УДК 340

РОЛЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОБЕСПЕЧЕНИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Романова Дарья Сергеевна
студент 4 курса
Южно-Уральский государственный университет
(Национально-исследовательский университет)
(Россия, г. Челябинск)

Поскольку информационные технологии широко используются в бизнесе, политике и национальном развитии, они стали привлекательной целью для хакерских атак, а также очень мощным инструментом, который может угрожать национальной безопасности государства.

В этой статье рассматривается вопрос информационных технологий и их роль в обеспечении и защите национальной безопасности, а также ключевые проблемы, связанные с усилением их влияния в мире.

Ключевые слова: информационные технологии, национальная безопасность, информационная безопасность, информационное пространство

THE ROLE OF INFORMATION TECHNOLOGIES IN THE PROVISION OF NATIONAL SECURITY

Romanova Daria Sergeevna
4-year student
South Ural State University (national research university)
(Russia, Chelyabinsk)

As information technologies are widely used in business, politics and national development, they have become an attractive target for hacker attacks; as well as a very powerful tool that can threaten the national security of the state.

This article addresses the issue of information technology and their role in ensuring and protecting national security, as well as key issues related to enhancing their influence in the world.

Key words: information technology, national security, information security, information space

В информатизации общества проблема обеспечения национальной безопасности не только сохраняется, но и приобретает ряд новых особенностей, связанных с возрастанием роли информации в обществе. Информационные технологии могут, как обеспечивать стабильность и безопасность, так и угрожать этим двумя компонентам. С одной стороны, информационные технологии можно использовать для распространения и обмена идеями и стратегиями в области безопасности, для организации помощи в миротворческих миссиях, а также для осуществления и координации планов и операций по обеспечению безопасности. Они являются важной составляющей всех государственных операций по обеспечению безопасности, от сбора разведывательной информации до командования и контроля. Однако, с другой стороны, информационные технологии могут быть использованы таким образом, чтобы угрожать стабильности и безопасности государства. Противник может уничтожить коммуникационные системы при помощи физического оружия (бомбы, ракеты) и электромагнитного оружия (ЭМО); использовать средства массовой информации (СМИ) для распространения лжи по всему миру; а также проникнуть или атаковать компьютерные сети с целью получения секретной информации или повреждения данных и систем.

Глобальное использование информационных технологий, с одной стороны, приводит к зависимости национальной безопасности государства от защищенности информационной инфраструктуры. С другой стороны, решающее значение для национальной безопасности имеет уровень развития информационной инфраструктуры, который должен обеспечивать эффективность проведения

государственной политики (обеспечение органов государственной власти полной и достоверной информацией; обеспечение современных информационных отношений в сфере бизнеса; реализация эффективного механизма включения информационного ресурса в хозяйственный оборот; обеспечение прав граждан на информацию и др.).

Основам национальной информационной безопасности посвящен ряд документов, разработанных Советом Безопасности РФ при помощи экспертного сообщества и утвержденных указами президента. Доктрины, концепции, стратегии рассматривают различные аспекты современной цифровой действительности, новые угрозы, меры противодействия им и направления активности государства, усиливающего свои геополитические позиции.

Национальная информационная безопасность является комплексным понятием, по-разному раскрываемым в различных публичных документах, учебных пособиях, статьях экспертов. Она не ограничивается только информационной безопасностью государства, его органов, сфер обороны и внутренней политики.

Доктрина информационной безопасности рассматривает в качестве объекта защиты сбалансированные интересы личности, общества и государства. Без охраны информационных интересов личности и гражданина невозможно восприятие государства как субъекта общественного договора и носителя суверенитета, без которого невозможна защита граждан. Также внутри понятия находится и защита информационной инфраструктуры, осуществляемая программными, физическими и техническими средствами, обеспечение безопасности научных разработок и ноу-хау.

Таким образом, под национальной безопасностью в цифровом пространстве, включающей обеспечение информационной безопасности личности, общества, государства и инфраструктуры, понимается состояние защищенности информационной среды, гарантирующей соблюдение прав и

законных интересов личности, общества и государства в информационной сфере, когда полностью обеспечиваются их защита, реализация и возможности развития вне зависимости от количества и качества внутренних и внешних угроз.

Доктрина информационной безопасности 2016 года дополняет, что в ситуации, когда национальная безопасность в сфере информации обеспечена, создается общество, в котором: происходит беспрепятственная и полная реализация конституционных прав человека; обеспечивается высокий уровень жизни; охраняется суверенитет, территориальная целостность и интенсивное экономическое развитие; угрозы обороне и безопасности государства своевременно и полностью отражаются.

В основе национальной информационной безопасности находятся технические, программные и научные ресурсы, которые, с одной стороны, сами являются объектом защиты, с другой стороны, обеспечивают безопасность. Увеличение мощности этого ресурса становится одной из основных задач государства в цифровую эру.

За последние несколько десятилетий мир полностью изменился, и большинство коммуникаций, финансовых трансакций, информационных архивов попали в Интернет. Это увеличило их доступность для третьих лиц по сравнению с эпохой только материальных носителей, и, соответственно, вместе с доступностью повысилась и уязвимость.

Интересы личности и общества, выражающиеся в сохранности информации или в защите от деструктивного информационного воздействия, постоянно подвергаются угрозам, в основе которых лежит не только коммерческий, но и психологический или идеологический интерес.

Интересы государств в области информационной безопасности, в свою очередь, также находятся под ударом не только хакерских группировок, но и отдельных государств. Доктрина информационной безопасности, принятая в 2016 году, в числе угроз называет стремление отдельных государств

доминировать в международном информационном поле. Это выражается не только в систематическом снижении значения международных организаций, в том числе в непризнании значимости принимаемых ими документов международного права в области информационной безопасности, но и в конкретных действиях.

Информационные технологии сегодня приобрели глобальный трансграничный характер, что создает невозможность как их регулирования на национальном уровне, так и безошибочного выявления источников угроз.

Система информационных угроз существенно изменилась за последние годы. Помимо хакерских группировок и террористических организаций, а также традиционно противоборствующих иностранных разведывательных организаций, генерировать угрозы начали экстремистские организации и деструктивные секты, часто также направляемые службами разведки. Угрозы усилились, участились попытки перехвата управления объектами критической инфраструктуры, посягательства на государственные информационные ресурсы и сети. Самостоятельной проблемой стали действия, направленные на подрыв авторитета России на международной арене.

Обеспечение национальной информационной безопасности возлагается на следующие службы и организации: Совет Безопасности РФ; Министерство обороны; органы внутренней безопасности; государственные органы, устанавливающие стандарты в области защиты информации, безопасности информационных потоков; бизнес; научные организации; гражданское общество.

Все участники процессов обеспечения информационной национальной безопасности в цифровом мире должны работать во взаимодействии, чувствуя потребности друг друга и изменение конъюнктуры. За общее планирование и стратегию отвечают Совет Безопасности и президент, которому

руководитель ведомства регулярно докладывает обстановку в области национальной безопасности.

Единый процесс обеспечения информационной безопасности представляет собой непрерывное и взаимосвязанное применение превентивных, защитных и направленных на усиление позиции мер следующего характера: технических; организационных; производимых в сфере ОРД; аналитических; пропагандистских; международно-правовых; кадровых; финансово-экономических; разведывательных.

Все меры должны быть направлены на снижение уровня угроз, прогнозирование новых рисков, отражение нападений, ликвидацию их последствий, наращивание технического, идеологического и информационного потенциала, обеспечение информационной безопасности Российской Федерации, граждан и общества.

Таким образом, особенностью современного общества является рост влияния информации и информационных технологий на все сферы жизни, а также перемещение центра борьбы в информационную область. Информация и информационные технологии становятся все более распространенными, мобильными и уязвимыми. Поэтому проблема обеспечения национальной безопасности в условиях информатизации общества становится еще более актуальной.

Список литературы

1. Гафнер В.В. Информационная безопасность / В.В. Гафнер. - М.: Феникс, 2017. - 336 с.

2. Казарин О.В., Скиба В.Ю., Шаряпов Р.А. Новые разновидности угроз международной информационной безопасности // Вестник РГГУ. Серия «Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность». 2016. № 1(3). С. 54–72.

3. Кузина С.И., Мякинченко Д.А. Информационное насилие: аспекты национальной безопасности // Государственное и муниципальное управление. Ученые записки СКАГС. 2015. № 3. С. 205–209.

4. Сивоволов Д.Л. Новые угрозы национальному суверенитету России в сфере национальной безопасности // Социум и власть. 2015. № 6(56). С. 82–88.

5. Чугунова К.Ю. Информационное оружие как угроза национальной безопасности Российской Федерации // Актуальные проблемы российского права. 2015. № 7(56). С. 59–64.

6. Шаньгин В.Ф. Информационная безопасность и защита информации / Шаньгин В.Ф. - М.: ДМК Пресс, 2017. - 195 с.

© Романова Д.С., 2020