ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ РЕСПУБЛИКИ КРЫМ «КРЫМТЕПЛОКОММУНЭНЕРГО»

Утверждено Приказом
ГУП РК «Крымтеплокоммунэнерго»
от 26 ноября 2018 г.
№ 663

Концепция обеспечения информационной безопасности в ГУП РК «Крымтеплокоммунэнерго»

Введение.

Настоящий документ представляет собой концепцию обеспечения информационной безопасности Государственного Унитарного Предприятия Республики Крым «Крымтеплокоммунэнерго»[1] и определяет:

- Основные принципы формирования перечня критичных ресурсов, нуждающихся в защите, формируемого в процессе проведения аудита безопасности и анализа рисков. Данный перечень должен включать в себя описание физических, программных и информационных ресурсов с определением стоимости ресурсов и степени их критичности для Предприятия.
- Основные принципы защиты, определяющие стратегию обеспечения информационной безопасности (далее - ИБ) и перечень правил, которыми необходимо руководствоваться при построении системы обеспечения информационной безопасности (далее - СОИБ) Предприятия[2].
- Модель нарушителя безопасности, определяемую на основе обследования ресурсов системы и способов их использования.
- Модель угроз безопасности и оценку рисков, связанных с их осуществлением, формируемую на основе перечня критичных ресурсов и модели нарушителя, которая включает определение вероятностей угроз и способов их осуществления, а также оценку возможного ущерба.

[1] Далее - Предприятие
[2] Приложение №1

- Требования безопасности, определяемые по результатам анализа рисков.
- Меры обеспечения безопасности организационного и программно-технического уровня, предпринимаемые для реализации перечисленных требований.
- Ответственность сотрудников Предприятия за несоблюдение установленных требований ИБ при эксплуатации информационной системы (ИС) Предприятия.

Организация системы ИБ.

Генеральный директор - определяет направления и меры по реализации Концепции информационной безопасности, предусматривает выделение средств и координирует работу подразделений по вопросам ИБ.

Подразделение, ответственное за обеспечение ИБ Предприятия[3]:

- разрабатывает предложения по совершенствованию функционирования систем информационной безопасности;
- проводят анализ угроз безопасности информации и выявление уязвимостей в них;
- обеспечивают в соответствии с требованиями по безопасности реализацию организационных мер и применение средств защиты информации;
- осуществляют реагирование на инциденты информационного характера в порядке, установленном законодательством Российской федерации и нормативными актами Предприятия;
- организуют проведение оценки соответствия объектов информационной инфраструктуры требованиям по безопасности;

Руководители подразделений Предприятия - обеспечивают выполнение всеми подчиненными сотрудниками установленных требований ИБ;

Обеспечение ИБ непосредственно на рабочих местах возлагается на сотрудников подразделений.

Ответственность за нарушение требований ИБ.

По степени опасности нарушения ИБ делятся на две группы:

- нарушения, повлекшие за собой наступление нежелательных для Предприятия последствий (утечку, искажение, изменения или уничтожение информации);
- нарушения, создавшие предпосылки нежелательных для Предприятия последствий (угроза уничтожения, искажения, изменения или

[3] На момент разработки концепции - информационно-вычислительный отдел (далее – ИВО)

утраты информации).

Нарушение требований локальных нормативных документов по ИБ является чрезвычайным происшествием и влечет за собой последствия, предусмотренные действующим законодательством Российской Федерации, нормативными актами и договорами, заключенными между Предприятием и сотрудниками. Степень ответственности за нарушение требований нормативных актов в области ИБ определяется исходя из размера ущерба, причиненного Предприятию.

Руководители структурных подразделений несут персональную ответственность за обеспечение ИБ в возглавляемых ими подразделениях.

Общие положения

СОИБ Предприятия представляет собой совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов Предприятия от угроз информационной безопасности. Меры защиты организационного уровня реализуются путем проведения соответствующих мероприятий, предусмотренных документированной Политикой информационной безопасности. Меры защиты программно-технического уровня реализуются при помощи соответствующих программно-технических средств и методов защиты информации.

Экономический эффект от внедрения СОИБ должен проявляться в виде снижения величины возможного материального, репутационного и иных видов ущерба, наносимого Предприятию, за счет использования мер, направленных на формирование и поддержание режима ИБ. Эти меры призваны обеспечить:

- доступность информации (возможность за приемлемое время получить требуемую информационную услугу);
- целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность информации (защита от несанкционированного ознакомления);
- неотказуемость (невозможность отрицания совершенных действий);
- аутентичность (подтверждение подлинности и достоверности электронных документов).

Концепция ИБ Предприятия определяет состав критичных информационных ресурсов и основные принципы их защиты. Принципы обеспечения ИБ обуславливают необходимость применения определенных методов и технологий защиты. Определение способов реализации этих принципов путем применения конкретных программно-технических средств защиты информации (далее - СЗИ) и системы организационных мероприятий является предметом конкретных Проектов и Политик информационной

безопасности, разрабатываемых на основе данной Концепции.

Настоящая Концепция должна пересматриваться по мере выявления новых методов и технологий осуществления атак на информационные ресурсы. Подобный пересмотр также должен производиться по мере развития информационных систем Предприятия и внесения изменений в действующее законодательство. Рекомендуемый срок пересмотра Концепции составляет три года (при условии отсутствия коренных изменений в законодательстве, структуре системы, в технологиях управления и передачи информации).

Подготовка настоящего документа, внесение в него изменений и общий контроль выполнения требований по обеспечению ИБ Предприятия осуществляется сотрудниками службы безопасности, совместно с подразделением, ответственным за обеспечение ИБ Предприятия.

Ответственность за выполнение требований ИБ, определяемых настоящей Концепцией и другими организационно-распорядительными документами Предприятия, возлагается на пользователей и администраторов сети передачи данных Предприятия, а также их руководителей.

Перечень необходимых мер защиты информации определяется исходя из требований действующего законодательства РФ, по результатам аудита информационной безопасности компьютерной информационной сети (далее – КИС) Предприятия и анализа рисков с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, изменения, нарушения доступности информации и работоспособности программно-технических и аппаратных средств, обрабатывающих эту информацию.

Стратегия обеспечения ИБ строится в соответствии с Российским законодательством в области защиты информации и информационной безопасности, требованиями международных, отраслевых и технологических стандартов, требованиях ФСТЭК и ФСБ.

Настоящая концепция разработана на основе нормативных и распорядительных документов в области защиты информации информационной безопасности Российской Федерации.

Описание объекта защиты

Объектом защиты являются автоматизированные системы (как собственной, так и сторонней разработки), входящие в состав ИС Предприятия.

ИС Предприятия, представляет собой совокупность территориально разнесенных объектов, информационный обмен между которыми осуществляется посредством использования каналов передачи данных, как собственных, так и предоставленных сторонними операторами телекоммуникационных сетей (как проводных, так и беспроводных).

Назначение и основные функции информационной системы

ИС предназначена для обеспечения работоспособности

информационной инфраструктуры Предприятия, предоставления сотрудникам структурных подразделений различных видов информационных сервисов, автоматизации финансовой и производственной деятельности, а также бизнес-процессов Предприятия.

Группы задач, решаемых в информационной системе

Информационная сеть Предприятия предназначена для обеспечения автоматизации процессов организационной структуры Предприятия. Решение функциональных задач реализуется на базе информационной инфраструктуры сети Предприятия с использованием специализированных программных приложений и общедоступных информационных сервисов.

К специализированным приложениям относятся программные средства и системы, включенные в Перечень[4] программных средств, допущенных к использованию на Предприятии.

К общедоступным сетевым сервисам относятся средства обработки информационных потоков на сетевом и операционном уровне, такие как:

- Система обмена электронной почтой
- Файловые сервисы
- Веб-сайт предприятия
- Система IP-телефонии
- Информационные системы Предприятия
- Автоматические системы управления (АСУ) оборудованием Предприятия

Классификация пользователей системы

Пользователем ИС является любой сотрудник Предприятия, зарегистрированный в информационной системе, в соответствии с установленным Порядком[5], и прошедший идентификацию в службе каталогов, которому предоставляется доступ к информационным ресурсам сети Предприятия и приложениям, в соответствии с его должностными обязанностями, а так же пользователи сторонних организаций, которым предоставлен доступ к ИС в соответствии с заключенными соглашениями (договорами, контрактами).

Доступ к специализированным автоматизированным системам осуществляется в соответствии с действующей нормативной базой и должностными инструкциями, утвержденными руководством Предприятия.

Особую категорию пользователей сети составляет руководство Предприятия, а также сотрудники Предприятия, допущенные к работе с персональными данными и информацией, составляющей коммерческую тайну Предприятия. Автоматизированные рабочие места (далее - АРМ) данной категории пользователей подключены к КИС и нуждаются в использовании дополнительных (усиленных) мерах защиты информации, с

[4] Разрабатывается и корректируется ИВО, по согласованию со службой безопасности.

[5] Порядок определяется отдельными нормативными актами Предприятия.

целью предотвращения утечки, повреждения, изменения и модификации информации, составляющей коммерческую тайну Предприятия.

Организационная структура поддержки КИС

Административно-техническая поддержка КИС Предприятия осуществляется эксплуатирующим подразделением[6],по согласованию со службой безопасности.

Структура и состав комплекса программно-технических средств

КИС объекта защиты включает в себя сеть Предприятия в составе:

- Серверы.
- Рабочие станции, АРМ.
- Каналы передачи данных и активное сетевое оборудование.
- Система телефонной связи (IP - телефония).
- Специализированные сетевые устройства и системы.

Сеть Предприятия

В качестве базового сетевого протокола в сети Предприятия используется протокол - TCP/IP, IPX.

В качестве адресного пространства используется сеть, определенная документом IETFRFC1597 для частных IP-сетей. В сети Предприятия выделяются, при необходимости, отдельные подтипы адресных пространств.

Серверы

Серверная группа сети Предприятия функционально подразделяется на серверы поддержки специализированных приложений, серверы поддержки общедоступных сервисов и серверы, поддерживающие технологические службы сети Предприятия.

Рабочие станции

К информационной системе Предприятия подключены АРМ пользователей, оборудованных программными средствами, согласно Перечню программных средств, допущенных к использованию на Предприятии.

Каналы передачи данных и активное сетевое оборудование

Каналы обмена данными используются для обеспечения внешнего информационного взаимодействия КИС, с удаленными подразделениями Предприятия, для доступа к глобальной информационной сети Интернет и к информационным ресурсам сторонних организаций.

Виды информационных ресурсов, хранимых и обрабатываемых в системе

В КИС Предприятия хранятся и обрабатываются различные виды

[6] На момент разработки Концепции – информационно-вычислительный отдел

открытой и служебной (конфиденциальной) информации.

К конфиденциальной и служебной информации, циркулирующей в КИС Предприятия, относятся:

- информация, составляющая коммерческую тайну Предприятия[7];
- персональные данные сотрудников Предприятия, подрядчиков, абонентов и контрагентов[8];
- сообщения электронной почты и информация баз данных, содержащие служебные сведения, информацию о деятельности Предприятия и т.п.;
- конструкторская и технологическая документация, перспективные планы развития, модернизации производства, реализации услуг и другие сведения, составляющие научно-техническую и технологическую информацию, связанную с деятельностью Предприятия, не противоречащую действующему законодательству;
- финансовая документация, бухгалтерская отчетность, аналитические материалы исследований, результаты аудиторских и других проверок;
- другие сведения, составляющие служебную информацию о внутренней деятельности Предприятия.

К строго конфиденциальной информации, которая потенциально может циркулировать в КИС, относятся сведения стратегического характера, разглашение которых может привести к остановке (временной остановке) выполнения функций Предприятия, прямо влияющих на его жизнедеятельность и развитие, нанести невосполнимый ущерб деятельности и престижу Предприятия, сорвать решение стратегических задач, проводимой политики.

К категории открытой относится вся прочая информация, не относящаяся к конфиденциальной, согласно действующего законодательства РФ и внутренних нормативных актов.

Структура информационных потоков

Внутренние информационные потоки

Внутри КИС выделяются следующие информационные потоки:

- Передача файлов между файловыми серверами и пользовательскими рабочими станциями
- Передача сообщений электронной почты
- Передача информации между серверами баз данных и пользовательскими рабочими станциями, в том числе в рамках специализированных автоматизированных систем.
- Деловая переписка.
- Передача отчетной информации.
- Иные способы передачи информации (в том числе потоки видеонаблюдения и т.д.).

[7] На момент разработки Концепции - согласно Приказа №460 от 23.12.2016г.

[8] На момент разработки Концепции - согласно Приказа №459 от 23.12.2016г. и Приказа №559 от 20.10.2017г.

Внешние информационные потоки

В качестве внешних информационных потоков используются:

- Внутриведомственный и межведомственный обмен электронной почтой.
- Передача информации удаленным пользователям и сторонним организациям.
- Различные виды информационных обменов между КИС и сетью Интернет.
- Передача информации на различных носителях.

Характеристика каналов взаимодействия с другими системами и точек входа в КИС Предприятия используются следующие каналы взаимодействия с внешними сетями:

- Каналы взаимодействия с общегосударственными, региональными и глобальными информационными сетями, в том числе сетью Интернет;
- Каналы взаимодействия с ИС сторонних организаций.

Защита подключений к внешним сетям осуществляется при помощи специализированных и встроенных средств защиты магистрального маршрутизатора.

Доступ к информационным ресурсам сети Интернет открыт для выделенных пользователей КИС посредством использования кеширующего прокси-сервера на основе программного обеспечения SQUID 3.0.

Основные факторы, влияющие на информационную безопасность Предприятия

Основными факторами, влияющими на информационную безопасность Предприятия, являются:

- расширение сотрудничества Предприятия с подрядными организациями;
- автоматизация информационных процессов на Предприятии;
- расширение кооперации исполнителей при построении и развитии информационной инфраструктуры Предприятия;
- рост объемов информации Предприятия, передаваемой по телекоммуникационным каналам связи;
- рост числа преступлений в IT сфере.

Основные принципы обеспечения информационной безопасности

Построение архитектуры СОИБ Предприятия должно базироваться на соблюдении следующих основных принципов обеспечения ИБ:

- Простота архитектуры, минимизация и упрощение связей между компонентами, унификация и упрощение компонентов, использование минимального числа протоколов сетевого взаимодействия. Система должна содержать лишь те компоненты и связи, которые необходимы для ее функционирования (с учетом требований надежности и перспективного

развития).

- Апробированность решений, ориентация на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.
- Построение системы из компонентов, обладающих высокой надежностью, готовностью и обслуживаемостью.
- Управляемость, возможность сбора регистрационной информации обо всех компонентах и процессах, наличие средств раннего выявления нарушений информационной безопасности, нештатной работы аппаратуры, программ и пользователей.
- Простота эксплуатации, автоматизация максимального числа действий администраторов КИС.
- Этапность защиты - для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.
- Непрерывность защиты в пространстве и времени, невозможность обхода защитных средств - системы должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом принимаются меры по недопущению перехода систем в незащищенное состояние.
- Равнопрочность защиты по всем направлениям - осуществляется регламентация и документирование всех способов доступа к ресурсам сети. В соответствии с этим принципом запрещается создавать несанкционированные подключения к сети Предприятия и другими способами нарушать установленный Порядок[9] предоставления доступа к информационным ресурсам, который определяется:

«Политикой управления доступом к ресурсам сети Предприятия»; «Политикой обеспечения ИБ при взаимодействии с сетью Интернет»; «Политикой обеспечения ИБ удаленного доступа к ресурсам сети Предприятия».

- Профилактика нарушений безопасности - экономически оправданным является принятие предупредительных мер по недопущению нарушений информационной безопасности в отличие от мер по реагированию на инциденты, связанных с устранением угроз информационной безопасности. Однако это не исключает необходимости принятия мер по реагированию на инциденты и восстановлению поврежденных информационных ресурсов. В соответствии с данным принципом должен проводиться анализ рисков, опирающийся на модель угроз безопасности и модель нарушителя, определяемые настоящей Концепцией. Многие риски можно уменьшить путем принятия превентивных мер защиты.

[9] Разрабатываются и корректируются подразделением, ответственным за ИБ, по согласованию со службой безопасности.

• Минимизация привилегий - Политика безопасности строится на основе принципа «все, что не разрешено - запрещено». Права субъектов должны быть минимально достаточными для выполнения ими своих служебных обязанностей[10];

• Экономическая целесообразность. Обеспечение соответствия ценности информационных ресурсов Предприятия и величины возможного ущерба (от их разглашения, утраты, утечки, изменения, уничтожения и искажения) уровню затрат на обеспечение информационной безопасности. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать экономические показатели работы автоматизированных систем Предприятия, в которых эта информация циркулирует.

• Преемственность и непрерывность совершенствования. Обеспечение постоянного совершенствования мер и средств защиты информационных ресурсов и информационной инфраструктуры на основе преемственности организационных и технических решений, кадровых решений, анализа функционирования систем защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по ее защите, достигнутого отечественного и зарубежного опыта в этой области.

При выборе программно-технических решений по обеспечению ИБ Предприятия, предпочтение отдается решениям, обеспечивающим соблюдение основных принципов ИБ, а также удовлетворяющих следующим критериям:

• Поддержка международных, национальных, промышленных и Интернет стандартов (предпочтение отдается международным стандартам).

• Поддержка наибольшей степени интеграции с программно-аппаратными платформами и используемыми СЗИ;

• Унификация разработчиков и поставщиков используемых продуктов.

• Унификация средств и интерфейсов управления подсистемами ИБ.

Организация работ по защите информации

Организация и проведение работ по обеспечению ИБ Предприятия определяются настоящей концепцией, действующими государственными и международными стандартами и другими нормативными, правовыми и методическими документами.

Организация работ по обеспечению ИБ возлагается на руководителя эксплуатирующего подразделения, а методическое руководство и контроль над эффективностью предусмотренных мер защиты информации - на руководителя подразделения, ответственного за обеспечение ИБ Предприятия.

[10] Разделение обязанностей между администраторами телекоммуникационной сети определяется должностными инструкциями и регламентами администрирования.

Эксплуатация КИС Предприятия осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией, с учетом требований и положений, изложенных в соответствующих разделах настоящего документа.

Комплекс мер по защите информации на предприятии включает в себя следующие мероприятия:

- Аудит состояния ИБ Предприятия;
- Разработка, реализация, внедрение и контроль исполнения планов мероприятий, политик безопасности и других нормативных документов по обеспечению ИБ;
- Подготовка пользователей и технических специалистов к решению проблем, связанных с обеспечением ИБ Предприятия;
- Проектирование, развертывание и совершенствование технической инфраструктуры СОИБ;
- Назначение ролей и распределение ответственности за использование информационных ресурсов сети Предприятия;

Техническая инфраструктура СОИБ предназначена для решения следующих задач:

- Защиты телекоммуникационных сетей Предприятия от угроз со стороны внешних сетей за счет использования межсетевого экранирования, контроля удаленного доступа и мониторинга информационных взаимодействий.
- Защиты серверов за счет использования механизмов управления доступом к серверам баз данных, файловым, информационным и почтовым серверам, регистрации и учета событий, связанных с осуществлением доступа к ресурсам серверов Предприятия, механизмов мониторинга и аудита безопасности.
- Комплексной антивирусной защиты систем, входящих в состав сети Предприятия за счет распределения антивирусных средств (антивирусных сканеров, резидентных антивирусных мониторов и файловых ревизоров) по следующим уровням:

- Защиты внешнего шлюза в сеть Интернет, Защиты серверов,
- Защиты АРМ пользователей.
- Мониторинга сетевого трафика в реальном масштабе и времени с целью выявления противоправных действий пользователей сети и попыток осуществления несанкционированного доступа (далее НСД) к ресурсам сети со стороны внешних нарушителей (злоумышленников).
- Защиты прикладных подсистем, функционирующих в составе сети Предприятия, обеспечение доступности предоставляемых ими прикладных сервисов.
- Защиты межсетевых взаимодействий между сегментами КИС Предприятия.

Меры обеспечения информационной безопасности

Меры обеспечения информационной безопасности организационного уровня.

СОИБ реализуется путем сочетания мер организационного и программно-технического уровней. Организационные меры состоят из мер административного уровня и процедурных мер защиты информации. Основой мер административного уровня, то есть мер, предпринимаемых руководством Предприятия, является политика информационной безопасности. Под политикой информационной безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию Предприятия в области ИБ, а также ту меру внимания и количество ресурсов, которую руководство Предприятия считает целесообразным выделить.

Политика безопасности Предприятия определяется настоящей Концепцией, а также другими нормативными и организационно-распорядительными документами Предприятия, разрабатываемыми на ее основе. К числу таких документов относятся следующие:

- Политика защиты от НСД к информации;
- Политика предоставления доступа пользователей в КИС;
- Политика управления паролями;
- Политика восстановления работоспособности АС в случае аварии;
- Политика резервного копирования и восстановления данных;
- Политика предоставления доступа к ресурсам сети Интернет;
- Политика управления доступом к информационным ресурсам КИС Предприятия;
- Политика внесений изменений в программное обеспечение;
- Политика управления доступом к АРМ Пользователя;
- Политика использования электронной почты;
- Политика анализа защищенности КИС Предприятия;
- Политика внедрения и использования DLP сервисов.
- Политика внедрения и использования системы глобального слежения за передвижение транспортных средств ГЛОНАСС.
- Программа, методика и регламенты тестирования функций СЗИ от НСД к информации;
- Инструкция, определяющая порядок и правила регистрации распечатываемых документов, содержащих конфиденциальную информацию, в соответствии с перечнем информации, составляющей конфиденциальную и служебную информацию;
- Должностные инструкции для администраторов и специалистов, осуществляющих эксплуатацию и обслуживание КИС Предприятия;
- Инструкции для администраторов и специалистов по обеспечению режима информационной безопасности;
- Документированная процедура контроля целостности

программной и информационной частей КИС Предприятия.

Меры обеспечения информационной безопасности процедурного уровня

К процедурному уровню относятся меры безопасности, реализуемые сотрудниками Предприятия. Выделяются следующие группы процедурных мер, направленных на обеспечение информационной безопасности:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима информационной безопасности;
- планирование восстановительных работ.

В рамках управления персоналом, для каждой должности, должны существовать квалификационные требования по информационной безопасности. В должностные инструкции должны входить разделы, касающиеся защиты информации. Каждого сотрудника Предприятия необходимо обучить мерам обеспечения информационной безопасности теоретически и отработать выполнение этих мер практически.

Информационная безопасность КИС Предприятия зависит от окружения, в котором она работает. Необходимо принять меры для обеспечения физической защиты зданий и прилегающей территории, поддерживающей инфраструктуры и самих компьютеров.

При разработке проекта СОИБ предполагается реализация мер физической защиты административных зданий и других помещений, принадлежащих Предприятию, по следующим направлениям:

- физическое управление доступом;
- противопожарные меры;
- обеспечение гарантированным электроснабжением;
- защита поддерживающей инфраструктуры.

Предполагается также реализация следующих направлений поддержания работоспособности:

- поддержка пользователей КИС;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Программа информационной безопасности должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.

Реакция на нарушения режима информационной безопасности

преследует две главные цели:

- блокирование нарушителя и уменьшение наносимого вреда;
- недопущение повторных нарушений.

На Предприятии назначается сотрудник, отвечающий за реакцию на нарушения. Должны быть разработаны и внедрены процедуры первичной реакции на информационный инцидент.

Планирование восстановительных работ позволяет подготовиться к авариям КИС, уменьшить ущерб от них и сохранить способность к функционированию, в минимальном объеме.

Механизмы контроля, существенные для Предприятия с юридической точки зрения, включают в себя:

- Защиту данных и тайну персональной информации;
- Охрану документов организации;
- Права на интеллектуальную собственность.

В соответствии со стандартом ISO17799 и руководящими документами ФСТЭК, ключевыми также являются следующие механизмы контроля:

- Политика информационной безопасности;
- Распределение ролей и ответственности за обеспечение информационной

безопасности;

- Обучение и тренинги по информационной безопасности;
- Информирование об инцидентах безопасности;
- Управление непрерывностью производственного процесса.

Меры обеспечения информационной безопасности программно-технического уровня Программно-технические средства защиты располагаются на следующих рубежах:

- Защита внешнего периметра КИС;
- Защита внутренних сетевых сервисов и информационных обменов;
- Защита серверов и рабочих станций;
- Защита системных ресурсов и локальных приложений на серверах и рабочих станциях;
- Защита выделенного сегмента руководства Предприятия.

На программно-техническом уровне выполнение защитных функций КИС осуществляется следующими служебными сервисами обеспечения информационной безопасности:

- идентификация/аутентификация пользователей КИС;
- разграничение доступа объектов и субъектов информационного обмена;
- протоколирование/аудит действий авторизованных пользователей;
- экранирование информационных потоков и ресурсов КИС;
- шифрование информационных потоков, критической информации;

- контроль целостности;
- контроль защищенности;
- управление СОИБ.

На внешних ресурсах информационного обмена располагаются средства выявления угроз и контроля защищенности. Далее идут межсетевые экраны, защищающие внешние подключения. Они, вместе со средствами поддержки виртуальных частных сетей, объединяемых с межсетевыми экранами, образуют внешний периметр информационной безопасности, отделяющий информационную систему Предприятия от внешних сетей.

Сервис активного аудита СОИБ (как и управление) должен присутствовать во всех критически важных компонентах и, в частности, в защитных. Это позволит быстро обнаружить несанкционированный доступ, даже если по каким-либо причинам, он окажется успешным. Управление доступом также должно присутствовать на всех сервисах, функционально полезных и инфраструктурных. Доступу пользователя к КИС Предприятия должна предшествовать идентификация и аутентификация субъектов информационного обмена (пользователей и процессов). Средства шифрования и контроля целостности информации, передаваемой по каналам связи, целесообразно выносить на специальные шлюзы, где им может быть обеспечено квалифицированное администрирование.

Последний рубеж образуют средства пассивного аудита, помогающие оценить последствия реализации угроз информационной безопасности, найти виновного, выяснить, почему успех атаки стал возможным.

Расположение средств обеспечения высокой доступности определяется критичностью соответствующих сервисов или их компонентов.

Распределение ответственности и порядок взаимодействия

Ответственным за разработку мер и контроль над обеспечением защиты информации является руководитель подразделения, ответственного за обеспечение ИБ Предприятия. Ответственными специалистами осуществляются следующие виды работ по защите информации:

- Контроль защищенности ИТ инфраструктуры Предприятия от угроз ИБ, осуществляемый посредством:

- Проведения аудита безопасности КИС;

- Контроля выполнения правил утвержденных Политик безопасности администраторами и пользователями сети Предприятия;

- Контроля доступа к сетевым ресурсам.

- Предотвращение, выявление, реагирование и расследование нарушений ИБ посредством:

- Анализа и мониторинга журналов аудита критичных компонентов сети Предприятия, включая активное сетевое оборудование, серверы, рабочие станции и т.п.;

- Мониторинга сетевого трафика с целью выявления сетевых атак;

- Контроля процесса создания новых учетных записей пользователей и

предоставления доступа к ресурсам сети Предприятия и доступа к ресурсам сети интернет;

- Опроса пользователей и администраторов информационных систем;
- Внедрения и эксплуатации специализированных программных и программно-технических средств защиты информации;
- Координации деятельности всех структурных подразделений Предприятия по поддержанию режима ИБ.
- Руководителем подразделения, ответственного за обеспечение ИБ Предприятия, осуществляется планирование и реализация организационных мер по обеспечению ИБ, включая:
- Анализ и управление информационными рисками;
- Разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии Политик, Руководств, Концепций, Процедур, Регламентов и других организационно-распорядительных документов по обеспечению ИБ;
- Разработку планов мероприятий по повышению уровня ИБ Предприятия;
- Обучение пользователей информационных систем, с целью повышения их осведомленности в вопросах ИБ.

Наряду с подразделением, ответственным за обеспечение ИБ Предприятия, в разработке и согласовании организационно-распорядительных и нормативных документов по защите информации, включая составление перечней информационных ресурсов, подлежащих защите, также участвуют следующие подразделения Предприятия:

- Служба безопасности;
- Юридический отдел;
- Отдел кадров;
- Функциональные подразделения, филиалы, в которых обрабатывается информация, требующая защиты.
- Бухгалтерия
- Расчётный отдел
- Отдел мобилизационной подготовки
- Профсоюз

Квалификационные требования, предъявляемые к сотрудникам подразделений, отвечающих за обеспечение ИБ, содержатся в должностных инструкциях. Специалисты по защите информации должны проходить регулярную переподготовку и обучение.

Предоставление, изменение, отмена и контроль доступа к ресурсам сети Предприятия передачи данных производится уполномоченными сотрудниками исключительно по утвержденным заявкам, в соответствии с «Политикой предоставления доступа пользователей в КИС» и действующими нормативными актами Предприятия.

Сотрудники эксплуатирующего подразделения отвечают за осуществление настройки параметров информационной безопасности

серверов и рабочих станций сети Предприятия, передачи данных, в соответствии с утвержденными стандартами Предприятия, определяющими требуемые уровни обеспечения защиты информации для различных структурных и функциональных компонентов сети. Подразделение, отвечающее за обеспечение ИБ отвечает за разработку соответствующих спецификаций и рекомендаций по настройке параметров безопасности, а также за осуществление контроля их исполнения.

Обеспечение внешних подключений к сети передачи данных Предприятия, к сети Интернет и другим внешним сетям, предоставление сотрудникам удаленного доступа к сети Предприятия осуществляется сотрудниками эксплуатирующего подразделения с соблюдением требований информационной безопасности, определяемых «Политикой предоставления доступа к ресурсам сети Интернет» и «Политикой управления доступом к информационным ресурсам КИС».

Договоры на обслуживание клиентов заключаются по утвержденной типовой форме функциональными подразделениями. Если договоры предполагают электронное обслуживание с использованием технологических ресурсов Предприятия, то организация и контроль процедур безопасности осуществляется сотрудниками эксплуатирующего подразделения.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к конфиденциальной информации, либо к КИС Предприятия, с этими организациями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима ИБ при выполнении работ в КИС». Подготовка типовых вариантов этих соглашений осуществляется подразделением, отвечающим за обеспечение ИБ Предприятия, либо юридическим отделом.

Порядок категорирования защищаемой информации

Различаются следующие категории информационных ресурсов, подлежащих защите на Предприятии:

- Государственные информационные системы
- Информация, составляющая коммерческую тайну;
- Информация, составляющая служебную тайну;
- Персональные данные;
- Конфиденциальная информация (включая коммерческую тайну, служебную тайну и персональные данные), принадлежащая третьей стороне;
- Данные АСУ
- Данные, критичные для функционирования КИС и работы подразделений.

Первые пять категорий информации представляют собой сведения ограниченного распространения, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности информации путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

К последней категории «критичных» данных, относятся информационные ресурсы Предприятия, нарушение целостности или доступности которых может привести к сбоям функционирования КИС либо отдельных подразделений Предприятия.

Правила отнесения информации к коммерческой тайне и порядок работы с документами, составляющими коммерческую тайну, определяются «Положением о коммерческой тайне Государственного Унитарного Предприятия Республики Крым «Крымтеплокоммунэнерго».

Подходы к решению проблемы защиты информации на предприятии, в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования бизнес процессов Предприятия. Для этого выполняются следующие мероприятия:

- Определяется порядок допуска к работе с информацией, содержащей конфиденциальные сведения;
- Определяется порядок работы с документами, хранилищами информации, образцами, изделиями и др., содержащими конфиденциальные сведения;
- Разрабатываются Правила категорирования информации, позволяющие относить ее к различным видам конфиденциальных сведений и определять степень ее критичности для Предприятия;
- Устанавливается круг лиц и порядок доступа к подобной информации;
- Вырабатываются меры по контролю обращения документов, содержащих конфиденциальные сведения;
- В трудовые договоры с сотрудниками, допущенными к работе с конфиденциальной информацией, включаются обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

Форма подписки о неразглашении конфиденциальной информации должна содержаться в трудовом договоре.

Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых Предприятием с другими организациями.

Модель нарушителя информационной безопасности

Под нарушителем ИБ понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб информационным ресурсам Предприятия. Модель нарушителя безопасности разрабатывается подразделением, ответственным за обеспечение ИБ Предприятия.

Модель угроз информационной безопасности

Под моделью угроз информационной безопасности Предприятия понимается правовой акт, определяющий угрозы безопасности информации в КИС Предприятия, защита информации в которых обеспечивается в соответствии с Требованиями о защите информации, не составляющей государственную тайну. Модель угроз информационной безопасности разрабатывается подразделением, ответственным за обеспечение ИБ Предприятия.

Технические требования по обеспечению информационной безопасности

Общие технические требования по обеспечению информационной безопасности содержатся в «Перечне технических требований по составу основных подсистем системы обеспечения информационной безопасности». «Перечень...» разрабатывается подразделением, ответственным за обеспечение ИБ Предприятия.

Ответственность сотрудников за нарушение безопасности

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования политик безопасности Предприятия, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

За умышленное причинение ущерба, а также за разглашение сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, сотрудники Предприятия несут материальную ответственность в полном размере причиненного ущерба (Ст. 243 Трудового кодекса РФ).

Механизм реализации концепции

Реализация Концепции обеспечения информационной безопасности Предприятия должна осуществляться на основе утвержденных конкретных программ и планов, которые ежегодно уточняются с учетом:

- федерального законодательства и нормативной базы в области защиты информации;
- международных и отраслевых стандартов в области информационной безопасности и IT-безопасности;
- организационно-распорядительных документов Предприятия;
- реальных потребностей в средствах обеспечения информационной безопасности;
- объемов финансирования, выделяемых на обеспечение информационной безопасности Предприятия.

Перечень основных нормативных актов по обеспечению информационной безопасности, использованный при разработке настоящей Концепции

- Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646);
- Федеральный закон № 149-ФЗ от 27 июля 2006 года "Об информации, информационных технологиях и о защите информации";
- Федеральный закон № 152-ФЗ от 27 июля 2006 года "О персональных данных";
- Федеральный закон № 98-ФЗ от 29 июля 2004 года «О коммерческой тайне»;
- Федеральный закон № 187-ФЗ от 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Закон «О безопасности», № 2446-1, 1992 г
- Приказ ФСТЭК № 31 от 14.03.2014г.
- Приказ ФСТЭК № 21 от 18.02.2013г.
- Приказ ФСТЭК № 17 от 11.02.2013г.

Разработал:
Ведущий специалист
по информационной безопасности
ГУП РК «Крымтеплокоммунэнерго» Арзамасцев В.С

Согласовано:

И.О. заместителя генерального
директора по безопасности
ГУП РК «Крымтеплокоммунэнерго» В.В. Запорожец

Начальник информационно-
вычислительного отдела
ГУП РК «Крымтеплокоммунэнерго» О.Н. Иванов

Главный юрист –
начальник юридического отдела
ГУП РК «Крымтеплокоммунэнерго» Д.А. Консманова

Председатель профсоюзного
комитета Объединенной первичной
профсоюзной организации
ГУП РК «Крымтеплокоммунэнерго»
общероссийского профсоюза работников
жизнеобеспечения Н.Ф. Хойна