Содержание:

ВВЕДЕНИЕ

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.

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.

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.

1. ОБЩЕЕ ПОНЯТИЕ И ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1.Определение 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» [2] 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. [4] 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» [9].

1.2. Источник угроз информационной безопасности

Угрозами информационному обеспечению государственной политики Российской Федерации могут быть: монополизация информационного рынка государства, его обособленных секторов российскими и иностранными информационными структурами; блокирование деятельности федеральных средств массовой информации по информированию отечественной и иностранной аудитории; низкая результативность информационного обеспечения государственной политики Российской Федерации ввиду глобального дефицита специализированных кадров, не существования системы формализации и осуществления государственной информационной политики.

Угрозами развитию российской индустрии информации, в частности индустрию средств информатизации, телекоммуникации и связи, обеспечению нужд внутреннего рынка в ее продукции и выходу данной продукции на всемирный рынок, в частности обеспечению накопления, сохранности и результативного применения российских информационных ресурсов могут быть:

- ◦ противодействие доступу Российской Федерации к инновационным информационным технологиям, взаимообусловленному и равноправному участию отечественных производителей во всемирном разделении трудовой деятельности в сфере информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, в частности формирование условий для повышения технологической зависимости государства в сфере нынешних информационных технологий;
  - ◦ закупка органами федеральной власти импортных средств информатизации, телекоммуникации и связи при существовании российских аналогов, которые не уступают по собственным характерным свойствам иностранным образцам;

- вытеснение с российского рынка отечественных производителей средств информатизации, телекоммуникации и связи;
- повышение оттока за границу специалистов и правообладателей интеллектуальной собственности [7].

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и формируемых на территории России, могут быть:

- противоправные сбор и применение сведений;
- не соблюдение технологии обработки информации;
- внедрение в аппаратные и программные изделия элементов, осуществляющих функции, которые не предусмотрены соответствующей документацией на данные изделия;
- разработка и распространение программ, которые непосредственно нарушают соответствующее функционирование информационных и информационно - телекоммуникационных систем, в частности систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление либо же разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата сведений в технические средства обработки, хранения и передачи информации по каналам связи, в частности в служебные помещения органов федеральной власти, организаций, учреждений и компаний, не имея зависимости от формы собственности;
- уничтожение, повреждение, разрушение либо хищение машинных и иных носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование данной информации и навязывание ложной информации;
- применение несертифицированных российских и иностранных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при формировании и

развитии отечественной информационной инфраструктуры;
- несанкционированный доступ к информации, которая находится в банковских учреждениях и базах данных;
- не соблюдение законных ограничений на распространение сведений[10].

Доктрина информационной безопасности также подразделяет источники угроз информационной безопасности Российской Федерации на внешние и внутренние. Этот же подход воспроизводится и в научной литературе.

По сферам воздействия Доктрина подразделяет угрозы информационной безопасности на действующие в: сфере экономики; сфере внутренней политики; сфере внешней политики; в области науки и техники; сфере духовной жизни; сфере общегосударственных информационных и телекоммуникационных систем; сфере обороны; правоохранительной и судебной сферах.

Кроме того, классификация угроз информационной безопасности может быть проведена по целому ряду других критериев. Угрозы информационной безопасности могут быть также подразделены на видимые и невидимые, явные и неявные.

2.РЕАЛИЗАЦИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННОГО КАЗЕННОГО УЧРЕЖДЕНИЯ НОВОСИБИРСКОЙ ОБЛАСТИ «УПРАВЛЕНИЕ КОНТРАКТНОЙ СИСТЕМЫ»

2.1 Методология и виды угроз информационной безопасности

ПИБ ГКУ НСО «УКСис» является методологической базой для:

выработки и совершенствования комплекса согласованных нормативных, правовых, технологических и организационных мер, направленных на защиту информации;

обеспечения информационной безопасности;

координации деятельности отделов ГКУ НСО «УКСис» при проведении работ по соблюдению требований обеспечения информационной безопасности.

Для реализации ПИБ ГКУ НСО «УКСис» необходимо провести комплекс превентивных мер по защите информации, в том числе конфиденциальных данных, информационных процессов, включающих в себя требования в адрес персонала и технических служб. На основе ПИБ строится управление информационной безопасностью [12].

ПИБ сформирована на основе результатов информационного и технического обследования ГКУ НСО «УКСис» в рамках аудита, результатов анализа информационных рисков и оценки защищенности информации, в соответствии с требованиями нормативных актов, а также согласно рекомендациям международных стандартов в области защиты информации.

Целями защиты информации является предотвращение:

- утечки, хищения, утраты, искажения, подделки информации;

- несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

- других форм незаконного вмешательства в ресурсы ГКУ НСО «УКСис».

В общем контексте безопасность связана с защитой ресурсов от угроз, где угрозы классифицированы на основе потенциала злоупотребления защищаемыми активами.

При разработке ПИБ использована модель (рис.1), соответствующая международному стандарту ISO/IEC 15408 «Информационная технология – методы защиты – критерии оценки информационной безопасности», стандарту ISO/IEC 17799 «Управление информационной безопасностью».

Источники угроз – это силы природы, объекты окружающей среды, деструктивные социальные проявления и т.п., которые могут нанести хаотический ущерб ресурсам при возникновении, активизации или изменении своего состояния без стремления к достижению какой-либо цели.

Нарушители – это субъекты и объекты посредством субъектов, которые нанесли ущерб в результате неформализованных действий или бездействий.

Ресурсы – это данные, создаваемые в процессе функционирования и эксплуатации ПО ГКУ НСО «УКСис», а также программно-аппаратное обеспечение, входящее в эксплуатационный комплект.

Контрмеры – предупреждающие действия (решения), принимаемые ГКУ НСО «УКСис» для предотвращения уязвимости.

Риски – сочетание вероятности наступления уязвимости и его последствий для ресурсов ГКУ НСО «УКСис».

оценивают

хотят минимизировать

предпринимают чтобы уменьшить

которые

которые могут направлены на

быть уменьшены

могут знать

ведущие к

которые используют

которые для

повышают

порождают

для

хотят злоупотребить могут нанести ущерб

порождают

для

хотят злоупотребить и/или могут нанести ущерб

ВЛАДЕЛЬЦЫ

КОНТРМЕРЫ

УЯЗВИМОСТИ

РИСК

РЕСУРСЫ

ИСТОЧНИКИ УГРОЗ.

НАРУШИТЕЛИ.

УГРОЗЫ

Рисунок 1. Модель безопасности

Уязвимость – это потенциальные угрозы для функционирования ГКУ НСО «УКСис». В общем случае уязвимость ассоциируется с не соблюдением ПИБ, обусловленном неправильно заданным набором правил либо ошибкой в обеспечивающей безопасность компьютера программе.

Уязвимость – это состояние системы, которое дает возможность:

осуществлять команды от лица иного пользователя;

иметь прямой доступ к информации, закрытой от доступа для данного пользователя;

показывать себя как другого пользователя либо ресурс.

Отдельные категории нарушителей могут быть определены к ряду злоумышленников, определяемых как «лицо, которое осуществляет либо осуществило заблаговременно обдуманное действие с пониманием его опасных последствий, либо не предвидело, но должно было и могло предвидеть возможность наступления данных последствий». Так как данное определение применяется к нарушителю лишь по решению судебной коллегии, по понятным причинам далее используется термин «нарушитель» [8].

Потенциальные нарушители – это субъекты и объекты посредством субъектов, которые могут нанести ущерб в некоторых обстоятельствах при наступлении конкретных событий.

За сохранность рассматриваемых ресурсов отвечают их владельцы, для которых данные ресурсы представляют некую ценность. Имеющиеся либо предполагаемые нарушители в частности в состоянии придавать значение данным ресурсам и стремиться применять их вопреки интересам их владельца.

Владельцы воспринимают такие угрозы как потенциал влияния на ресурсы, приводящего к сокращению их ценности для владельца.

К специфическим нарушениям безопасности как правило определяют (но не обязательно ими ограничиваются):

- раскрытие ресурса несанкционированным получателем, наносящее ущерб (потеря конфиденциальности);

- ущерб ресурсу вследствие несанкционированной модификации (потеря целостности);

- несанкционированное лишение доступа к ресурсу (потеря доступности).

Владельцы ресурсов анализируют возможные угрозы, с целью разрешить, какие из них на самом деле свойственны их среде. В итоге анализа определяются риски. Анализ помогает при выборе контрмер для противостояния угрозам и сокращения рисков до приемлемого уровня.

Следовательно, ПИБ базируясь на модели, которая рассматривает три основных субъекта – владельца, службу информационной безопасности собственника, нарушителя. Владелец передает процессы обеспечения безопасности службе ИБ [7].

Изначально у службы ИБ отсутствуют сведения относительно нарушителя.

Для формирования модели нарушителя в данных обстоятельствах применяется принцип «черного ящика», действующего как генератор событий, ориентированных на активизацию угроз через уязвимости, что считается достаточным для обеспечения базового уровня безопасности.

В основу разработки и практической реализации ПИБ положены ниже приведенные принципы:

не способность миновать защитные средства;

усиление самого слабого звена;

недопустимость перехода в открытое состояние;

предельная минимизация привилегий;

разделение обязанностей;

многоуровневая защита;

разнообразие защитных средств;

простота и управляемость информационной системы;

обеспечение всеобщей поддержки мер безопасности.

Принцип невозможности миновать защитные средства предполагает, что все информационные потоки в подсистемы ГКУ НСО «УКСис» и из них должны проходить непосредственно через СЗИ.

Надежность любой СЗИ вычисляется самым слабым звеном. Зачастую данным звеном оказывается не компьютер либо программа, а человек, и тогда задача обеспечения информационной безопасности претерпевает нетехнический характер.

Принцип недопустимости перехода в открытое состояние предполагает, что при любых условиях (в частности и нештатных), СЗИ или полностью осуществляет собственные функции, или же должна всецело блокировать доступ.

Принцип минимизации привилегий предписывает выделять пользователям и администраторам лишь те права доступа, которые требуются им для осуществления служебных обязанностей.

Принцип разделения обязанностей означает данное распределение ролей и ответственности, при котором один гражданин не может нарушить критически важный для организации процесс. Данное в особенности имеет значение для предотвращения злонамеренных либо е неквалифицированных действий системного администратора[12].

Принцип многоуровневой защиты предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался на первый взгляд. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией — управление доступом и, как последний рубеж, — протоколирование и аудит. Эшелонированная оборона способна, по

крайней мере, задержать злоумышленника, а существование данного рубежа, как протоколирование и аудит, вещественно осложняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать разные по своей направленности оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками преодоления СЗИ.

Принцип простоты и управляемости информационной системы в общем и СЗИ в особенности определяет возможность формального либо неформального доказательства корректности реализации инструментов защиты. Лишь в простой и управляемой системе можно проверить согласованность конфигурации различных элементов и реализовать централизованное администрирование.

Принцип всеобщей поддержки мер безопасности носит нетехническую направленность. Рекомендуется с самого начала предусмотреть ряд мер, ориентированных на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

2.2 Методы и средства против угроз информационной безопасности ГКУ НСО «УКСис»

Основными действиями, которые производятся с информацией и могут содержать в себе угрозу, являются сбор, модификация, утечка и уничтожение данных. Эти действия являются базовыми для дальнейшего рассмотрения.

Все источники угроз ГКУ НСО «УКСис» разделяются на внешние и внутренние.

Источниками внутренних угроз являются:

работники организации;

ПО;

аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

ошибки пользователей и системных администраторов;

нарушения работниками установленных регламентов сбора, обработки, передачи и уничтожения информации;

ошибки в работе ПО;

отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:

компьютерные вирусы и вредоносные программы;

организации, службы и отдельные лица;

стихийные бедствия [12].

Формами проявления внешних угроз являются:

заражение компьютеров вирусами или вредоносными программами;

несанкционированный доступ (НСД) к корпоративной информации;

информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;

действия государственных структур и служб, сопровождающиеся сбором, модификацией, изъятием и уничтожением информации;

аварии, пожары, техногенные катастрофы.

Обеспечение информационной безопасности ГКУ НСО «УКСис» реализуется следующими формами защиты:

организационной;

программно-аппаратной.

Меры защиты призваны обеспечить:

- конфиденциальность информации (защита от несанкционированного ознакомления);

- целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

- доступность информации (возможность за приемлемое время получить требуемую информационную услугу) [14]

Организационной формой защиты являются (но не ограничиваются) мероприятия, предусмотренные данной ПИБ. К ним относятся:

мероприятия, осуществляемые при проектировании, строительстве и оборудовании технической инфраструктуры ГКУ НСО «УКСис» и других ассоциированных с ней объектов;

мероприятия по разработке правил доступа пользователей к ресурсам системы согласно ПИБ;

мероприятия, осуществляемые при подборе и подготовке персонала;

организация охраны и режима допуска к системе;

организация учета, хранения, использования и уничтожения документов и носителей информации;

распределение реквизитов разграничения доступа;

обучение вопросам безопасности.

Организационные меры защиты осуществляются и поддерживаются работниками ИТО.

Состав, назначение и функции ИТО должны соответствовать законодательству Российской Федерации.

Основной задачей ИТО является поддержка уровня ИБ организации на заданном уровне, определение направления развития мер, направленных на защиту информации от несанкционированного доступа, изменения, разрушения или отказа в доступе.

Это достигается путем внедрения соответствующих правил, инструкций и указаний.

ИТО отвечает за:

разработку и издание правил (инструкций и указаний) по обеспечению ИБ, соответствующих им правилам работы организации и требованиям к обработке информации;

внедрение программы обеспечения ИБ, включая классификацию информации и оценку деятельности;

проведение первичного инструктажа по основам информационной безопасности пользователей ИСПДн;

разработку и внедрение процедур пересмотра правил обеспечения информационной безопасности, а также рабочих программ, предназначенных для поддержки правил, инструкций, стандартов и указаний организации;

участие в описании, конструировании, создании и приобретении систем в целях соблюдения правил безопасности при автоматизации производственных процессов;

изучение, оценку, выбор и внедрение аппаратных и программных средств, функций и методик обеспечения информационной безопасности, применимых для компьютерных систем организации [16].

При необходимости на ИТО возлагается выполнение других обязанностей:

участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;

наблюдение за функционированием системы защиты и ее элементов;

организация проверок надежности функционирования системы защиты;

обучение пользователей и персонала ИС правилам безопасной обработки информации;

контроль за соблюдением пользователями и персоналом ИС установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;

принятие мер при попытках НСД к информации и при нарушениях правил функционирования системы защиты.

Организационно-правовой статус СИБ:

численность службы защиты должна быть достаточной для выполнения всех перечисленных функций;

подчиненность СИБ определяется структурой организации;

работники СИБ должны иметь право доступа во все помещения, где установлена аппаратура ИС, и право прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации;

руководителю СИБ должно быть предоставлено право запрещать включение в число действующих новые элементы ИС, если они не отвечают требованиям ИБ;

СИБ должна иметь все условия, необходимые для выполнения своих функций.

Критическое или чувствительное оборудование обработки информации должно быть размещено в охраняемых зонах, защищено определенными периметрами безопасности, оснащенными соответствующими барьерами безопасности и средствами контроля на входе. Они должны быть физически защищены от несанкционированного доступа, повреждения или создания помех в работе [13].

Применительно к безопасности окружающей среды должны быть разработаны (и применяться) меры по физической защите от ущерба в результате пожаров, наводнений, землетрясений, взрывов, массового гражданского неповиновения, а также от других видов бедствий естественного или искусственного характера.

Обеспечиваемая защищенность должна быть пропорциональна идентифицированным рискам.

Физическая безопасность реализуется совокупностью способов защиты на основе инженерных конструкций в сочетании с техническими средствами охраны, образующих физическую защиту. Составной частью физической защиты является инженерная защита и техническая охрана объектов (ИЗТОО).

Требуемый уровень информационной безопасности достигается многозональностью и многорубежностью защиты, которая должна быть обеспечена с помощью инженерной защиты и охраны системы ГКУ НСО «УКСис».

Организационно-технологическая среда представляет собой единый комплекс информационных и технических ресурсов, эксплуатирующего и обслуживающего персонала.

Сервера находятся в центре обработки данных департамента информатизации и развития телекоммуникационных технологий Новосибирской области, в виде виртуальных хостов, для реализации межсетевого взаимодействия провайдером предоставляется канал связи, построенный по технологии VLAN.

Помещение в ГКУ НСО «УКСис», где находятся коммутаторы, а также крипто-шлюз, запирается на ключ, доступ к ключу имеют лица из заранее утвержденного перечня.

В целях осуществления и поддержания соответствующего уровня информационной безопасности при использовании услуг, предоставляемых третьей стороной, организация должна проверять наличие в договорных обязательствах соглашений требований по вопросам ИБ, осуществлять мониторинг соответствия соглашений и управлять изменениями, гарантирующими, что предоставляемые услуги удовлетворяют всем требованиям соглашения с третьей стороной.

Носители, содержащие информацию, должны быть защищены от несанкционированного доступа, неправильного использования или повреждения при транспортировке вне физических границ организации.

Должны быть рассмотрены следующие рекомендации по защите носителей информации, транспортируемых между территориями:

следует использовать надежных курьеров или надежный транспорт;

список уполномоченных курьеров должен быть согласован с руководством организации;

должны быть разработаны процедуры проверки личности курьеров;

упаковка должна обеспечивать достаточную защиту контента от любого физического повреждения, которое, вероятнее всего, может возникнуть при транспортировке;

упаковка должна соответствовать спецификациям любых производителей;

упаковка должна обеспечивать защиту от любых факторов окружающей среды, которые могут уменьшить эффективность восстановления данных с носителей информации, например, из-за нагревания, влажности или электромагнитных полей;

при необходимости должны применяться средства управления, защищающие чувствительную информацию от несанкционированного раскрытия или изменения, например:

использование запираемых контейнеров;

доставка вручную;

запечатанная упаковка (обеспечивающая обнаружение попыток вскрытия);

в исключительных ситуациях – разбиение всего отправляемого груза на несколько партий, и отправка их к пункту назначения по различным маршрутам.

2.3. Программные и аппаратные формы защиты

Программными и аппаратными формами защиты являются (но не ограничиваются) мероприятия, предусмотренные данной ПИБ. К ним относятся:

идентификация и аутентификация пользователей;

разграничение доступа к ресурсам;

регистрация событий;

криптографические преобразования;

проверка целостности системы;

проверка отсутствия вредоносных программ;

программная защита передаваемой информации и каналов связи;

защита системы от наличия и появления нежелательной информации;

создание физических препятствий на путях проникновения нарушителей;

мониторинг и сигнализация соблюдения правильности работы системы;

создание резервных копий информации.

2.4. Защита электронного обмена данными

Информация, передаваемая в виде электронных сообщений, должна быть соответствующим образом защищена. При рассмотрении безопасности электронного обмена данными в этих системах необходимо учитывать следующее:

должна быть предусмотрена защита сообщений от несанкционированного доступа, изменения или отказа в обслуживании;

должна быть обеспечена правильная адресация и транспортировка сообщения;

должна быть обеспечена надежность и доступность обслуживания;

должны быть учтены требования законодательства Российской Федерации, в частности, требования, предъявляемые к электронным документам и ЭП;

должно быть предусмотрено использование более строгих правил идентификации при доступе из сетей общего пользования и обеспечен контроль их соблюдения.

Для уменьшения риска, которому подвергаются производственные процессы и система безопасности, связанного с использованием электронной почты, следует применять (по необходимости) соответствующие средства контроля. Необходимо учитывать:

уязвимость электронных сообщений по отношению к несанкционированному перехвату и модификации;

уязвимость данных, пересылаемых по электронной почте, по отношению к ошибкам, например, неправильная адресация или направление сообщений не по назначению, а также надежность и доступность сервиса в целом;

влияние изменения характеристик коммуникационной среды на производственные процессы, например, влияние повышенной скорости передачи данных или изменения системы адресации между организациями и отдельными лицами;

правовые соображения, такие, как необходимость проверки источника сообщений и др.;

последствия для системы безопасности от раскрытия содержания каталогов;

необходимость принятия защитных мер для контроля удаленного доступа пользователей к электронной почте.

Организации должны задать четкие правила, касающиеся статуса и использования электронной почты.

2.5. Защита от злонамеренного и мобильного кода

С целью защиты информации и программных средств от несанкционированного доступа и действия вредоносных программ при разработке и эксплуатации системы должны быть предприняты организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и устранение последствий этих действий. При этом руководство должно обеспечить неукоснительное выполнение следующих мероприятий:

Сертификация – действия третьей стороны, цель которых подтвердить (с помощью сертификата соответствия) то, что изделие (в том числе программное средство) или услуга, прямо или косвенно взаимодействующая с системой, соответствует определенным стандартам или другим нормативным документам в области защиты информации.

Профилактика – систематические действия эксплуатационного персонала, цель которых выявить и устранить неблагоприятные изменения в свойствах и характеристиках используемых программных средств, в частности проверить эксплуатируемые, хранимые и (или) вновь полученные программные средства на наличие компьютерных вирусов.

Ревизия – проверка вновь полученных программ специальными средствами, проводимая путем их запуска в контролируемой среде.

Вакцинирование – обработка файлов, дисков, каталогов, проводимая с применением специальных программ, создающих условия, подобные тем, которые создаются определенным компьютерным вирусом, и затрудняющих повторное его появление.

2.6. Средства управления для борьбы со злонамеренными программными кодами

В качестве мер для борьбы со злонамеренными программными кодами должны быть осуществлены средства управления для предотвращения его ввода, его обнаружения и восстановления системы после удаления злонамеренного программного кода, в частности поддержания компетентности пользователей в данной сфере.

К тому же берутся во внимание ниже следующие рекомендации:

необходимо внедрить правила, запрещающие использование нелегального ПО;

должны быть внедрены формальные правила защиты от рисков, связанных с получением файлов и ПО из внешней сети или на любом другом носителе;

необходимо проводить регулярные проверки ПО и баз данных систем, поддерживающих критические производственные процессы; должно формально исследоваться наличие любых подозрительных файлов или несанкционированных исправлений;

Должны быть обеспечены:

установка и регулярное обновление ПО для обнаружения злонамеренного кода и восстановления среды после его удаления (пакеты антивирусных программ и библиотеки к ним);

сканирование содержимого компьютеров и носителей информации в виде профилактического или регулярно выполняемого средства управления, обеспечивающего:

- проверку на злонамеренные коды перед использованием любых полученных файлов – на внешних носителях или через сети;

- проверку прикрепленных файлов электронной почты и загруженных файлов на злонамеренные коды перед их использованием. Эта проверка должна выполняться на различных участках, например, на серверах электронной почты, настольных компьютерах, на входе в сеть организации;

определение процедур управления и обязанностей, связанных с защитой систем от злонамеренного кода, обучение их использованию, уведомлению о злонамеренных кодах, восстановлению среды после атак, предпринятых злонамеренным кодом;

подготовка соответствующих планов непрерывного ведения работы, предусматривающих восстановление среды после атак, обусловленных злонамеренным кодом, в том числе все необходимые данные и ПО для копирования и мер по восстановлению;

осуществление процедур проверки информации, которые непосредственно касаются злонамеренного кода, гарантирование того, что бюллетени с предупреждениями точны и информативны; руководители обязаны гарантировать, что для того, чтобы различать мистификации от действительных злонамеренных кодов, будут применяться квалифицированные источники, допустим, журналы, имеющие отличную репутацию, надежные сайты в сети Интернет либо же поставщики защитного ПО; все пользователи должны быть оповещены о проблемах, которые прямо связаны с мистификациями и о том, что необходимо предпринять при получении мистифицированного злонамеренного кода.

В определенном для защиты от злонамеренных кодов ПО требуется обеспечить поддержку автоматического обновления файлов определения и утилит сканирования, что обеспечивает своевременное обновление защиты.

Помимо этого, это ПО может быть установлено на каждом рабочем месте для осуществления автоматических проверок.

Должны быть приняты меры предосторожности относительно защиты от ввода злонамеренных кодов во время обслуживания и процедур работы при чрезвычайных обстоятельствах, при которых могут игнорироваться традиционно применяемые средства управления защитой от злонамеренных кодов.

ЗАКЛЮЧЕНИЕ

Итак : по своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

- ○ угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности,

индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Таким образом, источники угроз информационной безопасности классифицированы законодателем исходя из их общей направленности на угрозы: конституционным правам и свободам человека и гражданина; информационному обеспечению государственной политики Российской Федерации; развитию отечественной индустрии информации; безопасности информационных и телекоммуникационных средств и систем. Угрозы информационной безопасности могут быть также подразделены на видимые и невидимые, внутренние и внешние, намеренные (организованные) и непреднамеренные (стихийные), явные и латентные (скрытые).

Соблюдение требований ПИБ обязательно для всех категорий работников, эксплуатирующих и пользующихся ИС ГКУ НСО «УКСис». Проведение планового аудита информационной безопасности является одним из основных методов проверки эффективности мер по защите информации. Результаты аудита могут служить основанием для пересмотра некоторых положений ПИБ и внесения в них необходимых корректировок. Проводить аудит информационной безопасности ИС ГКУ НСО «УКСис» целесообразно ежегодно.

Кроме этого, используемые информационные технологии и организация служебной деятельности непрерывно меняются, это приводит к необходимости корректировать существующие подходы к обеспечению информационной безопасности.

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.