ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ ВООРУЖЕННЫХ СИЛ. РАЗРАБОТКА И РЕАЛИЗАЦИЯ КОМПЛЕКСНОЙ СТРАТЕГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Хрипач Н.А.

Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь

Дудак М. Н. – магистр тех. Наук

Аннотация. Данный доклад посвящен обсуждению мер, которые необходимо реализовать для обеспечения защиты информационных ресурсов в войсках связи Вооруженных Сил Республики Беларусь от кибератак и других угроз безопасности. Рассмотрение данной темы позволит определить основные проблемы и слабые места в системах безопасности войск связи, а также предложить рекомендации по усовершенствованию существующих механизмов защиты.

С развитием информационных технологий и сетевых технологий в последние годы угрозы безопасности в информационной сфере становятся все более серьезными. Войска связи Вооруженных Сил Республики Беларусь, как и любые другие организации, подвергаются угрозам кибербезопасности, которые могут иметь негативное влияние на их работу и деятельность.

Защита информационных ресурсов от кибератак и других угроз безопасности является одной из важнейших задач в области кибербезопасности. Критические объекты, такие как войска связи Вооруженных Сил Республики Беларусь, требуют особого внимания в вопросах обеспечения их кибербезопасности.

Задача обеспечения защиты информационных ресурсов в войсках связи Вооруженных Сил Республики Беларусь от кибератак и других угроз безопасности является одной из ключевых проблем в области кибербезопасности [1].

Современные информационные технологии позволяют быстро и эффективно обрабатывать огромные объемы информации. Однако, это также открывает возможности для киберпреступников, которые могут использовать различные способы для получения несанкционированного доступа к информации, в том числе через войска связи.

Войска связи Вооруженных Сил Республики Беларусь имеют важное значение для обеспечения связи между военными и цивилизованными учреждениями, а также для связи между различными частями вооруженных сил. Поэтому, защита информационных ресурсов войск связи от кибератак и других угроз безопасности является ключевой задачей для обеспечения эффективности и безопасности их работы.

Основными угрозами для войск связи являются кибератаки, вирусы, трояны, фишинговые атаки, а также атаки на инфраструктуру связи. Кроме того, многие угрозы могут появиться изнутри организации, включая несанкционированный доступ к информации со стороны сотрудников и подрядчиков, несоблюдение правил безопасности, ошибки в процессе обработки информации и другие.

В настоящее время, во многих странах, включая Республику Беларусь, существует система защиты информационных ресурсов, которая включает в себя меры по предотвращению и обнаружению кибератак и других угроз. Однако, такие меры защиты не всегда эффективны и требуют дальнейшего усовершенствования.

Одним из основных способов обеспечения защиты информационных ресурсов в войсках связи является использование современных технологий кибербезопасности, включая программное и аппаратное [2].

Кроме того, важным элементом защиты информационных ресурсов в войсках связи является разработка и внедрение соответствующих стандартов и правил использования информационных систем и сетей. Это включает в себя установку средств защиты, таких как антивирусные программы, межсетевые экраны и системы обнаружения вторжений, а также контроль доступа и аутентификацию пользователей.

Кроме того, не менее важным является регулярное обновление и модернизация информационных систем и сетей. Это позволяет улучшать их защиту и приспосабливать к новым видам угроз. Важно также обучать персонал военной связи использованию информационных систем и сетей, а также правилам информационной безопасности, чтобы минимизировать ошибки и уязвимости, возникающие из-за неопытности или небрежности пользователей.

Однако, защита информационных ресурсов в войсках связи является более сложной задачей, чем просто установка антивирусного программного обеспечения или межсетевого экрана. Во-первых, военная связь имеет свои специфические особенности, например, большой объем информации, передаваемой в режиме реального времени, и необходимость быстрого реагирования на изменения в боевой обстановке. Во-вторых, военная связь подвергается более высоким угрозам, чем другие

организации, так как она играет ключевую роль в обеспечении боеспособности Вооруженных Сил Республики Беларусь.

Таким образом, для обеспечения защиты информационных ресурсов в войсках связи Вооруженных Сил Республики Беларусь от кибератак и других угроз безопасности необходимо использовать комплексный подход, который включает в себя как технические, так и организационные меры [3]. Это включает в себя не только установку антивирусного программного обеспечения и межсетевых экранов, но и разработку и внедрение соответствующих стандартов и правил использования информационных систем и сетей, а также обучение персонала военной связи.

Другой распространенной угрозой безопасности являются фишинговые атаки, которые часто используются для получения доступа к конфиденциальной информации. Фишинговые атаки могут быть выполнены путем отправки электронных писем, которые кажутся легитимными, но на самом деле являются поддельными и предназначены для получения доступа к информации, такой как логины, пароли или банковские данные. Чтобы защититься от фишинга, сотрудники войск связи должны быть обучены узнавать поддельные электронные письма и никогда не предоставлять личную информацию в ответ на такие письма.

С другой стороны, кибератаки могут быть проведены также с использованием вредоносных программ, таких как вирусы, трояны или черви. Эти программы могут проникнуть в информационную систему, чтобы украсть данные, вывести из строя систему или использовать ее в качестве платформы для других кибератак. Чтобы предотвратить атаки с использованием вредоносных программ, сотрудники войск связи должны использовать антивирусное программное обеспечение и обновлять его регулярно.

Помимо этого, войска связи могут стать жертвами кибершпионажа. Кибершпионы могут использовать различные методы, такие как перехват трафика, кража логинов и паролей, и другие, для получения доступа к конфиденциальной информации. Чтобы защититься от кибершпионажа, необходимо использовать шифрование данных, а также установить меры контроля доступа к конфиденциальной информации.

Одним из ключевых моментов в обеспечении безопасности информационных ресурсов является правильная организация процесса управления безопасностью. Войска связи должны иметь четкие процедуры и политики в отношении безопасности информации, которые должны строго соблюдаться всеми сотрудниками. Кроме того, необходимо проводить регулярную аудиторию информационных систем для выявления уязвимостей и устранения их вовремя.

Также важным моментом является контроль за доступом к информационным ресурсам военной связи. Военнослужащим следует выделять доступ к конкретным данным в соответствии с их должностными обязанностями и уровнем допуска. Это позволит уменьшить риски утечки конфиденциальной информации, а также предотвратить нежелательный доступ к данным со стороны третьих лиц.

Одним из наиболее эффективных способов защиты информационных ресурсов войск связи является использование специализированного программного обеспечения [4]. Такое ПО позволяет обнаруживать кибератаки и другие угрозы безопасности, блокировать подозрительный трафик, а также принимать меры по восстановлению работоспособности системы в случае атаки.

Но необходимо понимать, что технические средства не могут полностью защитить информационные ресурсы от кибератак. Поэтому решающим фактором становится обучение и профессиональная подготовка военнослужащих, ответственных за обеспечение безопасности информационных ресурсов. Только обученный персонал сможет быстро и эффективно реагировать на киберугрозы и предотвратить их негативные последствия.

Важно отметить, что задача обеспечения безопасности информационных ресурсов военной связи является многоплановой и требует комплексного подхода. Для достижения максимальной эффективности необходимо сочетать технические и организационные меры, включая контроль за доступом к информационным ресурсам, обучение и профессиональную подготовку военнослужащих, а также использование специализированного программного обеспечения.

Таким образом, обеспечение защиты информационных ресурсов в войсках связи Вооруженных Сил Республики Беларусь от кибератак и других угроз безопасности является важной задачей, требующей постоянного внимания и усилий. Необходимо развивать средства защиты информационных ресурсов и повышать квалификацию

Список использованных источников:

1. А. А. Минаев, А. А. Колесников, В. М. Гершман. Обеспечение безопасности информационных систем вооруженных сил. Материалы VII Международной научно-технической конференции "Информационная безопасность и защита информации", 2016.

2. М. М. Левин. Информационная безопасность в военном строительстве. Электронное научное издание "Вестник Южно-Уральского государственного университета", 2015.

3. И. А. Смирнов, В. Г. Кравцов. Комплексный подход к защите информации в военных организациях. Материалы конференции "Информационная безопасность в телекоммуникационных системах", 2017.

4. А. С. Поляков. Информационная безопасность в вооруженных силах. Материалы конференции "Актуальные проблемы информационной безопасности в современном мире", 2018.