1. ОБЩИЕ ПОЛОЖЕНИЯ
   1. Область применения

Политика информационной безопасности ООО”Wayne Enterprise” определяет высо­коуровневые цели, содержание и основные направления деятельности по обеспечению ин­формационной безопасности Компании.

Положения настоящего документа распространяются на все структурные подразде­ления Компании, независимо от их местонахождения и являются обязательными для испол­нения.

* 1. Термины и определения

|  |  |
| --- | --- |
| Термин | Определение |
| **Служебная информация** | Информация, создаваемая, обрабатываемая и используемая Компанией, доверенная Компании её клиентами и бизнес парт­нерами, а также информация, которую Компания должна защи­щать в соответствии с действующим законодательством Россий­ской Федерации |
| **Владелец информации** | Организационная роль сотрудника Компании по обеспечению ИБ информации, создаваемой в рамках своего подразделения. |
| **Организационная роль** | Совокупность обязанностей сотрудника Компании, возлагаемых на него отдельными поручениями руководства Компании или Ру­ководителем подразделения, и уточняющие отдельные положе­ния должностных обязанностей (например, участие в конкретной рабочей группе, кураторство нескольких конкретных филиалов, участие в разработке конкре тного проекта, и т.п.) |
| **Политика** | Настоящий документ |
| **Руководитель, Руководитель подразделения** | Руководитель Департамента, Управления, не входящего в струк­туру Департамента, Отдела, не входящего в структуру Дирекции или Департамента |
| **Информационная инфраструктура** | Система организационных структур, обеспечивающих функцио­нирование и развитие информационного пространства и средств информационного взаимодействия.  Примечание  Информационная инфраструктура:   * включает совокупность информационных центров, баз дан­ных и знаний, систем связи; * обеспечивает доступ потребителей к информационным ресур­сам. |
| **Информационная безопасность** | Безопасность, связанная с угрозами в информационной сфере. |
| **Угроза информацион­ной безопасности** | Опасность, предполагающая возможность потерь (ущерба) по причине нарушения свойств ИБ - доступности, целостности или конфиденциальности информационных активов. |
| **Инцидент информаци­онной безопасности** | Событие, указывающее на свершившуюся, предпринимаемую  или вероятную реализацию угрозы ИБ  Примечание.  Нарушение может вызываться источниками угроз ИБ: либо слу­чайными факторами (ошибкой персонала, неправильным функ­ционированием технических средств, природными факторами, например, пожаром или наводнением), либо преднамеренными действиями, приводящими к нарушению доступности, целостно­сти или конфиденциальности информационных активов. |
| **Нарушитель информа­ционной безопасности** | Субъект, реализующий угрозы ИБ, нарушая предоставленные ему полномочия по доступу к информационным активам или по распоряжению ими. |
| **Модель нарушителя информационной без­опасности** | Описание и классификация нарушителей ИБ, включая описание их опыта, знаний, доступных ресурсов, необходимых для реали­зации угрозы, возможной мотивации их действий, а также спо­собы реализации угроз ИБ со стороны указанных нарушителей. |
| **Модель угроз инфор­мационной безопасно­сти** | Описание источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, ис­пользуемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиден­циальности информационных активов); масштабов потенциаль­ного ущерба. |
| **Риск нарушения ин­формационной без­опасности** | Мера, учитывающая вероятность реализации угрозы ИБ и вели­чину потерь (ущерба) от реализации этой угрозы. |
| **Оценка риска наруше­ния информационной безопасности** | Систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей про­вести оценивание рисков нарушения ИБ. |
| **Обработка риска нарушении информа­ционной безопасности** | Процесс выбора и осуществления защитных мер, снижающих риск нарушения ИБ. или мер по переносу, принятию или уходу от риска. |
| **Остаточный риск нарушения информа­ционной безопасности** | Риск, остающийся после обработки риска нарушения ИБ. |

* 1. Сокращения

|  |  |  |
| --- | --- | --- |
| Сокращение | Расшифровка сокращения | |
| **Компания** | ООО”Wayne Enterprise” | |
| **ДИБ** | Департамент информационной безопасности - структурное подразделение Компании, уполномоченное на выполнение мероприятий в области инфор­мационной безопасности. | |
| **ИБ** | Информационная безопасность |  |

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ
   1. Цели деятельности по обеспечению информационной безопасности Компании
      1. Меры безопасности, реализуемые в рамках системы обеспечения информационной безопасности Компании, и процессы эксплуатации этих мер нацелены на минимизацию лю­бых выявленных угроз информационной безопасности.
      2. Основными целями обеспечения ИБ являются:
         * Соответствие требованиям законодательства, требованиям надзорных и регули­рующих органов;
         * Обеспечение стабильности функционирования Компании (обеспечение непре­рывности его бизнеса) посредством обеспечения необходимой доступности информаци­онных активов Компании;
         * Повышение доверия к Компании со стороны клиентов, контрагентов, партнеров, инвесторов и общественности в целом;
         * Предотвращение или снижение ущерба от инцидентов ИБ посредством обеспе­чения целостности и конфиденциальности чувствительных информационных активов Компании;
         * Защита законных прав Компании и её работников, в случаях неправомерного использования или злоупотребления информационными активами;
         * Защита капиталовложений в информационную инфраструктуру и реализуемые посредством ее технологические процессы Компании;
         * Формирование взвешенного подхода к защите от угроз ИБ посредством приме­нения экономически и технически обоснованных, а также необходимых и достаточных защитных мер информационной безопасности.
   2. Основные задачи и принципы информационной безопасности Компании
      1. Одним из наиболее ценных активов Компании является информация, создаваемая, обрабатываемая и используемая Компанией, доверенная Компании её клиентами и бизнес партнерами, а также информация, которую Компания должна защищать в соответствии с действующим законодательством РФ.
      2. Компания должна обеспечить конфиденциальность, целостность и доступность служебной информации и защитить се от повреждения, изменения, разглашения и утраты.
      3. Безопасность информационных ресурсов Компании должна быть обеспечена как от нарушителей (внутренних и внешних), так и от естественных (природных и техногенных) угроз.
      4. Для оценки угроз информационной безопасности в Компании должен быть реализо­ван процесс управления рисками информационной безопасности.
      5. Информационные активы Компании должны быть защищены на всех этапах их жиз­ненного цикла: разработка технических заданий - проектирование - создание и тестирование - приемка и ввод в действие - эксплуатация - сопровождение и модернизация - снятие с экс­плуатации.
      6. Для любой служебной информации должен быть определен и документально за­креплен Владелец информации.
      7. Настоящая Политика и соответствующие частные Политики должны периодически пересматриваться и при необходимости обновляться, при этом ответственность за пересмотр и обновление возлагается на Департамент информационной безопасности.
2. УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
   1. Основные принципы управления рисками информационной безопасности

Для оценки угроз информационной безопасности в Компании должен быть реализован процесс управления рисками информационной безопасности.

* + 1. Меры безопасности, реализуемые в рамках системы обеспечения информационной безопасности Компании, и процессы их эксплуатации нацелены на минимизацию любых вы­явленных угроз информационной безопасности и минимизацию связанных с ними операци­онных рисков основной деятельности Компании (бизнеса).
    2. Снижение рисков нарушения ИБ должно осуществляться до определенного остаточ­ного уровня. Оставшаяся (остаточная) часть риска должна быть признана приемлемой и при­нята, либо отклонена. В этом случае от риска следует либо уклониться (изменить среду дея­тельности), либо перевести на кого-нибудь (например, застраховать). Таким образом, уровень защищенности интересов Компании определяется, во-первых, величиной принятых остаточ­ных рисков, а во-вторых, эффективностью работ по поддержанию принятых рисков на допу­стимом, низком (остаточном) уровне.
    3. Риски нарушения ИБ должны быть согласованы и связаны с рисками основной дея­тельности Компании.
    4. Анализ и оценка рисков нарушения ИБ должна основываться на идентификации ак­тивов Компании, на их ценности для целей и задач Компании, на моделях угроз и нарушителей ИБ.
  1. Реализация процесса управления рисками информационной безопасности

Реализация процесса управления рисками информационной безопасности возлагается на ДИБ, при этом:

* + 1. ДИБ должен быть независим от подразделений, ответственных за реализацию и обеспечение информационных технологий в Компании;
    2. Для реализации требований Политики могут быть назначены Администраторы без­опасности из числа сотрудников структурных подразделений Компании.

1. ВЛАДЕНИЕ ИНФОРМАЦИЕЙ

Для любой служебной информации должен быть определен и документально закреплен Владелец информации.

* + 1. Руководители подразделений, для служебной информации, находящейся в зоне их ответственности (используемой подразделением), должны определить Владельцев информа­ции.
    2. Владелец информации должен классифицировать информацию в зоне своей ответ­ственности следующим образом:
* конфиденциальная,
* внутренняя,
* общедоступная.
  + 1. Каждый Руководитель является Владельцем информации, создаваемой в рамках сво­его подразделения, при этом, для одной и той же информации, может быть определен только один Владелец.
    2. На основе процесса управления рисками и классификации информации, Руководи­тель должен определить необходимый уровень защиты для служебной информации и убе­диться, что существующих мер защиты достаточно, чтобы соответствовать уровню приемле­мого риска.

1. МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЕЙ

Безопасность информационных ресурсов Компании должна быть обеспечена как от нарушителей (внутренних и внешних), так и от естественных (природных и техногенных) угроз.

* + 1. Модели угроз и нарушителей должны быть основным инструментом Компании при развертывании, поддержании и совершенствовании системы обеспечения ИБ.
    2. Модели угроз и нарушителей должны быть разработаны для Компании в целом, а также, при необходимости, для отдельных процессов и систем.
    3. При построении адекватной модели нарушителя необходимо классифицировать нарушителя по следующим параметрам:
* по отношению к системе (внутренний, внешний);
* по правам доступа;
* по мотивам нарушения;
* по уровню знаний о системе;
* по уровню возможностей (используемым методам и средствам);
* по времени действия;
* по месту действия.
  + 1. При построении адекватной модели угроз необходимо исходить из того, что основ­ными источниками угроз ИБ являются:
* работники Компании, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ);
* работники Компании, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками Компании, но осуществляющие попытки несанкционированного доступа (внешние нарушители ИЬ);
* неблагоприятные события природного, техногенного и социального характера;
* террористы и криминальные элементы;
* зависимость от поставщиков/провайдеров/партнеров/клиентов;
* сбои, отказы, разрушения/повреждения программных и технических средств;
* несоответствие требованиям действующего законодательства РФ.

1. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

В случае изменений законодательных и иных нормативных актов Российской Федера­ции, а также Устава Компании, настоящий документ, а также изменения к нему, применяются в части не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Компании.