УДК: 37.004

ПРИНЦИПЫ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Шахло Аскарова.
Ппреподаватель Ферганского государственного университета
Узбекистан, г. Андижан

Аннотация: Информация и информационные ресурсы становятся одним из решающих факторов развития личности, общества и государства. Широкий спектр компьютеров и информационных технологий позволяет автоматизировать мониторинг и управление государственными, экономическими, социальными, оборонными и другими объектами и системами, получать, собирать, обрабатывать и передавать информацию об этих процессах практически любым способом. с необходимой скоростью. Все это дает основание утверждать, что сегодня информация играет решающую положительную роль в человеческом развитии, что информационное общество объективно неизбежно.

Ключевые слова: Фобос, дезинформация, искусственный интеллект, микрокомпьютер, радиоэлектроника.

PRINCIPLES OF INFORMATION SECURITY EFFICIENCIES

Shakhlo Askarova.
Lecturer of Fergana State University
Uzbekistan, Andijan

Abstract: Information and information resources are becoming one of the decisive factors in the development of an individual, society and state. A wide range of computers and information technologies makes it possible to automate the monitoring and management of state, economic, social, defense and other facilities

and systems, to receive, collect, process and transmit information about these processes in almost any way. at the required speed. All this gives grounds to assert that today information plays a decisive positive role in human development, that the information society is objectively inevitable.

Key words: Phobos, disinformation, artificial intelligence, microcomputer, radio electronics.

Сегодня существует три основных принципа, обеспечивающих информационную безопасность: целостность информации, конфиденциальность информации и доступ к информации всех пользователей с правами доступа; Кроме того, некоторые сферы деятельности (правоохранительные органы, оборонные и специальные структуры, банковские и финансовые учреждения, информационные сети, системы государственного управления) предъявляют высокие требования к надежности своих информационных систем в зависимости от важности и характера решаемых вопросов. в них безопасность требует особых мер предосторожности.

Эффективность информационной безопасности определяется ее своевременностью, активностью, непрерывностью и сложностью. Комплексные меры защиты обеспечивают устранение опасных каналов распространения информации.

С точки зрения защиты информации в компьютерных системах существует три взаимосвязанных компонента: информация; железо и софт; уделяется внимание обслуживающему персоналу и пользователям.

Принципы информационной безопасности можно разделить на три группы: использование информационной безопасности в правовой, организационной и технической защите разведки и использование компьютерных технологий при обработке информации.

Практика использования систем защиты информации показывает, что эффективными могут быть только сложные системы защиты информации [1].

Помимо основных методов, используемых пользователем для защиты информации, очень важную роль играет метод духовной и образовательной защиты информации. Это человек, сотрудник предприятия или организации, который осведомлен о конфиденциальной информации, накапливает в своей памяти много информации и в одних случаях может стать источником утечки информации, а по его вине другие незаконно получают к ней доступ. информация. Обучение сотрудника методам духовно-просветительской защиты информации, проведение с ним специальной работы, направленной на формирование определенных качеств, взглядов (патриотизма, разъяснение важности защиты информации для него лично) и обучение правилам и методам защита информации, формирование практических навыков работы с конфиденциальными СМИ.

В области предупреждения преступности сотрудники правоохранительных органов обладают необходимым уровнем теоретических знаний и практических навыков для выполнения таких задач, как создание, редактирование, сбор, передача, получение и надежная защита информации в сети в различных формах и содержании [2].

Целями защиты информации являются:

• предотвращение несанкционированной утечки, кражи, потери, изменения, фальсификации информации;

• угроза безопасности личности, общества, государства - предотвращение опасности;

• предотвращение несанкционированных действий по загрузке, модификации, фальсификации, копированию, блокировке информации;

• предотвращение любого незаконного вмешательства в информационный резерв и информационную систему, обеспечение правопорядка в объеме документированной информации;

• защита конституционных прав граждан на неприкосновенность частной жизни и конфиденциальность персональных данных, содержащихся в информационной системе;

• защита государственной тайны, конфиденциальность документированной информации в соответствии с законодательством;

• Обеспечение прав субъектов при создании, развитии и применении информационных систем, технологий и их средств.

Информационное оружие - это радиоэлектронное оружие, набор программного обеспечения и средств массовой информации, предназначенных для уничтожения информационных возможностей противника.

Это уточняющее понятие важно, потому что существует также «простой» пропагандистско-психологический информационный инструмент, известный миру как «дезинформация», имеющий древнюю историю. В военно-исторической литературе есть много известных примеров дезинформации, успешно применявшихся в военное и мирное время. Деза до сих пор остается оружием спецслужб.

Но в 60-70-е годы «искусственный интеллект» стал «обычным» информационным оружием, а информационные системы стали оснащать компьютерами и микрокомпьютерами. В результате СМИ не только смогут бесконечно расширять сферу своей деятельности, но и смогут заменить массовые атаки, как утверждает Запад. Теперь дадим четкое представление об информационном инструменте, который предоставляют российские специалисты.

Информационный инструмент - это «средство уничтожения, взлома или кражи информационных массивов, получения от них необходимой информации после взлома системы безопасности, запрета или ограничения доступа законных пользователей, нарушения работы технических средств, взлома телекоммуникационных сетей. , демонтаж компьютерных систем, высокотехнологичное обеспечение общественной жизни и всех аспектов государственной деятельности »[3].

Конечно, компьютерные игры также играют определенную роль в появлении вредоносных программ на компьютерах сегодня. Деловые игры позволяют расширить рамки реальности, визуализировать последствия принимаемых решений. Позволяет визуализировать, опробовать альтернативные решения. Информация, которую фактически использует человек, неполная, неточная. В игре ему предоставляется неполная, но точная информация, что повышает уверенность в полученных результатах и поощряет процесс принятия на себя ответственности. В то же время информационная безопасность находится под вопросом даже на уровне увлечения играми. [4]

Обеспечение информационной безопасности человека подразумевает его право на объективную информацию и предполагает, что информация, полученная от человека из различных источников, не препятствует свободному формированию и развитию его личности. В процессе информатизации человек стал информационным «прозрачным». Если есть желание и средства, любая доступная информация о конкретном человеке доступна и может быть использована в своих целях другим человеком, группой людей, социальной группой и государством. Только небольшая часть населения может предотвратить несанкционированный доступ к своим данным. Большинство людей не имеют такой возможности и остаются беззащитными в этом отношении. Следовательно, информационная безопасность человека - это такое состояние дел, при котором человеку не

может быть причинен значительный ущерб, влияя на информационное пространство вокруг него.

Информационная безопасность общества - это такое состояние общества, при котором ему нельзя сильно повредить, влияя на его информационное поле. Если существуют информационные угрозы, они основаны на безопасности индивидуального сознания индивида, группы и общества, что в первую очередь должно включать информационное и психологическое воздействие. Действие этих угроз может привести к психоэмоциональной и социально-психологической напряженности, нарушениям моральных норм и норм, нарушениям моральной и политической ориентации и, как следствие, к ненадлежащему поведению отдельных лиц, групп и масс людей. В результате таких воздействий возможны глубокие изменения индивидуального, группового и массового сознания, негативные изменения морально-политического и социально-психологического климата в обществе.

Информационная безопасность государства - это состояние, в котором информационная сфера государства не может быть сильно повреждена его влиянием. Обеспечение информационной безопасности государства неразрывно связано с обеспечением национальной безопасности. В последние годы мы смогли увидеть, насколько серьезными могут быть последствия нарушений информационной безопасности, связанных с использованием современных технологий.

Строгое соблюдение правил информационной безопасности должно стать одним из главных требований в экономической, военной и научно-технической политике нашей страны. Эти правила необходимо четко систематизировать и уточнить. В общем, должен быть «информационный кодекс», который должен состоять из четких понятий: государственная информационная политика должна быть протекционистской, направленной

на развитие своих информационных технологий, защищая свой рынок от вторжения скрытых элементов ИНФОР. Нарушение Кодекса следует рассматривать как тяжкое преступление. Кодекс важен из-за массового импорта СМИ и их широкого использования не только в частном секторе, но и в государственных учреждениях. При этом следует учитывать, что пользователи импортных информационных систем уделяют особое внимание их бесперебойной работе и надежности, им все равно, что еще в этих системах.

Список литературы:

1. С.К. Ганиев, М.М. Ганиев, Каримов, К.А. Ташев. Информационная безопасность

2. Мирсодик Позилов, Ильяс Ибрагимов. «Об информационной безопасности» Ташкент 2016.

3. И. Алдашев. Создание имитационных и игровых моделей в педагогическом процессе. «Экономика и социум» №2 (81) 2021 www.iupr.ru

4. http://uz.infocom.uz/2005/05/22/ Об информационной безопасности /