Политика ИБ организации N

Основные сокращения, термины и определения:

ИБ – информационная безопасность.

ИС – информационная система.

ИЗ – информационная защита.

НПА – нормативный правовой акт.

НСД – несанкционированный доступ.

ПДн – персональные данные.

ИСПДн – информационная система персональных данных.

ПИБ – политика информационной безопасности.

ПО – программное обеспечение.

СЗИ – система защиты информации.

СИБ – служба информационной безопасности.

ЭП – электронная подпись.

ИТО – информационно-технический отдел организации N.

Администратор безопасности информационных систем – работник, обеспечивающий исполнение мер по информационной безопасности.

Атака – несанкционированная деятельность с вредоносными намерениями, использующая специально разработанный программный код или специальные методики.

Аутентификация – подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа реализованным в системе.

Авторизация – определение по данным аутентификации полномочий лица или информационного ресурса и элементов, к которым им следует предоставить доступ.

База данных (БД) – упорядоченная совокупность данных и структур их хранения, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, и предназначенная для обработки с помощью средств вычислительной техники.

Вероятность реализации угрозы через данную уязвимость – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях.

Вредоносное программное обеспечение – программное обеспечение, создаваемое с целью причинения вреда информационным системам и информационным ресурсам.

Защита информации – принятие правовых, организационных и технических (программно-технических) мер в целях обеспечения целостности сохранности информации, недопущения ее несанкционированного изменения или уничтожения, соблюдения конфиденциальности информации ограниченного доступа, реализации права на доступ к информации, а также недопущения несанкционированного воздействия на средства обработки, передачи и хранения информации.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых

документов или требованиями, устанавливаемыми собственником информации, которыми может быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита программных средств – организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и устранение последствий этих действий.

Защита информации от несанкционированного доступа – меры, направленные на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными правовыми актами или собственником, владельцем информации прав или правил доступа к ней.

Идентификатор – уникальный персональный код, присвоенный субъекту и объекту системы, предназначенный для регламентированного доступа к системе и ресурсам системы.

Идентификация – определение соответствия предъявленного для получения доступа в систему, к ресурсу идентификатора перечню идентификаторов, имеющихся в системе.

Несанкционированный доступ к информации – получение защищаемой информации, заинтересованным субъектом с нарушением установленных правил доступа к ней.

Несанкционированный доступ к программным средствам – доступ к программам, записанным в памяти ЭВМ или на машинном носителе, а также отраженным в документации на эти программы, осуществленный с нарушением установленных правил.

Пользователь – человек, организация, система, использующие в своей работе в той или иной мере компьютер, вычислительную систему, базу данных, сеть и пр.

Доступ – перемещение людей и других объектов в (из) помещения, здания, зоны и территории.

Разграничение доступа – порядок доступа лиц к техническим и программным средствам, защищаемой информации при ее обработке на средствах вычислительной техники в соответствии с заранее разработанными и утвержденными правилами.

Рабочее место – оборудованное рабочее место пользователя (администратора) — стол, стул, компьютер с установленным необходимым ПО.

Рабочая станция – комплекс технических и программных средств, предназначенных для решения определенного круга задач.

Система обеспечения информационной безопасности – система мер, направленная на выявление угроз информационной безопасности, предотвращение и пресечение их реализации, а также ликвидацию последствий, реализованных в результате НСД.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки информации, способных функционировать самостоятельно или в составе других систем.

Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные или используемые для защиты информации.

Средства криптографической защиты информации – средства, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности.

Средства обеспечения информационной безопасности – совокупность правовых, организационных, и технических мероприятий, средств и норм, направленных на предотвращение или существенное затруднение нанесения ущерба любого характера собственнику и потребителю информации.

Технический канал утечки информации – совокупность объекта разведки, технического средства разведки, с помощью которого добывается информация об объекте, и физической среды, в которой распространяется информационный сигнал.

Техническое обеспечение – комплекс технических средств, предназначенных для работы информационной системы, а также соответствующая документация на эти средства и технологические процессы.

Угроза доступности – угроза нарушения работоспособности информационной системы при доступе к информации.

Угроза конфиденциальности – угроза раскрытия информации.

Угроза целостности – угроза изменения информации.

Угрозы информационной безопасности – совокупность причин, условий и факторов, создающих опасность для объектов информационной безопасности, реализация которых может повлечь нарушение прав, свобод и законных интересов юридических и физических лиц в информационных процессах.

Утечка информации – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Ущерб – стоимость потерь, которые понесет сторона в случае реализации угрозы конфиденциальности, целостности или доступности по каждому виду ценной информации. Ущерб зависит только от стоимости информации, которая обрабатывается в информационной системе. Ущерб является характеристикой информационной системы и не зависит от степени ее защищенности.

ISO – Международная организация по стандартизации (International Organization for Standardization, ISO), занимающаяся выпуском стандартов.

IEC – Международная электротехническая комиссия (МЭК; англ. International Electrotechnical Commission, IEC) — международная организация по стандартизации в области электрических, электронных и смежных технологий.

ISO/IEC 17799 – стандарт информационной безопасности, опубликованный в 2005 организациями ISO и IEC. Озаглавлен как «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности» (англ. Information technology – Security techniques – Code of practice for information security management).

Стандарт – в рамках данного документа, под данным термином понимается стандарт информационной безопасности ISO/IEC 17799, если явно не указано

иное.

Используемые нормативные правовые акты:

- Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных»;
- Федеральный закон от 06 апреля 2011 № 63-ФЗ «Об электронной подписи»;
- Указ Президента от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

I. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая ПИБ описывает цели и задачи информационной безопасности, определяет совокупность правил, требований и руководящих принципов в области информационной безопасности, которыми в своей деятельности руководствуется организация N. ИТО является ответственным за реализацию ПИБ и поддержание её в актуальном состоянии.

Требования ПИБ обязательны для выполнения всеми работниками и пользователями информационных систем организации N.

ПИБ разработана в соответствии с законодательством Российской Федерации в области обеспечения информационной безопасности.

Главной целью, на достижение которой направлены все положения ПИБ, является надежное обеспечение информационной безопасности организации N и, как следствие, недопущение нанесения материального, физического, морального или иного ущерба.

Под обеспечением информационной безопасности организации N понимается также обеспечение информационной безопасности сопровождаемых организацией N информационных систем.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующего состояния:

- доступность обрабатываемой информации для зарегистрированных пользователей;
- устойчивое функционирование организации N;
- обеспечения конфиденциальности информации организации N, хранимой, обрабатываемой на средствах вычислительной техники и передаваемой по каналам связи;
- целостность и аутентичность информации, хранимой и обрабатываемой в организации N и передаваемой по каналам связи.

Для достижения поставленной цели решаются следующие задачи:

- защита от вмешательства посторонних лиц в процесс функционирования организации N;
- разграничение доступа зарегистрированных пользователей к информации аппаратными, программными и криптографическими средствами защиты, используемыми в организации N;
- регистрация действий пользователей при использовании ресурсов организации N в системных журналах;
- периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов специалистами информационной безопасности;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защита информации от несанкционированной модификации, искажения;
- контроль целостности используемых программных средств, а также защита системы от внедрения вредоносных кодов, включая компьютерные вирусы;
- обеспечение аутентификации пользователей, участвующих в информационном обмене;
- своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции;
- создание условий для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабления негативного влияния и ликвидации последствий нарушения безопасности информации.

II. РЕАЛИЗАЦИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПИБ организации N 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 организации N при проведении работ по соблюдению требований обеспечения информационной безопасности.

Для реализации ПИБ организации N 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.

ПИБ сформирована на основе результатов информационного и технического обследования организации N 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.

III. МЕТОДОЛОГИЯ И ПРИНЦИПЫ ПОСТРОЕНИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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 организации N.

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.

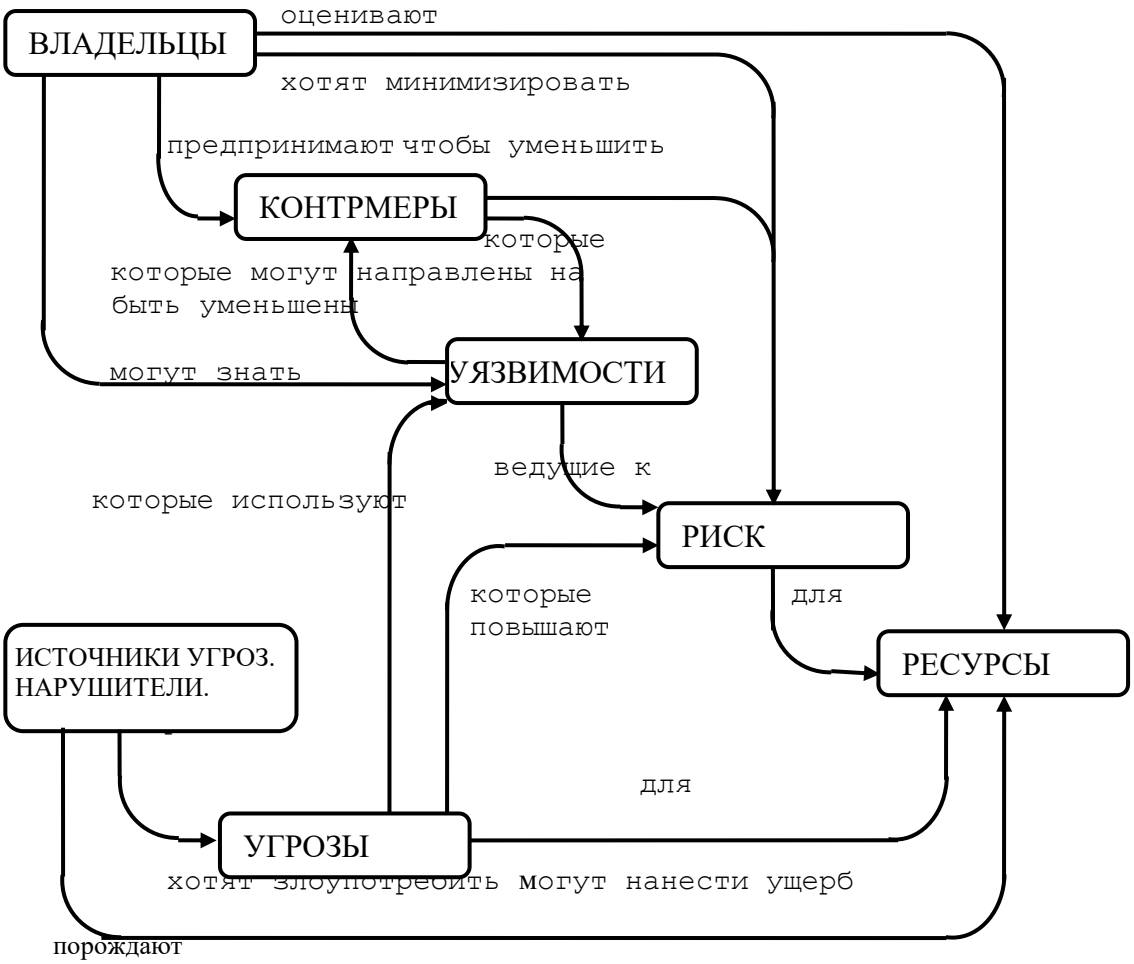
Нарушители – это субъекты и объекты посредством субъектов, которые нанесли ущерб в результате неформализованных действий или бездействий.

Ресурсы – это данные, создаваемые в процессе функционирования и эксплуатации ПО организации N, а также программно-аппаратное обеспечение, входящее в эксплуатационный комплект.

Контрмеры – предупреждающие действия (решения), принимаемые организацией N для предотвращения уязвимости.

Риски – сочетание вероятности наступления уязвимости и его последствий для ресурсов организации N.

Рисунок 1 – Модель безопасности



Уязвимость – это потенциальные опасности для функционирования организации N. В общем случае уязвимость ассоциируется с нарушением ПИБ, вызванным неправильно заданным набором правил или ошибкой в обеспечивающей безопасность компьютера программе.

Уязвимость – это состояние системы, которое позволяет:

- исполнять команды от имени другого пользователя;
- получать доступ к информации, закрытой от доступа для данного пользователя;
- показывать себя как иного пользователя или ресурс.

Отдельные категории нарушителей могут быть отнесены к разряду злоумышленников, определяемых как «лицо, которое совершает или совершило заранее обдуманное действие с осознанием его опасных последствий, или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий». Поскольку такое определение применяется к нарушителю только по решению суда, по понятным причинам далее применяется термин «нарушитель».

Потенциальные нарушители – это субъекты и объекты посредством субъектов, которые могут нанести ущерб в определенных условиях при наступлении определенных событий.

За сохранность рассматриваемых ресурсов отвечают их владельцы, для которых эти ресурсы имеют ценность. Существующие или предполагаемые нарушители также могут придавать значение этим ресурсам и стремиться использовать их вопреки интересам их владельца.

Владельцы воспринимают подобные угрозы как потенциал воздействия на ресурсы, приводящего к понижению их ценности для владельца.

К специфическим нарушениям безопасности обычно относят (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, чтобы решить, какие из них действительно присущи их среде. В результате анализа определяются риски. Анализ помогает при выборе контрмер для противостояния угрозам и уменьшения рисков до приемлемого уровня.

Таким образом, ПИБ основывается на модели, которая рассматривает три основных субъекта – владельца, службу информационной безопасности собственника, нарушителя. Владелец передает процессы обеспечения безопасности службе ИБ.

Изначально у службы ИБ отсутствуют знания о нарушителе.

Для построения модели нарушителя в этих условиях используется принцип «черного ящика», действующего как генератор событий, направленных на активизацию угроз через уязвимости, что является достаточным для обеспечения базового уровня безопасности.

В основу разработки и практической реализации ПИБ положены следующие принципы:

1) невозможность миновать защитные средства;
2) усиление самого слабого звена;
3) недопустимость перехода в открытое состояние;
4) минимизация привилегий;
5) разделение обязанностей;
6) многоуровневая защита;
7) разнообразие защитных средств;
8) простота и управляемость информационной системы;
9) обеспечение всеобщей поддержки мер безопасности.

Принцип невозможности миновать защитные средства означает, что все информационные потоки в подсистемы организации N и из них должны проходить через СЗИ.

Надежность любой СЗИ определяется самым слабым звеном. Часто таким звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

Принцип недопустимости перехода в открытое состояние означает, что при

любых обстоятельствах (в том числе и нештатных), СЗИ либо полностью выполняет свои функции, либо должна полностью блокировать доступ.

Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно для предотвращения злонамеренных или неквалифицированных действий системного администратора.

Принцип многоуровневой защиты предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. 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 наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру 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 целом и СЗИ в особенности определяет возможность формального или неформального доказательства корректности реализации механизмов защиты. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование.

Принцип всеобщей поддержки мер безопасности носит нетехнический характер. Рекомендуется с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

IV. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, МЕТОДЫ И СРЕДСТВА

4.1. Виды угроз

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 организации N разделяются на внешние и внутренние.

Источниками внутренних угроз являются:

1) работники организации;

2) ПО;

3) аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

1) ошибки пользователей и системных администраторов;

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

3) ошибки в работе ПО;

4) отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:

1) компьютерные вирусы и вредоносные программы;

2) организации, службы и отдельные лица;

3) стихийные бедствия.

Формами проявления внешних угроз являются:

1) заражение компьютеров вирусами или вредоносными программами;

2) несанкционированный доступ (НСД) к корпоративной информации;

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

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

5) аварии, пожары, техногенные катастрофы.

4.2. Методы и средства информационной безопасности

Обеспечение информационной безопасности организации N реализуется следующими формами защиты:

1) организационной;

2) 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).

4.2.1. Организационные формы защиты

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

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании технической инфраструктуры организации N 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:

1) разработку и издание правил (инструкций и указаний) по обеспечению ИБ, соответствующих им правилам работы организации и требованиям к обработке информации;
2) внедрение программы обеспечения ИБ, включая классификацию информации и оценку деятельности;
3) проведение первичного инструктажа по основам информационной безопасности пользователей ИСПДн;
4) разработку и внедрение процедур пересмотра правил обеспечения информационной безопасности, а также рабочих программ, предназначенных для поддержки правил, инструкций, стандартов и указаний организации;
5) участие в описании, конструировании, создании и приобретении систем в целях соблюдения правил безопасности при автоматизации производственных процессов;
6) изучение, оценку, выбор и внедрение аппаратных и программных средств, функций и методик обеспечения информационной безопасности, применимых для компьютерных систем организации.

При необходимости на ИТО возлагается выполнение других обязанностей:

1) участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;
2) наблюдение за функционированием системы защиты и ее элементов;
3) организация проверок надежности функционирования системы защиты;
4) обучение пользователей и персонала ИС правилам безопасной обработки информации;
5) контроль за соблюдением пользователями и персоналом ИС установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;
6) принятие мер при попытках НСД к информации и при нарушениях правил функционирования системы защиты.

Организационно-правовой статус СИБ:

1) численность службы защиты должна быть достаточной для выполнения всех перечисленных функций;
2) подчиненность СИБ определяется структурой организации;
3) 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;

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

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

4.2.2. Физическая безопасность

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.

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 организации N.

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

4.2.3. Требования к рабочему месту пользователя (администратора)

В состав типового рабочего места входят:

1) компьютер (комплект – системный блок, монитор, клавиатура, манипулятор «мышь», многогнездная розетка-удлинитель (опция), источник бесперебойного питания);

2) мебель рабочего места (стол письменный (канцелярский), стул, тумбочка).

В целях обеспечения требований физической безопасности компьютер как комплект должен быть проверен на информационную безопасность и опломбирован. В случае обнаружения факта изменения состава комплекта или нарушения пломбы пароль администратора информационной безопасности считается отозванным, дальнейшее использование компьютера прекращается и

может быть возобновлено только после смены пароля администратора информационной безопасности.

Должно быть минимизировано количество путей доступа к ресурсам компьютера, удалить (физически отключить) «лишние», неиспользуемые для повседневной штатной работы порты (COM, USB, RS), флоппи и CD/DVD дисководы.

Монитор следует располагать таким образом, чтобы исключить возможность просмотра содержимого экрана посторонними лицами, в том числе извне с помощью оптических приборов.

Особое внимание следует уделять условиям хранения носителей с резервными копиями ресурсов, а также ключей физической защиты (Aladdin, eToken и т.д.). Они должны храниться в запираемом металлическом шкафу. Должен быть обеспечен быстрый доступ к носителю в условиях чрезвычайной ситуации.

Должен использоваться хранитель экрана с паролем.

В качестве носителей информации должны использоваться носители, полученные пользователем непосредственно в организации.

Для хранения носителей с оперативными резервными копиями данных и состояния системы должны быть определены место и средства хранения и соблюдены условия хранения применительно к типу конкретного носителя.

Поскольку состав рабочего места администраторов в целом соответствует вышеприведенному, аналогичные требования и рекомендации распространяются также и на рабочие места администраторов.

4.3. Требования к серверному оборудованию и серверному помещению

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

Помещение в организации N, где находятся коммутаторы, а также крипто-шлюз, запирается на ключ, доступ к ключу имеют лица из заранее утвержденного перечня.

4.4. Управление услугами, предоставляемыми третьими сторонами

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.

4.5. Транспортировка физических носителей информации

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:

1) следует использовать надежных курьеров или надежный транспорт;
2) список уполномоченных курьеров должен быть согласован с руководством организации;
3) должны быть разработаны процедуры проверки личности курьеров;
4) упаковка должна обеспечивать достаточную защиту контента от любого физического повреждения, которое, вероятнее всего, может возникнуть при транспортировке;
5) упаковка должна соответствовать спецификациям любых производителей;
6) 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;
7) при необходимости должны применяться средства управления, защищающие чувствительную информацию от несанкционированного раскрытия или изменения, например:
    a) использование запираемых контейнеров;
    b) доставка вручную;
    c) запечатанная упаковка (обеспечивающая обнаружение попыток вскрытия);
    d) в исключительных ситуациях – разбиение всего отправляемого груза на несколько партий, и отправка их к пункту назначения по различным маршрутам.

4.6. Программные и аппаратные формы защиты

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

1) идентификация и аутентификация пользователей;
2) разграничение доступа к ресурсам;
3) регистрация событий;
4) криптографические преобразования;
5) проверка целостности системы;
6) проверка отсутствия вредоносных программ;
7) программная защита передаваемой информации и каналов связи;
8) защита системы от наличия и появления нежелательной информации;
9) создание физических препятствий на путях проникновения нарушителей;
10) мониторинг и сигнализация соблюдения правильности работы системы;
11) создание резервных копий информации.

4.7. 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:

1) должна быть предусмотрена защита сообщений от несанкционированного доступа, изменения или отказа в обслуживании;
2) должна быть обеспечена правильная адресация и транспортировка сообщения;
3) должна быть обеспечена надежность и доступность обслуживания;
4) должны быть учтены требования законодательства Российской Федерации, в частности, требования, предъявляемые к электронным документам и ЭП;
5) 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:

1) уязвимость электронных сообщений по отношению к несанкционированному перехвату и модификации;
2) 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;
3) влияние изменения характеристик коммуникационной среды на производственные процессы, например, влияние повышенной скорости передачи данных или изменения системы адресации между организациями и отдельными лицами;
4) правовые соображения, такие, как необходимость проверки источника сообщений и др.;
5) последствия для системы безопасности от раскрытия содержания каталогов;
6) необходимость принятия защитных мер для контроля удаленного доступа пользователей к электронной почте.

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

4.8. 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:

1) 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.

2) 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.

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

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

4.9. Средства управления для борьбы со злонамеренными программными кодами

В качестве мер для борьбы со злонамеренными программными кодами должны быть реализованы средства управления для предотвращения его ввода, его обнаружения и восстановления системы после удаления злонамеренного программного кода, а также поддержания компетентности пользователей в этой области.

При этом учитываются следующие рекомендации:

1) необходимо внедрить правила, запрещающие использование нелегального ПО;

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

3) 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:

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

2) 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;

3) 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;

4) 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;

5) реализация процедур проверки информации, касающейся злонамеренного кода, гарантирование того, что бюллетени с предупреждениями точны и информативны; руководители должны гарантировать, что для того, чтобы отличить мистификации от реальных злонамеренных кодов, будут использоваться квалифицированные источники, например, журналы, имеющие хорошую репутацию, надежные сайты в сети Интернет или поставщики защитного ПО; все пользователи должны быть оповещены о проблемах, связанных с мистификациями и о том, что следует делать при получении мистифицированного злонамеренного кода.

В установленном для защиты от злонамеренных кодов ПО необходимо обеспечить поддержку автоматического обновления файлов определения и утилит сканирования, что гарантирует своевременное обновление защиты.

Кроме того, это ПО может быть установлено на каждом рабочем месте для выполнения автоматических проверок.

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

V. ПЕРЕСМОТР ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Соблюдение требований ПИБ обязательно для всех категорий работников, эксплуатирующих и пользующихся ИС организации N. 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 организации N целесообразно ежегодно.

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

VI. ОТВЕТСТВЕННОСТЬ ЗА СОБЛЮДЕНИЕ ПОЛОЖЕНИЙ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Общее руководство обеспечением информационной безопасности осуществляет начальник ИТО организации N.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в систему информационной безопасности несет администратор информационной безопасности, назначенный приказом директора организации N.

Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

Администратор информационной безопасности несет ответственность за все действия, совершенные от имени его учетной записи или системной учетной записи, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками организации N – пользователей ИС правил, связанных с безопасностью ИС, они несут ответственность, установленную действующим законодательством Российской Федерации.

VII. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ПОЛОЖЕНИЙ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Общий контроль состояния информационной безопасности осуществляется начальником ИТО организации N.

Текущий контроль соблюдения настоящей Политики осуществляет ИТО. Контроль осуществляется путем проведения мониторинга и управления инцидентами информационной безопасности организации N, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

ИТО осуществляет контроль соблюдения настоящей Политики на основе проведения внутреннего аудита информационной безопасности.

Контроль эффективности средств по защите должен осуществляется на периодической основе, не реже одного раза в год. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы средств защиты (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности ИС.

Контроль может проводиться как сотрудниками организации N, так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Мероприятия по осуществлению контроля:

- контроль над соблюдением режима защиты;
- контроль над соблюдением режима обработки ПДн;
- контроль над выполнением антивирусной защиты;
- контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена;
- проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн;
- контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИС;
- контроль за обеспечением резервного копирования;
- организация анализа и пересмотра имеющихся угроз безопасности ИС, а также предсказание появления новых, еще неизвестных, угроз;
- поддержание в актуальном состоянии нормативно-организационных документов;
- контроль за разработкой и внесением изменений в ПО собственной разработки или в штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями.