УДК: 159.9.075
DOI: 10.25629/HC.2022.02.11

ПОНЯТИЯ И ВИДЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сухов А.Н.
Рязанский государственный университет имени С.А. Есенина

Аннотация. В данной статье раскрывается актуальность исследования проблемы, связанной с информационной безопасностью. а также рассматривается сущность социально-психологического подхода к её пониманию. С данным видом безопасности связана модель развития информационного общества. Поэтому не случайно наиболее важной задачей является создание полноценной теории информационной безопасности. Анализируются внешние и внутренние угрозы информационной безопасности. К их числу относятся: хакерские атаки, взломы, вмешательство, вторжение в национальную информационную систему; криминальные информационные угрозы; информационно-психологическая война и др. В статье так же анализируется практика преодоления данных угроз в целях обеспечения информационной безопасности. Без этого невозможно вести речь об эффективном её обеспечении. Это достижимо только путём устранения ряда негативных последствий процесса информатизации общества.

Ключевые слова: информационная безопасность, внешние внутренние угрозы, информационные угрозы, информационно-психологическая война, социально-психологическая компетентность, профиль, принятие решения, информационное общество.

Введение

Социально-психологический подход к пониманию различных видов безопасности, в том числе информационной позволяет: 1) сформулировать понятие, структуру и стадии обеспечения безопасности; 2) выявить внешние и внутренние угрозы, влияющие на уровень безопасности; 3) проанализировать и определить механизм воздействия внешних и внутренних угроз; 4) обосновать социально-психологические технологии обеспечения безопасности.

С учётом этого можно сказать, безопасность- это система действий субъектов путём использования различных средств и технологий в целях выявления (диагностирования), идентификации и ликвидации внешних и внутренних угроз, представляющих собой деструктивное воздействия на объекты безопасности в целях обеспечения их надёжного функционирования или сохранения на основе минимализации рисков для них.

Актуальность анализа информационной безопасности связана с раскрытием реальной роли информации в современном обществе.

Главными отличительными особенностями постиндустриального общества являются рост научного знания и перемещение центра общественной жизни из экономики в сферу науки, прежде всего в научные организации. В нем ключевым фактором выступает информация, помноженная на распространение образования и внедрение передовых технологий. Таков мировой тренд.

Цель статьи

– раскрыть возможности информатизации общества и пути преодоления внешних и внутренних угроз, в том числе ряда деструктивных последствий, возникающих при этом.

Результаты и обсуждение

Уровень обеспеченности информационной безопасности зависит от эффективности (своевременности, точности) выявления внешних и внутренних угроз, тяжести их последствий, а также профессионализма в области применения контртехнологий.

На стадии диагностики угроз встречаются различные трудности, которые преодолеваются при наличии профессиональной социально-психологической компетентности.

Анализ угроз информационной безопасности позволяет дать их адекватную характеристику.

Внешние угрозы национальной информационной безопасности:

1) использование иностранной информационной платформы, что таит в себе опасность тотального информационного контроля;

2) трудности доступа в определённых случаях в иностранные поисковые, социальные, видео сети;

3) хакерские атаки, взломы, вмешательство, вторжение в национальную информационную систему;

4) криминальные информационные угрозы;

5) информационно-психологическая война.

При этом есть угрозы, которые представляют опасность для той или иной информационной системы. Но в качестве таковых может выступать сама информация.

Тотальный информационный контроль- одна из главных угроз не только для информационной безопасности, но и для всей национальной безопасности в целом.

Интенсивное внедрение и постоянное усовершенствование электронных и телекоммуникационных технологий позволяют оперативно получать сведения о рынках, потребителях, регионах, налоговых системах в разных уголках земного шара. Такая форма контроля в периодических изданиях и СМИ получила название электронного контроля.

Способы электронного контроля – запись информации, поступающей через компьютерную сеть, доступ к любым контактам в социальных сетях и адресам электронной почты всех пользователей интернета на территории различных государств, доступ к персональным базам данных, хранящимся в электронном виде, Приложениях и др. – декларируются как новые технологии безопасности.

Но на практике электронный контроль используется для иных целей. Созданы и действуют специальные информационные структуры и подразделения. Поэтому крайне необходима своя национальная независимая информационная платформа.

Информационное противоборство между конкурирующими сторонами достигла апогея. Они обвиняют друг друга в том, чем сами на самом деле постоянно занимаются.

Так, сложился трэнд по обвинению России в нарушении свободы слова, вторжении в предвыборные компании других стран, хакерских атаках и т.д. Однако реально очень часто всё обстоит наоборот.

Повлиять на политику блокировок в крупных социальных сетях пока не получается даже на их родине, в США. В частности, известны случаи, когда учёных США не допускали в социальные сети потому, что они занимались исследованием их рекламной деятельности.

Социальные сети могут блокировать даже лидеров государств. Неоднократно аналогичные действия со стороны социальных сетей предпринимались и в отношении представителей РФ. Именно поэтому необходимо эффективное регулирование их деятельности по соблюдению прав граждан на свободный доступ к получению информации.

Миф о «злых русских» известен из американского кино 80-х годов. «Русофобия» приобрела характер жёсткой информационной войны.

Транснациональную преступность определяют как коммерческую деятельность законспирированных криминальных организаций, осуществляемую на территории нескольких стран противоправными средствами и с привлечением современных информационных технологий, зарубежных товаров и услуг, а также как международный терроризм и экстремизм.

Технологически террористическая сеть соответствует самым современным требованиям. В основании транснациональной террористической сети, лежит обмен информацией между всеми её участниками. При этом сеть способна свернуть свою деятельность в одной точке мира и перенести свою активность в другое место, образовав совершенно новую конфигурацию, в случае угрозы её деятельности.

Но в любом случае суть транснациональной преступности связана с различными видами преступлений, выходящих за пределы одного государства.

В настоящее время наиболее опасным видом транснациональной преступности является международный терроризм и экстремизм. Современный терроризм значительно отличается от терроризма, существовавшего в историческом прошлом. Он не знает ни территориальных границ, ни финансовых, ни информационных преград. В этой связи ни одно государство в современном мире не может чувствовать себя в полной безопасности перед лицом новых угроз.

Однако далеко не все международные политические элиты хотели признавать, что бороться с терроризмом можно только сообща, при тесном сотрудничестве государств, общества и взаимном обмене информацией.

Современные средства криминогенного общения-механизм транснациональной преступности.

Речь идёт о передачи разговорной речи через каналы, доступ к которым крайне ограничен и возможен только при наличии ключа. Что касается невербальных средств, то здесь прежде всего имеется в виду передача шифрованных сообщений с помощью математических методов преобразования информации с помощью криптографии и т.д. [17].

К числу главных внешних угроз информационной безопасности относится информационно-психологическая война.

По мнению экспертов, 22-ой век характеризуется интенсивным развитием средств и способов ведения информационно-психологической войны, которая проводится в целях:

1) прерывания, использования, кражи, искажения или уничтожения информации противоположной стороны: конкурента и т. д.;

2) защиты своих средств от аналогичных действий противника.

Информационно-психологическая война – устоявшееся понятие в области современной науки и практики. Однако корни её возникновения уходят в древность. В это трудно поверить, так как сточки зрения типичного пользователя информационно-психологическая война – это прежде всего компьютерные вирусы и воровство новых технологий. Таково её стереотипное восприятие.

На самом деле информационно-психологическая война опасна не только этим. Она ведется с помощью манипулирования информацией, охватывает СМИ, влияет на образование и разрушает традиционные культуры.

Директива 3600.1 Министерства обороны США определяет «информационно-психологическую войну» как «информационные операции, проводимые во время кризисов или конфликтов для достижения или пропаганды определенных целей по отношению к противнику».

Однако это не единственное её определение. Существуют и другие понятия информационно-психологической войны, в частности, как «акции, предпринимаемые для достижения информационного превосходства путем воздействия на информацию и средства информирования противника и защиты собственных информационных средств и процессов».

При анализе материалов на тему новейшего типа информационно- психологической войны в зарубежной литературе, можно отметить, что чаще всего рассматриваются инновационные технологии её ведения.

В литературе встречается понятие «информационное противоборство», трактуемое как «форма борьбы между государствами, представляющая собой целенаправленное использование информационного оружия для реализации политических и военных интересов и защиты

собственных информационных ресурсов». В мирное время оно носит скрытый характер и обеспечивает как решение текущих задач, так и постепенное накапливание необратимого превосходства.

Реальное развитие России непосредственно связано с состоянием её информационной безопасности.

Информация существует сегодня в двух измерениях: как один из главных технологических (цифровых) продуктов экономики постиндустриального общества и как «наступательное, так называемое мягкое оружие», которое делает прозрачными и незащищенными границы государств.

В военном и политическом лексиконе термин «информационно-психологическая война» означает систему воздействий, направленных на изменение социальных представлений в нужном направлении.

Стратегия и тактика ведения информационно-психологической войны одного государства против другого (или других) подразумевают определенного вида воздействия для достижения определённых целей. Если в идеологической борьбе используются методы противопоставления теоретический положений, доктрин, концепций, методы убеждения, то методы психологической войны базируются на психологическом воздействии.

Выделяются три уровня воздействия:

- усиление существующих в сознании нужных установок, идеалов, норм;
- частичные изменения взглядов на события;
- кардинальные изменения жизненных установок на основе сообщения необычной, «драматической» новой информации.

Механизм информационного воздействия основан на манипуляции сознанием масс и внесением в это сознание целенаправленной достоверной либо недостоверной информации (в последнем случае – дезинформации).

Этот тип управления личностью, группой, массой связан со стремлением так сформировать сообщение о реальной ситуации, чтобы несмотря на его неадекватность, человек принимал его как само собой разумеющееся и поступал соответствующим образом.

Под дезинформацией понимается информационная версия, имеющая целью сознательно ввести аудиторию в заблуждение, навязать им превратное, искаженное, а иногда и просто лживое представление о реальной действительности.

Секрет высокоэффективного информационного воздействия – обращение к бессознательному, в использовании приемов снятия барьеров восприятия и преодоления естественной толерантности человека к восприятию нового. Психологи умело находят «ключи к психике».

Психология влияния не обязательно должна быть манипулятивной. Это – эффективный инструмент, который в зависимости от личной этики специалистов по информационному управлению может быть использован как на пользу людям, так и во вред им.

Возможности информационного воздействия кроются в профессиональном умении использовать весь спектр слабостей, склонностей личности, в мастерском применении методов стимуляции многочисленных иллюзий и мечтаний.

В этом контексте особую актуальность приобрела гибридная информационно-психологическая война, в результате которой ложь от правды трудно отличить.

Совершенно «голой» остаётся проблема урегулирования гибридных конфликтов. Здесь прежде всего следует стараться «за уши» вытащить на «свет божий» истинные цели той стороны, которая тщательно их скрывает.

В этой связи со всей остротой встаёт так же задача, связанная с разработкой технологий по противодействию влияния информационно-психологической войны, контрпропаганды [18].

Внутренние угрозы информационной безопасности:

1) криминальные информационные угрозы;

2) не всегда позитивное и объективное, нередко деструктивное содержание информации, транслируемой через СМИ, передаваемой и содержашейся в социальных, видео - сетях, рекламных сообщениях, предвыборных агитационных роликах, плакатах и других информационных средствах; информационное манипулирование;

3)недостаточный уровень защищённости от: хакерского вторжения, взлома сетей, спама в целях кражи информации;

4)интернет-пиратство, плагиат, нарушение авторского права на интеллектуальную собственность;

5) межкорпоративные информационно-психологические войны;

6) информационная зависимость потребителей, пользователей информации: слушателей, подписчиков и т. д.

Как известно, одной из серьёзных криминальных информационных угроз являются средства криминогенного общения.

Традиционные средства криминогенного общения подверглись трансформации. Они претерпели модернизацию.

Информационные манипулятивные приемы широко используются в криминальной сфере. Так, мошенники применяют манипулятивные приемы для вымогательства денег от родственников и знакомых лиц, якобы совершивших ДТП. Делается это по сотовой связи. С помощью манипуляций совершается в большом количестве обман в виде предложений по совершении покупок по фантастически выгодным ценам. С помощью таких профессиональных ухищрений мошенники пытаются получить реквизиты счетов, снимают большие суммы.

Под криминальным информационным манипулированием при мошенничестве понимается система средств, направленного, скрытого психологического воздействия на жертву с целью завладения чужим имуществом или приобретения права на имущество.

К наиболее часто применяемым методам криминального манипулирования при мошенничестве относятся: использование психических автоматизмов, манипуляция содержанием и формой предоставляемой информации, изменение темпа ее изложения, эксплуатация фоновых состояний, использование группового давления на личность.

Указанные методы используются и в ходе вовлечения и удержания жертв финансовых пирамид по типу так называемых элитных закрытых бизнес-клубов. В то же время через социальные сети с помощью манипулирования происходит вербовка в экстремистские группы, террористические организации, распространение наркотиков, вовлечение детей в сексуальные отношения, склонение к суициду и т.п. [17].

В принципе поисковые сети интернета, социальные, видео сети помогают преодолевать типичные негативные социально-психологические явления: одиночество, социальные страхи, аутизм, найти работу, друзей, получить поддержку, организовать дистанционное обучение детей-инвалидов и т.п. В данном случае они имеют неоспоримое преимущество перед остальными технологиями.

Однако социальные сети приводят и к негативным социально-психологическим последствиям. Они известны. Большую роль не только в позитивном развитии, но и деформации социальных представлений различных групп населения играют массовые информационные технологии: СМИ, социальные сети и т. д.

Коммерция здесь играет не последнюю роль. В результате получается замкнутый круг: массовые технологии влияют на содержание социальных представлений, те на ценности, последние обратно на СМИ, рождая запрос на тематику, определяя рейтинги передач, статей на основе учёта частоты, интенсивности, количества обращений, контактов, «лайков», а СМИ, социальные сети вновь на социальные представления и т.п.

Деятельность СМИ в российском обществе продолжает нередко носить деструктивный характер [19].

Виртуальная реальность у подростков и молодежи все более вытесняет реальные события, чувства, деятельность, общение. Немало из них живут в «медиа» мире.

Компьютерные игры приходят на смену традиционным видам активного досуга. Специфический компьютерный сленг общения искажает родную речь. К средствам психологического воздействия на личность можно отнести печатную продукцию, радио- и телевещание, кино, видеофильмы, аудиоматериалы и другие носители аудио- и видеоинформации, компьютерные телекоммуникационные сети, даже предметы повседневного обихода, продукты питания и игрушки. С помощью этих средств человек уводится в вымышленный мир как активный участник разыгрывающихся виртуальных событий, оказываясь беспомощным и легко управляемым в мире реальном.

Массовые социально-психологические технологии воздействия посредством СМИ - это комплекс методов и приемов для оказания влияния на социальные представления населения. Их эффективность проявляется в способности устанавливать контакт с аудиторией и доверии к ним.

Известно, что в ходе практического использования интернет ресурсов возникают различные побочные явления, синдромы своего рода, а именно:

- информационная зависимость потребителей, пользователей информации: слушателей, подписчиков и т. д.

- интернет пиратство, плагиат, нарушение авторского права на интеллектуальную собственность.

Компьютерные игры или присутствие в интернете становятся для подростков средством квазиудовлетворения подлинных психологических потребностей – потребности в увлекательном занятии, общении, уважении, признании и др. Замечено, что долгое пребывание в виртуальном мире создаёт ощущение абсолютной ненужности естественного и повседневного (Коваль, 2013). Как следствие ухода подростков от реальности в мир виртуальной игры все чаще у них наблюдается личностный инфантилизм, нарушения процесса идентификации, неврозы, оппозиционно вызывающие расстройства поведения и др.

Поэтому ситуацию надо менять. Причём радикально. В этом контексте встаёт вопрос со всей остротой об обеспечения информационной безопасности, в том числе общественном контроле за СМИ, ТВ и т. д.

Если говорить кратко, то технологии обеспечения информационной безопасности сводятся к следующим видам: 1) правовой защите, обеспечивающей доступ к получению информации;2) общественному контролю за СМИ; 3) технико-информационной защите; 4) социально-психологическим технологиям обеспечения безопасности.

Краеугольным камнем, фундаментом устройства демократического государства выступают свобода слова и право выбора в области СМИ. Никто прямо не может навязывать, что слушать, что печатать.

Но при этом нельзя ошибочно полагать, что общественный контроль за массовыми информационными технологиями должен быть утрачен.

Массовые информационные технологии свою социализирующую роль могут выполнять через: социальное образование; связь с общественностью; социально-правовое просвещение; социальную рекламу; социальные сети**.**

Информационная безопасность должна прежде всего служить общественной безопасности. С этих позиций информация должна быть полной, истинной, непредвзятой и открытой. С другой стороны, в определенных случаях информационная безопасность должна обеспечивать интересы государства по сохранению государственной и военной тайны. С этих позиций информация должна содержать определенные ограничения.

В узком плане информационная безопасность означает средства защиты от проникновения в информационные сети, средства противодействия перехвату телефонных, пейджинговых сообщений и прослушивания переговоров [13].

Выход из сложившейся ситуации связан прежде всего с активизацией общественной дискуссии и формированием общественного мнения по вопросам защиты информационной системы. В других странах имеется опыт об общественном контроле за СМИ. Его следует использовать.

Борьба с интернет-пиратством, «плагиатством» способствует обеспечению информационной безопасности, интеллектуальной собственности, авторского права и повышению объективности рейтинга научно-педагогических сотрудников при его определении.

Существует много практических рекомендаций по преодолению интернет зависимости. Но они недостаточно научно проработаны. Поэтому пользоваться ими надо осторожно.

Выводы

Таким образом, проблема обеспечения информационной безопасности является одним из самых приоритетных направлений деятельности государственных и общественных структур.

Библиография

1. Бабаева Ю.Д., Одаренный ребенок за компьютером [Текст] / Ю.Д. Бабаева А.Е. Войскунский. – М.: Сканрус, 2003.

2. Баева И.А. Обеспечение психологической безопасности в образовательном учреждении/ – М., 2006.

3. Барсукова О.В. Телевидение как фактор формирования духовно-нравственных ценностей личности: Автореф. диссертации на соискание ученой степени кандидата филологических наук. [Текст] / О.В. Барсукова. –Воронеж,2 012.

4. Власов А., Кесарева Т., Лазарев Д. Проблема борьбы с преступностью в сети Интернет //Право и экономика. – 2000. - №12. – с.73-75.

5. Воробьев Г.Г., Молодежь в информационном обществе. М.: Молодая гвардия, 1990.

6. Доктрина информационной безопасности РФ // Российская газета. 2000, 28 сентября, с. 4-5.

7. Домозетов Х. Социологические проблемы компьютерного пиратства // Социологические исследования. – 1997. – №11. – с. 110-114.

8. Информационное общество: Информационные войны. Информационное управление. Информационная безопасность. СПб.: Издательство Санкт-Петербургского университета, 1999.

9. Коваль, Т.В. Личностная сфера подростков, склонных к развитию компьютерной зависимости: Автореф. дис. канд. психол. наук [Текст] / Т.В. Коваль. – М.,2013.

10. Коркина, А. Ю. Критерии психологической оценки компьютерных игр и развивающих компьютерных программ // Психологическая наука и образование. – 2008. – № 3. - С. 19-24.

11. Кочан И., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция. -1999. - №1. -с. 44-45.

12. Митрохина Е.Ю., Информационная безопасность как социологическая проблема. Безопасность. М., 1997, №№ 7-9 (39).

13. Рыбкин И.П. К безопасности – через согласие и доверие. М.: Софрино, 1997.

14. Смирнова Е.О., Радева. Р.Е. Образование и информационная культура // Социологические аспекты. Труды по социологии образования. – Т.V – Вып. VII / Под ред. В.С. Собкина. – М.-2000. С.12-26.

15. Старовойтов А. У кого в руках ключ к информации: Интервью с генеральным директором Федерального агентства правительственной связи и информации при Президенте РФ. // Российская газета – 1997 – 22 мая – С.3.

16. Сухов А.Н. Социальная психология безопасности. М., 2002. -256 с.

17. Сухов А.Н. Традиционные и современные средства криминогенного общения / Вестник Московского университета МВД России. 2020 №4. С. 267-272.

18. Сухов А.Н. Информационная безопасность: теоретико-практический аспект // Психолого-педагогический поиск. 2021. №1(57). С. 183-191.

19. Сухов А.Н. Социально-психологические технологии работы с различными группами населения. М., 2019.

CONCEPTS AND TYPES OF INFORMATION SECURITY THREATS

Sukhov A.N.

Russian State University named after S.A. Yesenin

Abstract. This article reveals the relevance of researching the problem related to information security. as well as the essence of the socio-psychological approach to its understanding is considered. This type of security is associated with a model for the development of the information society. Therefore, it is no coincidence that the most important task is to create a full-fledged information security theory. These include: hacker attacks, break-ins, interference, intrusion into the national information system; criminal information threats; information and psychological warfare, etc. The article also analyzes the practice of overcoming these threats in order to ensure information security. Without this, it is impossible to talk about its effective provision. This is achievable only by eliminating a number of negative consequences of the process of informatization of society.

Keywords: information security, external internal threats, information threats, information-psychological warfare, socio-psychological competence, profile, decision-making, information society.