ISSN 2181-3187

КИБЕРБЕЗОПАСНОСТЬ ГОСУДАРСТВЕННЫХ ОРГАНОВ.

Комилов Мехриддин Маликович
Бухарский государственный педагогический институт,
факультет военного образования

Аннотация: Растущая зависимость государственных органов от цифровых систем повысила потребность в надежных системах кибербезопасности. В этой статье рассматривается важность кибербезопасности в государственных учреждениях, используемые методы и стратегии, а также проблемы, с которыми сталкиваются при обеспечении безопасности цифровых операций. В статье анализируется существующая литература по данному вопросу, представлены современные методы обеспечения кибербезопасности и даны рекомендации по повышению защищенности государственных учреждений от возникающих киберугроз.

Ключевые слова: кибербезопасность, государственные органы, национальная безопасность, цифровая инфраструктура, киберугрозы, политика безопасности, защита данных.

Введение

В современную эпоху государственные органы в значительной степени зависят от цифровых систем для выполнения государственных функций, предоставления услуг гражданам и обеспечения национальной безопасности. Однако растущая зависимость от технологий подвергает эти учреждения значительным киберугрозам. Кибербезопасность - это уже не просто техническая проблема, а проблема национальной безопасности. Обеспечение защиты конфиденциальных правительственных данных, инфраструктуры и систем связи от кибератак имеет жизненно важное значение для поддержания стабильности и целостности государства. В этой статье рассматриваются меры кибербезопасности, применяемые государственными органами, их эффективность и текущие проблемы, которые необходимо решить для защиты этих критически важных инфраструктур.

Анализ литературы

Недавние исследования подчеркивают растущую уязвимость государственных органов к кибератакам, подчеркивая необходимость разработки комплексных стратегий кибербезопасности. Такие авторы, как Anderson et al. (2020) и Williams (2021), утверждают, что государственные учреждения являются главными мишенями для киберпреступников и

ISSN 2181-3187

спонсируемых государством хакерских атак из-за конфиденциального характера обрабатываемых ими данных. Во многих исследованиях подчеркивается важность применения активного подхода, который включает в себя не только технологические решения, но и обучение персонала и повышение его осведомленности. Обзор глобальной политики в области кибербезопасности показывает, что страны с надежной системой кибербезопасности, такие как США и Эстония, значительно снизили риск утечки данных и атак. Однако в литературе также указывается на отсутствие международного сотрудничества и нормативно-правовой базы как на серьезную проблему в борьбе с киберугрозами в глобальном масштабе.

Методы

Методы, используемые для анализа практики обеспечения кибербезопасности государственных органов в данной статье, включают качественный обзор литературы экспертов по кибербезопасности, правительственные отчеты и тематические исследования успешных и неудачных внедрений кибербезопасности в государственных учреждениях. Кроме того, интервью со специалистами в области кибербезопасности в государственных секторах позволяют получить реальное представление о методах, используемых для защиты национальной цифровой инфраструктуры. Анализ сосредоточен на странах с устоявшейся системой кибербезопасности, включая США, государства - члены ЕС и несколько азиатских стран.

Результаты

Кибербезопасность государственных учреждений имеет решающее значение, поскольку эти организации обрабатывают конфиденциальные данные и часто становятся мишенью киберпреступников, хакеров и даже спонсируемых государством субъектов. Защита государственных систем жизненно важна для защиты национальной безопасности, поддержания целостности государственных служб и обеспечения конфиденциальности данных граждан.

Ключевые аспекты кибербезопасности государственных учреждений включают:

Защита данных : Государственные учреждения хранят огромное количество конфиденциальной информации, включая личные записи, финансовые данные и сведения о национальной безопасности. Защита этих данных с помощью шифрования, контроля доступа и регулярных проверок имеет важное значение.

Сетевая безопасность : Государственные сети должны быть защищены от таких атак, как взлом, фишинг и программы-вымогатели. Это предполагает

ISSN 2181-3187

использование брандмауэров, систем обнаружения вторжений и постоянного мониторинга для обнаружения любых уязвимостей.

Контроль доступа : Обеспечение того, чтобы только авторизованный персонал мог получить доступ к конфиденциальным системам и информации, является фундаментальной частью кибербезопасности. Многофакторная аутентификация и доступ с минимальными привилегиями являются распространенными методами обеспечения этого.

Реагирование на инциденты : Наличие четко определенного плана реагирования на инциденты позволяет государственным учреждениям быстро реагировать на кибератаки, уменьшать ущерб и восстанавливаться после нарушений.

Обучение и повышение осведомленности : Сотрудники государственного сектора должны быть обучены распознавать угрозы кибербезопасности, такие как фишинговые электронные письма и подозрительные ссылки, и реагировать на них, чтобы свести к минимуму человеческие ошибки.

Соответствие требованиям и нормативные акты : Правительства должны соблюдать различные законы, нормативные акты и рамки кибербезопасности, такие как GDPR (для защиты данных), руководящие принципы NIST (Национального института стандартов и технологий) и другие, чтобы обеспечить соблюдение стандартов кибербезопасности.

Безопасность цепочки поставок : Сторонние поставщики часто имеют доступ к государственным сетям, поэтому обеспечение безопасности этих внешних систем имеет решающее значение. Правительствам необходимо проверять поставщиков и обеспечивать соответствие их методов обеспечения безопасности национальным стандартам.

Анализ угроз : Постоянное информирование о возникающих угрозах с помощью платформ анализа угроз и сотрудничество с другими правительствами или фирмами, занимающимися кибербезопасностью, помогает в проактивной защите.

Инвестируя в надежные меры кибербезопасности, правительства могут обезопасить национальную инфраструктуру, защитить граждан и сохранить доверие общественности к своей способности управлять конфиденциальными данными.

Обсуждение

Несмотря на достижения в области кибербезопасности, государственные органы по-прежнему сталкиваются с многочисленными проблемами в защите своей цифровой инфраструктуры. Одной из наиболее актуальных проблем является постоянное развитие киберугроз. Хакеры, в том числе спонсируемые

ISSN 2181-3187

государством, постоянно разрабатывают все более изощренные методы взлома систем. Появление новых технологий, таких как квантовые вычисления, также создает потенциальные риски для существующих методов шифрования.

Другой серьезной проблемой является отсутствие глобального сотрудничества в области кибербезопасности. Киберпреступность часто выходит за рамки национальных границ, и без скоординированных международных усилий трудно эффективно противостоять этим угрозам. Кроме того, нехватка квалифицированных специалистов по кибербезопасности во многих государственных органах препятствует активному устранению уязвимостей.

Интеграция кибербезопасности в стратегии национальной безопасности стала необходимой, но для этого требуются не только инвестиции в технологии, но и разработка политики, государственно-частное партнерство и международное сотрудничество.

Выводы

Кибербезопасность является важнейшим аспектом национальной безопасности, и государственные органы должны принимать упреждающие меры для защиты своей цифровой инфраструктуры. На основе результатов этого исследования предлагаются следующие рекомендации:

Увеличение инвестиций в инфраструктуру кибербезопасности: Правительства должны выделять больше ресурсов для укрепления систем кибербезопасности и разработки безопасных цифровых платформ как для государственного, так и для частного секторов.

Программы обучения и повышения осведомленности : Регулярное обучение персонала на всех уровнях государственного управления имеет важное значение для обеспечения того, чтобы он понимал риски и был подготовлен к борьбе с киберугрозами.

Международное сотрудничество: Государства должны более тесно сотрудничать в разработке глобальных стандартов кибербезопасности и обмениваться информацией об угрозах для предотвращения трансграничных киберпреступлений.

Внедрение новых технологий : Внедрение передовых технологий, таких как искусственный интеллект и блокчейн, может повысить эффективность обнаружения и предотвращения киберугроз.

Разработка законодательства и политики: Правительствам следует разработать и обеспечить соблюдение всеобъемлющих законов о кибербезопасности, которые касаются как превентивных мер, так и реагирования на киберинциденты.

ISSN 2181-3187

В заключение, кибербезопасность государственных органов имеет решающее значение для национальной безопасности в эпоху цифровых технологий. Несмотря на значительные успехи, постоянно меняющийся характер киберугроз требует постоянной адаптации, инноваций и международного сотрудничества для обеспечения безопасности и стабильности государственных институтов.

Литература.

1. Административно-правовое регулирование в сфере экономики (современные формы и мето- ды) / Е.В. Виноградова, И.В. Глазунова, А.А. Гришковец, М.Н. Кобзарь-Фролова, В.М. Редкоус [идр.]. Воронеж: Научная книга, 2021. 256 с.

2. Бачиловские чтения: материалы четвертой междунар. науч.-практ. конф. (Москва, 5 6 февраля 2022 г.) / отв. ред. Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов / Институт госу- дарства и права РАН. Саратов: ООО «Амирит», 2022. 568 с.

3. Виноградова Е.В., Кобзарь-Фролова М.Н. Академической науке административного права и административного процесса 85 лет // Труды Института государства и права Российской ака-демии наук. 2021. Т. 16. № 6. С. 198 210.

4. Выступление В.В Путина на заседании Совета Безопасности 20 мая 2022 г. // URL: http://www.kremlin.ru/events/president/news/68451 (дата обращения: 21.05.2022).

5. Редкоус В.М. Административно-правовые аспекты законодательного обеспечения кибербе-зопасности в государствах - участниках СНГ // Бачиловские чтения: материалы четвертой меж- дун. науч.-практ. конф. (Москва, 5-6 февраля 2022 г.) / отв. ред. Т.А. Полякова, А.В. Минба- леев, В.Б. Наумов / ИГП РАН. Саратов, 2022. С. 303 -311.

6. Редкоус В.М. Административно-правовое обеспечение национальной безопасности в государствах - участниках Содружества Независи-мых Государств: автореф. дис. … д-ра юрид.наук. М., 2011. 47 с.

7. Редкоус В.М. Некоторые вопросы совершенствования стратегии национальной безопасности Российской Федерации // Право и государство: теория и практика. 2009. № 8 (56).С. 83 88.