Научная статья
Original article

Анализ технологий кибербезопасности в государственных учреждениях Казахстана

Бекмарзаев А.А.
Южно-Казахстанский университет имени Мухтара Ауэзова, Шымкент, Казахстан
Автор-корреспондент: mr-bekmarzayev@bk.ru

Аннотация: Учитывая растущую зависимость государственных учреждений от цифровых технологий и постоянное увеличение киберугроз, вопрос повышения кибербезопасности в государственных структурах Казахстана становится все более актуальным и требует детального исследования. В данной статье проводится анализ текущей практики использования технологий кибербезопасности в государственном секторе Казахстана. В статье обсуждается общепризнанная терминология и ключевые концепции кибербезопасности, представляется широкий обзор существующих технологий, их эффективности и применения в государственных учреждениях. Статья подробно рассматривает важные инциденты, связанные с кибербезопасностью, которые произошли в Казахстане, выявляет и анализирует слабые места и потенциальные угрозы в существующих системах кибербезопасности. В дополнение к этому, внимание уделяется поиску возможных путей улучшения текущего состояния кибербезопасности, предлагаются конкретные решения и технологии для повышения уровня защиты информации.

Ключевые слова: кибербезопасность, информационная безопасность, государственное управление, государство, Казахстан.

Для цитирования: Бекмарзаев А.А. Анализ технологий кибербезопасности в государственных учреждениях Казахстана. 2023. Т.3, №2, с. 90-96

Development of a methodology for teaching colloquial speech using the Internet

Bekmarzaev A.A.
South Kazakhstan University named after Mukhtar Auezov, Shymkent, Kazakhstan
Corresponding author: mr-bekmarzayev@bk.ru

Abstract: Considering the growing dependence of public institutions on digital technologies and the constant increase in cyber threats, the issue of increasing cybersecurity in the state structures of Kazakhstan is becoming increasingly relevant and requires detailed study. This article analyzes the current practice of using cybersecurity technologies in the public sector of Kazakhstan. The article discusses the commonly accepted terminology and key concepts of cybersecurity, provides a broad overview of existing technologies, their effectiveness and application in government institutions. The article examines in detail the important cybersecurity incidents that occurred in Kazakhstan, identifies and analyzes weaknesses and potential threats in existing cybersecurity systems. In addition to this, attention is paid to finding possible ways to improve the current state of cybersecurity, specific solutions and technologies are proposed to increase the level of information protection.

Keywords: cyber security, information security, public administration, state, Kazakhstan.

For citation: Bekmarzaev A.A. Analysis of cybersecurity technologies in public institutions of Kazakhstan. 2023. Vol. 3, №2, pp. 90-96

Введение

В современном мире, который все больше переходит в цифровую среду, вопрос кибербезопасности становится особенно острым. Киберугрозы становятся все более многообразными и сложными, и государственные учреждения, которые обычно управляют большим объемом ценной информации, становятся основной целью киберпреступников. Государственные учреждения Казахстана не исключение. Актуальность исследования определяется постоянным развитием цифровых технологий и их интеграцией в работу государственных органов. Все больше функций и сервисов переходит в цифровой формат. Это относится как к внутренним процессам, так и к взаимодействию с гражданами. Таким образом, уровень кибербезопасности напрямую влияет на эффективность работы государственных органов и качество предоставляемых услуг. По данным международных исследований, в последние годы наблюдается значительное увеличение числа кибератак, и этот тренд сохраняется. Следует отметить, что киберпреступления становятся все более сложными и изощренными, что требует постоянного усовершенствования систем кибербезопасности.

Стоит отметить, что кибератаки могут нанести серьезный ущерб как отдельным государственным учреждениям, так и государству в целом. В случае успешной кибератаки могут быть скомпрометированы персональные данные граждан, что подрывает доверие к государственным учреждениям и может привести к серьезным политическим последствиям. Кроме того, могут быть нарушены критически важные функции государственных органов, что может привести к серьезным последствиям в случае непредвиденных ситуаций. Таким образом, вопрос повышения уровня кибербезопасности в государственных учреждениях связан не только с оптимизацией внутренних процессов, но и с обеспечением безопасности граждан и стабильности государства в целом.

Параллельно с ростом киберугроз и развитием цифровых технологий, развиваются и технологии кибербезопасности. Существуют различные методы и инструменты, которые могут быть использованы для защиты от кибератак. Однако выбор оптимальных решений требует не только знания современных технологий, но и понимания специфики работы государственных органов и особенностей киберугроз, с которыми они сталкиваются.

Для выбора эффективных решений в области кибербезопасности необходимо провести анализ текущего состояния систем кибербезопасности в государственных учреждениях, выявить их слабые места и потенциальные угрозы. Кроме того, необходимо изучить современные технологии кибербезопасности и оценить возможность их использования в государственных органах. Все это делает актуальным исследование технологий кибербезопасности в государственных учреждениях Казахстана. Но проблема кибербезопасности актуальна не только для Казахстана, но и для многих других стран. Исследование этой проблемы может быть полезным не только для ученых и специалистов в области кибербезопасности, но и для руководителей государственных учреждений, а также

для законодателей, задача которых - создать надежные правовые рамки для обеспечения кибербезопасности.

Основные концепции и терминология

Для анализа технологий кибербезопасности, необходимо дать основную терминологию по информационной безопасности

Кибербезопасность — это мера защиты информационных систем от киберугроз, таких как вирусы, хакерские атаки, кража данных и прочие. Цель кибербезопасности - сохранить конфиденциальность, доступность и целостность информации, а также предотвратить ее несанкционированный доступ или утечку.

Киберугроза — это потенциальная возможность для нарушителя (хакера или киберпреступника) воспользоваться уязвимостями системы для нанесения ущерба или получения выгоды. Киберугрозы могут быть различного рода, от фишинга и DDoS-атак до сложных целенаправленных атак APT (Advanced Persistent Threats).

Система обнаружения вторжений (IDS) — это инструмент или программное обеспечение, которое мониторит сеть или систему на предмет подозрительной активности или нарушений политик безопасности.

Межсетевой экран или файерволл — это система безопасности, которая контролирует входящий и исходящий сетевой трафик на основе заданных правил безопасности.

Шифрование — это процесс преобразования информации в код с целью предотвратить несанкционированный доступ к данным. Шифрование широко используется для защиты данных во время передачи или хранения.

Государственные учреждения используют широкий спектр технологий кибербезопасности для обеспечения защиты своих информационных систем.

Межсетевые экраны устанавливаются для контроля входящего и исходящего трафика, а также для блокировки потенциально вредоносных активностей. Файерволы могут быть как аппаратными, так и программными, и они служат первой линией обороны против кибератак.

Системы обнаружения вторжений и системы предотвращения вторжений (IPS) используются для мониторинга сети и системы на предмет лю бой подозрительной активности и для блокировки такой активности. Эти системы используются для обнаружения широкого спектра угроз, включая сканирование портов, DDoS-атаки, вирусы и другие вредоносные программы.

Антивирусное программное обеспечение также является важной частью стратегии кибербезопасности. Эти программы сканируют системы на наличие известных вредоносных программ и блокируют их. Многие из них также имеют функции обнаружения и блокировки вредоносного поведения, что позволяет им обнаруживать и блокировать неизвестные вредоносные программы.

Шифрование используется для обеспечения конфиденциальности данных во время их передачи или хранения. Шифрование может использоваться для защиты всех видов данных, от электронной почты до персональных данных граждан. Для управления ключами шифрования и сертификатами часто используются системы управления ключами и системы PKI (Public Key Infrastructure).

В государственных учреждениях также широко используются технологии управления доступом, такие как системы управления идентификацией и доступом (IAM). Эти системы управляют тем, кто и когда может получить доступ к определенным ресурсам. Для противодействия киберугрозам используются технологии SIEM (Security Information and Event Management). Эти системы собирают и анализируют данные из разных источников с целью обнаружения, мониторинга и отчетности о киберугрозах. Для управления рисками и соответствия требованиям законодательства и стандартов используются технологии управления рисками и соответствия требованиям (GRC).

Обзор состояния кибербезопасности в государственных учреждениях Казахстана

Политика кибербезопасности в государственных учреждениях Казахстана основывается на ряде законодательных и регулятивных документов. Основными из них являются "Закон Республики Казахстан о кибербезопасности" и "Государственная программа кибербезопасности Казахстана". Эти документы определяют основные принципы и подходы к обеспечению кибербезопасности, а также устанавливают требования к организации защиты информации в информационных системах государственных органов.

Согласно этим документам, государственные органы обязаны разрабатывать и реализовывать меры по обеспечению кибербезопасности, включая разработку и внедрение политики безопасности, проведение регулярных оценок безопасности и аудита, обучение персонала, использование современных технологий кибербезопасности и т.д.

В Казахстане также приняты ряд стандартов в области кибербезопасности, которые дополняют законодательство и содержат конкретные требования и рекомендации по обеспечению кибербезопасности.

Государственные учреждения Казахстана активно используют различные технологии кибербезопасности. Основными из них являются антивирусное программное обеспечение, межсетевые экраны, системы обнаружения вторжений и системы управления идентификацией и доступом. Кроме того, наблюдается активное использование технологий облачных вычислений и виртуализации, что также требует особого подхода к обеспечению кибербезопасности. Также следует отметить, что внедрение и использование технологий кибербезопасности сопровождаются рядом проблем и вызовов. Среди них - ограниченные ресурсы, недостаток квалифицированных специалистов, сложности внедрения и интеграции различных решений, а также риск кибератак и угроз.

В последние годы в Казахстане произошло несколько значимых инцидентов, связанных с кибербезопасностью. Одним из них была крупномасштабная кибератака на государственные информационные системы, которая привела к значительным нарушениям их работы. Этот инцидент подчеркнул важность и необходимость обеспечения кибербезопасности и привел к пересмотру и усилению мер по обеспечению кибербезопасности.

Кроме того, были зафиксированы случаи утечки данных, включая персональные данные граждан, из некоторых государственных учреждений. Эти инциденты подчеркнули важность защиты данных и необходимость использования современных технологий кибербезопасности, включая шифрование и управление доступом.

Учитывая постоянно усиливающуюся угрозу кибератак и утечек данных, государственным учреждениям Казахстана следует уделить особое внимание развитию и усовершенствованию своих систем и мер кибербезопасности. Также необходимо продолжать работу над развитием национальной политики и стратегии в области кибербезопасности, включая законодательное регулирование, стандарты, обучение и повышение осведомленности общественности о важности кибербезопасности.

Идентификация слабых мест и возможных угроз

Применение технологий кибербезопасности в государственных учреждениях Казахстана достаточно обширно, однако эффективность их использования варьируется. Антивирусные программы, межсетевые экраны, системы обнаружения вторжений и системы управления идентификацией и доступом — это основные инструменты, которыми обладают учреждения для защиты своих информационных систем. Однако, регулярные киберинциденты, включая утечки данных и нарушения работы систем, указывают на то, что эффективность применения этих технологий может быть неадекватной.

Одним из основных слабых мест систем кибербезопасности государственных учреждений Казахстана является недостаточное обучение персонала. Сотрудники организаций часто не обладают необходимыми знаниями и навыками для эффективного использования технологий кибербезопасности, что увеличивает риск кибератак.

Также стоит отметить недостаток квалифицированных специалистов в области кибербезопасности, что затрудняет разработку и внедрение новых решений, а также регулярное обновление и настройку существующих систем.

Среди возможных угроз следует выделить растущую активность киберпреступников, увеличение сложности и хитроумности методов атак, а также использование новейших технологий, таких как искусственный интеллект и квантовые компью теры, для обхода систем защиты.

Также следует учесть возможные угрозы в связи с активным использованием облачных технологий и виртуализации, которые требуют специального подхода к обеспечению кибербезопасности.

Для усовершенствования систем кибербезопасности государственных учреждений Казахстана возможно использование ряда современных технологий и подходов.

В частности, активное использование технологий искусственного интеллекта и машинного обучения может значительно улучшить эффективность обнаружения и предотвращения кибератак. Эти технологии могут анализировать большое количество данных и быстро находить аномалии, указывающие на возможные угрозы.

Также возможно использование технологии блокчейн для обеспечения безопасности транзакций и защиты данных. Блокчейн может обеспечить высокий уровень защиты от подделки и несанкционированного доступа.

Важное значение имеет и улучшение процесса обучения персонала. Сотрудники должны не только обладать навыками работы с технологиями кибербезопасности, но и понимать актуальные угрозы и методы их предотвращения. В этом могут помочь специализированные обучающие программы и курсы.

Кроме того, следует продолжать разработку и внедрение национальных стандартов и политики в области кибербезопасности, включая регулярный мониторинг и аудит систем кибербезопасности, а также создание координационных центров для реагирования на инциденты кибербезопасности.

В целом, обеспечение кибербезопасности требует комплексного подхода, включающего использование современных технологий, обучение персонала, разработку и внедрение эффективной политики и стандартов, а также сотрудничество с другими странами и международными организациями.

Выводы

В рамках данного исследования был проведен анализ технологий кибербезопасности в государственных учреждениях Казахстана. Важность этого исследования обусловлена увеличивающейся активностью киберугроз и необходимостью адаптации и совершенствования системы кибербезопасности в соответствии с этими изменениями. Исследование позволило установить, что основными инструментами кибербезопасности, применяемыми в государственных учреждениях Казахстана, являются антивирусные программы, межсетевые экраны, системы обнаружения вторжений и системы управления идентификацией и доступом. Однако, несмотря на их использование, регулярно происходят киберинциденты, что указывает на недостаточную эффективность этих мер.

Идентифицированные в ходе исследования слабые места в системе кибербезопасности включают недостаточное обучение персонала и отсутствие квалифицированных специалистов. Основные угрозы связаны с растущей активностью киберпреступников и использованием ими новейших технологий для обхода систем защиты. Для усовершенствования системы кибербезопасности предложены следующие направления: активное использование искусственного интеллекта и машинного обучения, использование технологии блокчейна, улучшение процесса обучения персонала, разработка и внедрение национальных стандартов и политики в области кибербезопасности.

Очевидно, что проблема кибербезопасности в государственных учреждениях Казахстана требует дальнейшего исследования. Возможные направления для будущих исследований могут включать более глубокий анализ специфических угроз и технологий кибербезопасности, а также изучение вопросов внедрения и использования искусственного интеллекта и машинного обучения в системах кибербезопасности. Кроме того, может быть полезно изучение международного опыта в области кибербезопасности и возможности его применения в Казахстане.

В заключение следует отметить, что кибербезопасность в государственных учреждениях Казахстана — это сложная и многогранная проблема, требующая комплексного и системного подхода. Данное исследование является важным шагом на пути к созданию эффективной системы кибербезопасности, однако многие аспекты этой проблемы еще предстоит исследовать и преодолеть.

Список литературы

1. Андреев, С. А. Методы защиты пользователей в сети Интернет: темные паттерны / С. А. Андреев, Д. М. Назаров // BI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики : Материалы X Международной научно-практической очно-заочной конференции, Екатеринбург, 02 декабря 2022 года / Ответственные за выпуск: А.Ю. Коковихин, Д.М. Назаров, ответственный редактор: С.В. Бегичев. – Екатеринбург: Уральский государственный экономический университет, 2023. – С. 3-6. – EDN PRNDDC.
2. Гаськова, Д. А. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры / Д. А. Гаськова, А. Г. Массель // Вопросы кибербезопасности. – 2019. – № 2(30). – С. 42-49. – DOI 10.21681/2311-3456-2019-2-42-49. – EDN HJXBPF.
3. Жарова, А. К. Концепция проектируемой конфиденциальности для обеспечения безопасности персональных данных / А. К. Жарова // Информационное право. – 2021. – № 3. – С. 27-30. – EDN JDCKOT.
4. Кряжевских, К. А. Противодействие угрозам информационной безопасности в цифровой среде / К. А. Кряжевских // Умная цифровая экономика. – 2022. – Т. 2, № 1. – С. 37-40. – EDN LPSOMM.
5. Лобач, Д. В. Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам / Д. В. Лобач, Е. А. Смирнова // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2019. – Т. 11, № 4. – С. 23-32. – DOI 10.24866/VVSU/2073-3984/2019-4/023-032. – EDN YNKQEY.
6. Метельков, А. Н. Киберучения: зарубежный опыт защиты критической инфраструктуры / А. Н. Метельков // Правовая информатика. – 2022. – № 1. – С. 51-60. – DOI 10.21681/1994-1404-2022-1-51-60. – EDN NMTEXO.
7. Ромашкина, Н. П. Стратегические риски и проблемы кибербезопасности / Н. П. Ромашкина, Д. В. Стефанович // Вопросы кибербезопасности. – 2020. – № 5(39). – С. 77-86. – DOI 10.21681/2311-3456-2020-05-77-86. – EDN TYCIVU.
8. Сейткулов Е. Критический анализ технологических решений в области обеспечения кибербезопасности сотовых сетей / Е. Сейткулов, Н. Ташатов, Б. Ергалиева [и др.] // Вестник Казахской академии транспорта и коммуникаций им. М. Тынышпаева. – 2023. – Т. 124, № 1. – С. 222-229. – DOI 10.52167/1609-1817-2023-124-1-222-229. – EDN XPLZPS.
9. Туркин, В. А. Оценка рисков эксплуатации судовых технических средств с учетом возможности возникновения киберинцидентов / В. А. Туркин, Д. А. Давыдов, А. А. Стяжкин // Морские интеллектуальные технологии. – 2021. – № 2-4(52). – С. 58-66. – DOI 10.37220/MIT.2021.52.2.070. – EDN NKZIEN.