ПБ.К.01.01

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Концепция обеспечения информационной безопасности

Днепродзержинск

2006

ПБ.К.01.01, редакция 1 от 07.07.2006

Политика информационной безопасности предприятия.

Концепция обеспечения информационной безопасности предприятия.

Данная концепция информационной безопасности является фундаментом политики информационной безопасности предприятия и основой при разработке регламента обеспечения информационной безопасности предприятия.

В концепции определены возможные угрозы для информационной безопасности предприятия, методы защиты информационных ресурсов и требования контроля обеспечения информационной безопасности. Также оговариваются средства и методы организации постоянной информационной защиты и обеспечения непрерывности процессов, связанных с использованием информационных систем.

Концепция должна быть учтена при подготовке всех руководящих документов (инструкций, приказов и т.д.).

Оглавление

1 Политика информационной безопасности

Целями и основными задачами обеспечения информационной безопасности предприятия являются:

- защита информации от несанкционированного использования (разглашения, перехвата);
- обеспечение целостности и достоверности информации;
- обеспечение оперативности получения информации.

Политика информационной безопасности – это общая стратегия предприятия в области защиты информации, которая отражается в наборе внутренних нормативных документов, носящих обязательный для исполнения характер, и содержит регламентирующие положения для всех операционных процессов, связанных с использованием конфиденциальной информации предприятия.

Политика информационной безопасности предприятия, как и набор фиксирующей ее организационно-распорядительной документации, подразделяется на три уровня:

- стратегический уровень;
- уровень регламента (он же регламентный уровень или уровень технического регламента);
- руководящий уровень.

На стратегическом уровне политика информационной безопасности представлена:

1. стратегией обеспечения информационной безопасности предприятия, намеченной приказом Председателя Правления №__ от «__»_____ 2005 года;
2. концепцией обеспечения информационной безопасности, представленной данным документом.

На уровне регламента политика информационной безопасности представлена регламентом обеспечения информационной безопасности, который содержит детализацию методов и подходов для реализации намеченной концепции

обеспечения информационной безопасности. Также на уровне технического регламента оговаривается применение программно-технических средств защиты информации.

На руководящем уровне политика обеспечения информационной безопасности представлена набором должностных и технологических инструкций, положений, а также эксплуатационной документацией средств активной и пассивной защиты информации.

Ряд документов, составляющих политику информационной безопасности предприятия, должен быть доведен до каждого сотрудника предприятия, отвечающего за обеспечение режима информационной безопасности. Уровень ответственности сотрудника и перечень предъявляемых ему требований зависит от занимаемой должности.

2 Организация защиты информации на предприятии

При организации защиты выделяют следующие этапы:

- регулярный периодический пересмотр существующей защиты информации, а также требований к ее организации;
- определение основных угроз, которым подвергаются информационные ресурсы;
- пересмотр и оценка случаев нарушения информационной безопасности;
- проведение организационно-технических мероприятий, разработка и внедрение средств по улучшению информационной безопасности.

Для обеспечения информационной безопасности необходимо:

- определить информационные ресурсы и классифицировать их по уровню конфиденциальности;
- определить операционные процессы, по которым необходимо обеспечить защиту информации;
- определить средства защиты информации, а также механизм их внедрения по каждому операционному процессу и на предприятии в целом;
- определить обязанности сотрудников по каждому операционному процессу;
- определить ответственность сотрудников за обеспечение информационной безопасности;
- обеспечить авторизацию сотрудника при получении доступа к информации и при ее использовании;
- определить механизм информационного обмена предприятия со сторонними организациями.

Для успешного проведения данного комплекса задач на уровне должностных инструкций и приказов определяются обязанности и ответственность для каждого

сотрудника предприятия, проводится внедрение и дальнейшее совершенствование средств, направленных на повышение защиты информации.

Для операционных процессов, включающих использование автоматизированных информационных систем, обеспечиваются дополнительные меры:

- новые автоматизированные информационные системы и программное обеспечение внедряется только после анализа и обоснования необходимости их использования без ущерба информационной безопасности предприятия;
- тестируется совместимость аппаратных и программных средств, а также их совместимость с другими действующими системами или системами, применение которых планируется;
- программное обеспечение для работы с коммерческой и секретной информацией проходит дополнительную проверку на соответствие требованиям информационной безопасности.

Для эффективного функционирования системы обеспечения информационной безопасности предприятия необходимо:

- регулярное проведение совещаний руководящего состава предприятия с целью координации действий по реализации и совершенствованию политики информационной безопасности;
- регулярное проведение независимой экспертной оценки обеспечения информационной безопасности предприятия.

3 Классификация информационных ресурсов

Целью классификации и организации доступа к информационным ресурсам является обеспечение их целостности и конфиденциальности. Для этого необходимо:

- определить уровень секретности информации по каждому информационному ресурсу;
- закрепить ответственных сотрудников за обеспечение информационной безопасности информационных ресурсов.

По уровню секретности выделяются следующие категории информации:

1. Общедоступная – информация с неограниченным свободным доступом (не только для сотрудников предприятия). Копирование и любые операции по передаче информации данной категории ограничиваются только наличием авторских прав.
2. Конфиденциальная – любая внутренняя информация предприятия. Подлежит защите от несанкционированного доступа и защите от утери.
3. Строго конфиденциальная – информация, являющаяся коммерческой тайной предприятия. Подлежит защите от несанкционированного доступа и защите от утери.
4. Секретная – финансовая информация о деятельности предприятия и особо важная техническая информация. Подлежит защите от несанкционированного доступа, криптографической защите и защите от утери. По секретной информации ведется обязательный учет её использования.

4 Операционные процессы и обязанности

Под операционным процессом понимается совокупность взаимосвязанных действий и операций, которые производятся с использованием определенных ресурсов, и направлены на получение определенного результата.

Для обеспечения общей информационной безопасности предприятия:

а) выделяются и формализуются все операционные процессы, связанные с использованием информационных систем, –

возлагается на рабочие группы в составе представителей подразделений, участвующих в операционном процессе, а также на службы, задействованные на проектировании информационных систем;

б) выделяются и документируются все возможные инциденты[1] при выполнении операционных процессов, а также действия при возникновении этих инцидентов, –

возлагается на рабочие группы в составе представителей подразделений, участвующих в операционном процессе, а также на службы, задействованные на проектировании информационных систем;

в) определяются и применяются упреждающие меры по уменьшению рисков возникновения инцидентов, –

возлагается на рабочие группы в составе представителей подразделений, участвующих в операционном процессе, а также на службы, задействованные на проектировании информационных систем;

г) назначаются ответственные лица, ответственные за информационную безопасность по каждому операционному процессу, –

Назначаются приказами по предприятию (подразделениям);

---

[1] Под инцидентом понимается преднамеренные или случайные действия, несчастные случаи, аварии, стихийные бедствия и катастрофы, повлекшие за собой нарушение работы операционного процесса.

д) осуществляется контроль изменений и появления новых операционных процессов, –

возлагается на рабочие группы в составе представителей подразделений, участвующих в операционном процессе, а также на службы, задействованные на проектировании информационных систем.

По каждому операционному процессу подлежат рассмотрению вопросы:

- участия персонала в обеспечении информационной безопасности;
- физической безопасности;
- администрирования используемых в операционном процессе компьютерных систем и сетей;
- управления доступом к используемым в операционных процессах информационным системам;
- обеспечения бесперебойной работы;
- соответствия правовым нормам;
- контроля обеспечения информационной безопасности.

5 Информационная безопасность и персонал

С целью выполнения персоналом требований обеспечения информационной безопасности:

1. В должностные инструкции сотрудников предприятия включаются:
   - требования информационной безопасности и обязанности по их соблюдению, включая обязанности по защите определенных ресурсов или ответственность за выполнение определенных процедур или действий по защите информации;
   - ответственность за нарушение режима конфиденциальности и невыполнение требований политики информационной безопасности предприятия.
2. В случае предоставления информации работникам сторонних организаций, в договор со сторонней организацией включаются требования и обязанности по соблюдению информационной безопасности предприятия или оформляется дополнительное соглашение.
3. При переводе, увольнении или изменении служебных обязанностей сотрудника, имевшего доступ к информационным ресурсам предприятия, оповещается служба, ответственная за обеспечение информационной безопасности предприятия.
4. Проводится обучение персонала вопросам обеспечения режима конфиденциальности.
5. Производится контроль служебной корреспонденции.

Выполнение требований 1-3 возлагается на руководителей подразделений. Выполнение требования 4 возлагается на службу, задействованную в кадровых вопросах. Выполнение требования 5 возлагается на службу, ответственную за обеспечение информационной безопасности предприятия.

6 Физическая безопасность

Для обеспечения физической безопасности вводится:

1. Система обеспечения физической безопасности оборудования, задействованного в хранении, обработке или передаче информации[2]:
   - правила ввода и вывода оборудования из эксплуатации;
   - правила эксплуатации оборудования;
   - ограничение и контроль доступа к рабочим местам;
   - ограничение доступа к оборудованию лицам, не связанным с его обслуживанием;
   - изоляция мест хранения информации (в том числе на бумажных носителях);
   - использование специальных средств защиты оборудования от угроз, представляемых окружающей средой, другим оборудованием или прочими факторами, влияющими на процессы хранения, обработки и передачи информации.
2. Дополнительные требования к носителям информации:
   - гарантированное уничтожение отработанных носителей информации;
   - проверка на отсутствие важной информации на носителях перед их списанием или отправкой по гарантии;
   - контроль выноса с предприятия информации (на магнитных, оптических носителях, картах памяти, бумаге и т.д.).

[2] персональные компьютеры, сервера, линии связи, коммутационное оборудование и т.д.

7 Администрирование компьютерных систем и сетей

С целью сведения к минимуму риска случайного или преднамеренного злоупотребления информационными системами обязанности по сопровождению информационных систем и ресурсов подлежат максимально возможному разделению. Обязанности по администрированию сетей (сетевому администрированию) и администрированию аппаратного обеспечения (системному администрированию) подлежат обязательному разделению. Администрирование сетей, аппаратного обеспечения, информационных систем и прочих сервисов и ресурсов проводится скоординировано.

7.1 Проектирование систем

При проектировании новых компьютерных систем:

а) определяются угрозы и риски для информационной безопасности предприятия, которые могут возникнуть при использовании системы;

б) проводится оценка планируемой нагрузки на систему;

в) анализируются требования операционной системы и прикладных программ, которые будут использоваться.

Выполнение этих требований возлагается на службы, задействованные на проектировании информационных систем, а также на обслуживании компьютерных систем и сетей.

7.2 Установка систем и запуск их в эксплуатацию

Перед установкой компьютерных систем проводится комплексное тестирование с целью выявления рисков и угроз для информационной безопасности предприятия.

При установке и запуске в эксплуатацию новых компьютерных систем назначаются лица, ответственные за информационную безопасность и сопровождение устанавливаемых компьютерных систем.

7.3 Обслуживание систем

При обслуживании компьютерных систем:

а) обеспечивается контроль изменений, вносимых в компьютерные системы и сети;

б) регистрируются все значимые события, связанные с работой компьютерных систем;

в) регистрируются и подлежат анализу все сбои компьютерных систем;

г) соблюдаются требуемые условия эксплуатации компьютерных систем;

д) производится оценка запаса производительности работающих систем;

е) соблюдаются правила утилизации устаревших и вышедших из строя компьютерных систем.

Соблюдение требований обслуживания систем возлагается на службы, задействованные в процессе обслуживания компьютерных систем и сетей.

7.4 Защита систем от вредоносного программного обеспечения

С целью защиты компьютерных систем и сетей от вредоносного программного обеспечения:

а) обеспечивается контроль установки, изменения и удаления программного обеспечения компьютерных систем;

б) обеспечивается интеграция в компьютерные системы средств защиты от злонамеренного программного обеспечения, в том числе средств антивирусной защиты;

в) заранее определяются действия при обнаружении вредоносного программного обеспечения.

Выполнение этих требований возлагается на службы, задействованные в процессе обслуживания компьютерных систем и сетей.

7.5 Резервирование систем

С целью обеспечения бесперебойной работы предприятия проводится резервирование систем, связанных с критическими процессами работы

предприятия, а также регулярно проверяется работоспособность резервных систем.

7.6 Сетевое администрирование

С целью обеспечения безопасности информации, которая передается по компьютерным сетям:

а) определяется, документируется и контролируется структура компьютерных сетей и схема сетевых подключений;

б) определяются и документируются настройки сети;

в) обеспечивается конфиденциальность и целостность данных, передаваемых по сетям.

Выполнение этих требований возлагается на службы, задействованные в процессе обслуживания компьютерных систем и сетей.

7.7 Оперирование с носителями информации и их защита

С целью обеспечения информационной безопасности при работе с носителями информации:

а) соблюдаются правила хранения и использования носителей информации;

б) определяются и документируются процедуры оперирования с данными, находящимися на носителях информации;

в) определяются и используются методы и средства защиты носителей информации и данных на них;

г) соблюдаются правила утилизации носителей информации.

Выполнение этих требований возлагается на службы, отвечающие за аудит информационной безопасности.

7.8 Обмен данными и программами

С целью обеспечения информационной безопасности при обмене данными и программами:

а) заключаются соглашения об обмене информацией с организациями, с которыми производится такой обмен;

б) определяются и выдерживаются меры защиты при транспортировке носителей информации;

в) обеспечивается контроль доступа к источникам электронного обмена информацией;

г) определяются и выдерживаются меры защиты информации во время электронного обмена.

Выполнение этих требований возлагается на службы, задействованные в процессе обслуживания компьютерных систем и сетей.

8 Управление доступом к информационным системам

Для обеспечения информационной безопасности при использовании информационных систем необходимо:

1. разграничивать доступ к информационным системам предприятия;
2. обеспечить контроль использования информационных систем.

8.1 Разграничение доступа к информационным системам предприятия

Каждый сотрудник обладает определенным уровнем доступа к информации. Управление доступом производится службой информационной безопасности в следующих случаях:

- предоставление доступа для вновь принятых сотрудников;
- изменение уровня доступа в связи с изменением занимаемой должности или изменением служебных обязанностей;
- деактивация доступа при увольнении сотрудника.

Предоставление доступа сотруднику предприятия к информационным ресурсам, изменение уровня доступа или деактивация доступа производится службой информационной безопасности на основании:

- приказов по предприятию;
- заявок руководителей структурных подразделений.

8.2 Контроль использования информационных систем

Контроль использования информационных систем служит для анализа действий, которые могут привести или привели к:

- нарушению режима конфиденциальности;
- искажению данных.

Журнал доступа и изменения данных подлежит долгосрочному хранению без возможности изменения его кем-либо.

9 Информационная безопасность программного обеспечения

9.1 Информационная безопасность программного обеспечения в процессе разработки

При разработке программного обеспечения:

а) осуществляется контроль доступа к исходным текстам разрабатываемого программного обеспечения;

б) осуществляется контроль доступа к информационным ресурсам, которые используются при разработке программного обеспечения;

в) сборка конечных версий программного обеспечения проводится через систему контроля версий;

Выполнение данных требований возлагается на службы, задействованные на разработке программного обеспечения.

г) перед запуском информационных систем в эксплуатацию проводится тестирование программного обеспечения для выявления угроз и рисков информационной безопасности предприятия;

д) осуществляется контроль качества и безопасности программного обеспечения, разработанного сторонними организациями или подрядными лицами.

Выполнение данных требований возлагается на службы, задействованные на проектировании и тестировании программного обеспечения.

9.2 Безопасность программного обеспечения в процессе использования и сопровождения информационных систем

В процессе использования и сопровождения информационных систем:

а) осуществляется контроль всех изменений, как аппаратных, так и программных, которые производятся на рабочих станциях, задействованных в работе информационных систем;

б) перед установкой новой операционной системы на рабочие станции, проводится тестирование программного обеспечения на предмет совместимости и стабильности работы с новой операционной системой;

в) все изменения, которые вносятся в исходный код программного обеспечения, проводятся через автоматизированную систему контроля версий;

г) обновление модулей программного обеспечения, установленного на серверах предприятия и на рабочих станциях, осуществляется через автоматизированную систему обновлений;

д) для программного обеспечения, сопровождение которого ведется сторонними разработчиками, осуществляется контроль качества и безопасности при каждом обновлении.

Выполнение всех требований возлагается на службы, задействованные на сопровождении и тестировании программного обеспечения.

9.3 Интеграция средств защиты информации в программное обеспечение

С целью обеспечения информационной безопасности в программное обеспечение встраиваются средства защиты. В зависимости от типа информационной системы и информации, подлежащей обработке, применяются следующие средства защиты информации:

- аутентификация пользователей;
- шифрование данных.
- использование цифровой подписи для электронных документов;
- аутентификация сообщений.

Интеграция средств защиты информации в программное обеспечение возлагается на службы, задействованные на проектировании и разработке программного обеспечения. Проверка действия интегрированных средств безопасности выполняется службами, задействованными на тестировании программного обеспечения, а также службами, ответственными за аудит информационной безопасности.

10 Обеспечение бесперебойной работы процессов, связанных с использованием автоматизированных информационных систем

С целью обеспечения бесперебойной работы процессов, связанных с использованием АИС:

а) выделяются процессы, связанные с АИС, для которых важно обеспечить бесперебойность, –

возлагается на службы, задействованные на проектировании АИС для новых систем; для действующих систем – задействованные на проектировании и сопровождении АИС (аппаратной и программной части, сетевых коммуникаций в случае их использования);

б) по каждому процессу определяются возможные инциденты и последствия от них, –

возлагается на службы, задействованные на проектировании АИС;

в) по каждому из процессов разрабатывается система упреждающих мер для уменьшения вероятности возникновения инцидентов, –

возлагается на службы, задействованные на сопровождении АИС (аппаратной и программной части, сетевых коммуникаций в случае их использования);

г) по каждому из процессов разрабатывается план действий на случай возникновения инцидентов, включающий в себя описание:

- перехода на аварийный режим работы;
- действий по ликвидации последствий инцидента;
- по возобновлению нормальной работы;

возлагается на службы, задействованные на сопровождении АИС (аппаратной и программной части, сетевых коммуникаций в случае их использования).

д) по каждому из процессов разрабатывается система тестирования бесперебойной работы, –

Возлагается на службы, задействованные на сопровождении АИС (аппаратной и программной части, сетевых коммуникаций в случае их использования);

е) назначаются сотрудники, ответственные за обеспечение бесперебойной работы для каждого процесса, –

назначаются приказом по предприятию (подразделению);

ж) проводится постоянное совершенствование системы обеспечения бесперебойной работы, –

проводится службами, задействованными на проектировании АИС, а также службами, задействованные на сопровождении АИС (аппаратной и программной части, сетевых коммуникаций в случае их использования).

11 Соответствие правовым нормам

С целью предотвращения нарушения правовых обязательств и обязательств по соблюдению уголовного и гражданского права обеспечивается:

а) контроль за копированием и использованием ПО, защищенного законом об авторском праве, –

возлагается на руководителей структурных подразделений;

аудит производит служба информационной безопасности.

б) контроль использования и обеспечения сохранности информации, которая может потребоваться:

- для обеспечения надлежащей защиты от возможных гражданских или уголовных исков в качестве свидетельства того, что организация работает в соответствии с правовыми нормами;
- для подтверждения финансового состояния организации по отношению к держателям акций, партнерам и аудиторам, –

возлагается на службу информационной безопасности;

в) защита персональных данных от несанкционированного доступа, их изменения, раскрытия и уничтожения, а также от их случайной потери или уничтожения, —

возлагается на все службы и подразделения, задействованные в информационном обмене персональных данных сотрудников;

г) предотвращение незаконного использования информационных ресурсов Предприятия, путем регламентации порядка работы пользователей с информационными системами предприятия, —

возлагается на службу информационной безопасности.

12 Контроль обеспечения информационной безопасности

Для организации контроля обеспечения информационной безопасности предприятия:

а) по всем операционным процессам необходимо определить требования обеспечения информационной безопасности;

б) определить средства контроля, меры противодействия и обязанности для выполнения контроля требований.

По всем требованиям обеспечивается контроль их выполнения, для чего:

- выполняется планирование и согласование работ, связанных с аудитом информационных систем;
- осуществляется учет процесса аудита;

В случае нарушения информационной безопасности или в целях ее совершенствования по результатам аудита принимаются корректирующие меры, регулярно пересматривается методика обеспечения информационной безопасности и средства контроля выполнения ее требований.

Контроль обеспечения информационной безопасности осуществляется службой информационной безопасности предприятия.