данных граждан;

- государственных документов;
- финансовой информации;
- служебных материалов;
- данных критической инфраструктуры.

Однако расширение цифровой среды сопровождается увеличением числа киберугроз. Современные злоумышленники применяют сложные методы атак, направленные на получение доступа к информационным ресурсам, нарушение работы государственных сервисов и хищение конфиденциальной информации [2],[3].

Поэтому обеспечение надежной кибербезопасности государственных информационных систем становится одной из главных задач цифрового развития.

1. Основные угрозы информационным системам государственных органов

Государственные информационные системы являются привлекательной целью для злоумышленников из-за высокой ценности содержащейся в них информации[2].

Основными целями атак являются:

- получение конфиденциальных данных;
- нарушение работы государственных услуг;
- изменение или уничтожение информации;
- нарушение функционирования критической инфраструктуры.

1.1. Несанкционированный доступ к государственным информационным системам

Несанкционированный доступ является одной из наиболее распространённых угроз в сфере государственной информационной безопасности[2],[3].

Данная угроза возникает, когда злоумышленник получает возможность использовать информационную систему без соответствующего разрешения.

Основные способы получения доступа:

- подбор слабых паролей;
- кража учетных данных;
- использование уязвимостей программного обеспечения;
- заражение рабочих устройств вредоносными программами;
- применение методов социальной инженерии.

Особенно опасна компрометация учетных записей сотрудников государственных организаций. Получив доступ к аккаунту пользователя с

расширенными правами, злоумышленник может получить контроль над важными ресурсами [2],[3].

Последствиями таких атак могут быть:

- утечка персональных данных граждан;
- изменение официальной информации;
- нарушение работы государственных сервисов;
- раскрытие служебной информации.

Для предотвращения несанкционированного доступа применяются:

- многофакторная аутентификация;
- разграничение прав пользователей;
- биометрическая идентификация;
- контроль действий пользователей;
- системы анализа поведения.

Большое значение имеет принцип минимальных привилегий, при котором пользователь получает только необходимые права доступа.

1.2. Вредоносное программное обеспечение

Вредоносное программное обеспечение является одной из самых серьёзных угроз для государственных информационных систем[1],[3].

К основным видам вредоносных программ относятся:

Вирусы — программы, способные распространяться и изменять файлы системы.

Троянские программы — вредоносные приложения, скрывающиеся под видом обычного программного обеспечения.

Шпионские программы — используются для скрытого сбора информации.

Программы-вымогатели (Ransomware) — блокируют доступ к данным и требуют оплату за восстановление информации [5].

Для государственных органов атаки типа ransomware особенно опасны, поскольку могут привести к остановке важных цифровых сервисов.

Защита от вредоносного программного обеспечения включает:

- антивирусные решения нового поколения;
- постоянное обновление систем;
- резервное копирование;
- анализ поведения файлов;
- контроль сетевой активности.

1.3. DDoS-атаки

DDoS-атаки направлены на нарушение доступности государственных информационных ресурсов.

Во время атаки большое количество устройств одновременно отправляет запросы к одному серверу, что приводит к его перегрузке.

Основные последствия:

- недоступность государственных сайтов;
- нарушение работы электронных услуг;
- снижение доверия пользователей.

Для защиты используются:

- фильтрация сетевого трафика;
- системы распределения нагрузки;
- мониторинг активности;
- технологии искусственного интеллекта.

AI позволяет определить разницу между обычным пользовательским поведением и искусственно созданным вредоносным трафиком.

1.4. Социальная инженерия и фишинговые атаки

Человеческий фактор остаётся одной из наиболее распространённых причин успешных кибератак [6].

Социальная инженерия основана на психологическом воздействии на пользователей.

Злоумышленники используют:

- поддельные письма;
- фальшивые сайты;
- сообщения в социальных сетях;
- телефонные звонки.

Целью является получение:

- паролей;
- кодов подтверждения;
- служебной информации.

Для защиты необходимо:

- обучение сотрудников;
- повышение цифровой грамотности;
- использование фильтров электронной почты;
- применение многофакторной аутентификации.

2. Современные методы защиты государственных информационных

систем

Современная кибербезопасность требует комплексного подхода, включающего технические, организационные и интеллектуальные методы защиты[4].

2.1. Системы обнаружения и предотвращения вторжений (IDS/IPS)

IDS и IPS являются важными компонентами защиты государственных сетей.

IDS (Intrusion Detection System)

IDS предназначена для мониторинга активности в информационной системе.

Она анализирует:

- сетевой трафик;
- действия пользователей;
- системные журналы;
- работу приложений.

При обнаружении подозрительной активности система формирует предупреждение[3].

Примеры выявляемых угроз:

- попытки взлома;
- необычные подключения;
- сканирование портов;
- подозрительная передача данных.

IPS (Intrusion Prevention System)

IPS отличается от IDS тем, что способна самостоятельно реагировать на угрозы[3,4].

Она может:

- блокировать соединения;
- отключать подозрительные устройства;
- предотвращать атаки.

Современные IPS используют машинное обучение, что позволяет обнаруживать новые виды атак.

2.2. Искусственный интеллект в защите государственных систем

Искусственный интеллект становится одним из наиболее перспективных направлений развития кибербезопасности[4].

AI способен анализировать большие объёмы информации и находить скрытые угрозы.

Основные возможности AI:

- обнаружение аномального поведения;
- прогнозирование атак;
- автоматическое реагирование;
- анализ действий пользователей.

Например, система может определить:

- необычное место входа пользователя;
- массовое копирование файлов;
- подозрительное сетевое соединение.

Использование искусственного интеллекта позволяет значительно ускорить процесс обнаружения угроз[5].

2.3. Концепция Zero Trust

Современная модель Zero Trust основана на принципе:

«Никому не доверяй, всегда проверяй»

В традиционных системах пользователи внутри сети считались относительно безопасными.

Однако современные атаки показали, что угрозы могут исходить даже из внутренних систем.

Zero Trust предполагает:

- постоянную проверку пользователей;
- контроль устройств;
- ограничение доступа;
- минимальные права.

Преимущества:

- снижение риска утечки данных;
- защита от внутренних угроз;
- повышение уровня контроля.

2.4. Криптографическая защита информации

Криптография является основой защиты государственных данных.

Она обеспечивает:

Конфиденциальность - Информация доступна только уполномоченным лицам[7].

Целостность - Данные защищены от незаконного изменения.

Аутентификацию

Подтверждается личность пользователя.

Основные методы:

- шифрование данных;
- цифровые подписи;
- защищенные каналы связи.

Криптография используется при:

- электронном документообороте;
- работе государственных порталов;
- передаче конфиденциальной информации.

Заключение

Обеспечение кибербезопасности государственных информационных систем является важнейшим направлением развития цифрового государства.

Современные киберугрозы требуют применения новых подходов, включающих искусственный интеллект, IDS/IPS системы, криптографические методы, многофакторную аутентификацию и модель Zero Trust.

Однако технологии защиты должны постоянно совершенствоваться, так как методы атак также быстро развиваются.

Эффективная кибербезопасность возможна только при сочетании современных технических решений, квалифицированных специалистов и высокой культуры информационной безопасности.

REFERENCES

1. Stallings W. **Network Security Essentials: Applications and Standards.** Pearson, 2020.
2. Whitman M., Mattord H. **Principles of Information Security.** Cengage Learning, 2021.
3. National Institute of Standards and Technology. **Cybersecurity Framework.** https://www.nist.gov/cyberframework
4. International Organization for Standardization. **ISO/IEC 27001 Information Security Management Systems.** https://www.iso.org/
5. European Union Agency for Cybersecurity. **Cybersecurity Practices and Policies.** https://www.enisa.europa.eu/