2. Dabholkar P. A. Consumer evaluations of new technology-based self-service options: An inves- tigation of alterantive models of service quality // International Journal of Research in Marketing. 1996. Vol. 13. P. 28–51.
3. Bateson J. E. G. Self-Service Consumer: An Exploratory Study // Journal of Retailing. 1985. Vol. 61. P. 49–76.
4. Evans K. R., Brown S. W. Strategic options for service delivery systems // Ingene C. A., Frazier G. L. Proceedings of the AMA Summer educators' conference. Chicago, 1988. P. 207–212.

УДК 35

В.Э. Василевская
Академия управления при Президенте Республики Беларусь,
Минск, Республика Беларусь

КИБЕРБЕЗОПАСНОСТЬ КАК ВЕДУЩЕЕ НАПРАВЛЕНИЕ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ

Аннотация. *В статье рассматривается сущность и специфика функционирования механизма кибербезопасности. Внимание концентрируется на особенностях государственной политики в области информационной безопасности.*

V.E. Vasilevskaya
Academy of Management under the President of the Republic of Belarus
Minsk, Republic of Belarus

CYBERSECURITY AS A LEADING DIRECTION OF STATE POLICY

Abstract. *The article examines the essence and specifics of the functioning of the cybersecurity mechanism. Attention is focused on the specifics of the state policy in the field of information security.*

В современных реалиях становления нового типа цивилизации – информационного общества, одним из фундаментальных понятий является информация. Будучи базисным элементом общественной системы, информация имеет широкое употребление. В связи с чем, интерпретаций данного понятия в научном пространстве бесчисленное количество, традиционным считается определение информации как в первую очередь, обмен сведениями (вербальными и невербальными

признаками). С точки зрения философского осмысления, информация есть отражение материального и духовного мира, подобно материи и энергии, она выступает первоначалом бытия.

Обращаясь к прагматическим свойствам категории информация, следует обратить внимание на диахронию такого свойства как защищенность. Согласно теоретическому токованию, защищенность информации – это свойство, определяющее недопустимость её несанкционированного пользования [3, с. 15]. Однако на практике обеспечить «защищенность» (безопасность) информационного ресурса, достаточно сложно, ввиду существования многообразия киберугроз. Информационная безопасность, как состояние защищенности информационной среды, является предметом различных аспектов жизнедеятельности (экономические, политические, военные и другие интересы). Методы и средства её защиты трансформируются в соответствии с тенденциями исторического развития.

Еще в Древнем мире использовались формы защищенности информации, например известный современности феномен «шифр Цезаря» (V в. до н.э.), позволял шифровать секретную информацию, путем подмены каждого из символов на третью в алфавитном ряду букву. Ярким примером криптографии информации, также является древнеегипетское иероглифическое письмо (IV–III тыс. до н.э.), представляющее собой рисуночный способ изложения информации.

Сегодня криптография информационного материала характеризуется электронным способом кодирования символов и применяется не только с целью ограничения её потребления, но и другими жизненно необходимыми целями. Общими задачами современной информационной безопасности являются:

– обеспечение права граждан на получение, хранение и распространение необходимой информации;

– обеспечение безопасной коммуникации между различными субъектами (государствами, бизнесом, гражданами);

– формирование эффективного механизма оперативного реагирования и пресечения информационной преступности;

– борьба с противозаконными действиями в информационной сфере;

– защита граждан и объектов хозяйственной собственности от информационных угроз (киберугроз).

На настоящем этапе весомость киберугроз достаточно велика, трансформация общественного сознания под влиянием информационных атак, дестабилизация экономического потенциала

предприятий, разжигание политических конфликтов, на фоне утечки национальной тайны и многие другие последствия. Кибератаки как естественный результат информационного развития общества, продуцируют социальные, экономические, политические, культурные барьеры. К примеру, результатом экономического дисбаланса является потеря финансового фундамента предприятий на фоне блокировки системного обеспечения, вследствие «вирусного заражения». Согласно проведенному «Лабораторией Касперского» исследованию, девять из десяти предприятий (91%) являлись объектами различных кибератак (сетевые атаки, веб-угрозы, спам, вредоносная почта и др.). Так, по результатам анализа, наибольшее количество угроз сетевых атак и вредоносной почты зафиксировано в Государстве Самоа (13,82% и 7,69%), веб-угрозы нанесли ущерб большому количеству предприятий Тунисской Республики (22,05%). Наиболее пострадавшими от угроз неуправляемого спама стали Соединенные Штаты Америки (19,26%) [4].

В зависимости от очага заражения информационные угрозы подразделяются на внутренние и внешние. К источникам *внутренних* угроз на предприятии относят программные обеспечения, устройства компьютерной системы, халатность сотрудников. Нелицензированный доступ к корпоративным материалам, информационный мониторинг конкурентов, вирусная блокировка системного обеспечения являются следствием *внешних* угроз. Данные виды угроз могут иметь умышленный и неумышленный характер воздействия. Институт компьютерной безопасности (Computer Security Institute) провёл исследование на предмет определения превалирования данных факторов, в соответствие с которым 50% киберугроз являются результатом халатности сотрудников предприятий, а частота рецидива составила 21% [1, с. 9].

Кибербезопасность является одним из важнейших стратегических направлений государственной политики. Состояние национальной информационной безопасности определяет уровень защищенности личности и общества в целом от внутренних и внешних информационных угроз, что непосредственным образом выражает функциональную обязанность государства по реализации конституциональных прав граждан, сохранению суверенитета и территориальной целостности, обеспечения социально-экономического развития. С целью предупреждения и нейтрализации рисков и угроз киберпреступности, государственные органы формируют, совершенствуют и реализуют меры обеспечения

национальной безопасности. Так, выделяют четыре уровня мер государственного воздействия на информационный механизм:

1) *законодательный* уровень, предусматривает формирование нормативно-правового базиса в работе с информационными ресурсами (законодательная регламентация эксплуатации компьютерных систем, стандарты их применения, нормативы ответственности);

2) *административный* уровень, характеризуется организационным управлением деятельности субъектов информационного сектора (разработка программ информационного развития, контроль их выполнения);

3) *процедурный* уровень, отражает непосредственные действия субъектов в конкретных ситуациях, по реализации мер информационной безопасности;

4) *программно-технический* уровень, включает разработку программного обеспечения, выполняющего функции защиты (обеспечение доступа, идентификация пользователей, криптография информации и т.д.) [3, с. 26].

В соответствии с задачами государственной политики, реализуется непрерывный процесс мониторинга, анализа, оценки и прогнозирования состояния информационной безопасности. Совершенствуется научно-технологический фундамент государственного механизма защиты, с целью своевременного реагирования на информационные риски. Важно отметить, что необходимой задачей государственного контроля также является повышение осведомленности граждан о мерах индивидуальной защиты от информационных атак. А также сбор информации о степени защищенности и устойчивости индивидуального и массового сознания к действию киберугроз.

Согласно мировой статистике, количество кибератак увеличивается на 3% в месяц, что существенно усложняет организацию защиты безопасности. В условиях постоянного нарастания информационного риска, политика государства в данной сфере достаточно неустойчива. Более того, принимая во внимание глобальный (открытый) характер системы киберпреступности, когда источником вирусов являются представители разных стран, обеспечить единый механизм государственной защиты в цифровых отношениях достаточно сложно. В глобальной цепочке кибератак, отсутствует доверие между государствами, что препятствует формированию международной системы борьбы с киберпреступностью. В условиях разжигания международных противоречий, государственная политика отдельных стран стремиться в первую очередь, обеспечить сохранение

национального информационного суверенитета. В связи с чем, современные вызовы информационной эпохи, кардинально трансформируют традиционную систему государственной безопасности, в которой базисное положение занимает ресурс информации.

Список использованных источников

1. Вангородский, С.Н. Основы кибербезопасности / С. Н. Вангородский. – М. : Дрофа, 2019. – 238 с.

2. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова. – Екатеринбург : Изд-во Урал. ун-та, 2019.– 204 с.

3. Гафнер, В.В. Информационная безопасность: учебное пособие в 2 ч. / В. В. Гафнер. – Екатеринбург :иГОУ ВПО «Урал. гос. пед. ун-т», 2009.– 155 с.

4. Статистика киберугроз от «Лаборатории Касперского [Электронный ресурс]. – Режим доступа: https://statistics.securelist.com/ru/intrusion. – Дата доступа: 21.11.2021.

УДК 629.048.3

В.К. Вершинин, Р.Ю. Уневский, А.С. Фимушин
ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина»
Воронеж, Российская Федерация

КОНЦЕПЦИЯ ПРИМЕНЕНИЯ ЭЛЕКТРИФИЦИРОВАННОЙ СИСТЕМЫ КОНДИЦИОНИРОВАНИЯ ВОЗДУХА И ПРОТИВООБЛЕДЕНИТЕЛЬНОЙ СИСТЕМЫ

Аннотация. *В статье рассмотрена возможность применения электрифицированной системы кондиционирования воздуха и противообледенительной системы с целью снижения отбора мощности двигателя на обеспечение работы данных систем.*

V.K. Vershinin, R.Yu. Unevsky, A.S. Fimushin
VTSC “AFA named after N.E. Zhukovsky and Yu.A. Gagarin
Voronezh. Russian Federation