Proceedings of International Conference on Scientific Research in Natural and Social Sciences
Hosted online from Toronto, Canada.
Date: 5th February, 2024
ISSN: 2835-5326 **Website:** econferenceseries.com

ВОПРОС ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ИХ РОЛЬ В ЗАЩИТЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ А ТАКЖЕ КЛЮЧЕВЫЕ ПРОБЛЕМЫ, СВЯЗАННЫЕ С УСИЛЕНИЕМ ИХ ВЛИЯНИЯ В МИРЕ

Рахимов Алихан Исломович

АННОТАЦИЯ

Результаты анализа развития информационных технологий выявили проблемы, порождающие угрозы национальной безопасности в различных сферах жизнедеятельности государства. Показаны противоречия между ростом объема применений информационных технологий хозяйствующими субъектами и достижением приемлемого уровня их информационной безопасности. Приведены возможные пути инновационного развития средств и технологий обеспечения информационной безопасности средствами базовых защитных установок.

Ключевые слова: информационные технологии, информационные угрозы, информационная структура, базовые защитные установки.

В ходе эволюции информационных технологий и инфраструктуры, приобретающих глобальный трансграничный характер, возникают негативные процессы, порождающие угрозы национальной безопасности государства в экономической, оборонной, информационной и других сферах. Показано, что эффективное применение информационных технологий во всех сферах деятельности личности, общества и государства, являющееся фактором ускорения экономического развития и формирования информационного общества, в значительной мере ограничивается возможностями средств обеспечения информационной безопасности, их экстенсивным развитием, обуславливающим значительное технологическое отставание от инноваций в сфере информационных технологий.

Существующий автократический контроль системы обеспечения информационной безопасности приводит к неизбежному снижению

эффективности инновационной деятельности в сфере информационных технологий.

В ряду сложных проблем, сопровождающих процессы реформирования социально-экономической политики Российской Федерации, первостепенное значение в последние годы приобрели вопросы национальной безопасности в информационной сфере. В связи с этим в Доктрине информационной безопасности Российской Федерации отмечено, что основные информационные угрозы, вызванные глобализацией и трансграничностью информационных технологий и инфраструктуры, обусловлены (см. рис. 1):

• возможностями информационно-технического воздействия зарубежных стран на информационную инфраструктуру в военных целях;

• деятельностью организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса;

• использованием информационных технологий для информационно-психологического воздействия на население с целью дестабилизации социальной и внутриполитической ситуации, нагнетания межнациональной напряженности;

• ростом масштабов преступности в кредитнофинансовой сфере;

• увеличением числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина в части неприкосновенности частной жизни, личной и семейной тайны;

• невозможностью реализовать совместное справедливое, основанное на принципах доверия, управление ресурсами, необходимыми для обеспечения безопасного и устойчивого функционирования сети «Интернет». Преодоление и предупреждение перечисленных угроз предполагает:

• совершенствование системы обеспечения информационной безопасности; • инновационное развитие отрасли информационных технологий;

• ликвидацию зависимости отечественной промышленности от зарубежных информационных технологий;

• создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия. Решение перечисленных задач служит достижению национальных интересов в информационной сфере, и прежде

всего — обеспечению устойчивого и бесперебойного функционирования информационной инфраструктуры России. Но не скрыто ли здесь противоречие между желанием эффективно использовать информационные технологии для экономического развития и формирования информационного общества, увеличением в этой связи информационных потребностей должностных лиц органов управления (субъектов хозяйствования), и возможностями средств обеспечения информационной безопасности, которым свойственно технологическое отставание? Для ответа на этот непростой вопрос необходимо рассмотреть основные признаки эволюции информационных технологий, информационной инфраструктуры и средств обеспечения информационной безопасности, связать основные понятия, характеризующие данные признаки, в концептуальные схемы.

Развитие инфокоммуникаций в XXI веке происходит настолько интенсивно, что принято говорить об информационной научно-технической революции, результатом которой является ряд качественных изменений в общественных отношениях. На удовлетворение растущих в условиях сокращения циклов управления потребностей должностных лиц в информационных услугах ориентируется все больше и больше отраслей и сфер экономики. Одновременно существует и обратная тенденция: под воздействием технологий меняются формы экономической деятельности и общественных отношений.

Основой «взрывного» развития элементов информационной инфраструктуры являются достижения «высоких» технологий в областях сверхвысокой очистки материалов, сверхточного формирования элементов интегральных микросхем и внедрение высокотехнологичных компонентов в технические средства, составляющие информационную инфраструктуру. Общим свойством «высоких» технологий является их критическая зависимость друг от друга, приводящая к распространению процессов интеграции и конвергенции. Путем взаимопроникновения и поглощения происходит интеграция процессов электросвязи, устройств, сетей и служб. Взаимосвязь основных тенденций и факторов, определяющих развитие систем и сетей связи, составляющих материальную основу информационной инфраструктуры, представлена на рис.

Под воздействием развития «высоких» технологий и роста информационных потребностей потребителей информационных услуг сокращается жизненный цикл технических решений — информационных технологий, и возрастает ассортимент информационных услуг. Основой информационных услуг становится программное обеспечение, устанавливаемое в терминальные устройства абонентов, и специальные «интеллектуальные» сети, предназначенные для облегчения реализации новых услуг.

В результате интеграции связи и информационных технологий отрасль «связь» оказалась способной оказывать непосредственно информационные услуги, образуя инфокоммуникационную инфраструктуру общества, доводя в перспективе транспортные потоки непосредственно до потребителя услуг. Собственники информации выступают господствующей социальной группой общества, получившего наименование «глобального информационного общества». Участие любого государства в процессах глобализации необходимо для сохранения его статуса, приобретения и сохранения требуемых темпов экономического развития, получения своей доли во всемирном производстве и рынках сбыта. С другой стороны, стремительное совершенствование методов целенаправленного воздействия на информационные процессы и системы управления противоборствующих сторон способно не только повлиять на складывающийся в мире стратегический баланс сил, но и изменять ныне существующие критерии оценки такого баланса на основе соотношения геополитических, экономических и военных факторов.

Системы управления позволяют реализовать в течение часов политические решения, с которыми согласен лишь очень узкий круг лиц, а число людей, локальные действия которых могут иметь глобальные последствия (операторы АЭС, химического комплекса, финансовые структуры, террористы и экстремисты), резко увеличилось. Коридор того, что может позволить себе человечество, не рискуя вызвать глобальные катастрофические изменения, очень невелик: интегрированные распределенные (глобальные и трансграничные) информационные технологии и инфраструктуры (см. рис. 3) обладают широким ассортиментом особенностей, не присущих ныне архаичным выделенным (локализованным) системам связи и АСУ.

Злоумышленник, осуществляющий некоторую совокупность деструктивных воздействий из всего арсенала доступных ему средств, стремится влиять на качество решений, принимаемых оппонентом.

Для этого он реализует действия, которые можно условно расположить в диапазоне от перехвата управления информационной системой (взятия ее под свой контроль) до перевода ее в неисправное состояние (так называемый «отказ в обслуживании»). Последняя фаза всегда очевидна для защищающейся стороны и далеко не всегда выгодна для злоумышленника, так как он, во-первых, компрометирует свои действия, и, во-вторых, сам теряет связь с объектом воздействия. В любом случае обязательным условием для реализации планов злоумышленника является возможность мониторинга состояния объекта защиты. Такой мониторинг можно определить, как процесс, направленный на добывание информации о составе, структуре, алгоритмах функционирования, местоположении и принадлежности информационной системы (технологии), а также данных, хранимых, обрабатываемых и передаваемых в ней.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Доктрина информационной безопасности Российской Федерации. Утверждена указом Президента Российской Федерации от 5 дек. 2016 г. № 646//Российская газета. 6 декабря 2016 г.
2. И. А. Мамзелев и др. Основы сертификации и построения оборудования телекоммуникаций/Под ред. И. А. Мамзелева, Л. В. Юрасовой. М.: Радио и связь, 2005. 304 с.
3. М. Кастельс. Галактика Интернет: Размышления об Интернете, бизнесе и обществе/Пер. с англ. А. Матвеева; под ред. В. Харитонова. Екатеринбург: У-Фактория (при участии Гуманитарного ун-та). 2004. 328 с.
4. В. П. Шейнов. Скрытое управление человеком. М.: Изд-во Харвест, 2007. 816 с.