КИБЕРБЕЗОПАСНОСТЬ КАК ОСНОВНОЙ ФАКТОР НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Дыбаль С.А.
Научный руководитель: ст.преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Современный мир сталкивается с многообразными угрозами кибербезопасности. В Республике Беларусь они также представляют серьезную опасность для национальной безопасности, экономики, гражданского общества и личности. К основным видам угроз относятся:

- Кибератаки на государственные информационные системы и инфраструктуру. Это могут быть попытки кражи конфиденциальной информации, нарушения работы государственных служб, дестабилизации политической ситуации.
- Киберпреступность, включая кражу персональных данных, мошенничество, шантаж, распространение вредоносного ПО.
- Кибершпионаж, направленный на получение информации о государственных секретах, военных технологиях, экономической деятельности.
- Пропаганда и дезинформация, распространяемые через интернет, социальные сети, средства массовой информации. Это может быть направлено на подрыв общественного порядка, манипулирование общественным мнением, разжигание межнациональных конфликтов. [2]

Угрозы могут поступать из различных хакерских групп и от отдельных киберпреступников, мотивированных финансовой выгодой, государственных структур других стран, осуществляющих кибершпионаж, пропаганду, дестабилизацию.

Также некоторые недобросовестные сотрудники государственных и коммерческих организаций допускают утечку информации, что приравнивается к мошенничеству.

Основными документами, которые регулируют обеспечение кибербезопасности в Республике Беларусь являютя Конституция Республики Беларусь, Закон Республики Беларусь "Об информации, информатизации и защите информации", Закон Республики Беларусь "О защите персональных данных, Закон Республики Беларусь "О критической информационной инфраструктуре".

Ключевую роль в обеспечении кибербезопасности играют такие государственные органы, как:

– Государственный комитет по информатизации отвечает за разработку и реализацию государственной политики в сфере информатизации, обеспечивает функционирование государственных информационных систем, занимается сертификацией средств защиты информации.

– Министерство внутренних дел (МВД) осуществляет правоохранительную деятельность в сфере киберпреступности, проводит расследование киберпреступлений, борется с кибертерроризмом.

– Комитет государственного контроля (КГК) контролирует деятельность государственных органов и организаций в сфере информатизации, предотвращает коррупционные нарушения, связанные с информационными технологиями.

– Служба безопасности Президента Республики Беларусь (СБ) обеспечивает информационную безопасность государства, проводит разведку и контрразведку в сфере информационных технологий, борется с кибершпионажем.

– Министерство обороны Республики Беларусь отвечает за киберзащиту военных объектов, информационных систем и систем связи.

Все эти органы координируются Советом Министров Республики Беларусь.

Кроме того, в обеспечении кибербезопасности принимают участие другие государственные органы, например, Министерство образования, Министерство здравоохранения, Национальный банк Республики Беларусь. Взаимодействие между этими органами имеет ключевое значение для эффективного противодействия киберугрозам. [1]

В Республике Беларусь функционирует многоуровневая система мониторинга и реагирования на кибератаки, включающая в себя:

– Системы мониторинга киберугроз: используются для сбора и анализа информации о киберактивах, обнаружения признаков кибератак, прогнозирования потенциальных угроз.

– Центры реагирования на инциденты информационной безопасности (CERT): отвечают за оперативное реагирование на кибератаки, информирование о киберугрозах, предоставление консультационной помощи по обеспечению кибербезопасности.

– Системы выявления и блокировки вредоносных программ: предназначены для обнаружения, изоляции и нейтрализации вредоносного ПО, защиты от вирусных атак.

– Системы контроля доступа и аутентификации: обеспечивают защиту информационных ресурсов от несанкционированного доступа, идентифицируют пользователей и проверяют их права доступа.

Кроме того, государство активно проводит информационно-пропагандистскую работу по повышению киберграмотности населения, обучению навыкам безопасного поведения в интернет-пространстве.

Защита критической инфраструктуры от кибератак

Критическая инфраструктура представляет собой комплекс объектов и систем, которые играют ключевую роль в обеспечении жизнедеятельности государства и общества в целом. В Республике Беларусь к критической инфраструктуре относятся не только энергетическая система, транспортные сети, связь, финансовые учреждения и здравоохранение, но и такие важные элементы, как

управление воздушным движением, системы водоснабжения и канализации, а также учреждения, обеспечивающие безопасность и правопорядок. Нарушение работы этих систем может привести к серьезным последствиям, включая угрозу безопасности, экономическим потерям и дестабилизации общественной жизни.

Защита критической инфраструктуры от кибератак становится особенно актуальной в условиях современного мира, где киберугрозы постоянно эволюционируют и становятся все более сложными. В Беларуси для обеспечения безопасности этих объектов и систем принимаются комплексные меры. Во-первых, разрабатываются и внедряются стандарты информационной безопасности, которые учитывают специфические риски и угрозы, характерные для каждого сектора критической инфраструктуры. Это включает в себя создание четких протоколов реагирования на инциденты и регулярное обновление программного обеспечения.[1]

Во-вторых, проводятся регулярные аудиты и тестирования систем безопасности, что позволяет выявлять уязвимости и оперативно их устранять. Эти мероприятия помогают не только поддерживать высокий уровень безопасности, но и повышать общий уровень осведомленности о киберугрозах среди сотрудников.

Обучение персонала является еще одной важной составляющей кибербезопасности. Специалисты проходят тренинги, на которых знакомятся с актуальными методами защиты информации, а также с новейшими киберугрозами. Это позволяет не только улучшить навыки работы с информационными системами, но и формировать культуру безопасности в организациях.

Кроме того, создаются резервные системы и планы восстановления, которые позволяют минимизировать последствия в случае кибератаки. Эти планы включают в себя не только технические решения, но и организационные меры, такие как распределение ролей и обязанностей в кризисных ситуациях.

Взаимодействие с международными организациями также играет важную роль в обеспечении кибербезопасности. Беларусь активно участвует в обмене информацией и опытом с другими странами, что позволяет адаптировать лучшие практики и технологии для защиты своей критической инфраструктуры. Это сотрудничество включает в себя участие в международных учениях и конференциях, что способствует повышению квалификации специалистов и укреплению международных связей в области киберзащиты.

Таким образом, комплексный подход к защите критической инфраструктуры в Беларуси включает в себя разработку стандартов, регулярные проверки, обучение персонала, создание резервных систем и международное сотрудничество. Это позволяет не только обеспечивать безопасность ключевых объектов, но и повышать устойчивость государства к киберугрозам в целом.[2]

Беларусь активно наращивает усилия по обеспечению национальной кибербезопасности, понимая её критическую роль в поддержании стабильности государства и функционировании критически важной инфраструктуры. Ключевым

направлением является создание единого центра мониторинга и реагирования на кибератаки. Этот центр, помимо сбора и анализа информации о киберугрозах в режиме реального времени, будет играть роль координационного узла, объединяющего усилия различных государственных органов, предприятий критической инфраструктуры и частного сектора. Планируется, что центр будет оснащен передовыми технологиями анализа данных, искусственным интеллектом для выявления аномалий и прогнозирования угроз, а также системой быстрого реагирования на инциденты, позволяющей минимизировать ущерб от кибератак. Его создание требует значительных инвестиций в высококвалифицированные кадры, современное оборудование и программное обеспечение, а также тесную интеграцию с международными партнерами для обмена разведданными.

Международное сотрудничество является неотъемлемой частью белорусской стратегии кибербезопасности. Активно развиваются двусторонние отношения с рядом стран, в рамках которых проводятся обмены опытом, совместные тренировки и разработка соглашений о взаимной помощи в случае кибератак. Особое внимание уделяется сотрудничеству в рамках Организации Договора о коллективной безопасности (ОДКБ). В рамках ОДКБ проводятся масштабные совместные учения, симулирующие различные сценарии кибератак на объекты критической инфраструктуры, государственные органы и финансовые институты. Эти учения позволяют отработать взаимодействие между различными службами безопасности государств-членов, совершенствовать методы обнаружения и реагирования на угрозы, а также обмениваться актуальной информацией о новых типах вредоносных программ и тактиках киберпреступников. Кроме того, в рамках ОДКБ разрабатываются общие стандарты кибербезопасности, правовые основы сотрудничества и механизмы взаимной поддержки.

Беларусь активно участвует в деятельности международных организаций, таких как Международный телекоммуникационный союз (МТСС), Международный союз электросвязи (МСЭ), а также в работе специализированных комитетов ООН и других международных форумов по кибербезопасности. Это позволяет не только быть в курсе последних тенденций в области киберугроз и лучших мировых практик, но и вносить свой вклад в разработку международных стандартов и норм в сфере кибербезопасности. Участие в таких организациях способствует обмену опытом с ведущими экспертами мирового уровня, содействует развитию национальной нормативно-правовой базы и позволяет получать доступ к передовым технологиям и решениям в области защиты от киберугроз.[3]

Однако, перед Беларусью стоят серьезные вызовы. Быстрое развитие искусственного интеллекта, расширение использования Интернета вещей (IoT) и появление новых, более изощренных методов кибератак, таких как атаки с использованием квантовых компьютеров и целенаправленные атаки на основе искусственного интеллекта (AI-driven attacks), требуют постоянного совершенствова-

ния стратегии кибербезопасности. Необходимо постоянно адаптироваться к изменяющейся глобальной обстановке, учитывая растущую роль киберпространства в геополитических процессах и потенциальные угрозы со стороны государственных и негосударственных акторов. Это требует значительных инвестиций в научные исследования и разработки в области кибербезопасности, постоянное повышение квалификации специалистов и внедрение современных технологий защиты информации. [4]

Развитие национальной системы кибербезопасности требует комплексного подхода, охватывающего правовые, организационные, технические и кадровые аспекты, чтобы обеспечить непрерывную защиту критически важной инфраструктуры и национального цифрового суверенитета. В частности, важно уделять внимание кибергигиене населения и повышению уровня киберграмотности, чтобы минимизировать риски, связанные с человеческим фактором.Государство проводит активную политику по обеспечению кибербезопасности, развивает систему мониторинга и реагирования на кибератаки, защищает критическую инфраструктуру, подготавливает кадры в этой области, укрепляет международное сотрудничество. Однако перед Республикой Беларусь стоят серьезные вызовы, связанные с развитием информационных технологий, появлением новых угроз, усложнением кибератак. Поэтому необходимо постоянно усовершенствовать систему кибербезопасности, адаптируя ее к изменяющимся условиям. [1]

Я считаю, что в будущем кибербезопасность будет играть еще более важную роль в обеспечении безопасности и развития Республики Беларусь. От ее эффективности зависит не только защита от киберугроз, но и использование цифровых технологий для достижения экономического и социального прогресса страны.

Литература

1. Что такое кибербезопасность? [Электронный ресурс] – Режим доступа:https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security. – Дата доступа: 03.11.2022.

2. Кибербезопасность[Электронный ресурс] - Режим доступа: https://www.mpt.gov.by/ru/kiberbezopasnost

3. Кибербезопасность [Электронный ресурс] – Режим доступа: http://digitalbusiness.by/napravleniya-sotrudnichestva/natsionalnyj-bank-respubliki-belarus/kiberbezopasnost.– Дата доступа: 03.11.2022.

4. Важность обеспечения кибербезопасности [Электронный ресурс] – Режим доступа: https://spravochnick.ru/informacionnaya_bezopasnost/kiberbezopasnost_i_informacionnaya_bezopasnost/. – Дата доступа: 03.11.2022.