Введение

Актуальность темы исследования. На современном этапе развития общества, связанном с массовым использованием информационных технологий и созданием единого информационного пространства, в котором происходит накопление, обработка, хранение и обмен информацией, проблемы информационной безопасности приобретают первостепенное значение во всех сферах общественной и общественной деятельности.

Угрозы информационной безопасности представляют собой совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере.

В современном обществе именно информация становится важнейшим стратегическим ресурсом, основной производственной силой, обеспечивающей ее дальнейшее развитие. Именно поэтому, как и любой другой традиционный ресурс, информация также нуждается в особой защите. Наряду с термином "информационная безопасность" также широко используется термин "информационная безопасность". Если информационная безопасность характеризует процесс создания условий, обеспечивающих необходимую безопасность информации, то информационная безопасность отражает достигнутое состояние такой безопасности.

Проблема информационной безопасности приобрела особое значение в современных условиях широкого использования автоматизированных информационных систем, основанных на использовании компьютерных и телекоммуникационных средств. При обеспечении информационной безопасности угрозы, вызванные умышленными (злонамеренными) действиями людей, стали вполне реальными. Первые сообщения о несанкционированном доступе к информации были в основном связаны с хакерами, или "электронными разбойниками". Последнее десятилетие нарушения информационной безопасности прогрессируют с использованием программного обеспечения и через глобальную сеть Интернет. Довольно распространенной угрозой информационной безопасности также стало заражение компьютерных систем так называемыми вирусами.

Таким образом, в связи с возрастающей ролью информационных ресурсов в жизни современного общества, а также в связи с реальностью многочисленных угроз в

плане их безопасности, проблема информационной безопасности требует постоянного и повышенного внимания. Системный характер воздействия на информационную безопасность большого множества различных обстоятельств, имеющих к тому же различную физическую природу, преследующих разные цели и вызывающих разные последствия, приводят к необходимости комплексного подхода в решении данной проблемы.

Объект исследования: угрозы информационной безопасности.

Предмет исследования: состав угрозы информационной безопасности.

Цель работы состоит в определении видов угроз информационной безопасности и их состава.

Для достижения цели работы необходимо выполнить следующие задачи:

- описать проблемы оценки информационной безопасности;

- рассмотреть понятие и структура угроз защищаемой информации;

- указать источники, виды и способы дестабилизирующего воздействия;

-привести формы и виды проявления уязвимости защищаемой информации;

- проанализировать источники угроз информационной безопасности Российской Федерации.

Глава 1. Теоретические основы угроз информационной безопасности

1.1 Проблемы оценки информационной безопасности

Качество и эффективность функционирования информационной системы определяется уровнем ее защищенности от внешнего и внутреннего воздействий. Данные мировой и отечественной статистики свидетельствуют о тенденции роста масштаба компьютерных злоупотреблений, которые приводят к значительным финансовым потерям субъектов хозяйствования разного уровня. Устранение и предотвращение информационным угрозам различного характера предполагает построение четкой системы диагностики, которая должна базироваться на оценке информационных рисков и оценке изменения экономических, социальных, технико-технологических и других показателей, вызванных изменением состояния информационной системы предприятия. Оценке информационной безопасности занимаются с начала появления информационных технологий.

По этой тематике есть много работ, но наиболее актуальными и фундаментальными трудами являются нормативные документы, которые внесли весомый теоретический и практический вклад в решение задач обеспечения информационной безопасности, а именно: «Оранжевая книга» [1], в которой изложены и систематизированы критерии оценки защиты компьютерных систем; Европейские критерии оценки безопасности информационных технологий [2], что учли все недостатки и ограничения, изложенные в «Оранжевой книге»; Канадские критерии оценки безопасности надежности компьютерных систем [3]; Федеральные критерии США [4], разработанные по заказу правительства США и направлены на устранение ограничений, и тому подобное.

Однако, концептуальные основы оценки информационной безопасности возникли еще в 70-х гг., при формировании модели безопасности с полным перекрытием (модели Клементса-Хоффмана) [14]. В своем первоначальном виде модель Клементса-Хоффмана была «идеализированная», однако именно в процессе анализа данной модели и возникла проблема необходимости оценки информационных угроз. Модель построена исходя из постулата, что система информационной безопасности должна иметь, по крайней мере, одно средство для обеспечения безопасности на каждом возможном пути воздействия нарушителя на информационную систему. Для описания системы защиты информации с полным перекрытием рассматриваются три подмножества [14]:

множество угроз: $U = \{Ui\}$, $i = 1, m$;

множество объектов защиты $O = \{Oj\}$, $j = 1, n$;

множество механизмов защиты $M = \{Mk\}$, $k = 1, r$.

Элементы множеств U и O находятся между собой в отношениях «угроза – объект». Дуга множество существует тогда, когда Ui – средство получения доступа к объекту Oj.

Взгляды современников на проблемы оценки информационной безопасности имеют другую направленность в отличие от основополагающих концепций. Следовательно, Реверчук Н. И. предлагает использовать показатели информационной безопасности предприятия как производительность информации, коэффициент информационной вооруженности и коэффициент защищенности информации [13]. Такой перечень коэффициентов является достаточно ограниченным. Стоит отметить, что все три показателя отражают только финансовый аспект информационной безопасности, поскольку в качестве исходных

данных для расчета указанных показателей выступают затраты на приобретение информационных ресурсов [7].

В противовес Ильяшенко С. М. уровень информационной безопасности определяет долей неполной, неточной и противоречивой информации, которая используется в процессе принятия управленческих решений, то есть дает оценку лишь в качестве информации, предоставляемой лицам, принимающим решения. Перечень индикаторов нуждается в дополнении различными показателями, характеризующими состояние программно-технической защищенности информации и информационной надежности персонала [8].

Кравчук Е. Я. и Кравчук П. Я. для оценки уровня информационной безопасности предлагают рассчитывать пять показателей, характеризующих уровень информационно-аналитического сопровождения деятельности предприятия, защиты коммерческой информации и безопасности документооборота, уровень деловой репутации и имиджа продукции [10].

Путем сочетания вышеупомянутых методических подходов к оценке уровня информационной безопасности Журавель Н.Ю., Полозова Т.В., Стороженко А.В. использует диагностику уровня информационной безопасности проводить по трем ключевым направлениям: оценка программно-технической защищенности информации, оценка информационной надежности персонала, оценка информации, предоставляемой лицам, принимающим решения, информационной службой предприятия [7].

Велигура А. В. предлагает при оценке использовать три основных показателя. Первым показателем служит оценка опасностей, с которыми сталкивается предприятие. Путем оценки опасностей определяются угрозы для информации, ее уязвимость и вероятность возникновения угроз, а также возможный ущерб. Второй показатель – это законодательные, нормативные и договорные требования, которые должна соблюдать организация, ее партнеры по бизнесу, подрядчики и поставщики услуг. Третий показатель – это определенный набор принципов, целей и требований к обработке информации, разработанных организацией для поддержки своей деятельности.

Определение требований к безопасности проводится путем методической оценки рисков. Расходы на поддержание безопасности необходимо сбалансировать с вредом для бизнеса, который может возникнуть при нарушении безопасности.

Методы оценки опасностей могут применяться ко всей организации или к ее частям, а также к отдельным информационным системам, системным компонентов и сервисов, в зависимости от того, что окажется наиболее практичным, реалистичным и полезным [6]. Также она обращает внимание на целесообразности методом применение метода критических сценариев, когда в сценариях анализируются ситуации, как мнимый преступник наносит ущерба информационной системе предприятия и соответственно снижает способность поддерживать управления в пределах оптимальных параметров [6].

В зависимости от выбранного для оценки критерия Андрианов В. В. разделяет способы оценки информационной безопасности предприятия на оценку за эталоном, риск - ориентированную оценку и оценку по экономическим показателям. Способ оценки информационной безопасности за эталоном сводится к сравнению деятельности и мер по обеспечению информационной безопасности организации с требованиями, закрепленными в эталоне. То есть проводится оценка соответствия системы организации информационной безопасности предприятия установленным эталоном.

Под оценкой соответствия информационной безопасности организации установленным критериям понимается деятельность, связанная с прямым или косвенным определением выполнения или невыполнения соответствующих требований информационной безопасности в организации. С помощью оценки соответствия информационной безопасности измеряется правильность реализации процессов системы обеспечения информационной безопасности организации, и идентифицируются недостатки такой реализации. Риск - ориентированная оценка организации представляет собой способ оценки, при котором рассматриваются риски, возникающие в информационной сфере организации, и сопоставляются существующие риски информационной безопасности и принятых мерах по их обработке. В результате должна быть сформирована оценка способности организации эффективно управлять рисками информационной безопасности для достижения своих целей. Способ оценки на основе экономических показателей оперирует понятными для бизнеса аргументами о необходимости обеспечения и совершенствования информационной безопасности.

Для проведения оценки в качестве критериев эффективности системы организации информационной безопасности используются, например, показатели совокупной стоимости владения (Total Cost of Ownership – TCO) [5].

Морозова В. И., Врублевский К. Э. утверждают, что эффективность комплексная система защиты информации оценивается как на этапе разработки, так и в процессе эксплуатации. В процессе оценки эффективности комплексной системы защиты информации, они выделяют три подхода: классический, официальный, экспериментальный [12]. Под классическим подходом к оценке эффективности понимается использование критериев эффективности, значения которых получаются путем моделирования или определяются по характеристикам реальной информационной системы. Такой подход используется при разработке и модернизации комплексной системы защиты информации.

Официальный подход предполагает, что политика безопасности информационных технологий проводится государством и должна опираться на нормативные акты. Такие документы должны содержать требования к защищенности информации различных категорий конфиденциальности и важности. Требования могут задаваться перечнем механизмов защиты информации, которые необходимо иметь в информационной системе, чтобы она соответствовала определенному классу защиты. Несомненным преимуществом классификаторов (стандартов) является их простота использования. Во всех развитых странах разработаны свои стандарты защищенности информационных систем. Так, в Министерстве обороны США используется стандарт TCSEC, который известен как Оранжевая книга. Согласно Оранжевой книге для оценки информационных систем рассматривается четыре группы безопасности: A, B, C, D [11]. Под экспериментальным подходом понимается организация процесса определения эффективности существующих комплексной системы защиты информации путем попыток преодоления защитных механизмов системы специалистами, выступающими в роли злоумышленников. Составляется план проведения эксперимента. В нем определяются очередность и материально-техническое обеспечение проведения экспериментов по определению слабых звеньев в системе защиты. Служба безопасности до момента преодоления защиты «злоумышленниками» должна ввести в комплексной системе защиты информации новые механизмы защиты или изменить старые, чтобы избежать «взлома» системы защиты. Одним из недостатков такого подхода является то, что автор рассчитывает большинство показателей на основе экспертного метода, что значительно усиливает влияние субъективного фактора на конечный результат расчетов. Также предложена система индикаторов не учитывает всех аспектов информационной безопасности предприятия. В частности, как и представленная методика не включает показателей, характеризующих информационную надежность персонала и программная защищенность информации.

Максименко В. Н. и Ясюк Е. В. выделяют два основных подхода к оценке информационной безопасности предприятия [11]. Первый ориентируется на основные стандарты в области информационной безопасности или другой набор требований. Тогда критерий достижения цели в области безопасности – это выполнение заданного набора требований. Критерий эффективности – минимальные суммарные затраты на выполнение поставленных функциональных требований. Однако необходимый уровень защищенности в данных документах не всегда строго определен, поэтому определить эффективный уровень защищенности информационной системы достаточно сложно. Второй подход связан с оценкой и управлением рисками. Сначала он определялся в соответствии с принципом «разумной достаточности» примененного к сфере обеспечения информационной безопасности предприятия. Этот принцип описывается набором утверждений: абсолютно непреодолимой защиты достичь невозможно; либо необходимо соблюдать баланс между расходами на защиту и получаемым и получаемым эффектом; стоимость средств защиты не должна превышать стоимости информации, которая защищается; расходы нарушителя на несанкционированный доступ к информации должны превышать тот эффект, который он получит, осуществив подобный доступ. Наряду с важнейшим назначением оценки информационной безопасности – создание информационной потребности для совершенствования информационной безопасности, возможны и другие цели проведения оценки информационной безопасности такие, как: определение степени соответствия установленным критериям отдельных областей обеспечения информационной безопасности, процессов обеспечения информационной безопасности, защитных мер; выявление влияния критических элементов (факторов) и их сочетание; и сравнение зрелости различных процессов обеспечения информационной безопасности и и сравнения степени соответствия различных защитных мер установленным требованиям [5, 7, 8, 12].

Таким образом, проведенный анализ позволил определить два основных подхода к оценке информационной безопасности предприятия: первый – на основе характеристик защитных для объекта оценки механизмов и достаточности системы защиты. Суть подхода в том, что вывод об уровне информационной безопасности осуществляется на основании значения показателя эффективности системы защиты. При этом в рамках данного подхода внимание уделяется лишь одному из аспектов информационной безопасности – защита информации от несанкционированного доступа. Второй подход основан на тесной связи системы показателей количественных оценок информационной безопасности с эффективностью функционирования информационной системы в условиях

воздействия всех видов угроз информационной безопасности. Второй подход является методологически более правильным с точки зрения системного анализа, так как в этом случае выполняется один из основных принципов системного подхода, который заключается в том, что каждый элемент системы, выполняя определенную функцию, способствует достижению цели (выполнению общесистемной функции). Обобщая формы, методы и подходы целесообразно предложить группе показателей оценки информационной безопасности, базирующихся на основных направлениях защиты информации и учитывают: оценку программно-технической защищенности информации, оценку затрат на обеспечение информационной безопасности, оценка информационной надежности персонала, оценку информации, предоставляемой лицам, принимающим решения, информационной службой предприятия, оценка риска, надежности, гибкости и управляемости системы защиты информации.

1.2 Понятие и структура угроз защищаемой информации

Существует три различных подхода к выявлению угроз::

1. угроза рассматривается как потенциально существующая ситуация (возможность, опасность) нарушения информационной безопасности, а информационная безопасность означает, что информация находится в такой защищенной форме, которая способна противостоять любым дестабилизирующим воздействиям;

2. угроза трактуется как явление (событие, случай или возможность их возникновения), следствием которого могут быть нежелательные воздействия на информацию;

3. угроза определяется как реальное или потенциальное действие или условие, приводящее к той или иной форме информационной уязвимости.

Любая угроза не сводится к чему-то однозначному, она состоит из определенных взаимосвязанных компонентов, каждый из которых сам по себе не создает угрозу, но является частью ее. Сама угроза возникает только при совокупности и их взаимодействии.

Угрозы защищаемой информации связаны с ее уязвимостью, то есть неспособностью информации самостоятельно противостоять дестабилизирующим воздействиям, нарушающим ее статус. А нарушение статуса защищаемой информации - это нарушение физической безопасности, логической структуры и

содержания, доступности для авторизованных пользователей, конфиденциальности (секретности для посторонних лиц), и выражается посредством реализации шести форм проявления уязвимости информации.

Прежде всего, угроза должна иметь какие-то существенные проявления, а любое проявление называется явлением, поэтому одним из признаков и одновременно одной из составляющих угрозы должно быть явление.

В основе любого явления лежат глубинные причины, которые являются его движущей силой и которые в свою очередь вызваны определенными обстоятельствами или предпосылками. Эти причины и обстоятельства являются факторами, создающими возможность дестабилизирующего воздействия на информацию. Таким образом, факторы являются ее одной из особенностей и составляющей угрозы.

Еще одним определенным признаком угрозы является ее направленность, то есть результат, который может привести к дестабилизирующему воздействию на информацию.

Угроза защищаемой информации – это совокупность явлений, факторов и условий, создающих опасность нарушения статуса информации.

Для выявления структуры угроз необходимо указать признаки угроз по содержательной части, что в свою очередь должно выявить природу явлений и факторов, определить состав и состав условий.

К существенным проявлениям угрозы относятся:

1. источник дестабилизирующего воздействия на информацию (от кого и откуда исходят эти воздействия);

2. виды дестабилизирующего воздействия на информацию (как);

3. методы дестабилизирующего воздействия на информацию (какие методы, действия осуществляются и реализуются виды дестабилизирующих воздействий).

К факторам, отличным от причин и обстоятельств, относится наличие каналов и методов несанкционированного доступа к конфиденциальной информации с целью воздействия на информацию лиц, не имеющих к ней разрешенного доступа.

Глава 2. Угрозы информационной безопасности

2.1 Источники, виды и способы дестабилизирующего воздействия

К источникам дестабилизирующего воздействия на информацию относятся:

1. люди;

2. технические средства отображения, хранения, обработки, воспроизведения, передачи информации, средства связи;

3. системы обеспечения функционирования технических средств;

4. технологические процессы отдельных категорий промышленных объектов;

5. природное явление.

Люди являются наиболее распространенным, многообразным и опасным источником дестабилизирующего воздействия на защищаемую информацию. Это связано с тем, что влияние на защищаемую информацию могут оказывать разные категории людей, как работающих, так и не работающих на предприятии.

Этот источник включает в себя:

(а) работники предприятия;

б) лица, не работающие на предприятии, но имеющие доступ к охраняемой информации в силу служебного положения;

В) сотрудники государственных разведывательных органов других стран и конкурирующих предприятий;

г) лица из криминальных структур.

Технические средства являются вторым наиболее важным источником дестабилизирующего воздействия на защищаемую информацию в силу их многообразия.

Этот источник включает в себя:

а) электронно-вычислительных;

б) электрические и автоматические машины и копировальные аппараты;

в) средства видео-и звукозаписывающей и воспроизводящей аппаратуры;

г) средства телефонной, телеграфной, факсимильной связи, громкоговорители;

д) радио-и телевещание;

е) радиосвязь.

Третий источник дестабилизирующего воздействия на информацию включает системы электроснабжения, водоснабжения, теплоснабжения, кондиционирования воздуха. Этот источник примыкает к вспомогательным электрическим и электронным системам и установкам.

Четвертый источник включает технологические процессы переработки различных объектов атомной энергетики, химической промышленности, радиоэлектроники, а также объектов по производству отдельных видов вооружения и военной техники, изменяющих естественную структуру окружающей среды.

Пятый источник - природные явления, которые включают в себя две составляющие:

а.) стихийное бедствие;

б) атмосферные явления.

Со стороны людей возможны следующие виды дестабилизирующих воздействий:

1. прямое воздействие на защищенные носители;

2. несанкционированное распространение конфиденциальной информации;

3. нарушение режима работы технических средств отображения, хранения, обработки, воспроизведения, передачи информации, связи и технологий обработки информации;

4. выход системы технических средств и средств связи;

5. выход из строя системы и нарушение режима работы систем поддержки функционирования указанных средств.

Методы прямого воздействия на носители защищаемой информации могут быть:

а) физическое уничтожение средств массовой информации;

б) создание чрезвычайной ситуации для перевозчиков;

в) удаление информации из СМИ;

д) создание искусственных магнитных полей для размагничивания носителей;

д) ввод фальсифицированной информации.

Несанкционированное распространение конфиденциальной информации может быть:

а) вербальная коммуникация (размытие);

б) передача копий носителя информации;

с) отображение медиа;

г) ввод информации в компьютерные сети и системы;

е) опубликование информации в открытой печати;

(е) использование информации в публичных заявлениях;

ж) утрата носителей информации может также привести к несанкционированному распространению информации.

Способы нарушения работы технических средств и обработки информации могут быть:

(а) повреждение отдельных компонентов оборудования

б) нарушение правил эксплуатации средств

в) изменения порядка обработки информации

д) заражение программ обработки информации вредоносными программами

е) выдача неправильных команд программы

е) превышение расчетного числа запросов

г) помехи в радио-эфире с помощью дополнительного звукового или шумового фона, изменения (наложения) частот передачи информации

д) передача ложных сигналов

и) подавляющее соединение фильтров в информационных цепях, цепочке питания и заземлении

к) нарушение режима работы систем обеспечения функционирования средств

Четвертый тип включает следующие методы:

а) неправильная установка технического оборудования;

б) разрушение (обрыв) средств, в том числе, повреждение (разрыв) кабельных линий;

В) создание чрезвычайных ситуаций для технических средств;

г) отключение средств от электросетей;

г) отключение или нарушение режима работы средств систем поддержки эксплуатации;

е) установка разрушающих закладок радио и программного обеспечения в электронных компьютерах.

К способам отключения и нарушения работы систем обеспечения функционирования технических средств можно отнести:

а) неправильный монтаж систем;

б) разрушение или поломка систем или их отдельных элементов;

В) создание аварийных ситуаций для систем;

г) отключение систем от источников питания;

д) нарушения правил эксплуатации систем.

К видам дестабилизирующего воздействия второго источника относятся:

а) отказ установок;

б) неисправности средств;

в) создание электромагнитного излучения.

Основными способами дестабилизирующего воздействия второго источника являются:

1. технические поломки и аварии;
2. возгорание технических средств;
3. выход из строя систем обеспечения функционирования средств;
4. негативные воздействия природных явлений;
5. воздействия измененной структуры окружающего магнитного поля;
6. воздействия вредоносных программных продуктов;
7. разрушение или повреждение носителя информации;
8. возникновение технических неисправностей элементов средств.

Видами третьего источника дестабилизирующего воздействия на информацию являются:

1. выход систем из строя;
2. сбои в работе системы.

К способам этого вида относятся:

1. возгорания;
2. поломки и аварии;
3. воздействия природных явлений;
4. выход из строя источников питания;
5. появление технических неисправностей элементов системы;
6. изменения химического состава окружающей среды (на объектах химической промышленности);
7. изменения естественного радиационного фона окружающей среды (на объектах ядерной энергетики);
8. изменения локальной структуры магнитного поля происходящего вследствие деятельности объектов радиоэлектроники и при изготовлении некоторых видов вооружения и военной технике.

К стихийным бедствиям и одновременно видам воздействия следует отнести наводнения, землетрясения, оползни, ураган (смерч), лавины, извержения вулканов.

К атмосферным явлениям (видам воздействия) относятся: гроза, дождь, снег, град, мороз, жара, изменения влажности воздуха и магнитные бури.

2.2 Формы и виды проявления уязвимости защищаемой информации

Виды уязвимости защищаемой информации:

1. кража носителя информации или информации, отображаемой на нем (кража);

2. потеря носителя информации (потеря);

3. несанкционированное уничтожение носителя информации или отображаемой на нем информации (уничтожение);

4. искажение информации (несанкционированное изменение, модификация, подделка, фальсификация и т. д.));

5. блокирование информации (временное или постоянное);

6. разглашение информации (несанкционированное распространение или раскрытие).

Виды угроз информационной безопасности Российской Федерации

По общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие типы:

1. угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуального, группового и общественного сознания, духовного возрождения России;

2. угрозы информационному обеспечению государственной политики Российской Федерации;

3. угрозы развитию отечественной индустрии информации, включая индустрию информации, Телекоммуникации и связь, для удовлетворения потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

4. угрозы безопасности информационно-телекоммуникационных объектов и систем, как уже развернутых, так и созданных на территории России.

Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуального, группового и

общественного сознания, духовного возрождения России может быть:

1. принятие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

2. создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;

3. противодействие, в том числе и от криминальных структур, реализации гражданами конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;

4. нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;

5. незаконное использование специальных средств воздействия на индивидуальное, групповое и общественное сознание;

6. отказ федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;

7. неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам и другой открытой социально значимой информации;

8. дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;

9. нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

10. вытеснение российских информационных агентств, СМИ с внутреннего информационного рынка и усиления зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных

структур;

11. девальвация духовных ценностей, пропаганда массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;

12. снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новых технологий, в том числе информации;

13. манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозы информационному обеспечению государственной политики Российской Федерации может быть:

1. монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;

2. блокирование деятельности государственных СМИ по информированию российской и зарубежной аудитории;

3. низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозы развитию отечественной индустрии информации, включая индустрию информации, Телекоммуникации и связь, для удовлетворения потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут быть:

1. противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, информационных, телекоммуникационных, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;

2. закупка органами государственной власти импортных средств информатизации, Телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;

3. вытеснение с внутреннего рынка российских производителей информации, телекоммуникаций и связи;

4. увеличился отток специалистов и правообладателей интеллектуальной собственности за рубежом.

Угрозы безопасности информационно-телекоммуникационных объектов и систем, как уже развернутых, так и созданных в России, могут быть:

1. незаконный сбор и использование информации;

2. нарушения технологии обработки информации ;

3. введение аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

4. разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем информационной безопасности;

5. уничтожение, повреждение, электронное подавление или уничтожение средств и систем обработки информации, телекоммуникаций и связи;

6. влияние на системы парольной защиты автоматизированных систем обработки и передачи информации;

7. компрометация ключей и средств криптографической защиты информации;

8. утечки информации по техническим каналам;

9. внедрение электронных устройств для перехвата информации в технических средствах обработки, хранения и передачи информации по каналам связи, а также в органах государственной власти, на предприятиях, в учреждениях и организациях независимо от форм собственности;

10. уничтожение, повреждение, уничтожение или хищение машин и других средств массовой информации;

11. перехват информации в сетях передачи данных и линиях связи, дешифрование этой информации и навязывание ложной информации;

12. использование несертифицированных отечественных и зарубежных информационных технологий, информационной безопасности, информации, Телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;

13. несанкционированный доступ к информации в банках и базах данных;

14. нарушение законных ограничений на распространение информации.

2.3 Источники угроз информационной безопасности Российской Федерации

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

К внешним источникам относятся:

1. стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
2. деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
3. деятельность международных террористических организаций;
4. обострение международной конкуренции за обладание информационными технологиями и ресурсами;
5. деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
6. увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
7. разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

критическое состояние отечественных отраслей промышленности;

1. неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
2. недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
3. недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
4. неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
5. недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
6. недостаточная экономическая мощь государства;
7. снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
8. недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
9. отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Информация стала производительной силой и товаром, который продается и покупается, одновременно являясь средством защиты и нападения в отстаивании

государственных, корпоративных и личных интересов субъектов властных отношений. Нормальная жизнедеятельность человека, общества и государства стала целиком определяться уровнем развития, качеством функционирования и безопасностью информационной сферы, где решающими являются качество и скорость обработки информации. Следует заметить, что развитие информационной сферы не признает национально-государственных границ и ведет к образованию глобальных информационных ресурсов, контролируемых межгосударственными организациями и корпорациями, которые навязывают свои стандарты поведения и мышления. Поэтому выражение "Кто владеет информацией - тот владеет миром" - сполна подтверждается политической и экономической практикой. Стоит также обратить внимание на то, что в современной геополитической ситуации меняется политика практически всех европейских стран, а также роль и место военно-политических механизмов обеспечения безопасности и обороны.

На первый план выдвигается проблема строительства новой системы европейской и национальной безопасности, которая должна включать все существующие институты безопасности и обороны за четкого разделения их функций. С геополитической точки зрения новая информационная эра меняет традиционные представления о символах могущества и способы достижения мирового господства. Испокон веков речь шла о наземном пространстве, затем - о воздушном и морском, а ныне речь идет об актуализации роли информационного пространства и о новом поле геополитического противоборства – информационной сфере.

Сейчас еще идут споры о единой глобальной информационной инфраструктуре, об универсальных способах доставки информации, но сказалась вполне определенная тенденция: господствующей роли приобретает интернет, неоспоримым лидером освоения которого является США. Однако уже сегодня существует мнение о необходимости оптимизации путей глобальных информационных потоков. То есть уже можно говорить о том, что мир стоит на пороге новой схватки за контроль над информационным пространством и «транспортировкой информации». Безусловно, в современных геополитических условиях растет значение информационного фактора. Четко прослеживается тенденция повышения роли информационного ресурса государств в общей системе оборонного потенциала. К важнейшим его элементам относятся информационные системы и средства стратегического предупреждения, управления войсками и оружием, навигации, разведки, радиоэлектронной борьбы. Достижение информационного преимущества (доминирование) обеспечивает возможность опережать соперника в принятии военно-политических решений и является основой и во многом залогом успеха в

военных действиях. Как отмечают современные отечественные исследователи, научно-техническая революция создала глобальное информационное пространство, в котором обладание информационными ресурсами становится главным фактором геополитической конкуренции, поэтому информационная отрасль относится к стратегическим интересам любой страны и требует особого внимания. Технологический отрыв США, Японии и ряда европейских стран, развертывание ими работ по созданию на базе современных информационных технологий информационного оружия и военной техники нового поколения ведут к качественно новому этапу гонки вооружений. Приоритетное развитие систем и средств предупреждения о ракетно-ядерном нападении, ПВО и ПРО, оружия на новых физических принципах в совокупности приводит к критическому снижению роли ядерного сдерживания. Результаты исследований некоторых ученых свидетельствуют, что воздействие на информационный ресурс может стать одним из источников опасности для национальных интересов. В последние годы наиболее сложной формой влияния считается рефлексивное управление процессом принятия военно-политических решений с помощью целевого формирования информации или дезинформации, что побуждает совершать желаемые действия. Например, этому вопросу уделяется большое внимание в рамках принятой в США стратегической концепции соперничества.

Результаты проведенных исследований позволяют выделить следующие основные геополитические изменения в информационной сфере:

1) информационное пространство западных государств стремительно превращается в единое глобальное информационное пространство, где доминирующую роль в контроле над информационными потоками играют США и страны ЕС;

2) формируется глобальная информационная инфраструктура на основе сети Интернет, что может рассматриваться как усиление пространственной взаимозависимости государств;

3) существенно расширился военно-информационное пространство, контролируемое странами НАТО;

4) в современном информационном пространстве усиливаются процессы, связанные с развитием отношений партнерства и глобального информационного противостояния;

5) одной из основных сфер геополитического противоборства становится информационное пространство глобального, регионального и национального уровней.

При этом его приоритет на указанных уровнях зависит от конкретных целей государства и может постоянно меняться. По долгосрочным прогнозам, перспективы мирового развития будет определять глобальное перегруппировка сил в результате информационного прогресса в США, ЕС, Японии, Китае, Индии и России. Предусматривается развитие трех мощных информационных «центров мира»: американского (США), европейского (Европейский Союз) и азиатского (Китай, Индия, Япония).

Подобным центром информационного влияния в современных условиях пытается стать и Российская Федерация. При этих условиях в различных странах мира, в частности в России, активно разрабатываются и применяются на практике информационно-психологические средства ведения глобального информационного противоборства. Прежде всего, они касаются сферы использования информации против человеческого интеллекта.

Несмотря на то, что средства воздействия (дезинформация, слухи, пропаганда, агитация, мифы и т. п.) остались прежними, принципиально новым элементом стали средства получения и доставки информации. Это, в частности, системы глобального и межрегионального телерадиовещания, с помощью которых реальные события с соответствующими комментариями и специально подобранные факты и аргументы становятся доступны аудитории во многих странах мира. Крайне важной в контексте информационной безопасности человека, общества и государства является проблема противодействия информационному насилию, информационным операциям и глобальному информационному противоборству (войнам).

Ключевые проблемы информационной безопасности:

– в информационной сфере человечества происходят революционные изменения и трансформации, которые активизируют новые глобальные вызовы и угрозы;

– большинство стран мира уже столкнулась с проблемами кибертерроризма, киберпреступности и другими проблемами информационной безопасности;

– в течение последних десятилетий наблюдается тенденция к распространению информационной агрессии и насилия;

– получают распространение попытки манипуляции сознанием человека, агрессивная реклама, периодически проводятся информационно-психологические операции;

– почти в 120 странах мира ведутся разработки информационного оружия или ее элементов (для сравнения – разработки оружия массового уничтожения осуществляются почти в 20 странах);

– последствия использования современной информационной оружия (согласно заключению ученых и экспертов европейских стран, РФ и США) могут быть сопоставимыми с применением оружия массового поражения;

– новейшие вызовы и угрозы в информационной сфере представляют реальную угрозу безопасности человечества и международного правопорядка.

По нашим оценкам, ни одно государство мира в условиях информационной глобализации не способна самостоятельно обеспечить собственную информационную безопасность.

Обобщая характер внешних угроз информационной безопасности РФ, к их основным источникам следует отнести: 1) деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов РФ в информационной сфере; 2) стремление ряда стран к доминированию и ущемлению интересов РФ в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков; 3) обострение международной конкуренции за обладание информационными технологиями и ресурсами; 4) увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных отечественных информационных технологий; 5) деятельность космических, воздушных, морских, наземных технических и иных средств (видов) разведки иностранных государств; 6) разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран, нарушение нормального функционирования информационных и телекоммуникационных систем, информационных ресурсов, получение несанкционированного доступа к ним.

Кроме этого, в контексте данного исследования стоит обратить внимание на основные виды угроз информационной безопасности: – вытеснение отечественных информационных агентств, средств массовой информации с внутреннего

информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни от зарубежных информационных структур; – манипулирование информацией (дезинформация, сокрытие или искажение информации). Из числа внешних угроз информационной безопасности в сфере внешней политики наибольшую опасность представляют: – информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию внешней политики государства; – распространение за рубежом дезинформации о внешней политике РФ; – нарушения прав граждан и юридических лиц в информационной сфере в РФ и за рубежом; – попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру органов государственной власти, реализующих государственную внешнюю политику.

Таким образом, в последнее десятилетие сказались основные потенциальные угрозы информационной безопасности РФ. В мире произошли определенные позитивные изменения, которые благоприятно сказались на геополитическом положении постсоветских стран, однако, современный мир все-таки не стал более стабильным и безопасным. На смену прежнему идеологическому противоборству пришло геополитическое соперничество новых центров силы. Информационное противостояние этносов, религий и цивилизаций стало выходить на передний план в системе межгосударственных отношений. Специфика периода, который сейчас переживает РФ, характеризуется поиском вектора политической ориентации в межгосударственном и геополитическом пространстве. Так, после обретения независимости качественно ухудшились ее экономические, военные возможности, возникло множество связанных с агрессивностью факторов, которые угрожают национальным интересам или способных при дальнейшем неблагоприятном развитии событий трансформироваться в реальные угрозы их безопасности. Угрозы такого типа являются постоянными и присущими как стабильным, так и транзитивным социальным системам. Однако в условиях социокультурного транзита появляется большое количество новых угроз, которые разрушают основы информационной безопасности человека, общества и государства. В общем, традиционный подход к определению угроз информационной безопасности позволяет выделить следующие основные группы угроз.

Первая группа связана с бурным развитием нового класса оружия – информационного, которое способно эффективно воздействовать и на психику, сознание людей, и на информационно-техническую инфраструктуру общества и

армии.

Вторая группа – информационно-технические угрозы для человека, общества и государства – это новый класс социальных преступлений, которая основывается на использовании современной информационной технологии (махинации с электронными деньгами, компьютерное хулиганство и тому подобное).

Третья группа – электронный контроль за жизнью, настроениями, планами граждан, политических организаций.

Четвертая группа – использование новых информационных технологий с политической целью.

Предложенный подход к анализу системы информационного обеспечения и информационной безопасности позволяет выделить следующие основные группы угроз:

1) угрозы, связанные с разрушением или деградацией базисной информационной подсистемы общества, обеспечивающей сохранение и развитие его информационно-культурного ядра. Реальным носителем и хранителем этого ядра является система образования и воспитания новых поколений общества. Реальной угрозой для нее является, с одной стороны, недостаточное внимание самого общества к защите и развитию своего информационно-культурного базиса, а с другой – лишний и не всегда положительное информационное воздействие на эту систему со стороны других государств, заинтересованных в ее трансформации в приемлемом для них направлении;

2) угрозы, связанные с разрушением или деградацией динамической продуктивной информационной подсистемы общества. Реальными производителями в этой сфере являются все научные, технические, аналитические, идеологические центры, создающие или импортирующие соответствующую информационную продукцию и информационные технологии. В условиях динамического формирования и развития информационного общества и глобального информационного пространства практически невозможно определить исчерпывающий перечень угроз информационной безопасности.

Заключение

Информационная безопасность является сложным, системным, многоуровневым явлением, на состояние которого влияют внешние и внутренние факторы, в частности политическая обстановка в мире; внутриполитическая обстановка в государстве; состояние и уровень информационно-коммуникационного развития страны и тому подобное. Угрозы информационной безопасности в основном сопровождают возникновение и реализацию угроз в экономической и политической сферах, в сфере исполнения функций государства и т.д., и причинение вреда в информационные сфере является, прежде всего, средством достижения других целей. Наряду с чисто корыстной целью в современных условиях информационные угрозы связаны с разжиганием межнациональной, межконфессиональной и другой вражды, дискредитацией правоохранительной системы и органов государственной власти в целом, причинением вреда чести, достоинства и деловой репутации физических лиц, в том числе публичных, формированием «образа врага», «зомбированием» населения для создания условий по управлению массовым сознанием. При этом потенциал информационной сферы из-за ее интегрируемых характер и способность «проникновение» в другие сферы жизнедеятельности общества вследствие их информационного обслуживания пока недостаточно осознается политиками и правоохранителями (за исключением проявлений киберпреступности), однако успешно используется представителями организованных преступных сообществ и политическими противниками нашего государства.

Особенностью предлагаемой системы показателей оценки информационной безопасности предприятия является то, что она охватывает экономические показатели, технические и программные параметры системы информационной безопасности и предоставляет оценку персонала, осуществляющего управление указанным подсистемой. Также такая система показателей оценки информационной безопасности предприятия может быть применена на любом предприятии, независимо от его размера, сферы и направления деятельности, что делает ее универсальной. В то же время, стоит отметить, что в зависимости от цели диагностики уровня информационной безопасности показатели в каждой группе могут быть дополнены или заменены. Важной проблемой остается взаимосогласованность предлагаемых показателей в группе и между собой, а также разработка интегрального показателя информационной безопасности предприятия, и является перспективным направлением дальнейших исследований.

Список литературы

1. Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28 - STD, 1985 [Electronic resource]. – Access mode : http://csrc.nist.gov/publications/history/ dod85.pdf
2. Information Tecnhology Security Evaluation Criteria, v. 1.2. – Office for Official ublications of the European Communities, Printed and published by the Department of Trade and Industry, London, 1991. – 164 p.
3. Канадские критерии безопасности компьютерных систем (Canadian Trusted Computer Product Evaluation Criteria. – [Электронный ресурс]. – Режим доступа: https://www.resear chgate.net/publication/3506169_The_Canadian_Trusted_Computer_Product_Evaluation_Crit CTCPEC 4
4. Федеральные критерии безопасности информационных технологий» (Federal Criteria for Information Technology Security. – [Электронный ресурс]. – Режим доступа: https://www.com moncriteriaportal.org/files/ccfiles/ccpart1v2.3.pdf
5. Андрианов В. В. Оценка информационной безопасности бизнеса / В. В. Андрианов, В. Бы. Голованов, Н. А. Голдуев, С. Л. Зефиров. – 2-е изд., перераб. и доп. – М.: ЦИПСиР: Альпина Паблишерз, 2011. – 373 с. + 8 с. вкл.
6. Велигура А. В. Оценка состояния информационной безопасности предприятия / А. В. Велигура // Управление проектами и развитие производства. – 2014. – №4(52). - С. 28-39.
7. Журавль М. Ю. Формирование системы показателей оценки уровня информационной безопасности предприятия / Журавель м. Ю., Полозова Т. В., Стороженко О. В. / / Вестник экономики транспорта и промышленности. - 2011. - №33. - С. 171-177.
8. Ильяшенко С. М. Экономический риск [Текст]: учеб. пособ. 2-е изд., доп., переработка. / С. М. Ильяшенко – К.: Центр учебной литературы, 2004. - 220 С.
9. Кононова В. О. Оценка средств защиты информационных ресурсов / Кононова В. О, Харкянен О. В., Грибков С. В. / / Вестник Национального университета. Компьютерные системы и сети. – 2014. – № 806. – С. 99-105.
10. Кравчук Е. Я. Диагностика уровня и критерии оценки корпоративной безопасности субъектов хозяйствования / А. Я. Кравчук, П. Я. Кравчук // Экономические науки. Серия «Экономика и менеджмент»: сборник научных трудов. - Выпуск 1. Редкол.: ОТП. ред. д.э.н., проф. Герасимчук И. В. – Л., 2004. – С. 85-109.
11. Максименко В. Н. Основные подходы к анализу и оценке рисков информационной безопасности / В. Н. Максименко, Е. В. Ясюк // Экономика и качество систем святи. - 2017. - 2/2017. - С. 42-48.

12. Морозова В. И., Врублевский К. Э. Защита информации в вычислительных системах: [учеб. пособ.] / Под ред. В.Ы.Морозовой – М.: МИИТ, 2008 – 122 с.
13. Реверчук Н.И. Управление экономической безопасностью предпринимательских структур: [монограф.] / Н . И. Реверчук. – Л.: ЛБИ НБУ, 2004. – 195 с.
14. Хоффман Л. Дж. Современные методы защиты информации // Пер. с англ. – М.: Советское радио, 1980. – 264 с.