Содержание:

ВВЕДЕНИЕ

На сегодняшний день увеличивается значимость и заинтересованность к экономической и информационной безопасности как к аспекту функционирования предприятия. В современных условиях обеспечение безопасности является основой существования отдельных хозяйствующих субъектов (предприятий, фирм), различных форм собственности. Существует множество определений экономической безопасности предприятия, но в общем, под ней понимается способность предприятия наиболее эффективно достигать основной цели (получать прибыль) в рыночной экономике, за счет четкого выполнения предприятием своих функций в условиях воздействия внутренних и внешних угроз.

Современные информационные технологии не только открывают значительные возможности, но и порождают новые проблемы развития российского общества и государства, несут новые опасности, вызовы и угрозы его безопасности, одной из важнейших составляющих которой является информационная безопасность.

Целью данной работы является изучение источников угроз информационной безопасности.

Объектом исследования является совокупность общественных отношений по обеспечению информационной безопасности РФ .

Предметом исследования выступают теоретико правовые проблемы информационной безопасности и ее правового обеспечения в интересах человека, общества и государства.

Задачи работы:

Дать определение информационной безопасности;

Рассмотреть виды и источники угроз информационной безопасности;

Изучить реализацию информационной безопасности государственного казенного учреждения Новосибирской области «Управление контрактной системы»

Методологическая основа исследования представлена традиционным диалектическим методом познания объективной действительности в сочетании с приемами и методами формальной логики.

ГЛАВА 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1.Общее понятие об информационной безопасности

Информационная безопасность не является проблемой, специфичной только для России. Практически все страны с развитой экономикой на уровне государственных органов, предпринимательских структур разрабатывают и применяют комплексные меры, направленные на обеспечение информационной безопасности. Эти вопросы относятся к числу тех, которые требуют постоянного внимания государства и приоритетного решения, повышения степени государственного контроля за соблюдением требований безопасности в информационном пространстве. Существенный вклад в обеспечение информационной безопасности может внести формирование современного законодательства в данной сфере [6].

Исследование современных угроз информационной безопасности невозможно без четкого уяснения юридической сущности таких понятий как безопасность, информационная безопасность и угроза информационной безопасности.

Безопасность – предельно широкая категория. Так, можно говорить о национальной безопасности, продовольственной безопасности, экологической безопасности, финансовой безопасности и т.п. Ныне не действующий Закон РФ от 5 марта 1992 г. № 2446-1 «О безопасности»[1] справедливо определял безопасность как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, в то время как Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» не дает законодательного определения безопасности. Данное обстоятельство необходимо признать законодательным пробелом, т.к. точное применение норм права невозможно без легального закрепления сущности основных понятий.

Согласно п. 6 Стратегии национальной безопасности Российской Федерации до 2020 года, утвержденной Указом Президента РФ от 31 декабря 2015 г. № 683[3], национальная безопасность Российской Федерации (далее – национальная безопасность) – состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации (далее – граждане), достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности.

Другими словами, безопасность характеризуется комплексностью, а информационная безопасность является ее составляющей.

Стратегия национальной безопасности РФ до 2020 года, утвержденная Указом Президента РФ от 31 декабря 2015 г. № 683, является базовым документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты Российской Федерации, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление национальной безопасности Российской Федерации и обеспечение устойчивого развития страны на долгосрочную перспективу. А Доктрина информационной безопасности РФ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Также, необходимо отметить, что информационная безопасность представляет собой институт информационного права. Как поясняет И.Л. Бачило, категория «институт права» выполняет роль связи норм отдельных отраслей права с реальными отношениями, реализуемыми в определенных областях через методы и формы воздействия на поведение участников этих отношений. При этом институт информационной безопасности относится, по мнению ученой, к общим правовым институтам информационного права. В этой связи спорной представляется точка зрения М.А. Ефремовой, согласно которой «необходимо вести речь об информационной безопасности как объекте уголовно-правовой охраны и об информационной безопасности как о сложном институте уголовного права».

1.2 Источники, виды и факторы угроз ифнормационной безопасности

Понятие «угрозы безопасности» предполагает изменение во внешней и внутренней среде субъекта, которые приводят к негативному изменению предмета безопасности. В качестве предмета угроз могут выступать такие параметры составной части хозяйственной системы предприятия, которые могут выйти за допустимый интервал, считающийся безопасным. Имеется большое число различных классификаций угроз с точки зрения экономической безопасности предприятия. Каждая классификация в той или иной степени условна. Безусловно, нижеуказанные виды угрозы не являются взаимоисключающими, а пересекаются друг с другом. [5]

Относительно субъекта виды угрозы безопасности делят на внешние и внутренние. Внешние угрозы определяются воздействием внешней среды – непостоянность в политике и экономике, усугубление глобальных экологических проблем, непрогнозируемая реакция торговых партнеров и др.; внутренние угрозы – состоянием самого предприятия. Подчеркнем что, внутренние угрозы могут как усиливать, так и ослаблять действие внешних угроз, и наоборот. Угрозы можно разделить на реальные, перемены которые произошли, и потенциальные, которые могут случиться при определенных условиях. Относительно времени различают угрозы, которые порождают негативные изменения через короткие интервалы времени (регулярные и спорадические), и перспективные, которые проявляются через длительный промежуток времени после возникновения данной угрозы. Относительно степени возникновения имеются угрозы целенаправленные, создаваемые другими субъектами с определенными целями, и возникающие спонтанно, которые возникают вследствие неожиданных происшествий. Относительно степени влияния бывают угрозы, носящие опосредованный характер, функционируют при определенных дополнительных условиях, или проявляться непосредственно, непосредственно стимулируя негативные изменения.

По виду деятельности угрозы подразделяются на экономические, политические, социальные и экологические. В настоящее время получила наиболее широко распространенная классификация угроз экономической безопасности согласно сферам их появления: предприятию как целому – экономическая несостоятельность, малограмотное руководство или порча репутации (ведущие к несостоятельности); информации – потеря наиболее важных сведений;

материальным активам – физическая утрата (уничтожение или пропажа) или порча; нематериальным активам – их устранение (к примеру, отзыв лицензии, не продление сертификата и пр.); финансам – утрата; перспективам развития – неблагоприятные рыночные обстоятельства. Классификация угроз информационной безопасности:

1. Разглашение это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним.

2. Утечка это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

3. Несанкционированный доступ это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам. Сравнительно источника появления угрозы экономической безопасности предприятия можно разделить на объективные и субъективные.

Объективные источники возникают без участия и помимо желания предприятия или его служащих, независимо от решений, действий принятых менеджером – это состояние финансовой конъюнктуры, научные открытия, форс мажорные обстоятельства и т. д. Субъективные источники появляются из за действий людей, умышленные или неумышленные, различных органов и организаций, в том числе государственных и международных предприятий, конкурентов. Объективные источники необходимо уметь распознавать и обязательно учитывать в управленческих решениях. Предотвращение субъективных источников во многом связано с воздействием на субъекты экономических отношений. [3]

В качестве источников угроз финансовой защищенности могут выступать:

1) внешние источники:

рынок – изменение спроса, курсов валют, продуктовой линейки, стоимости кредитов, повышение конкуренции;

недобросовестная конкурентная борьба либо незаконные воздействия третьих лиц, нацеленные против предприятия;

угрозы репутации компании по политическим, религиозным и иным мотивам, идущие от органов государственной власти и общественных организаций;

промышленные катастрофы, аварии, террористические акты, стихийные бедствия.

2) внутренние:

служащие предприятия – оглашение конфиденциальных данных, целенаправленные нарушения контрольных процедур с целью хищения, безответственность, саботаж;

недоработка процессов контрольных процедур (отсутствие требуемого контроля, неосведомленность их персоналом).

Факторы экономической безопасности предприятия – это совокупность окружающих обстоятельств, которые влияют на характеристики безопасности. Факторы финансовой защищенности делят на внутренние и внешние. Внешние факторы можно разбить на три подгруппы:

1) макроэкономические: этап формирования экономики государства, устойчивость хозяйственного законодательства, уровень инфляции, соотношение валют, покупательская способность населения, положение финансовой системы, государственная политика (антимонопольная, инвестиционная, налоговая, инновационная, регуляторная, внешнеэкономическая, ценовая);

2) рыночные: потребительский и производственный спрос, уровень цен на сырьевые материалы и готовую продукцию, динамика конкурентной борьбы в регионе и отрасли, действия конкурентов, емкость рынка, платежеспособность контрагентов; 3) прочие: темпы научно технического прогресса, демографические тенденции, криминогенная ситуация, природно климатические условия и др. [6]

Совокупность внутренних факторов финансовой защищенности можно разбить на следующие группы:

1) финансовые: состав и ликвидность активов, состав капитала, обеспеченность собственным оборотным капиталом, степень рентабельности, прибыльность инвестиционных проектов, дивидендная политика;

2) производственные: применение оборотных и основных средств, положение и состав основных фондов, система контроля качества, состав себестоимости;

3) кадровые: организационная структура управления, мотивирование персонала, наличие стратегии развития, квалификация и состав персонала, параметры оплаты труда, степень рационализаторской инициативности, социальные мероприятия;

4) материально технического обеспечения: уровень диверсификации поставок сырья, качество поставляемого сырья, периодичность поставок, применение современных технологий;

5) инвестиционно технологические: НИОКР, наличие вкладываемых ресурсов, уровень инновационной активности; 6) сбытовые: выбор продукции, ценовая политика, набор заказов, степень диверсификации покупателей, политика расчетов с потребителями, готовность отправляемой продукции, осуществление маркетинговых исследований;

7) экологические: введение новых технологий, реализация природоохранных мероприятий. В заключении хочется отметить, что для обеспечения безопасности экономических данных предприятия необходимо учесть все возможные варианты защиты экономических данных и обеспечить полную конфиденциальность данных на предприятии. Тем самым защита экономической безопасности это комплекс мероприятий, направленных на обеспечение экономической безопасности, которая обеспечит предприятию необходимый аспект ведения бизнеса в условиях агрессивной рыночной экономики

1.3 Источники угроз информационной безопасности РФ

В современных условиях на фоне усиления роли информационной сферы и интенсивного развития информационных технологий существенно возрастают потребности общества и государства в решении вопросов обеспечения информационной безопасности. Сфера жизнедеятельности общества, учитывая динамику научно-технического прогресса, все больше становится зависимой от информационной среды и информационных технологий. Соответственно, от состояния информационной безопасности и мер, принимаемых государством по защите различных видов информации, а также результативности деятельности субъектов ее обеспечения зависит в целом безопасность жизнедеятельности общества и государства. [12]

Современные информационные технологии не только открывают значительные возможности, но и порождают новые проблемы развития российского общества и государства, несут новые опасности, вызовы и угрозы его безопасности, одной из важнейших составляющих которой является информационная безопасность.

Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе развития технического прогресса, быстрыми темпами растущего использования современных информационных технологий эта зависимость неизбежно возрастает. Значимость информационной безопасности для Российской Федерации обусловлена тем, что информационная сфера обеспечивает функционирование всех остальных сфер жизни общества и государства.

Информационная безопасность не является проблемой, специфичной только для России. Практически все страны с развитой экономикой на уровне государственных органов, предпринимательских структур разрабатывают и применяют комплексные меры, направленные на обеспечение информационной безопасности. Эти вопросы относятся к числу тех, которые требуют постоянного внимания государства и приоритетного решения, повышения степени государственного контроля за соблюдением требований безопасности в информационном пространстве. Существенный вклад в обеспечение информационной безопасности может внести формирование современного законодательства в данной сфере.

Исследование современных угроз информационной безопасности невозможно без четкого уяснения юридической сущности таких понятий как безопасность, информационная безопасность и угроза информационной безопасности.

Безопасность – предельно широкая категория. Так, можно говорить о национальной безопасности, продовольственной безопасности, экологической безопасности, финансовой безопасности и т.п. Как пишет Е.С. Недосекова, «в сущности, национальная безопасность – только составляющая общего понятия безопасности. Ныне не действующий Закон РФ от 5 марта 1992 г. № 2446-1 «О безопасности» справедливо определял безопасность как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, в то время как Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» не дает законодательного определения безопасности. Данное обстоятельство необходимо признать законодательным пробелом, т.к. точное применение норм права невозможно без легального закрепления сущности основных понятий.

Согласно п. 6 Стратегии национальной безопасности Российской Федерации до 2020 года, утвержденной Указом Президента РФ от 31 декабря 2015 г. № 683, национальная безопасность Российской Федерации (далее – национальная безопасность) – состояние защищенности личности, общества и государства от

внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации (далее – граждане), достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности.

Другими словами, безопасность характеризуется комплексностью, а информационная безопасность является ее составляющей.

По данным Ю.И. Мигачева и Н.А. Молчанова, «правовое регулирование вопросов, касающихся отдельных видов безопасности, осуществляется на основании более чем 70 федеральных законов, 200 указов Президента РФ, около 500 постановлений Правительства РФ, а также других подзаконных актов. Большинство из них имеют фрагментарный характер, касаются частных угроз и порождают локальные, разрозненные массивы правовых норм, относящиеся к различным отраслям права».

В «Модельном информационном кодексе для государств-участников СНГ» законодатель предлагает считать обеспечение информационной безопасности одной из составляющих совокупности систем национальной информационной инфраструктуры (т.е. понятие «информационная структура» шире, чем понятие «информационная безопасность»). [10]

В научной литературе отсутствует единство подходов к юридической сущности понятия «безопасность».

Учитывая, что детальный анализ категории «безопасность» невозможен в рамках настоящего исследования, применительно к его предмету представляется возможным присоединиться к позиции В.Н. Конина. Данный автор предлагает следующее определение: «безопасность – это система общественных отношений (государственных, правовых, политических, экономических, культурных, духовных, религиозных и др.), образующих особое состояние жизнедеятельности социума, его структур и институтов, при которых обеспечивается сохранение их качественной определенности, гармоничное функционирование и поступательное развитие».

Основным документом, определяющим политику нашей страны в сфере информационной безопасности, является Доктрина информационной безопасности Российской Федерации. Доктрина определяет цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. В этом документе информационная безопасность Российской Федерации понимается как состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

ГЛАВА 2. ЗАЩИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1 Информационная безопасность в управлении современной организацией

Согласно Постановлению Правления Пенсионного Фонда РФ от 26.01.2001 № 15 «О введении в системе Пенсионного фонда Российской Федерации криптографической защиты информации и электронной цифровой подписи», под информационной безопасностью следует понимать состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.д..

Уровень информационной безопасности можно определить следующими критериями:

1. Целостностью информации, заключающейся в обеспечении защиты информации от различного рода сбоев, которые приводят к повреждению или ее полному уничтожению.

2. Конфиденциальностью информации, согласно которой информация не должна быть доступна посторонним пользователям.

3. Доступность информации авторизованным пользователям. Итак, хранение и использование информации в современной организации должно быть

спланировано таким образом, чтобы вышеперечисленные принципы были соблюдены. Систему финансовой безопасности составляют следующие аспекты: компьютерная безопасность, которая зависит от принятия технологических и административных решений, обеспечивающих качественную работу всех аппаратных компьютерных систем; безопасность данных – защита информации от случайных нарушений или преднамеренных атак; безопасное программное обеспечение, направленная на обеспечение безопасной работы всех систем и безопасную обработку данных; безопасность коммуникаций, обеспечивающаяся благодаря аутентификации систем телекоммуникаций, предотвращающих доступность информации неавторизированным пользователям. [9]

Итак, современная организация, в которой наблюдается непрерывное увеличение количества информации, сталкивается с рядом угроз, имеющих как внешние, так и внутренние источники. атаки хакеров и вредоносных программ извне; стихийные бедствия (пожары, наводнения, аварии в энергосистемах), приводящие к повреждению или полной утере информации; сотрудники организации, являющиеся инсайдерами, преднамеренно наносящие угрозу информационной безопасности; сотрудники организации, являющиеся незлонамеренными нарушителями по причине недостаточного уровня профессионализма [3].

Следует отметить, что преднамеренные нарушения со стороны сотрудников случаются гораздо реже, чем утечки информации, совершаемые по неосторожности или из-за технической безграмотности сотрудников организации. В целях обеспечения информационной безопасности организации рекомендуется реализация следующих мер:

1. Формирование четкой и продуманной политики организации в сфере информационной безопасности.

2. Применение технических и программных средств защиты информации.

3. Разработка и реализация ряда организационных мероприятий. Таким образом, информационная безопасность организации представляет собой совокупность решений, направленных на защиту коммерческой информации от различного рода угроз в целях качественного ведения бизнеса. Это могут быть данные о покупателях и поставщиках, управленческие и бухгалтерские документы, персональные данные сотрудников организации, информация о технологиях и многое другое. Для обеспечения безопасности информационных систем, руководством организац.

Следует отметить, что большинство исследований определяют безопасность через преобладание мощи над другими государствами, либо с позиций взаимодействия государств, то есть создания оптимальных условий развития всей системы международных отношений. Таким образом, вопросы информационной безопасности являются ключевыми для обеспечения законности и равноправия в «информационном обществе». Информационная безопасность как категория, находящаяся на стыке различных наук, отражает связь безопасности с нацией. Следует также констатировать, что успешное решение проблемы безопасности в Кыргызстане требует применения комплексного подхода и участия в этом процессе практически всех государств вне зависимости от их различия в общественно-политическом строе и социально-экономическом развитии.

2.2 Классификация угроз безопасности бизнеса

Классификация угроз безопасности может быть осуществлена разделением угроз на связанные с внутренними и внешними факторами .
Множество непреднамеренных угроз, связанных с внешними (по отношению к бизнесу) факторами, обусловлено влиянием воздействий, неподдающихся предсказанию (например, угрозы связанные со стихийными бедствиями, теногенными, политическими, экономическими, социальными факторами, развитием информационных и коммуникационных технологий, другими внешними воздействиями).

К внутренним непреднамеренным относят угрозы, связанные с отказами вычислительной и коммуникационной техники, ошибками программного обеспечения, персонала, другими внутренними непреднамеренными воздействиями. Отдельно следует выделить угрозы связанные с преднамеренными ошибками, возникающие за пределами бизнеса. К таким угрозам относят следующее:

несанкционированный доступ к информации, хранящейся в системе;
отрицание действий, связанных с манипулированием информацией (например, несанкционированная модификация, приводящая к нарушению целостности данных);

ввод в программные продукты и проекты «логических бомб», которые срабатывают при выполнении определенных условий или по истечении определенного периода времени и частично или полностью выводят из строя компьютерную систему;

разработка и распространение компьютерных вирусов;
небрежность в разработке, поддержке и эксплуатации программного обеспечения, приводящие к краху компьютерной системы;

изменение компьютерной информации и подделка электронных подписей;
хищение информации с последующей маскировкой (например, использование идентификатора, не принадлежащего пользователю, для получения доступа к ресурсам системы);

перехват (например, нарушение конфиденциальности данных и сообщений);

отрицание действий или услуги (отрицание существования утерянной информации);

отказ в предоставлении услуги (комплекс нарушений, вызванных системными ошибками, несовместимостью компонент и ошибками в управлении). [11]

Под несанкционированным доступом (НСД) к ресурсам информационной системы понимаются действия по использованию, изменению и уничтожению исполняемых модулей и массивов данных системы, проводимые субъектом, не имеющим права на подобные действия.

К сожалению, приходится констатировать, что унифицированный подход к классификации угроз информационной безопасности отсутствует. И это вполне объяснимо, так как при всем том многообразии информационных систем, направленных на автоматизацию множества технологических процессов, которые затрагивают различные сферы человеческой деятельности, жесткая систематизация и классификация угроз неприемлема.

Наиболее приемлемой в настоящее время можно считать следующую классификацию (см. рис. 1).

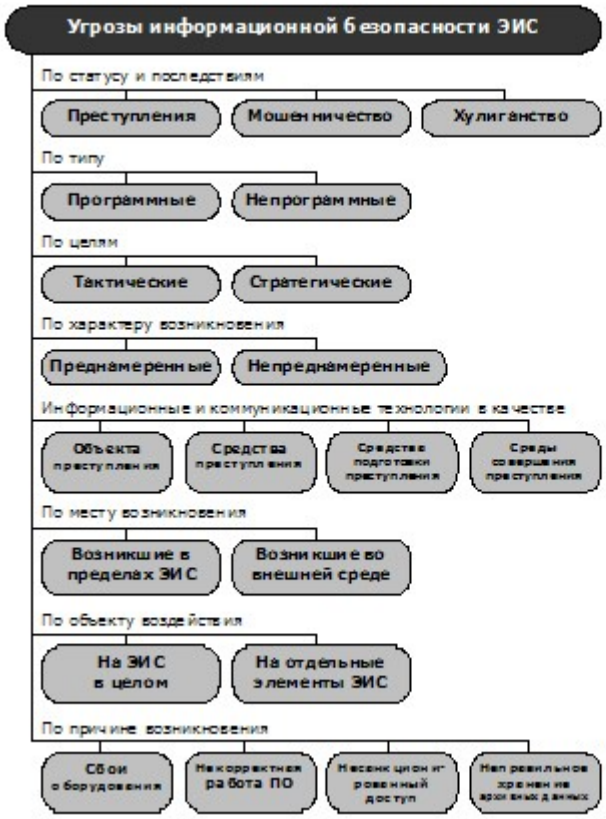

Рис. 1. Классификация угроз информационной безопасности

Как видно из рисунка, по составу и последствиям ПЗ представляются в виде преступлений, мошенничеств и хулиганств.

Под компьютерным преступлением (КП) следует понимать комплекс противоправных действий, направленных на несанкционированный доступ, получение и распространение информации, осуществляемых с использованием средств вычислительной техники, коммуникаций и ПО.

Компьютерное мошенничество отличается от других видов компьютерных нарушений тем, что его целью является незаконное обогащение нарушителя.

Компьютерное хулиганство, на первый взгляд, является безобидной демонстрацией интеллектуальных способностей, но последствия подобных действий могут быть весьма серьезными, поскольку они приводят к потере доверия пользователей к вычислительной системе, а также к краже данных, характеризующих личную или коммерческую информацию.

По типу реализации можно различать программные и непрограммные злоупотребления. К программным относят злоупотребления, которые реализованы в виде отдельного программного модуля или модуля в составе программного обеспечения. К непрограммным относят злоупотребления, в основе которых лежит использование технических средств для подготовки и реализации компьютерных преступлений (например, несанкционированное подключение к коммуникационным сетям, съём информации с помощью специальной аппаратуры и др.).

Компьютерные злоумышленники преследуют различные цели и для их реализации используют широкий набор программных средств. Исходя из этого, представляется возможным объединение программных злоупотреблений по целям в две группы: тактические и стратегические. К тактическим относят злоупотребления, которые преследуют достижение ближайшей цели (например, получение пароля, уничтожение данных и др.). К группе стратегических относятся злоупотребления, реализация которых обеспечивает возможность получения контроля над технологическими операциями преобразования информации, влияние на функционирование компонентов ИС (например, мониторинг системы, вывод из строя аппаратной и программной среды и др.).
По характеру возникновения различают непреднамеренные и преднамеренные злоупотребления. [8]

Непреднамеренные угрозы связаны со стихийными бедствиями и другими неподдающимися предсказанию факторами, сбоями и ошибками вычислительной техники и программного обеспечения, а также ошибками персонала.
Преднамеренные угрозы обусловлены действиями людей и ориентированы на несанкционированное нарушение конфиденциальности, целостности и/или доступности информации, а также использование ресурсов в своих целях.
При реализации угроз безопасности информационные и коммуникационные технологии могут выступать в качестве объекта преступления, средства преступления, средства подготовки преступления или среды совершения преступления.

По месту возникновения угроз безопасности ЭИС можно различать угрозы, возникающие в пределах ЭИС и угрозы, возникающие во внешней среде.

По объекту воздействия следует выделять угрозы, воздействующие на ЭИС в целом и угрозы, воздействующие на отдельные ее элементы.
По причине возникновения различают такие угрозы, как сбои оборудования, некорректная работа операционных систем и программного обеспечения,

несанкционированный доступ и неправильное хранение архивных данных, вследствие чего они могут быть утеряны (уничтожены).

Реализация нарушителями угроз безопасности ЭИС приводит к нарушению нормального функционирования ЭИС и/или к снижению безопасности информации, определенное конфиденциальностью, целостностью и доступностью.

2.3 Методы защиты информационной безопасности

В современном мире информационные ресурсы являются важным элементом собственности государства. Они находятся в ведении соответствующих органов и организаций, подлежат учёту и защите. К информационным ресурсам относят не только отдельные документы или массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и других информационных системах). В связи с борьбой за конфиденциальность информации вопросы защиты информационных ресурсов являются наиболее актуальными.

Информационная безопасность довольно ёмкая и многогранная проблема. Сохранение втайне коммерчески важной информации позволяет успешно конкурировать на рынке производства и сбыта товаров и услуг. На сегодняшний день существует несколько видов угроз информационной безопасности: угрозы, находящиеся в самой системе, угрозы в пределах зоны системы, угрозы вне контролируемой группы компьютерной системы [5]. К методам защиты информационных систем относятся регламентация (используется криптографический способ закрытия); принуждение (персонал соблюдает определённые правила пользования системой), побуждение (регламент, которому следует персонал). Так же создаётся защита информации, передаваемая по каналам связи и обменами данных в локальных сетях, копирование носителей информации с преодолением мер защиты, маскировка под запросы системы, расшифровка информации специальными программами. Схемы реализации этих криптоалгоритмов открыто опубликованы и тщательно проанализированы многими исследователями. В этих криптосистемах секретным является только ключ, с помощью которого осуществляется шифрование и дешифрование информации.

Данные криптосистемы могут использоваться не только для шифрования, но и для проверки подлинности (аутентификации) сообщений. Появлению асимметричной

криптографии с открытым ключом способствовали несколько проблем, которые не удавалось решить в рамках классической симметричной одноключевой криптографии (распространение и сохранность секретных ключей, а так же формирование электронной цифровой подписи). В асимметричных криптосистемах с открытым ключом используются два ключа, по крайней мере, один из которых невозможно вычислить из другого.

Один ключ используется отправителем для шифрования информации; другой получателем для расшифрования получаемых шифртекстов. Обычно в приложениях один ключ должен быть несекретным, а другой секретным. Если ключ расшифрования невозможно получить из ключа зашифрования с помощью вычислений, то секретность информации, зашифрованной на несекретном (открытом) ключе, будет обеспечена. Однако этот ключ должен быть защищен от подмены или модификации, иначе отправитель может быть обманут и будет выполнять зашифрование на поддельном ключе, соответствующий ключ расшифрования которого известен противнику. Для того чтобы обеспечить закрытие информации, ключ расшифрования получателя должен быть секретным и физически защищенным от подмены. [8]

Так работает канал обеспечения конфиденциальности (секретности) информации. Если же, наоборот, вычислительно невозможно получить ключ шифрования из ключа расшифрования, то ключ расшифрования может быть несекретным, а секретный ключ шифрования можно использовать для формирования электронной цифровой подписи под сообщением.

В этом случае, если результат расшифрования цифровой подписи содержит аутентификационную информацию (заранее согласованную законным отправителем информации с ее потенциальным получателем), эта подпись удостоверяет целостность сообщения, полученного от отправителя. Так работает канал аутентификации сообщения. Кроме задачи аутентификации сообщения в проблеме аутентификации можно выделить еще две: задачу аутентификации пользователя и задачу взаимной аутентификации абонентов сети в процессе установления соединения между ними.

Обе эти задачи также успешно решаются с привлечением криптографических методов и средств. Все эти меры защиты информации требуют высокого уровня знаний и подготовленности для обеспечения и создания наиболее эффективных методов защиты информации. Понимая под безопасностью состояние защищённости жизненно-важных интересов личности, предприятия, государства

от внутренних и внешних угроз, можно выделить и компоненты безопасности такие как: персонал, материальные и финансовые средства и информацию . Мы выделяем следующие принципы информационной безопасности:

1. Открытость архитектуры и простота использования информационной системы (Чем сложнее выполнение операции, тем больше ошибок. Данный принцип не означает простоту архитектуры и снижения функциональности информационных систем).

2. Непрерывный контроль над всеми операциями (доступ к объекту должен осуществляться при наличии определённого правила).

3. Разграничение доступа к информации и её носителям в соответствии с его полномочиями (минимизация прав и необходимых функциональных возможностей программы).

4. Сложность вычислительных задач и минимизация идентичности процедур пользователя (одинаковые логины, пароли, электронные адреса). Для более чёткого и полного понимания принципа обеспечения информационной безопасности необходимо чётко осознавать и выполнять основные задачи, необходимые для этого. В первую очередь, это относится к совершенствованию законодательства Российской Федерации в сфере обеспечения информационной безопасности.

Сюда относят: формирование и реализация единой государственной политики по обеспечению защиты национальных интересов от угроз в информационной сфере; создание условий для успешного развития негосударственного компонента в сфере обеспечения информационной безопасности, осуществление эффективного гражданского контроля над деятельностью органов государственной власти; совершенствование и защита отечественной информации инфраструктуры; ускорение развития новых информационных технологий и их широкое распространение; унификация средств поиска, сбора, хранения, обработки и анализа информации с учётом вхождения России в глобальную информационную инфраструктуру; организация международного сотрудничества по обеспечению информационной безопасности при интеграции России в мировое информационное пространство. [7]

Исходя из всего вышесказанного, информация должна обладать свойствами конфиденциальности, целостности, доступности, подлинности или аутентичности. Изучив правовую литературу, мы пришли к выводу, что к правовым методам

обеспечения безопасности относятся: разработка, изменение и дополнение нормативных правовых актов, регламентирующих отношения в информационной сфере, нормативных методических документов, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, её противоправное копирование, искажение, противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, содержащей коммерческую тайну.

В заключении, мы делаем вывод, что вышесказанного комплексная система защиты информации должна быть непрерывной, плановой, целенаправленной, активной и надёжной. Она должна опираться на систему видов собственного обеспечения, способного реализовать её функционирование не только в повседневных условиях, но и в критических ситуациях. Следует так же отметить, что способы обеспечения информационной безопасности должны быть ориентированы на упреждающий характер действий, направляемых на заблаговременные меры предупреждения возможных угроз

2.4 Модель угроз безопасности и защита конфедециальных переговоров

Подсистема технической защиты информации (ПТЗИ) является важнейшей составляющей системы защиты информации объектов информатизации (ОИ) на предприятии. Вместе с этим актуализация ПТЗИ в соответствии с реальными условиями эксплуатации объекта защиты возможна только на основе разработки модели угроз безопасности информации подсистемы. Существующие известные модели в недостаточной мере чётко и ясно формируют представление о составе и содержании модели угроз безопасности информации ПТЗИ ОИ (модель угроз) на предприятии, что определяет необходимость её разработки.

Модель угроз безопасности информации определяется как физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации [2].

Угроза безопасности информации организации совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб / вред) для организации [2]. При этом фактор явление, действие или процесс, результатом

которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

Классификация и перечень факторов, воздействующих на безопасность защищаемой информации, определены в ГОСТ Р 51275 [3].

Изложенное даёт основания представить структурную составляющую модели угроз (табл. 1).

В качестве основы разработки содержательной составляющей модели угроз представляется целесообразным использовать ранее предложенную модель ПТЗИ ОИ, предназначенных для ведения конфиденциальных переговоров [3].

Структурная составляющая модели угроз

На основании детального анализа модели (рис. 2) модель угроз ПТЗИ ОИ, предназначенных для ведения конфиденциальных переговоров, представлена в табл. 1.

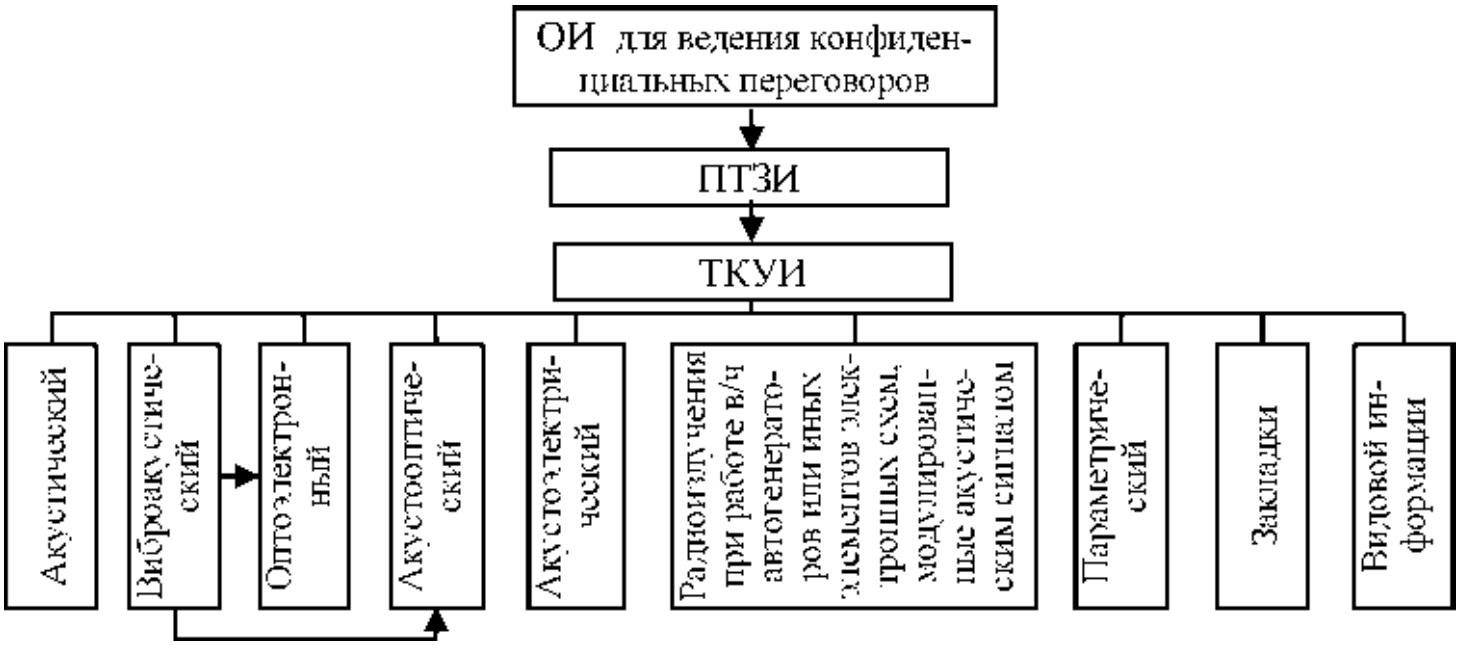

Рис. 2. Модель ПТЗИ ОИ, предназначенных для ведения конфиденциальных

переговоров

Таблица 1

Модель угроз ПТЗИ ОИ, предназначенных для ведения

конфиденциальных переговоров

Модель угроз ПТЗИ ОИ, предназначенных для ведения конфиденциальных переговоров

Угроза	Фактор	Условия
1. Угроза перехвата информации по акустическому ТКУИ	Процесс обработки защищаемой речевой акустической информации	Нарушение режима эксплуатации дверей и окон помещения ОИ в период проведения конфиденциальных переговоров. Неудовлетворительные технические характеристики его строительных конструкций (дверей, окон, вентиляции, стен, потолков, полов)
2. Угроза перехвата и_с по виброакустическому ТКУИ		Выход системы водоснабжения помещения ОИ за пределы КЗ. Неудовлетворительные технические характеристики его строительных конструкций
3. Угроза перехвата и_с по оптоэлектронному ТКУИ		Наличие вероятных мест размещения аппаратуры перехвата информативного сигнала в пределах видимости отражающих поверхностей помещения ОИ
4. Угроза перехвата и_с по параметрическому ТКУИ		Наличие вероятных мест размещения аппаратуры перехвата информативного сигнала. Наличие элементов ВТСС, параметры которых изменяются под воздействием акустических сигналов
5. Угроза перехвата и_с по акустоэлектрическому ТКУИ		Наличие акустоэлектрических преобразователей, имеющих выходы за пределы помещения ОИ
6. Угроза перехвата и_с по акустооптическому ТКУИ		Наличие в помещении ОИ ВОЛС, имеющих выход за пределы помещения, а также за пределы КЗ
7. Угроза перехвата и_с по каналам радиоизлучения		Наличие ВЧ-автогенераторов, радиоизлучение которых выходит за пределы КЗ

Для уточнения разрабатываемой модели угроз на предприятии представляется целесообразным использовать Банк данных угроз безопасности информации ФСТЭК России [5].

Разработанная модель угроз безопасности информации ПТЗИ ОИ, предназначенных для конфиденциальных переговоров, решает поставленную в исследовании задачу, является универсальной и позволяет системно решать задачи технической защиты информации.

Угрозы безопасности информации на предприятии актуальны только по совокупности соответствующих факторов и условий. При этом отсутствие либо несоответствие любого из составляющих предопределяет угрозу несостоятельной.

Модель даёт чёткое представление о составе и содержании модели угроз безопасности информации ПТЗИ ОИ, предназначенных для ведения конфиденциальных переговоров на предприятии.

Модель угроз безопасности информации применима в задачах разработки ПТЗИ всех типов ОИ, предназначенных для ведения конфиденциальных переговоров, и будет способствовать повышению эффективности информационной безопасности объекта защиты.

Модель угроз безопасности информации имеет практическое значение, так как была апробирована в учебном процессе и при выполнении выпускных ква-

лификационных работ по информационной безопасности студентов ТУСУРа, а также может быть использована в задачах разработки ПТЗИ на предприятии.

Используемые сокращения:

ВОЛС волоконно-оптические линии связи;

ВП/ЗП выделенное помещение/защищаемое помещение;

ВТСС вспомогательные технические средства и системы;

ВЧ высокочастотный;

и_с информативный сигнал;

КЗ контролируемая зона;

ОИ объект информатизации;

ПТЗИ подсистема технической защиты информации;

ТКУИ технический канал утечки информации.

ЗАКЛЮЧЕНИЕ

Бурное развитие информационных технологий и их проникновение в сферы деловой активности становится причиной того, что одной из основных задач современной организации становится надежное обеспечение информационной безопасности.

Информационная безопасность, наряду с экономической, социальной, оборонной, экологической и иными видами безопасности, играет важную роль в обеспечении национальных интересов государства. Так, анализ существующих разработок определения «информационной безопасности» показывает, что содержание этого термина раскрывается посредством обеспечения защиты общества. Как известно, социальная сфера образуется из совокупности общественных отношений, возникающих в связи с необходимостью обеспечения жизнедеятельности и воспроизводства человека и социальной инфраструктуры общества.

Так, информационная сфера, образуется посредством совокупности информации и информационной инфраструктуры общества, а также общественных отношений,

объектом которых являются информация и информационная инфраструктура. В политической жизни общества современные информационные технологии изменяют способы ведения политической борьбы. Информационное обеспечение стало важной частью государственной политики по поддержанию общественного диалога, установлению взаимодействия между властью и обществом.

С развитием современных средств информатизации возросли возможности по распространению научных, политических и иных взглядов, доведению их до большого числа людей, их пропаганде. В социальной сфере информационные технологии усилили зависимость благосостояния и безопасности человека от правильности информации, накапливаемой и хранящейся в общественных и государственных информационных системах, от способности государственных и общественных организаций обеспечить соблюдение необходимого режима использования информации. В трудах как отечественных, так и зарубежных философов, социологов, правоведов, политологов отмечается, что постиндустриальное общество имеет информационную природу, строится на всеобщем кодифицированном знании, циркулирующей в открытых системах. Результатом информационной революции конца XX века является становление общественного уклада, и неразрывно связанной с ним информацией сть важное и очень сложное, многообразное направление в общей системе национальной безопасности государства. Информационная безопасность затрагивает проблемы военной, экономической, политической, этнической, демографической, идеологической, продовольственной и др. безопасности государства. Информационная безопасность традиционно является, прежде всего, категорией политической, затем уже социологической и в меньшей мере – объектом исследования юридической науки, что само по себе обеспечивает ее особую привлекательность. Каждая из них разрабатывает различные аспекты информационной безопасности и, соответственно, вносит свой вклад в развитие ее теории.

СПИСОК ЛИТЕРАТУРЫ

Нормативные акты

1. Закон РФ от 05.03.1992 N 2446-1 (ред. от 26.06.2008) "О безопасности"// Ведомости СНД и ВС РФ. – 1992. – № 15. – Ст. 769. Утратил силу.

2. Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 05.10.2015) "О безопасности"// "Российская газета", N 295, 29.12.2010
3. Указ Президента РФ от 31.12.2015 N 683 "О Стратегии национальной безопасности Российской Федерации" // Собр. законодательства Рос. Федерации. – 2016. – № 1 (часть II). – Ст. 212.

Специальная литература

1. Бачило И.Л. Информационное право. М.: Юрайт, 2011. С. 126-129.
2. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право. СПб.: Юридический центр Пресс, 2001. С. 311-312.
3. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2013. — 136 с.
4. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2010. — 324 с.
5. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2010. — 384 с.
6. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга… — М.: ЮНИТИ-ДАНА, 2013. — 239 с.
7. Ефремова М.А. Информационная безопасность как объект уголовно-правовой охраны // Информационное право. 2014. № 5. С. 24.
8. Недосекова Е.С. К вопросу об объектах безопасности // Административное и муниципальное право. 2011. № 9. С. 49 67.
9. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2012. — 432 с.
10. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2012. — 296 с.
11. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2010. — 277 с.
12. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2010. — 336 с.
13. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. — 416 с.
14. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — М.: ДМК, 2014. — 702 с

15. Холопова Е.Н., Бойцов А.С. Информационная безопасность пограничных органов на современном этапе: понятие, структура // Информационное право. 2014. № 5. С. 4-9.