УДК 004.056:654

АКТУАЛЬНОСТЬ ПОДГОТОВКИ ВОЕННЫХ СПЕЦИАЛИСТОВ ПО СПЕЦИАЛЬНОСТИ «ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИЯХ»

ХОЖЕВЕЦ О.А., ХОРУЖИЙ А.А.

Белорусский государственный университет информатики и радиоэлектроники

Аннотация. Рассмотрена актуальность подготовки военных специалистов по специальности «Защита информации в телекоммуникациях», актуальность защиты информации в телекоммуникациях.

Ключевые слова: защита информации, телекоммуникации, подготовка специалистов, актуальность подготовки, педагогика, образование, военное образование.

Основой инфокоммуникационных технологий являются системы телекоммуникаций, которые представляют собой сложные аппаратнопрограммные комплексы и используются в организации национальных и международных транспортных сетей телекоммуникаций, сетей беспроводной и мобильной связи, систем и средств цифрового радиовещания и телевидения, спутниковых систем связи и навигации.

В настоящее время в области телекоммуникаций происходят значительные изменения, связанные с разработкой и совершенствованием технологий информационной безопасности (электронная цифровая подпись, инфраструктура идентификации, защита сетевых протоколов, антивирусная защита, фильтрация содержания и многое другое). [1]

Острота проблемы обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более возрастает. Этому есть целый ряд объективных причин.

Прежде всего - это расширение сферы применения средств вычислительной техники и возросший уровень доверия к автоматизированным системам управления и обработки информации. Компьютерным системам доверяют самую ответственную работу, от качества выполнения которой зависит жизнь и благосостояние многих людей. ЭВМ управляют технологическими процессами на предприятиях и атомных электростанциях, управляют движением самолетов и поездов, выполняют финансовые операции, обрабатывают секретную и конфиденциальную информацию.

Для информационно-коммуникационных сетей составной и неотъемлемой частью обеспечения их защищенности является сбалансированность интересов потребителей, операторов и органов государственного управления. Развиваются службы, основным видом деятельности которых на предприятиях, учреждениях и офисах является обеспечение безопасности, которая реализуется различными методами и средствами, в том числе с применением конкретной аппаратуры, компьютерных программ, технических, организационно-правовых и методологических средств. Особая актуальность подготовки военных специалистов данного профиля связана с совершенствованием систем электронной коммерции и развитием современных платежных систем.

Актуальность вопросов защиты информации в телекоммуникациях особенно возросла в настоящее время в связи со стремительным повышением роли и значения информации в развитии современного общества вообще и в экономике в частности. Информация в настоящее время стала стержнем развития экономики. В ведущих индустриальных странах мира большая часть служащих занята обработкой информации

Информационная безопасность компании, общественной организации или производственного предприятия – это комплекс мероприятий, направленных на предотвращение несанкционированного доступа к внутренней IT-инфраструктуре, незаконного завладения конфиденциальной информацией и внесения изменений в базы данных. Цель обеспечения информационной безопасности – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения. Учитывая важность информации в современном мире, защите от утечек конфиденциальной информации необходимо уделять повышенное внимание. Возможный ущерб может быть намного больше, чем стоимость всех материальных активов предприятия.

Актуальность проблемы защиты информационных технологий в современных условиях определяется следующими основными факторами:

− обострением противоречий между объективно существующими потребностями общества в расширении свободного обмена информацией и чрезмерными или наоборот недостаточными ограничениями на ее распространение и использование

− расширением сферы использования ЭВМ, многообразием и повсеместным распространением информационно-управляющих систем, высокими темпами увеличения парка средств вычислительной техники и связи

− повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности

− вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей, наличием интенсивного обмена информацией между участниками этого процесса

− концентрацией больших объемов информации различного назначения и принадлежности на электронных носителях

− количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам

− отношением к информации, как к товару, переходом к рыночным отношениям в области предоставления информационных услуг с присущей им конкуренцией и промышленным шпионажем

− многообразием видов угроз и возникновением новых возможных каналов несанкционированного доступа к информации

− ростом числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими нежелательных программно-математических воздействий на системы обработки информации

− увеличением потерь (ущерба) от уничтожения, фальсификации, разглашения или незаконного тиражирования информации (возрастанием уязвимости различных затрагиваемых субъектов)

− развитием рыночных отношений (в области разработки, поставки, обслуживания вычислительной техники, разработки программных средств, в том числе средств защиты). [2]

Уровень информационной безопасности зависит в первую очередь от защищенности каналов, по которым сведения из информационной базы компании могут попасть в сеть Интернет. Специально разрабатываемые программные средства способны перекрыть эти каналы и снизить риск утечки, похищения или несанкционированного доступа к информации. Растущий уровень угроз приводит к необходимости подготовки специалистов по защите информации в телекоммуникациях. [3]

Задача специалистов по защите информации – обеспечение защиты средств электросвязи сетей электросвязи от несанкционированного доступа к ним путем применения программных, технических и криптографических средств защиты информации. Вид данной трудовой деятельности включает в себя следующие базовые направления:

− эксплуатация защищенных ИКС, а также методов и средств обеспечения их безопасности;

− администрирование и эксплуатация аппаратно-программных средств защиты информации в ИКС;

− разработка и применение методов оценки уровня безопасности ИКС по заданному критерию; аттестация объектов информатизации;

− проектирование и разработка специальных технических и программно-алгоритмических средств защиты информации ИКС.

Актуальность угроз целостности и конфиденциальности информации требует внимательного отношения к задаче ее защиты. 20 лет назад задача обеспечения безопасности информации решалась при помощи средств криптографической защиты, установления межсетевых экранов, разграничения доступа. Сейчас этих технологий недостаточно, любая информация, имеющая финансовую, конкурентную, военную или политическую ценность, подвергается угрозе. Дополнительным риском становится возможность перехвата управления критическими объектами информационной инфраструктуры.

Информационная безопасность вооруженных сил как важнейшего государственного института является и гарантией безопасности самого государства. Защита информационных ресурсов войск должна стать приоритетной задачей для специалистов по безопасности. Таким образом, подготовка специалистов по специальности «Защита информации в телекоммуникациях» является актуальной задачей в настоящее время.

Список источников:

1. Информационные технологии: учебник / Ю. Ю. Громов [и др.]. – Тамбов: ФГБОУ ВПО «ТГТУ», 2015. – 260 с.

2. Проект профстандарта “Разработка, техническая эксплуатация и управление средствами и системами защиты инфокоммуникационных систем от несанкционированного доступа к ним” [Электронный ресурс]. – Режим доступа: https://www.mpt.gov.by/sites/default/files/profstantart_noyabr.doc.

3. Дедович Д.К., Евдокименко М.Н., Микулик Т.Н., Николаенко В.Л., Сечко Г.В. Повышение производственной безопасности учреждений образования и науки за счет использования служебных гаджетов // Межд.науч.-техн. сборник «Теоретическая и прикладная механика». 2019. Вып. 34. С. 291–295.